AXIS Perimeter Defender with Milestone VMS

User manual

AXIS Perimeter Defender with Milestone VMS

Table of Contents

AXIS Perimeter Defender with Milestone VMS

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) and for XProtect Professional+, Express+, and Essential+, you can:
  - trigger "User Defined" events when AXIS Perimeter Defender generates an alarm or when the status changes
  - trigger "Analytics" events when AXIS Perimeter Defender generates an alarm or when the status changes
  - trigger "Alarms" when AXIS Perimeter Defender generates an alarm or when the status changes
  - 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 Corporate, Expert, and Professional+ you can also:
  - insert a bookmark in the corresponding video sequence

This document describes how to configure both XProtect and AXIS Perimeter Defender to achieve these two types of integration. Note that there are some differences in the configuration depending on the specific XProtect product that is used. Check the relevant XProtect documentation when in doubt.

About this document

About this document

The next sections describe:

- 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 cameras 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. If that is enough for your needs, you can stop reading there.

If you need metadata display and recording or if you need to trigger further actions by tweaking the XProtect configuration, then you can go to the chapter that is related to your specific product. These chapters include:

- How to connect the metadata from AXIS Perimeter Defender to Milestone to automatically show overlay on top of the relevant video streams in live and playback mode, and to export the overlay with the images when you export a video sequence using the Smart Client.
- How to leverage the Milestone Alarms, User Defined Events and Analytics Events to trigger further actions in your Milestone system (like activating a recording, sending an e-mail or an SMS or trigger a hardware output).
- How to operate the Smart Client.

Advanced configuration on page 52 include:

- A complete system architecture schema with emphasis on network communications between the different modules. See *Network communication on page 52*.
- How to extend an already installed and configured system by adding additional cameras. See *Add new video sources to the system on page 52*.
- How to increase the number of the metadata channels of the MIP driver. See *Increase the number of channels of the MIP Driver on page 55*.
- How to remove video sources that have been removed from the system also from the bridge configuration. See *Remove video sources from the bridge configuration on page 58*.
- How to change the bridge server IP address. See *Change the IP address of the bridge server on page 59*.
- How to change the Axis video source IP address. See *Change the IP address of an Axis device on page 60*.
- How to enable XProtect to export the recorded metadata when exporting the corresponding video footages. See *Enable metadata export when exporting video footage on page 60*.
- How to upgrade a previous system to the latest version of the software without losing the existing configuration.
- How to manually configure the alarm reception parameters of the *AXIS Perimeter Defender Bridge to Milestone XProtect* if it sits behind a NAT with respect to the AXIS Perimeter Defender cameras.
- How to manually associate a MIP driver channel to a video source if, for whatever reason, the automatic association routine fails.
- How to change the log settings (verbosity, size, position on disk).
- How to change the XP Server to which an already configured *AXIS Perimeter Defender Bridge to Milestone XProtect* is attached.

About this document

Note

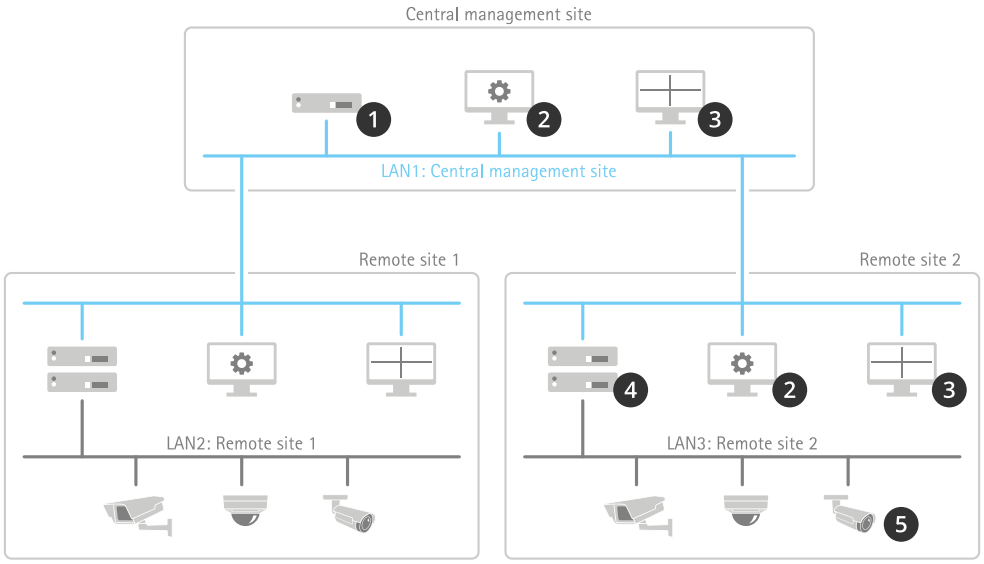
The *AXIS Perimeter Defender Bridge to Milestone XProtect* is shortened *APD Bridge* in this document. Both terms indicate the same software module.

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.

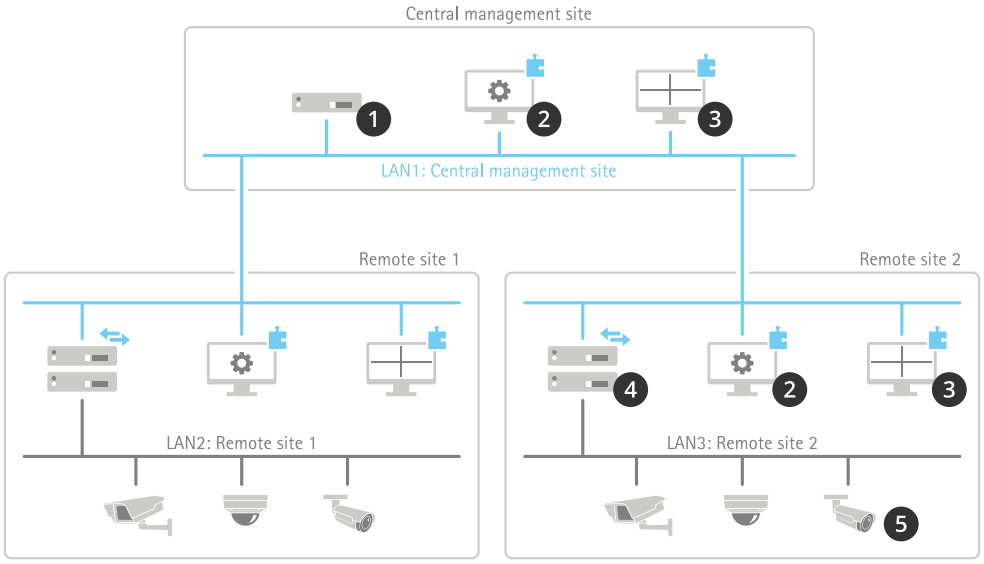


1 *XProtect Management Server*
2 *XProtect Management Client*
3 *XProtect Smart Client*
4 *XProtect Recording Server(s)*
5 *Cameras running AXIS Perimeter Defender*

In the typical installation in the above image, there is a central management site where the management server is located. An XProtect Management Client and an XProtect Smart Client provide central configuration and monitoring capabilities. Several remote sites are connected to the central management site through a dedicated management LAN. On remote sites there are one or more recording servers, an (optional) management client, and an (optional) smart client. Those are also connected to the management LAN. The recording servers are also connected to a separate camera LAN, to which all the video devices are connected. On each remote site there is one or more instance of AXIS Perimeter Defender installed.

The Milestone AXIS Perimeter Defender Bridge to XProtect components install on this architecture in the following way:

AXIS Perimeter Defender integration



1 *XProtect Management Server*
2 *XProtect Management Client with MIP Plugin for AXIS Perimeter Defender*
3 *XProtect Smart Client with MIP Plugin for AXIS Perimeter Defender*
4 *XProtect Recording Server(s) with AXIS Perimeter Defender Bridge*
5 *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 automates the configuration of the system and allows you 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. It also automatically exports the recorded metadata associated to a live sequence when the user exports it.
- The AXIS Perimeter Defender Bridge to Milestone XProtect (APD Bridge) runs as a Windows Service on XProtect Recording Servers (optionally, you can install and run it on any other server connected by LAN to the Axis cameras). Each bridge is virtually connected to a recording server and feeds it 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:

- A PC with Windows 11 x64, Windows 10 x64, Windows Server 2012 R2 x64, Windows Server 2016 x64, or Windows Server 2019 x64
- Microsoft .NET 4.7 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
- One of the following XProtect products, with the specified version or later. Some versions require specific hotfixes to be installed. Check the release notes and the Milestone documentation.
  - XProtect Corporate/Expert 2014 (7.0d)

  - XProtect Professional+/ Express+/Essential+ 2017 R1 (11.0a)

- AXIS Perimeter Defender 2.0.0 or later

Important additional prerequisites:

- The cameras that run AXIS Perimeter Defender must be time-synchronized with the XProtect server (i.e. the cameras and the server where XProtect is installed must be configured on the same time zone and have the same time). We strongly recommend that you configure all the cameras and the XProtect server to use a time server to synchronize and stay synchronized over time.
- The instances of AXIS Perimeter Defender that run on the cameras must be properly configured (calibrated and with scenarios defined to trigger alarms) before you integrate them with XProtect. See *AXIS Perimeter Defender user manual* for more information on how to calibrate and configure.
- The APD Bridge needs HTTP/HTTPS network connectivity to the Management Server.
- The APD Bridge needs HTTP/HTTPS network connectivity as root or as privileged user (with the right to configure the AXIS Perimeter Defender application on the camera/server) to the cameras running AXIS Perimeter Defender.

To maximize the performance of the AXIS Perimeter Defender instances that run on the cameras:

- limit the video stream resolution to 1080p @ 12 fps, or if possible, to 720p @ 12 fps.
- when you show two video streams at the same time from one camera, limit the video stream resolutions to
  - stream 1: 1080p @ 12 fps
  - stream 2: 720p @ 12 fps

Important

If you use higher resolutions or greater frame rates than recommended, it can result in missed detections or false alarms.

Licensing

You don't need a licence to receive alarms from AXIS Perimeter Defender and to leverage XProtect User Defined Events, XProtect Analytics Events, XProtect Alarms, and XProtect Bookmarks.

For the XProtect system to receive and record the metadata, however, the AXIS Perimeter Defender Bridge requires a MIP driver device to be added to a Milestone recording server. Each MIP driver device requires an additional device licence key (DLK) (independently from the number of metadata channels implemented by the MIP driver). This license is a standard DLK to purchase from Milestone. For example:

- The system has 5 recording servers. All the recording servers, the management server, and the video devices are connected to the same LAN. The cameras running AXIS Perimeter Defender are distributed on the 5 recording servers. In this case, a single APD Bridge can be used, a single MIP Driver needs to be added to one of the recording servers, and hence the number of additional DLKs needed is 1.
- Same as before, however each recording server is connected to a sub-group of cameras via a dedicated LAN. The cameras running AXIS Perimeter Defender are distributed on the 5 recording servers. In this case, one APD Bridge instance per recording server is necessary; hence, 5 MIP Driver devices need to be added to the system, one per recording server, and the number of additional DLKs needed is 5.
- Same as before, however 1 of the recording servers has no cameras running AXIS Perimeter Defender attached. In this case, that recording server does not need to have an APD Bridge, and no MIP Driver device attached to it. The total number of additional DLKs needed in this case is 4, for the MIP Driver devices attached to the other 4 recording servers.
- Same as before, however the user only wants to receive the alarms triggered by AXIS Perimeter Defender and is not interested in metadata. In this case, 4 APD Bridges need to be installed on the 4 recording servers with AXIS Perimeter Defender video devices, however no MIP Driver device will be attached to these recording servers. No additional DLKs are needed.

Installation and first configuration steps

The first part of this chapter describes how and on which host(s) to install the software. The second part describes how to connect your AXIS Perimeter Defender device(s) to your XProtect system.

- To install the necessary software, go to *Installation on page 10*.
- To connect AXIS Perimeter Defender devices to your XProtect system, go to *Add Axis devices running AXIS Perimeter Defender to XProtect on page 15*.

At the end of this chapter, your system is ready to receive Alarms, Analytics Events and User Defined Events.

Installation considerations

Before you install the different software components, you have to determine how many APD Bridges are needed and where to install them.

First, consider each management server independently and plan the installation for each one independently. One management server equals one system in the next paragraphs, two servers equals two systems, and so on. Even if the management servers are federated, they must be considered as completely separate systems here. The federation is automatically handled with no additional configuration steps.

When you plan a system installation, consider:

- For the chosen management server, count the number of recording servers with a camera running AXIS Perimeter Defender. (Such a recording server will be referred to as a recording server running AXIS Perimeter Defender.) If there is only one, you only need one APD Bridge.
- If you have more than one recording server running AXIS Perimeter Defender, the next question is if it's possible to give one of the recording servers (or to a separate host) network connectivity (HTTP/HTTPS) to all the AXIS Perimeter Defender devices. If the answer is yes, then you only need one APD Bridge. However, depending on the number of video devices it handles and the performance of the host where it's installed, you might have to split the load on two APD Bridges installed on two separate hosts. Usually, a production-grade server with no additional CPU-intensive applications running, an APD Bridge can handle hundreds of video devices.
- If you have more than one recording server running AXIS Perimeter Defender, and each one is connected to the cameras through a separate and independent network, you need one APD Bridge per recording server running AXIS Perimeter Defender.

When you configure an APD Bridge, the first required step is to connect it to an XProtect server. It's important to establish which XProtect server to connect the bridge to.

- An APD Bridge only has access to video devices connected to its server. This means that if a bridge is connected to a specific recording server, it only has access to the video devices connected to that recording device. If it's connected directly to the management server, it has access to the video devices of all the recording servers.
- When a bridge is connected to a recording server, the MIP Driver device that the bridge implements must be connected to the same recording server. On the other hand, when the bridge is connected to the management client, the MIP Driver device can be connected to any of the recording servers.
- An APD Bridge can be connected to the management server if it's the only one present in that system.

This table describes some of the most typical installation scenarios:

Site type	Description	Installation guidelines
Single site	Single site with a management server, one or more recording servers and a single network.	Install a single bridge, either on one of the XP Recording Servers or on a separate host. Attach it to the management server. Attach the corresponding MIP Driver to the recording server.

Single site with separate LANs and fewer than 100 AXIS Perimeter Defender devices.	Single site with a management server, multiple recording servers and separate LANs (one management LAN between the management server and the recording servers, and one video devices LAN between the recording servers and the video devices). The total number of video devices with AXIS Perimeter Defender video analytics is less than 100.	Install a single bridge, on a separate host or on the XP Recording Server with the largest number of devices. Attach the bridge to the XP Management Server. Attach the corresponding MIP Driver to the recording server where the bridge is installed, or on the recording server with the largest number of AXIS Perimeter Defender video devices.
Single site with separate LANs and more than 100 AXIS Perimeter Defender devices.	Single site with a management server, multiple recording servers and separate LANs (one management LAN between the management server and the recording servers, and one video devices LAN between the recording servers and the video devices). The total number of video devices with AXIS Perimeter Defender Video Analytics exceeds 100.	Install one bridge per recording server with AXIS Perimeter Defender video devices attached. Install them either on separate hosts or on the corresponding recording server. Attach them to the corresponding recording server. Attach the MIP Driver to the corresponding recording server.
Multiple interconnected sites with separate LANs	Multiple sites interconnected to a central site where the management server is installed. There is a common management LAN interconnecting all recording servers (on site) with the central management server. There is an independent video device LAN on each site connecting the site recording servers and the site video devices.	On each site, install one bridge per recording server with AXIS Perimeter Defender video devices attached. Install them either on separate hosts or on the corresponding recording server. Attach them to the corresponding recording server. Attach the MIP Driver to the corresponding recording server.

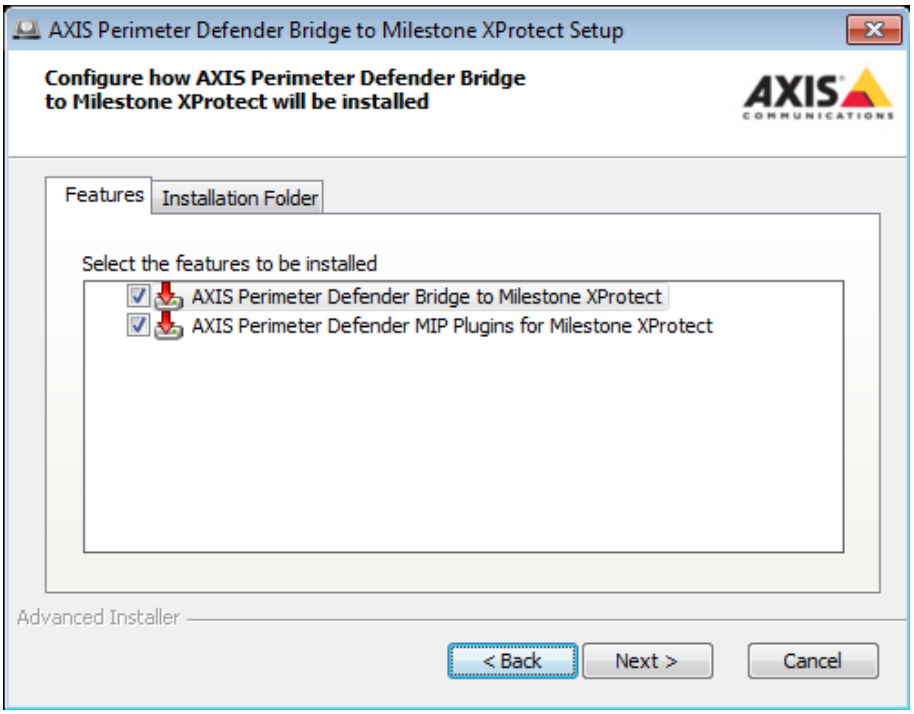
Note

The bridge must always have network connectivity to the management server and to all the AXIS Perimeter Defender devices attached to the XP Recording server that it's attached to.

Installation

The installation file *AXIS_Perimeter_Defender_Bridge_to_Milestone_XProtect.exe* contains both the APD Bridge and the MIP Plugins for AXIS Perimeter Defender. Double-click the file to start the installation. A dialog lets you select which component(s) to install:

Installation and first configuration steps



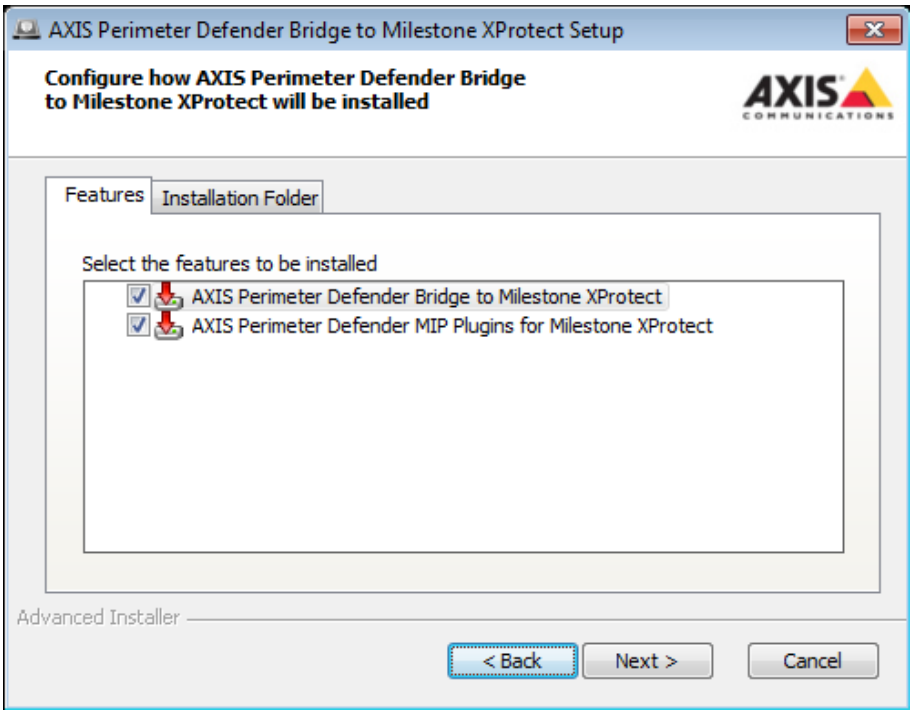
1. You must run the installer and select the **AXIS Perimeter Defender MIP Plugins for Milestone XProtect** component on every PC where the XProtect Smart Client is installed and where you want the metadata display. If metadata display is not a requirement, you can skip this part.
2. You must also run the installer and select the **AXIS Perimeter Defender MIP Plugins for Milestone XProtect** component on every PC where the XProtect Management Client is installed and where you want to administer (configure) the AXIS Perimeter Defender integration.
3. Finally, you must run the installer and select the **AXIS Perimeter Defender Bridge to Milestone XProtect** component on all hosts where, according to the installation plan described in *Installation considerations on page 9*, a bridge must be installed.

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 Bridge to Milestone XProtect X.Y.Z.W.exe".
2. Click **Next**.
3. Accept the EULA and click **Next**.
4. If you plan to run the APD 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**.



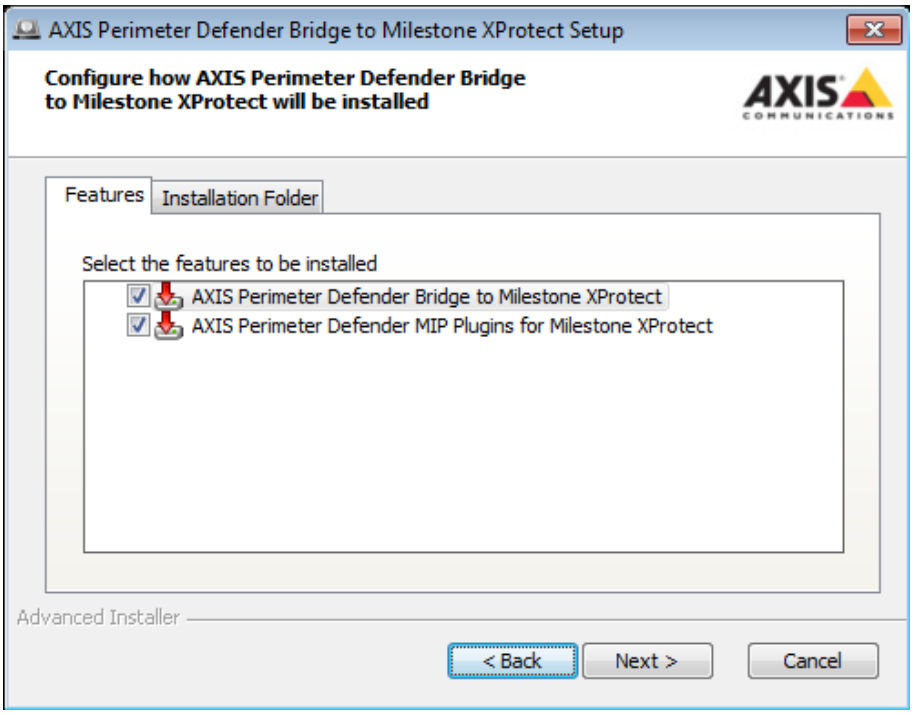
5. Click **Install**.
6. Wait for the installation to be completed, then click **Finish**.

Software installation on the host running the XProtect Recording Server

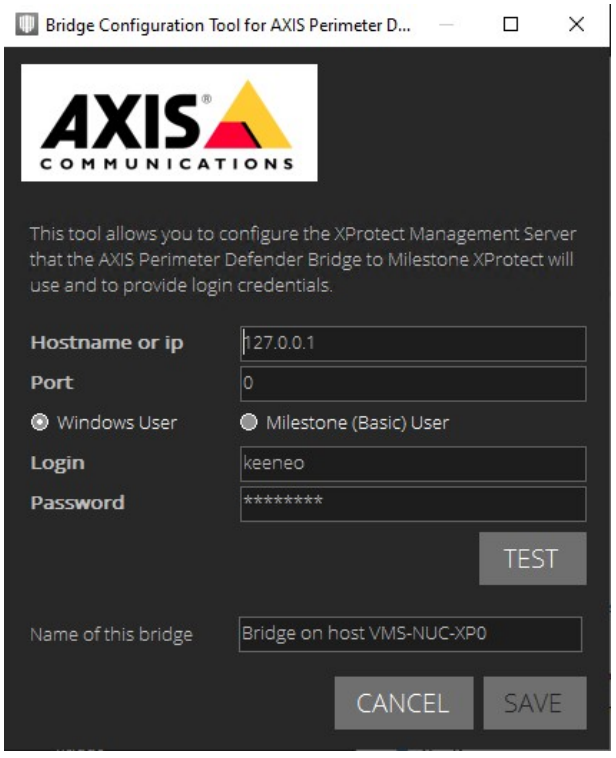
Important

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

1. As administrator, run "AXIS Perimeter Defender Bridge to Milestone XProtect X.Y.Z.W.exe".
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, select **AXIS Perimeter Defender MIP Plugins for Milestone XProtect**. In any case, select the **AXIS Perimeter Defender Metadata Bridge to Milestone XProtect**.



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



7. In the Bridge Configuration Tool for AXIS Perimeter Defender:

   7.1 In **Hostname or ip**, enter the DNS name or ip address of the XProtect Corporate Management server. 127.0.0.1 can be used if the Management server is installed on the same host.

   7.2 **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 0. Otherwise, use the custom port value you have set up.

   7.3 Select if the login uses an existing **Windows user** or a **Milestone user** defined in the XProtect System.

   7.4 In **Login**, 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, use only the username.

   7.5 Enter the password. For a Windows user, don't forget to provide the user password in this field.

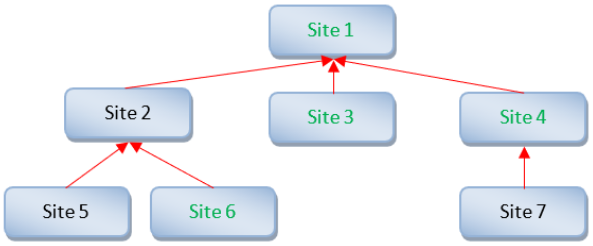
   7.6 Click **Test** to check the connection. If it fails, fix the problem by providing the correct information.

   7.7 You can give the bridge a name, or keep the default value "Bridge on host <HOSTNAME>, where <HOSTNAME> is the Windows name of the PC where the bridge is installed.

   7.8 Click **Save** to allow the APD Bridge to connect to the XProtect Server.

Software installation in a federated system

An XProtect federated system consists of a hierarchy of autonomous installations (Management Server, Recording Server(s), Event Server with one or more Management Clients and Smart Clients) linked together in a "father-son" relationship. A typical structure:



Each site has several video sources directly connected. Some of these might be cameras running AXIS Perimeter Defender (in the graphic, the sites in this situation are depicted in green, so sites 1, 3, 4, and 6).

You must install the APD Bridge on every server that has a camera running AXIS Perimeter Defender. You should also install the MIP Plugin component on the Management Clients and Smart Clients of that site. In the previous example, you must install the software on the different hosts of sites 1, 3, 4, and 6. When you do that, those sites can be configured and operated autonomously, as if they were not part of a larger federated system.

However, the user can also operate these sites as part of the federation, that is:

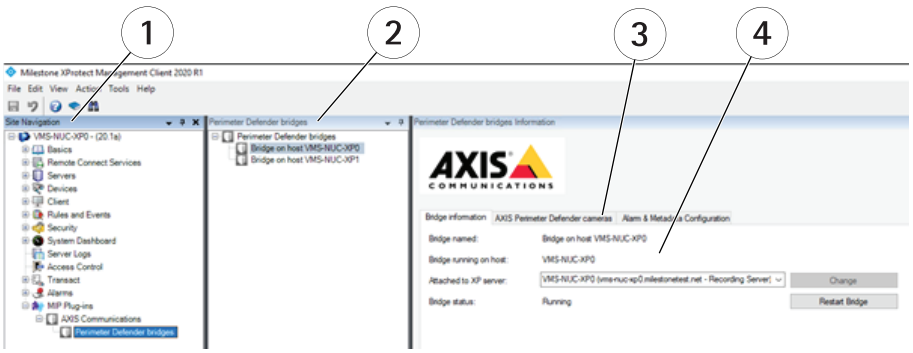
- From site 1, you can configure site 3, site 4, and site 6 by remotely logging into those with the XProtect Management Client. As site 1 has the AXIS Perimeter Defender MIP Plugin installed, it can configure the other sites of the federation as well. On the other hand, it is not possible to configure AXIS Perimeter Defender on site 6 from, for example, the Management Client of site 2, as this last one does not have the AXIS Perimeter Defender MIP Plugin
- From the Smart Client of site 1, you automatically have access to video streams and AXIS Perimeter Defender metadata and alarms of sites 3, 4, and 6. Therefore, it's possible to, for example, have a layout in the Smart Client of site 1 at the same time showing video streams and metadata of sites 1, 3, 4, and 6.

MIP Plugin interface

In the AXIS Perimeter Defender MIP Plugin interface:

1. Under **Site Navigation**, go to **MIP Plug-ins > AXIS Communications > Perimeter Defender bridges**.

2. Under **Perimeter Defender bridges**, click the one you want to configure. The names listed are the ones that have been configured in the Bridge Configuration Tool for AXIS Perimeter Defender. Right-click to change the name.
3. Under **Perimeter Defender bridges information**, configure the parameters of the chosen bridge.
   - **Bridge information** shows general information about the bridge.
   - **AXIS Perimeter Defender cameras** shows cameras attached to the Bridge recording servers.
   - **Alarm & Metadata Configuration** lets you configure User Defined Events that the bridge should generate, and several parameters related to the metadata streams.



1 Site Navigation
2 Bridges
3 Tabs
4 Information and parameters

NOTICE

If the **Perimeter Defender bridges** part of the screen hides the **Perimeter Defender bridges information**, click **View > Reset Application Layout** and restart the client.

Attach the bridge to an XP server

The first configuration step is to attach every installed APD Bridge to an XP server. You can find more information on how to decide which is the best (or mandatory) server to attach to, in *Installation considerations on page 9*. The server choice limits the video devices (cameras and encoders) that the APD Bridge can reach (for AXIS Perimeter Defender application running on them). If the attached server is:

- the management server: the APD Bridge can access all video devices in the system independently from the recording server they are attached to. However, you can attach the APD Bridge to the management server if there is only one APD Bridge in the system.
- a recording server: the APD Bridge can access all the video devices attached to that recording server. It is mandatory to attach an APD Bridge to a recording server if there is more than one APD Bridge in the system. You can't attach more than one APD Bridge to the same recording server.

The first APD bridge installed in the system is automatically attached to the management server. The next one is left unattached. If there is only one APD Bridge in your system, you can leave it attached to the management server. Otherwise you have to first detach it from the management server, then attach it to a recording server, and then attach all the other APD Bridges to their respective recording servers.

To attach a not yet configured APD Bridge to a server, use the combination box **Attached to XP Server** and select the one you want. If it's not listed, it means it's already attached to another APD Bridge. Then confirm the change by clicking **Change**. If you want to change the attached server of an already configured bridge, see *Attach an APD Bridge to a different XP server on page 66*.

Add Axis devices running AXIS Perimeter Defender to XProtect

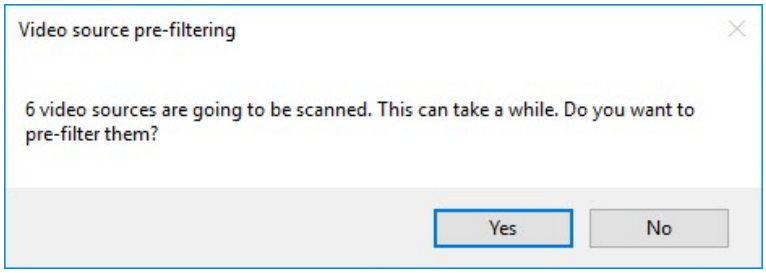
This section describes how to add the AXIS Perimeter Defender instances running on Axis devices connected to your XProtect system.

Note

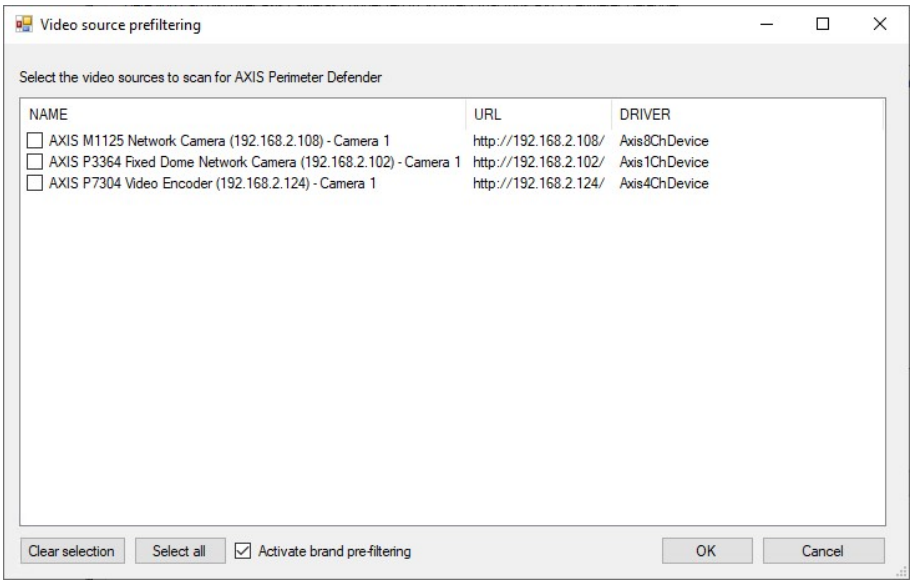
This section includes screenshot examples from an XProtect Corporate installation, but the steps are the same for XProtect Expert/Professional+/Express+/Essential+.

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

1. Add all the Axis devices to XProtect as video sources (see XProtect documentation). Make sure to attach these devices to the recording server that the bridge you are configuring is attached to. If a device is configured in HTTPS mode only (no HTTP), then you have to make sure the URL used by the VMS is correct. See *Add HTTPS devices to the system on page 54*.
2. Go to **MIP Plug-ins** >**AXIS Communications** > **Perimeter Defender bridges**.
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 recording server attached to the APD Bridge you are configuring.
   - If you click **Yes**, an additional dialog allows you to select a sub-set of the available cameras.



The advantage of selecting a sub-set of cameras is that it reduces the scanning time. Select **Activate brand pre-filtering** to filter out all non-Axis cameras, as these cannot run AXIS Perimeter Defender.



Important

When you scan new cameras, it only adds new video sources that run AXIS Perimeter Defender. It doesn't remove an already existing video source from the configuration, even if it has been disabled or removed from the system (and is hence not found during the scan). To remove a video source from the configuration, see *Remove video sources from the bridge configuration on page 58*.

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

Important

When new cameras have just been added to the system, they are not always found by the MIP Plugin. If this happens, refresh the Management client configuration by pressing the F5 key and then click **Scan new cameras** again.

Note

If the scan doesn't find HTTPS devices with AXIS Perimeter Defender, you need to change the device configuration slightly. See *Add HTTPS devices to the system on page 54*.

6. Select one or more Axis cameras that run AXIS Perimeter Defender and choose the metadata display settings that you want to apply to the selected cameras.
7. Save the configuration.

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

Note

At this stage of the configuration process, if you have activated the alarm, analytics events, or bookmarks generation, you can receive them in XProtect without any further steps. However, to trigger more advanced rules within XProtect, you need to configure more steps to leverage the Analytics Events and User Defined Events. They are described in *Alarms, events, and bookmarks configuration through the Management Client Plugin on page 18*.

Alarms, events, bookmarks, and metadata

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 15*.
- 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 APD 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. Disable the unused channels once you have added the metadata source.
- The plugin allows the user to deactivate the automatic generation of XProtect Alarms when 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 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.
- The plugin allows the user to automatically generate diagnostic events, corresponding to unusual situations that the user needs to be aware of, for example that AXIS Perimeter Defender stopped. The user can remove diagnostic events that are irrelevant.

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

Important

Before you configure the software, you must install both the AXIS Perimeter Defender MIP Plugins for Milestone XProtect and the APD Bridge. In addition, you must also configure the APD Bridge to be able to access the XProtect System.

1. Open the Management client.
2. Under **Site Navigation**, go to **MIP Plug-ins** >**Axis Communication** > **Perimeter Defender bridges** .
3. Under **Perimeter Defender bridges**, select the bridge you want to configure.
4. Under **Perimeter Defender bridges information**, select the **Alarms & Metadata configuration** tab.
5. If you want to show or record metadata, go to *Configure metadata through the Management Client Plugin on page 21*. Otherwise, you can skip the configuration of the Metadata source.
6. 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 Analytics Event when AXIS Perimeter Defender generates an alarm, select **Automatically generate analytics events**.
   - If you want to insert a bookmark automatically in the corresponding XProtect video stream, select **Automatically generate bookmarks**. This option is not available in XProtect Express+ and XProtect Essential+.
   - In most cases, you don't need to manually specify the destination IP address and listening port for alarms (that is, the port that the APD 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 situations, like when there is a NAT or port forwarding between the AXIS Perimeter Defender devices and the host where the APD 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 to the APD Bridge. See *Set alarm reception parameters in specific situations on page 61* for more information.

7. If you want the AXIS Perimeter Defender alarms to trigger XProtect User Defined Events, you need to define these events. You can click **Generate user defined events** to automatically generate 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 APD Bridge triggers when AXIS Perimeter Defender generates the corresponding alarm. It will also generate several Diagnostic Events for each AXIS Perimeter Defender.

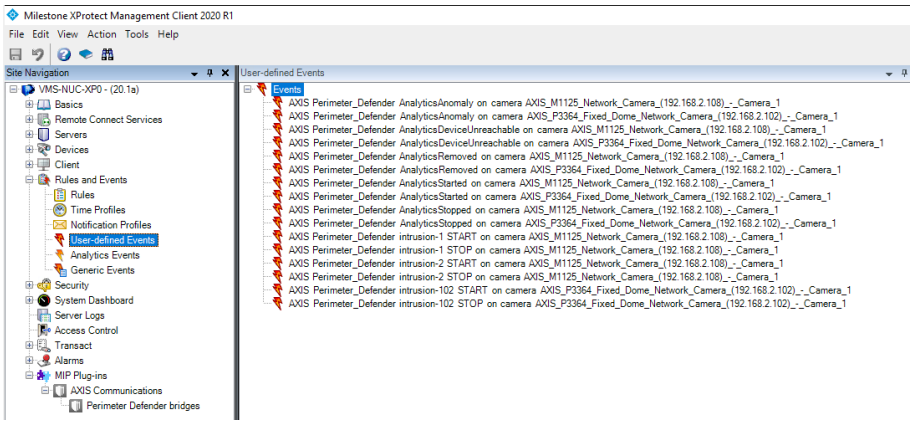
8. You can use the buttons **Scenario events only**, **Diagnostic events only** to limit the types of events generated. Select **All events** for both types.

9. When you have selected all relevant events, click **OK**.

10. Save the configuration.

11. If you want to use your new User Defined Events immediately and have no need of further modifcations, restart the APD Bridge service.

12. 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 APD Bridge does not find them and hence does not generate them.

You can delete the unwanted User Defined Events one-by-one. Under **Site Navigation**, go to **Rules and Events > User-defined Events**.

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 follows 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 User Defined 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 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 Thermal-11**: will be triggered by any AXIS Perimeter Defender alarm START or STOP related to any scenario from the XProtect Camera named "Thermal-11"
- **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 Thermal-11** : will be triggered by any AXIS Perimeter Defender alarms STOP related to the scenario "ZoneCrossing-1" from the XProtect camera named "Thermal-11"

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 21*
- When you change the User Defined Events names you must restart the APD Bridge service for the change to take effect.

Diagnostic Alarms and Events

The APD Bridge can automatically send Diagnostic Alarms, Analytics Events, and User Defined events when there is an important change or anomaly in one of the AXIS Perimeter Defenders. The generation and definition of these Alarms/Events follow the same rules as standard Alarms/Events:

- Diagnostic Alarms are triggered if **Automatically trigger alarms on AXIS Perimeter Defender alarm reception** is selected.
- Diagnostic Analytics Events are triggered if **Automatically trigger analytics events** is selected.
- Diagnostic User Defined Events are triggered if they are defined. By default, when you click **Generate user defined events**, the following set of diagnostic events are defined for every alarm and metadata source configured in the system:
  - AXIS Perimeter_Defender AnalyticsStarted on camera <MilestoneCameraName>
  - AXIS Perimeter_Defender AnalyticsStopped on camera <MilestoneCameraName>
  - AXIS Perimeter_Defender AnalyticsRemoved on camera <MilestoneCameraName>
  - AXIS Perimeter_Defender AnalyticsAnomaly on camera <MilestoneCameraName>
  - AXIS Perimeter_Defender AnalyticsDeviceUnreachable on camera <MilestoneCameraName>

Where <MilestoneCameraName> is the camera name associated with the Alarm and Metadata source as configured in the XProtect system, with spaces replaced by underscores (for example, "Camera 1" becomes "Camera_1") and the diagnostic events type corresponds to the following situations:

- "AnalyticsStarted" is triggered whenever an AXIS Perimeter Defender that was configured as Alarm and Metadata source changes from "stopped" to "started" by an external command.
- "AnalyticsStopped" is triggered whenever an AXIS Perimeter Defender that was configured as Alarm and Metadata source changes from "stopped" at the bridge start or has been stopped by an external command during the APD Bridge run.
- "AnalyticsRemoved" is triggered whenever an AXIS Perimeter Defender that was configured as Alarm and Metadata source is uninstalled from the edge device.
- "AnalyticsAnomaly" is triggered whenever an AXIS Perimeter Defender that was configured as Alarm and Metadata source doesn't behave as expected, for example is installed and running but doesn't generate a metadata stream. Usually when this happens, the AXIS Perimeter Defender application is badly configured and needs attention. For example, if the input video stream to AXIS Perimeter Defender changes its aspect ratio, the calibration is not valid anymore. AXIS Perimeter Defender can't run any longer for this video stream until a new calibration is performed.
- "AnalyticsDeviceUnreachable" is triggered whenever an AXIS Perimeter Defender can no longer be reached. This can be due to network issues, a disconnected cable, a reboot of the device, or the device being switched off.

If you are not interested in one or more of these User Defined Events, you can delete them as described previously.

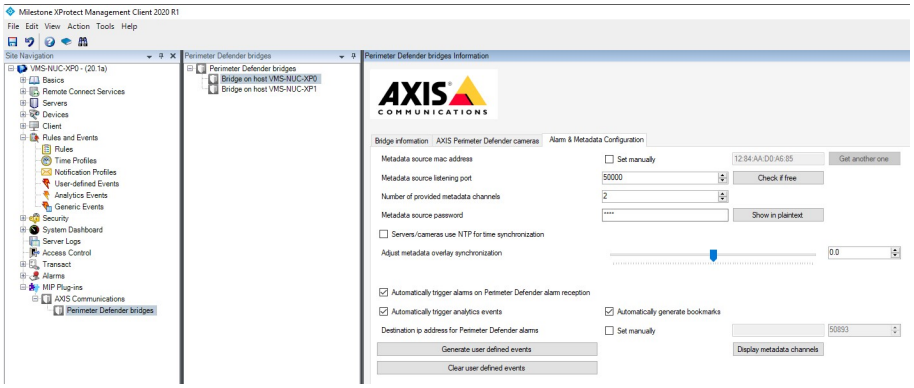
Configure metadata through the Management Client Plugin

Important

Before you can add the metadata source to the XProtect System, the APD Bridge must be fully installed and configured, that is, 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. XProtect considers the Metadata Source as a normal video source, and you have to add it as if it were a video source of its own.

1. Open the Management client.
2. Go to **MIP Plugins, Axis Communication, Perimeter Defender bridges** .
3. Click the bridge you want to configure.
4. Select the **Alarms & Metadata configuration** tab.



5. 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** 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.
- If you set a MAC address manually for the MIP Driver device, make sure there is no other device in the system with the same 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 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 **Check if free** . Note that this button requires that the APD Bridge is running.

- The number of provided metadata channels is automatically set to the number of AXIS Perimeter Defender configured for that bridge. 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

To increase or decrease the number of video channels in case you already added the metadata source to the Milestone system, you have to remove it and add it again, or use the Replace hardware functionality (see the XProtect User Guide).

- The Management Client requests a metadata source password when it adds the metadata source to the system. If you want to see the password, click and hold **Show in plaintext**. The default password is "pass".

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.

6. Only select **NTP synchronization** if all the following conditions are met:

   - All cameras and servers (including XProtect servers) are synchronized using a real NTP time server (the standard Windows time synchronization mechanism is not a valid alternative).
   - All cameras and servers have a correct time zone setting.
   - All cameras and servers have a correct daylight-saving time setting.

Under these conditions, alarms and metadata are synchronized with the images that use the source (the Axis devices where AXIS Perimeter Defender runs) time and date. If the checkbox is left cleared, alarm and metadata use a different, and in most cases reliable, synchronization algorithm.

Important

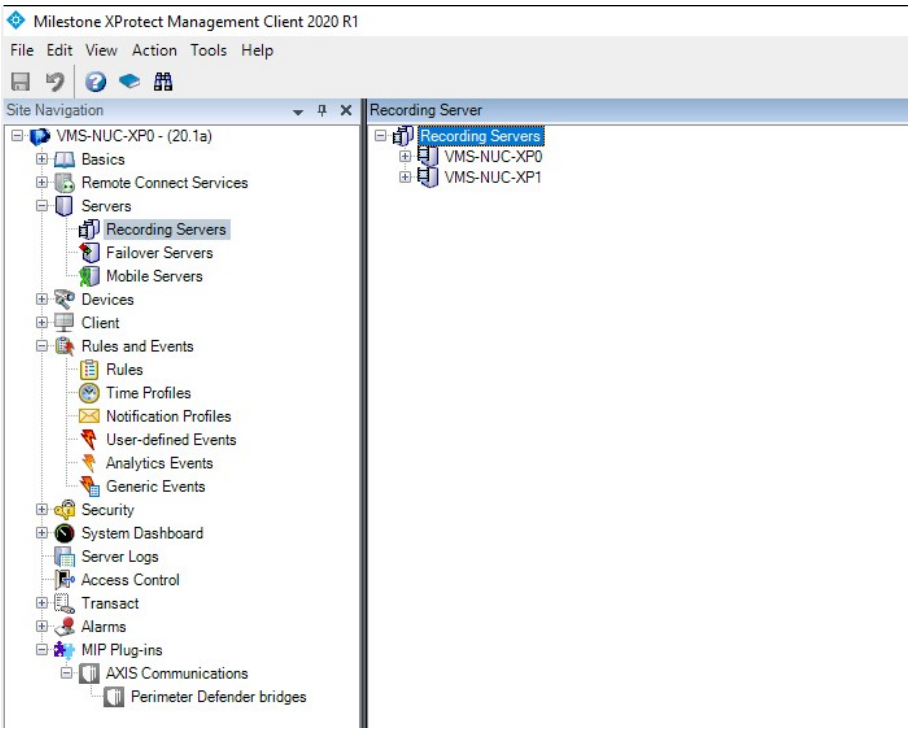
If you select **NTP synchronization** even though not all conditions are met, it can result in strange de-synchronization between images and alarms, bookmarks, events, and metadata.

7. The **Adjust metadata overlay synchronization** slider lets you change the synchronization time between images and metadata (in playback mode only) of an amount in the [-4s; +4s] interval. The slider can help adjust the position of the bounding boxes on top of the corresponding actors when these appears to be slightly preceding or slightly following the actor. This setting has no impact on the live mode. For further details, see *Fix desynchronization in metadata playback display on page 51*.

8. 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*Remove video sources from the bridge configuration on page 58*.

When the metadata source is configured, you need to add it to the XProtect system so that XProtect can pull metadata from the APD Bridge (which in turn pulls it from AXIS Perimeter Defender):

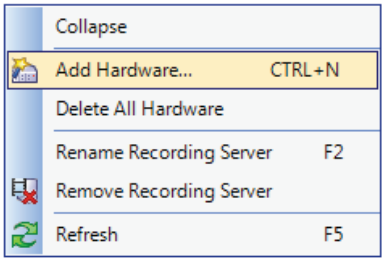
1. In the Management Client, go to **Servers** >**Recording Servers**.



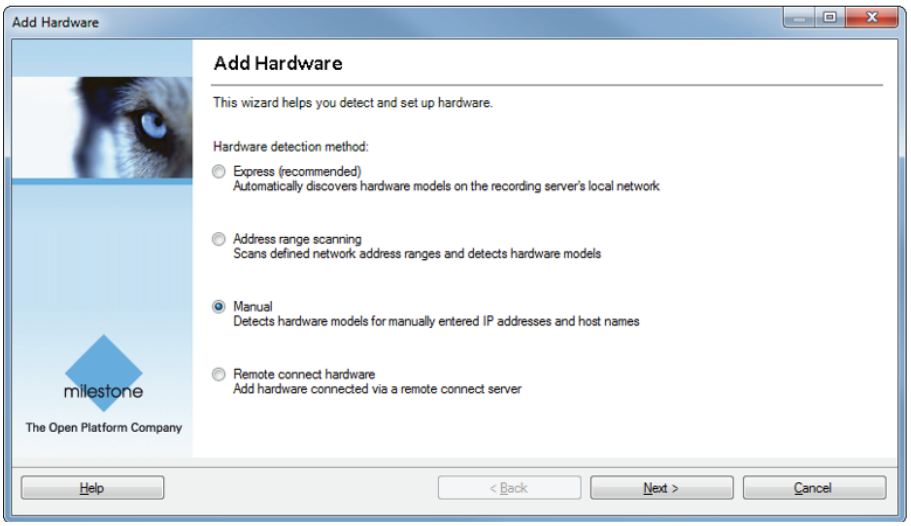
2. Select the recording server that you want to attach the MIP Driver device to. The choice depends on the XP server to which the bridge is attached:

   - If the APD Bridge (that represents the metadata source you are adding) is attached to the management server, you can choose any of the recording servers available.
   - If the APD Bridge is attached to a specific recording server, you have to attach the metadata source to that recording server.

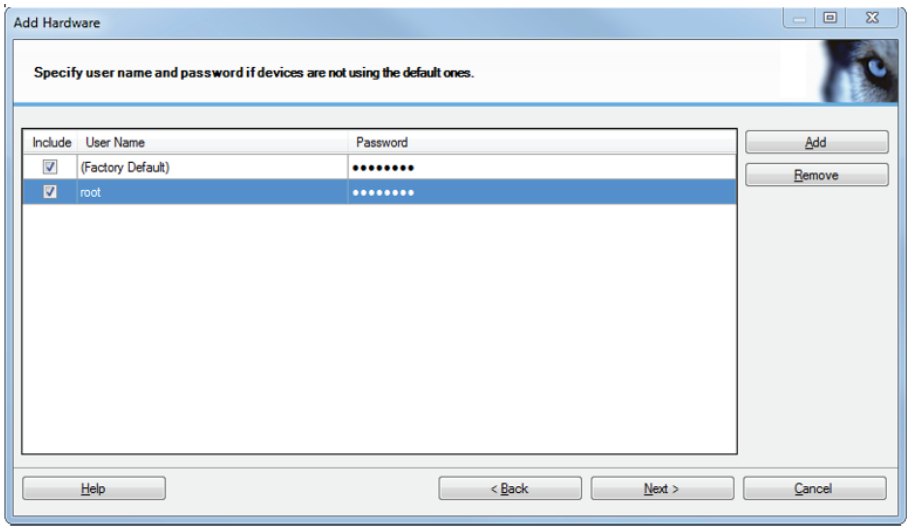
3. Right-click the server and select **Add hardware**.



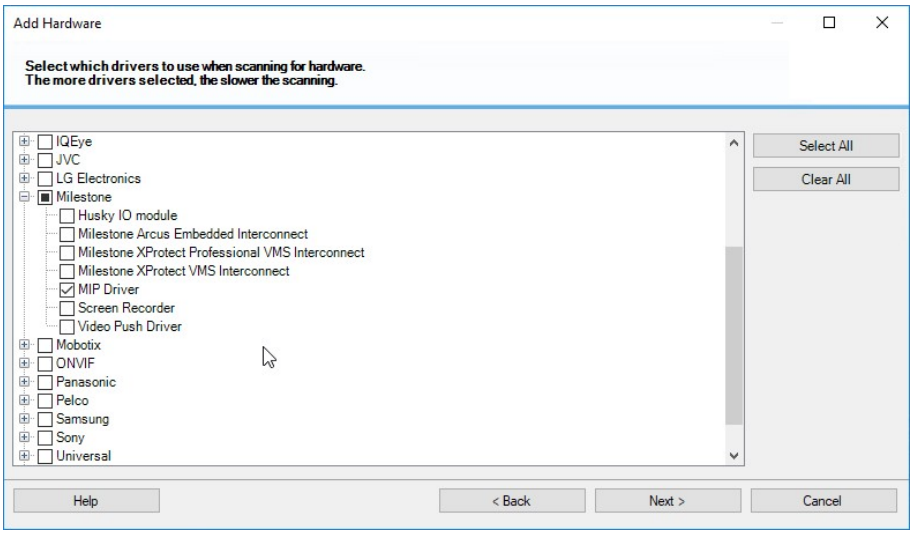
4. Select **Manual** and click **Next**.



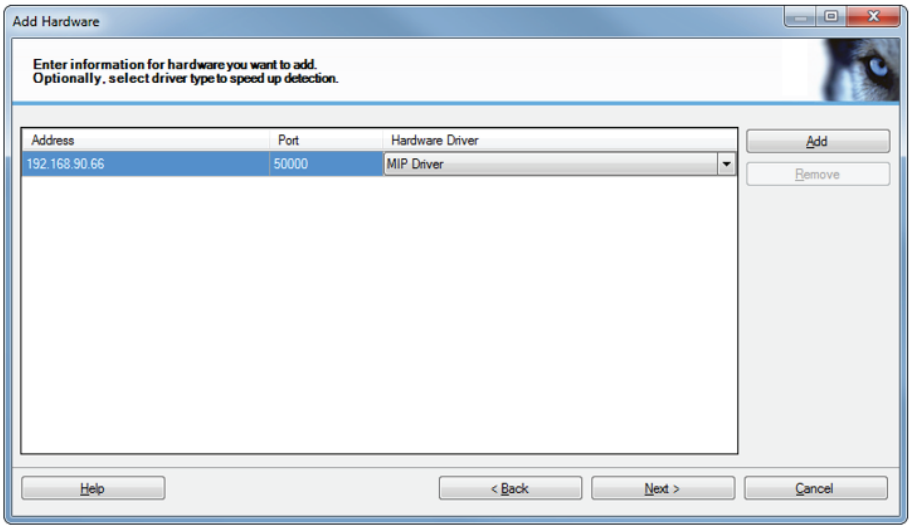
5. Add a new username and password, using "root" as login and the password you set for the Metadata source.
6. Click **Next**.



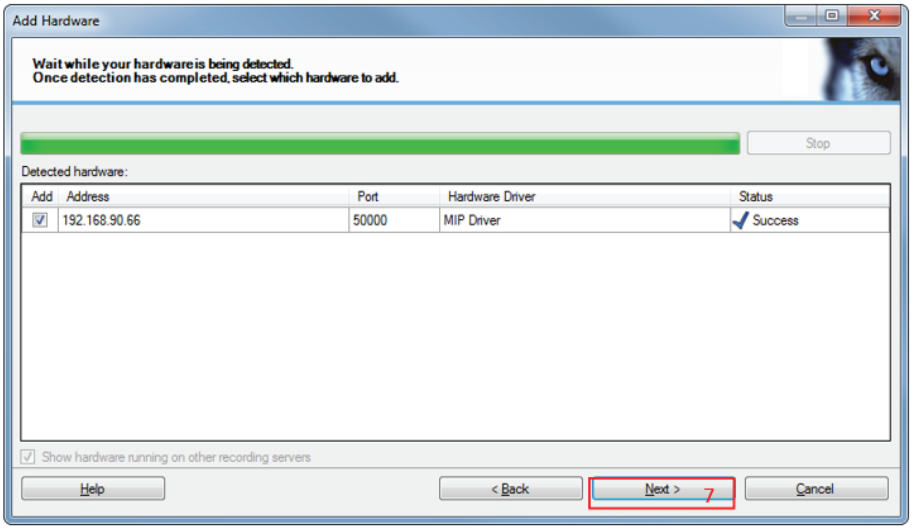
7. Select **Milestone** > **MIP Driver** as device type and click **Next**. If your XProtect version is before 2018 R3, the MIP Driver is under **Other** instead of Milestone.



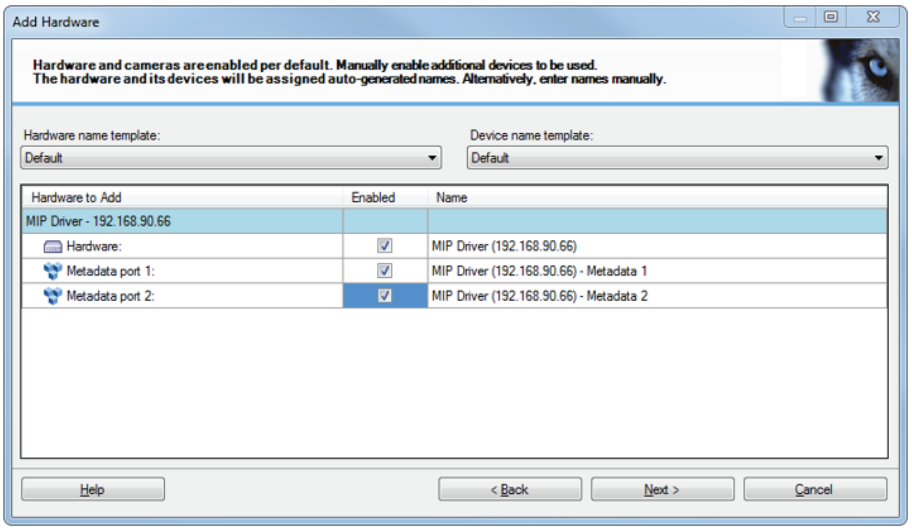
8. Enter the IP address of the host where the APD Bridge is installed. If the host that runs the APD Bridge has several IP interfaces, use the one that is visible from the Milestone Recording Server to which the MIP driver is attached. 50000 indicates the port number chosen in the **Metadata source listening port** field.
9. In the **Hardware Driver** drop-down list, select **MIP Driver**. Note that **Auto-Detect** does not work.
10. Click **Next**.



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

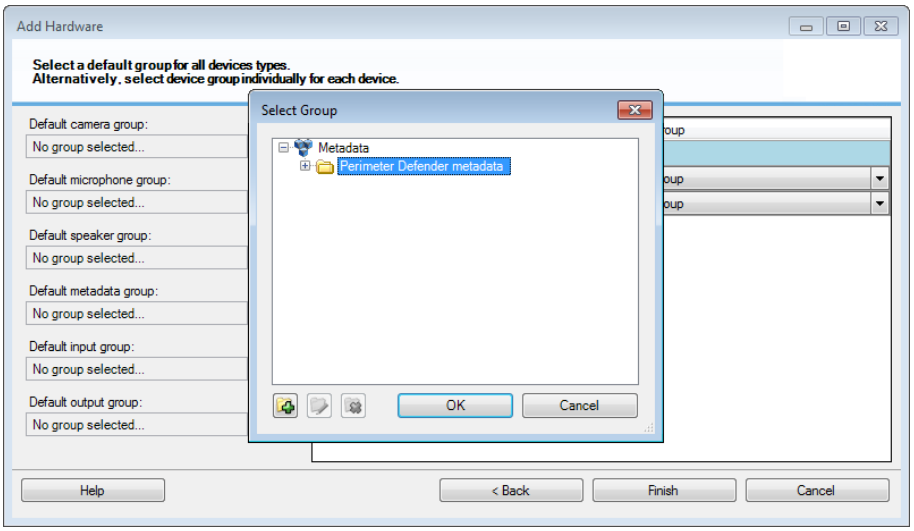


12. Select the metadata channels as the Axis cameras running AXIS Perimeter Defender that send metadata to the system. Usually this means all the metadata channels available on the source, except if you increased the number of channels manually to prepare future extensions. In this case, we recommend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

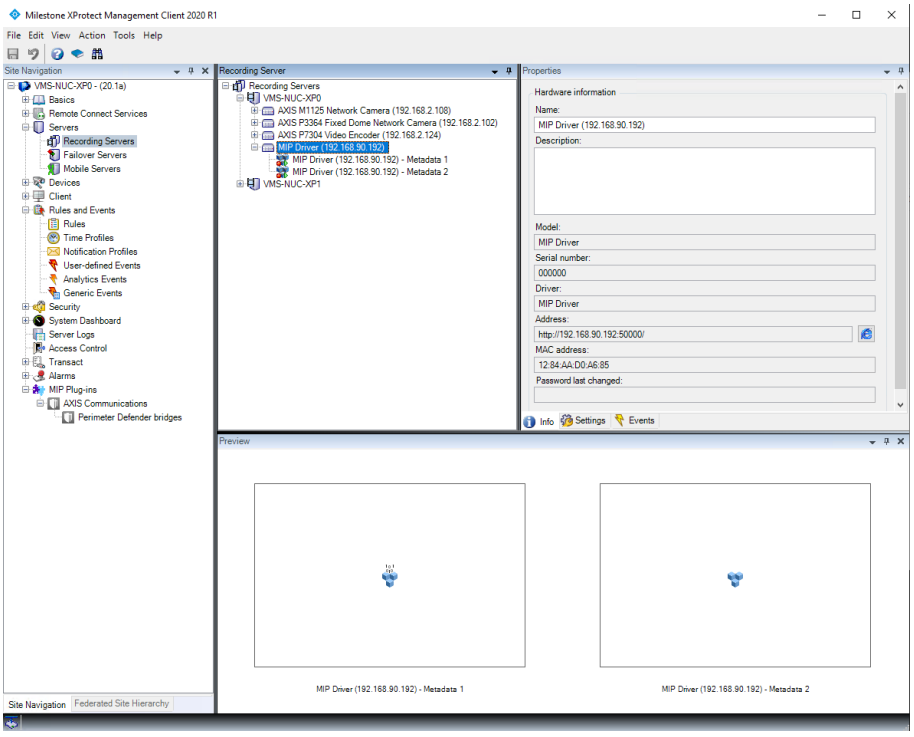


The screenshot shows how to enable channels provided by the metadata source.

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

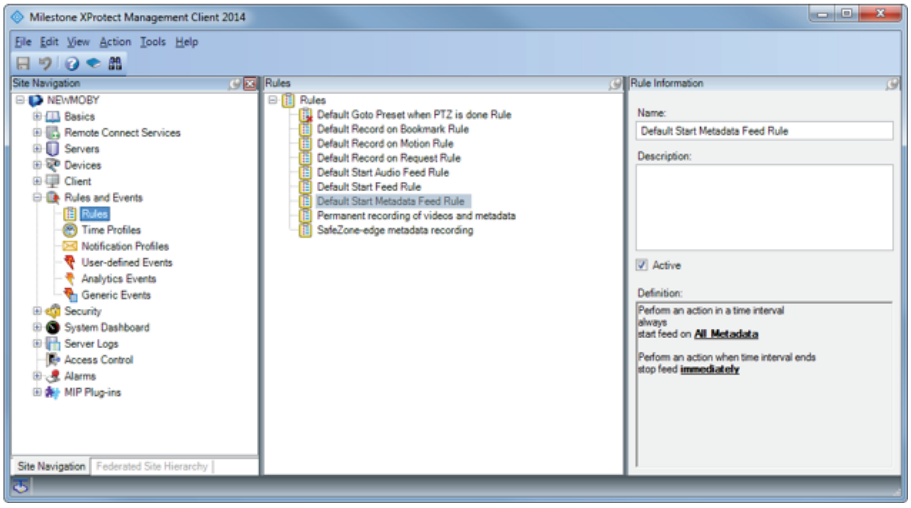


15. Select the newly added Metadata source "MIP Driver (192.168.90.66)" and check in the **Preview** window that a set of zeros and ones (0, 1) comes out from the central cubes. This means that XProtect is retrieving the metadata from the source.

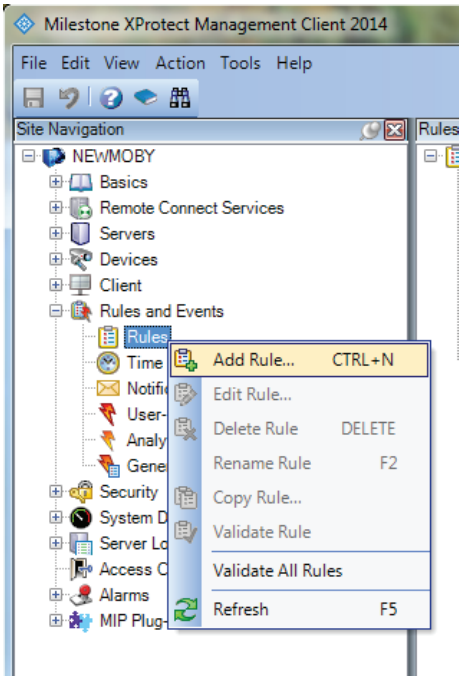


16. If you don't see any zeros and ones near the central cube, there is a problem with the metadata retrieval, probably due to the lack of a default rule. Do the following:

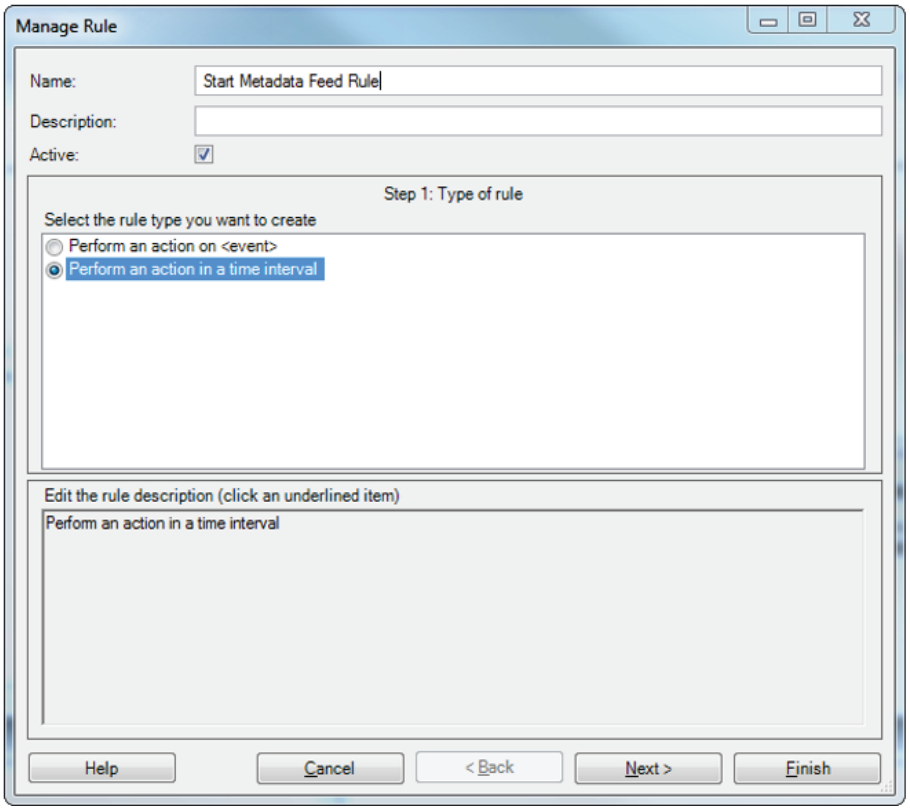
    - In the **Rules and Events** section, make sure that you have a **Default Start Metadata Feed Rule** and that the rule looks like in the following image.



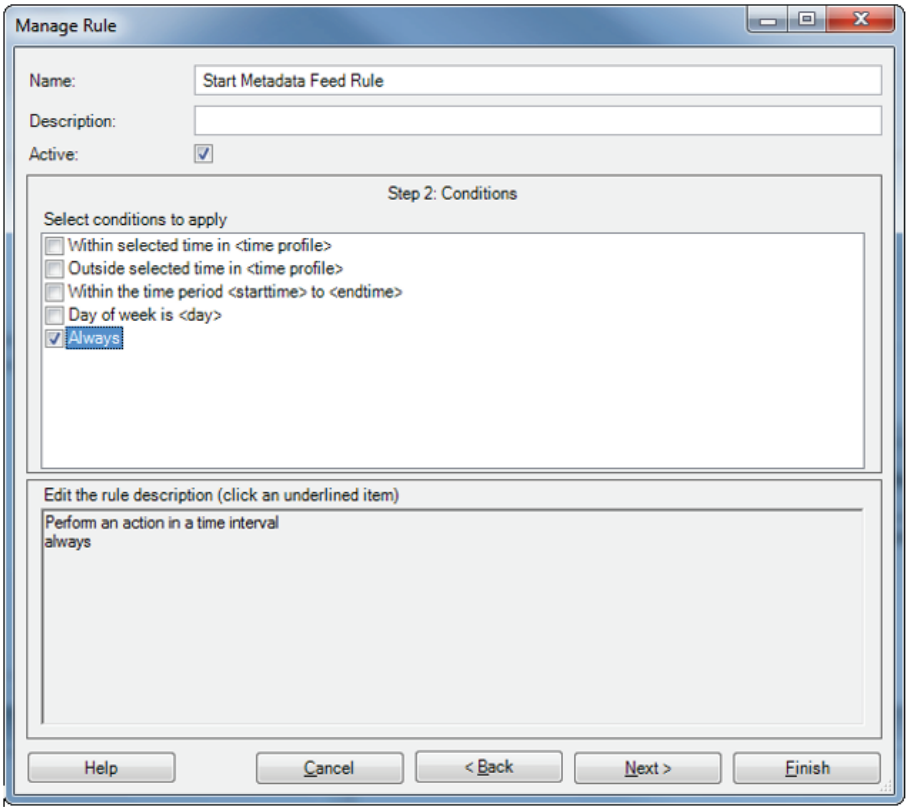
- If the rule is missing, you must define the rule:
- In the **Rules and Events** section, right-click **Rules** and select **Add Rule**.



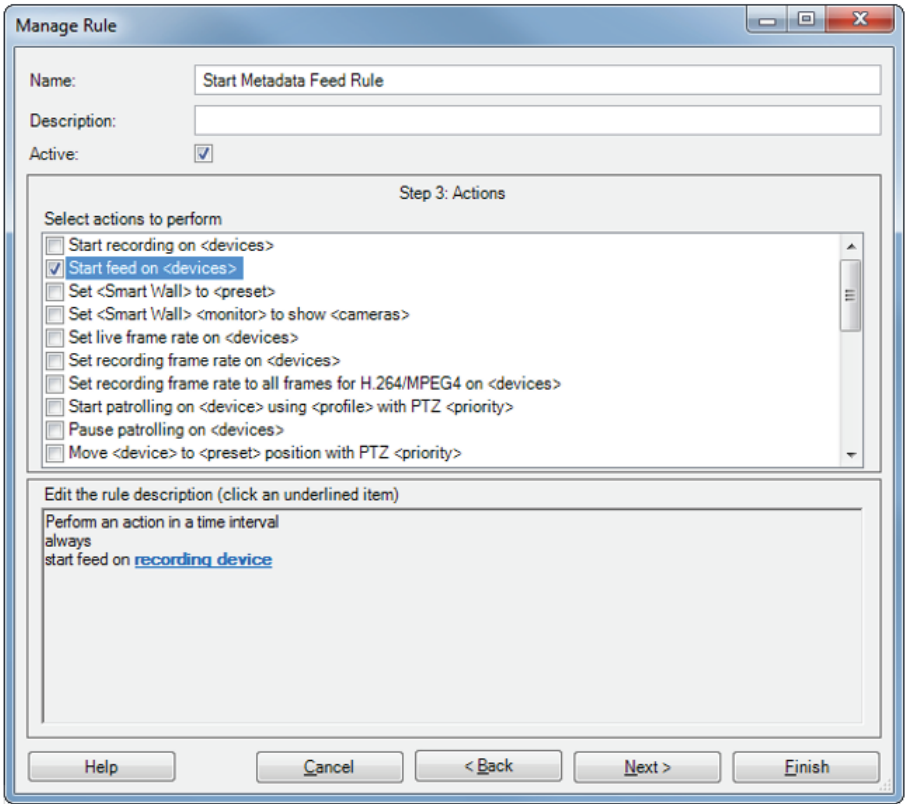
- Type name for the rule, then select **Perform an action in a time interval** and click **Next** .



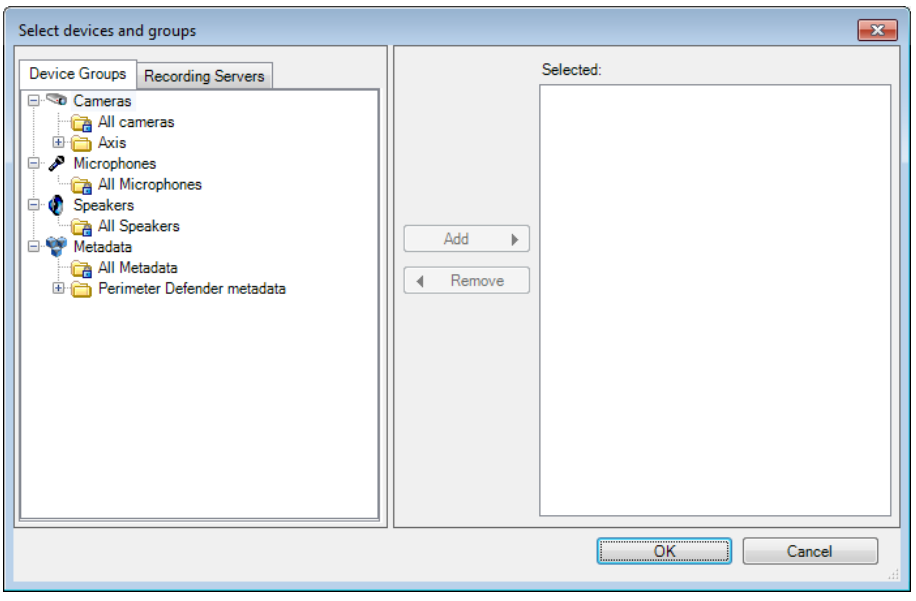
- Select **Always** and click **Next**.



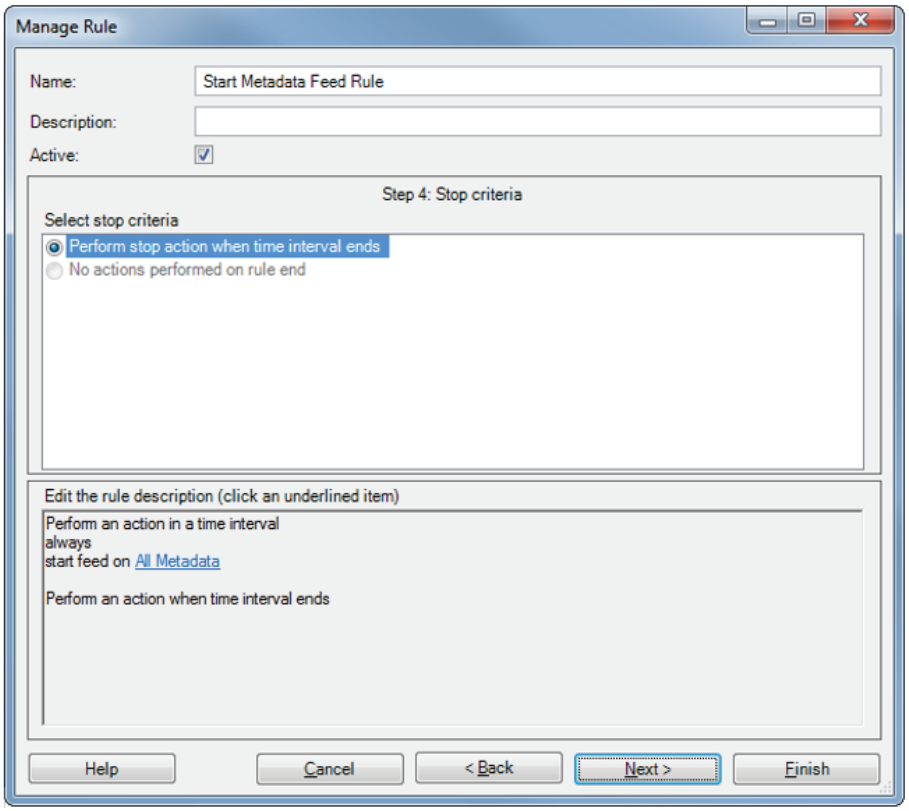
- Select **Start feed on <devices>**, then click **recording device**.



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



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



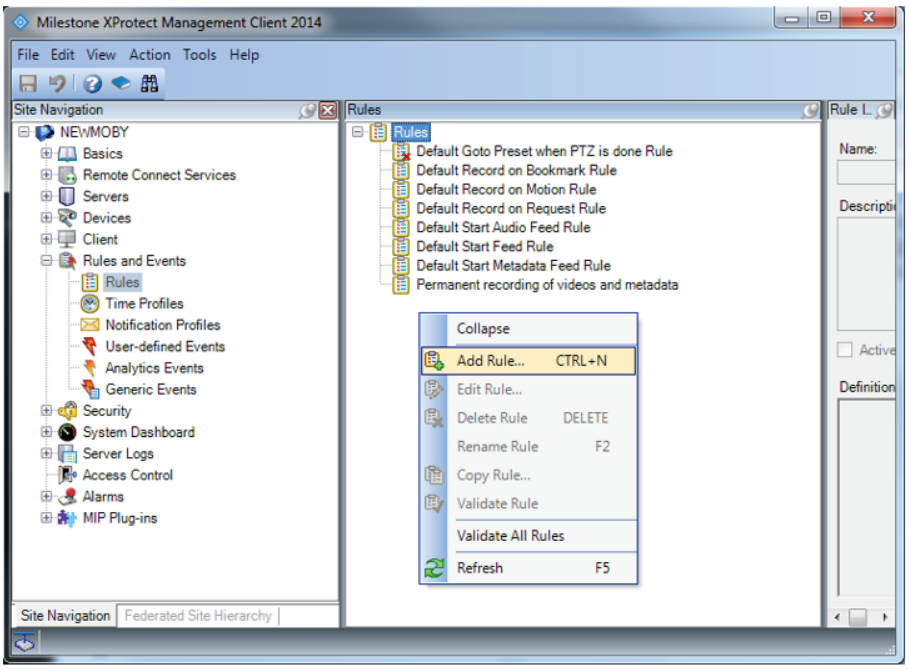
- Click **Finish**.

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 32*.

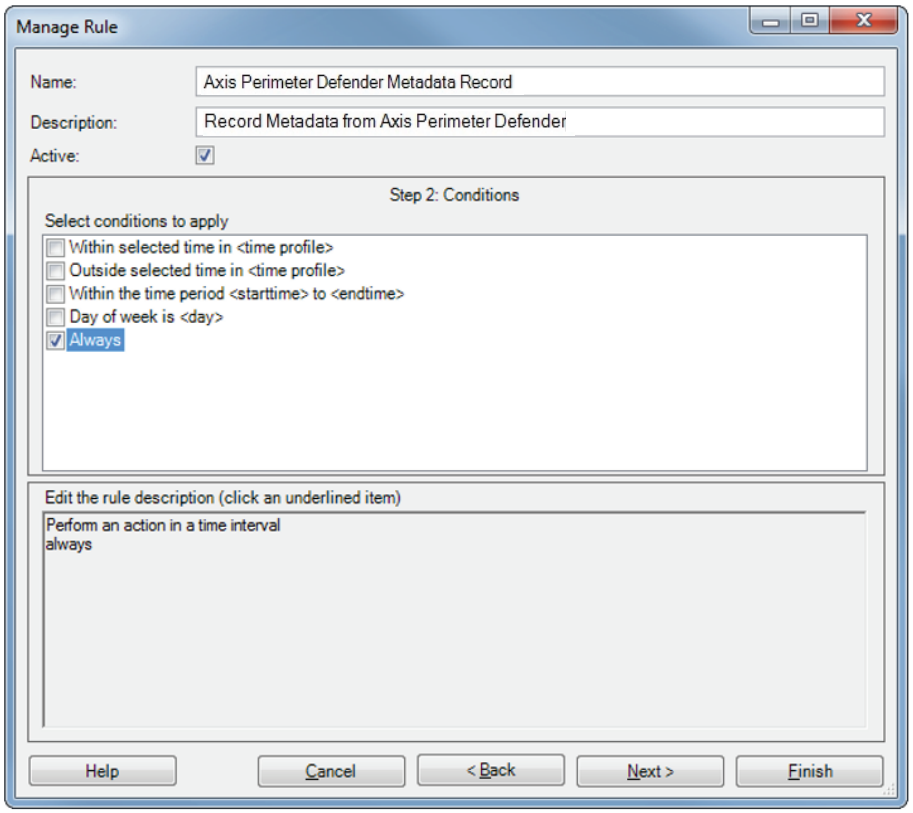
Activate metadata recording

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

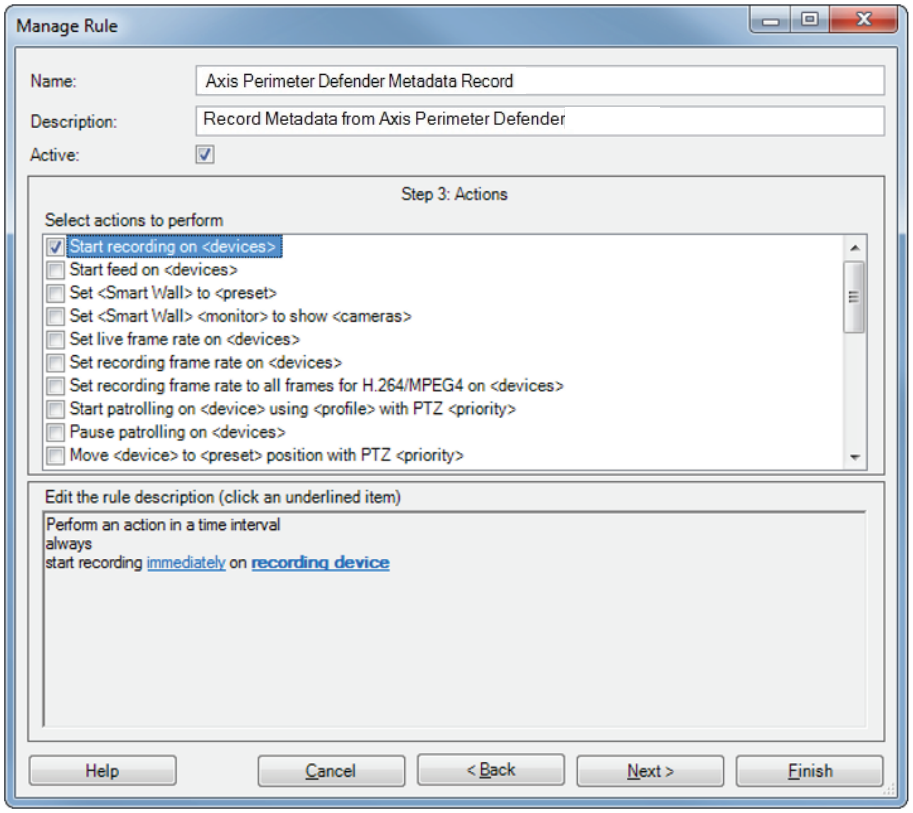
1. Open the Management Client.
2. Click **Rules and Events** and then **Rules**.
3. Right-click in the **Rules** window.



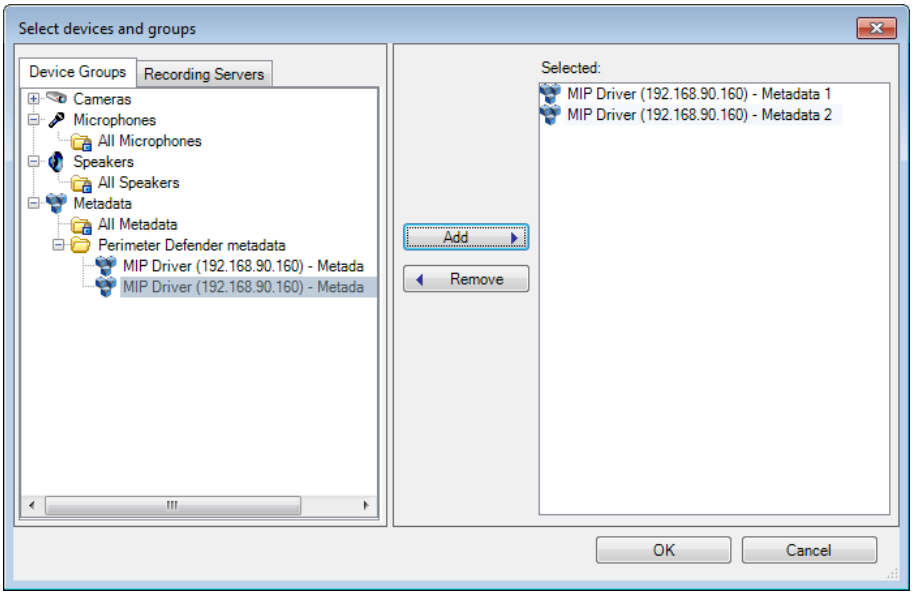
4. Select **Add Rule**.
5. Type a name and description for the new rule. Then select **Perform an action in a time interval** and click **Next**.
6. Select **Always** and click **Next**.



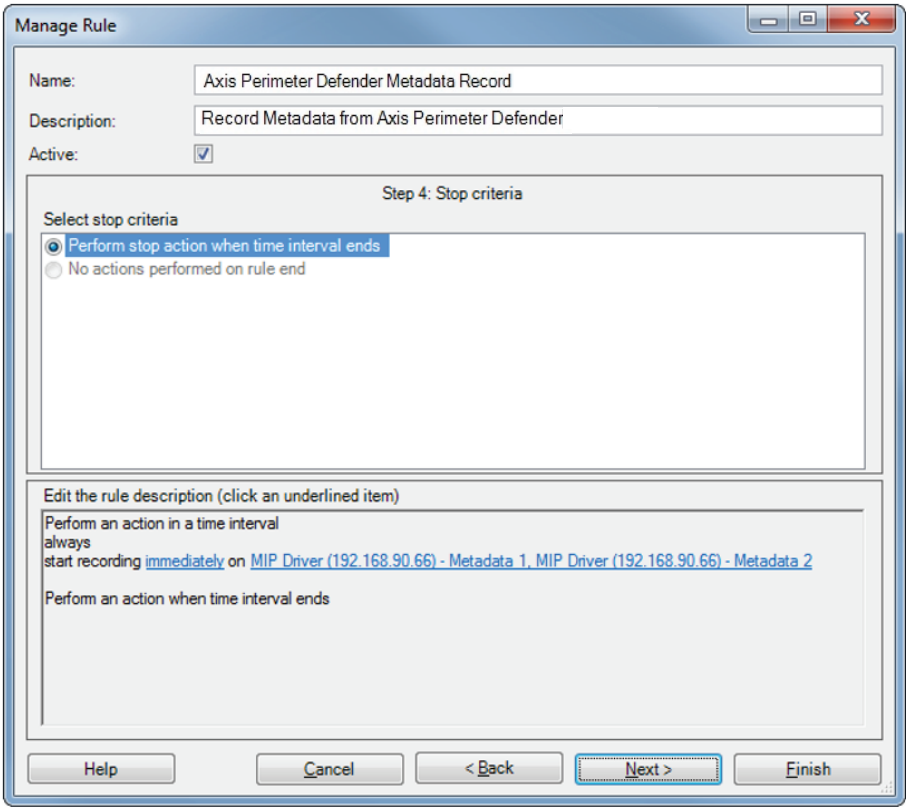
7. Select **Start recording on <devices>**, then click **recording device**.



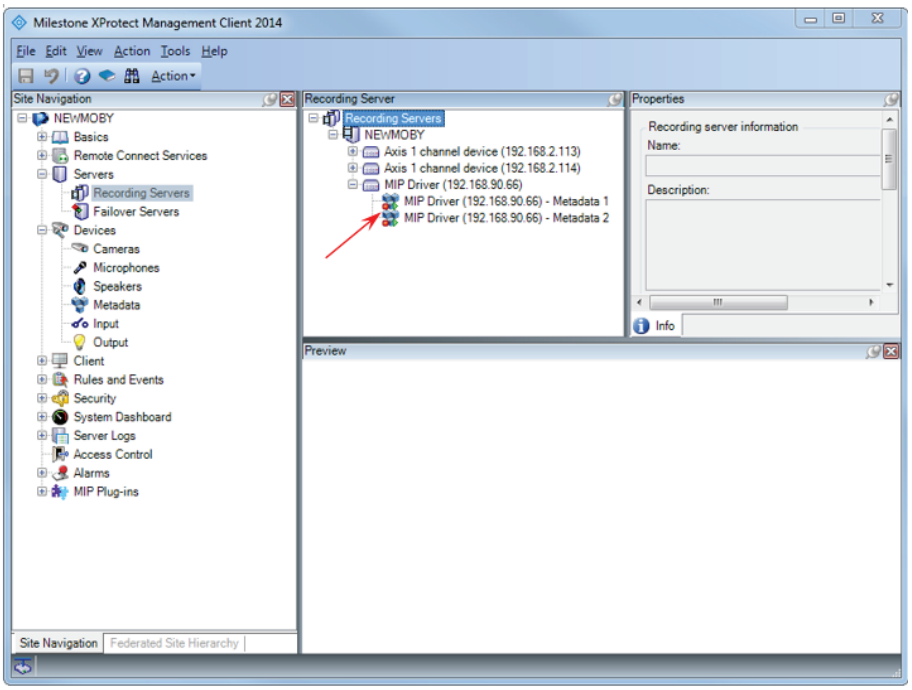
8. Select all the metadata channels and move them to the **Selected** panel by clicking **Add**.
9. Click **OK**.



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



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.

Select what metadata to show

You can fine-tune what part of the corresponding metadata stream to show (in live and/or in playback mode) for each camera.

Metadata consists of four types of graphical information:

1. Actors – graphical rectangles surrounding the persons or vehicles moving in the scene.
2. Trajectories – the path followed by an actor in its movement in the scene.
3. Alarms – a graphical indicator in the upper right corner of the image, normally green but turning red when an alarm is triggered.
4. Zones – the set of zones on the ground defining the scenarios to trigger.

You can choose which of the four types to show in live mode and/or in playback mode, and for each separate video stream.

1. Under **Site Navigation**, select **MIP Plug-ins > AXIS Communications > Perimeter Defender bridges**.
2. Under **Perimeter Defender bridges**, select the bridge whose metadata stream you want to configure.
3. Select the **AXIS Perimeter Defender cameras** tab.
4. Select the video stream(s) to configure.
5. Change the metadata display settings for the selected video stream(s).
6. Save the configuration.

How to use trigger further actions

The User Defined Events and Analytics Events triggered by the APD Bridge can be used to trigger further actions:

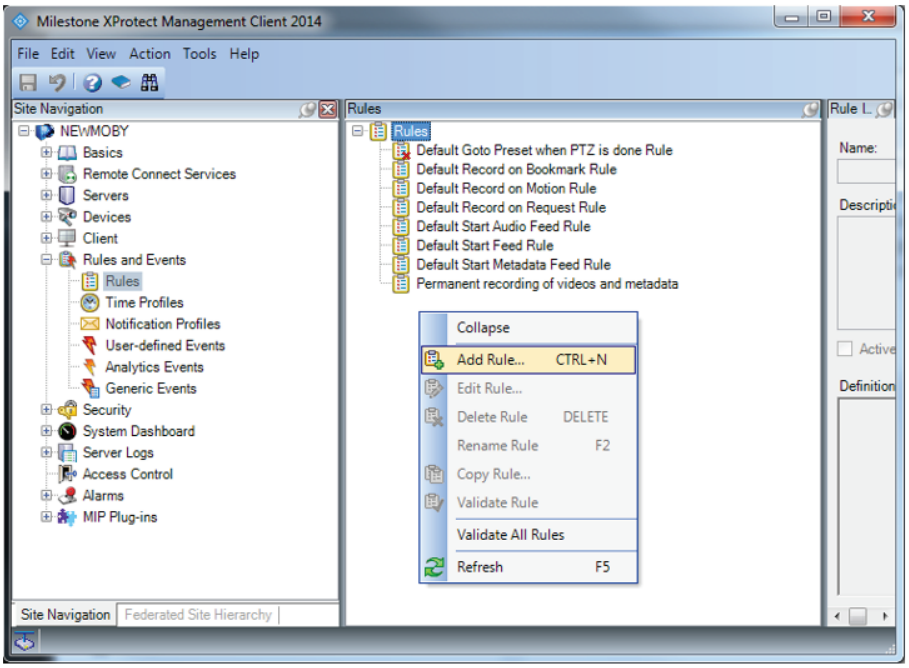
- Using the User Defined Events, specific rules can be used to:
  - Start image and metadata recording on alarms from AXIS Perimeter Defender or, in case a permanent recording is in place, to raise the quality, resolution and frame rate of the recording.

- 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.

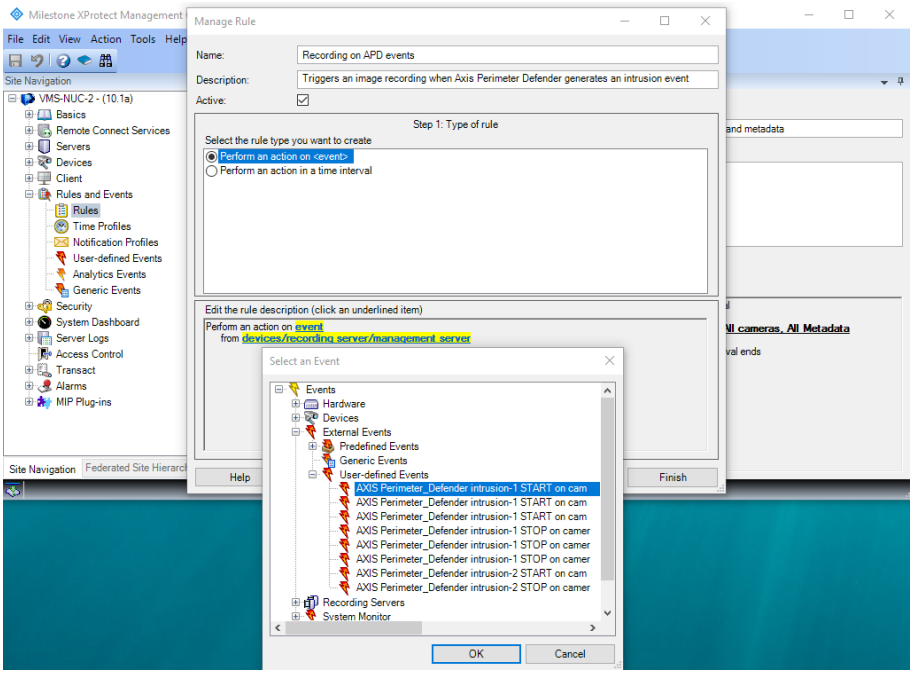
- Using the Analytics Event, a specific alarm can be triggered.

How to start image recording using User Defined Events

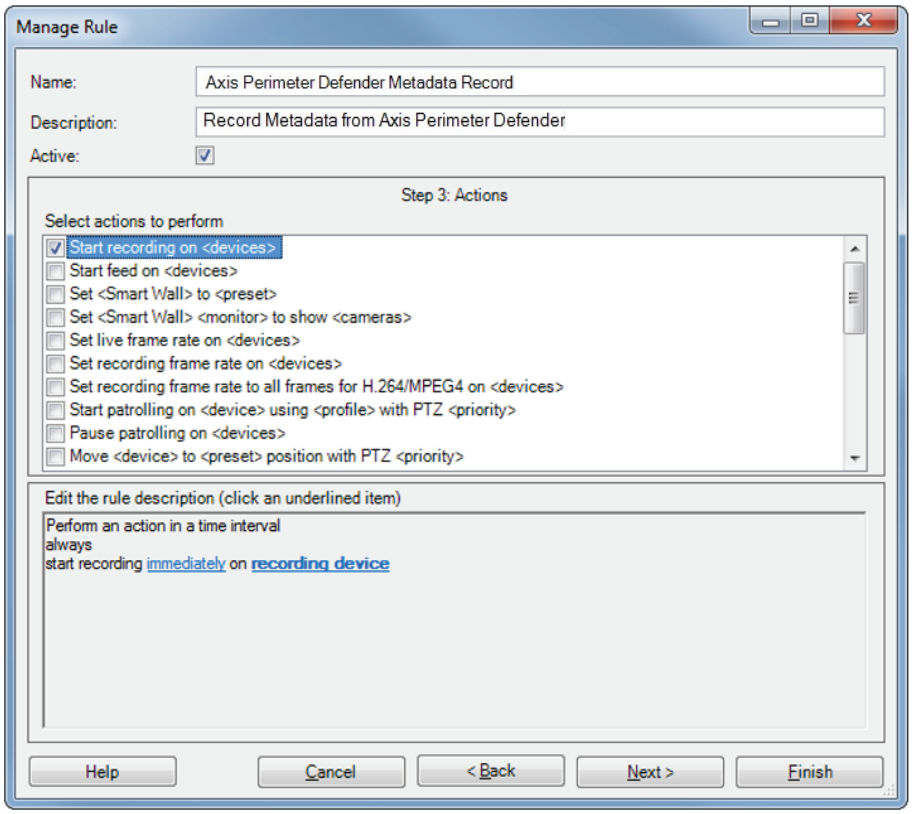
1. Select **Rules and Events**, then select **Rules**.
2. Right-click **Rule**.
3. Select **Add Rule...**.



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**.



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



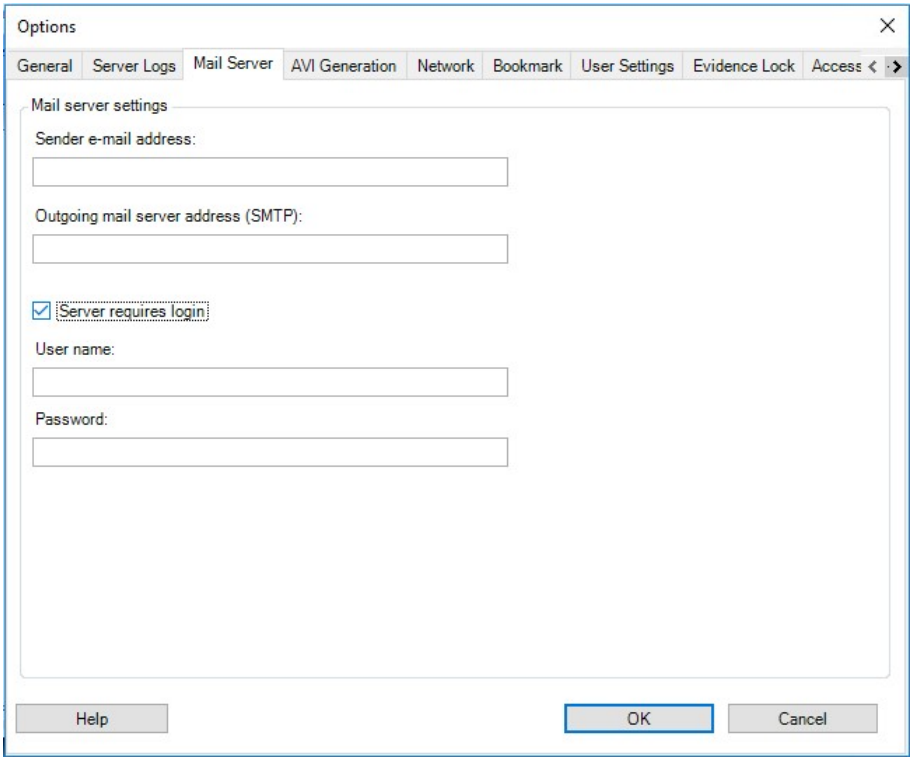
12. Select the action **Start recording on <devices>**

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.



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**.

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 39*. As action to trigger, select **Send notification to <profile>** and select the email notification profile defined in this section.

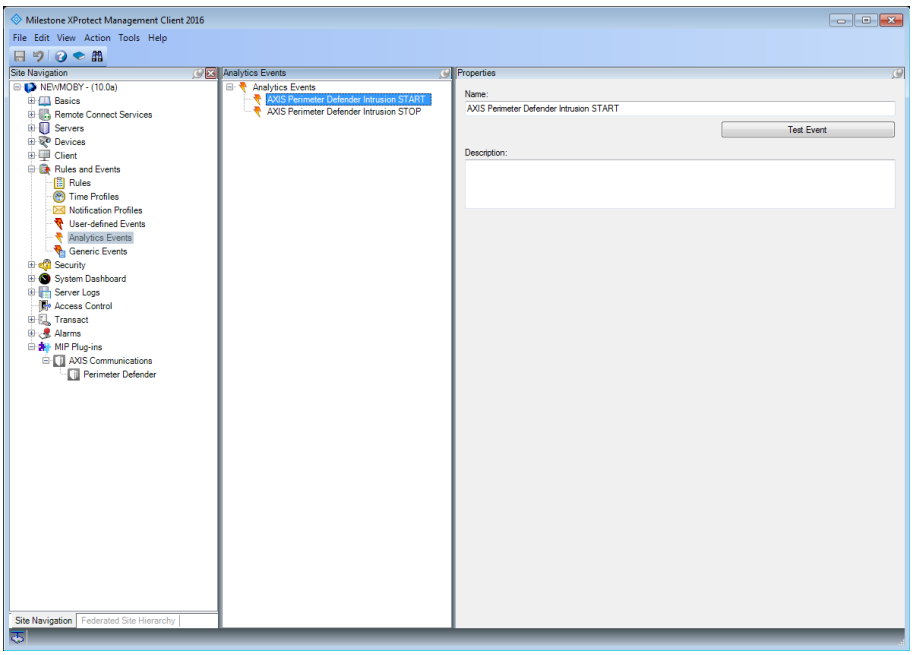
How to open and close a dry contact using User Defined Events

To activate an output, you have to define a rule as described in *How to start image recording using User Defined Events on page 39*. In step 12, select the action **Set device output to <state>**. Choose the device output and the state that you want.

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 select **Add New...**.

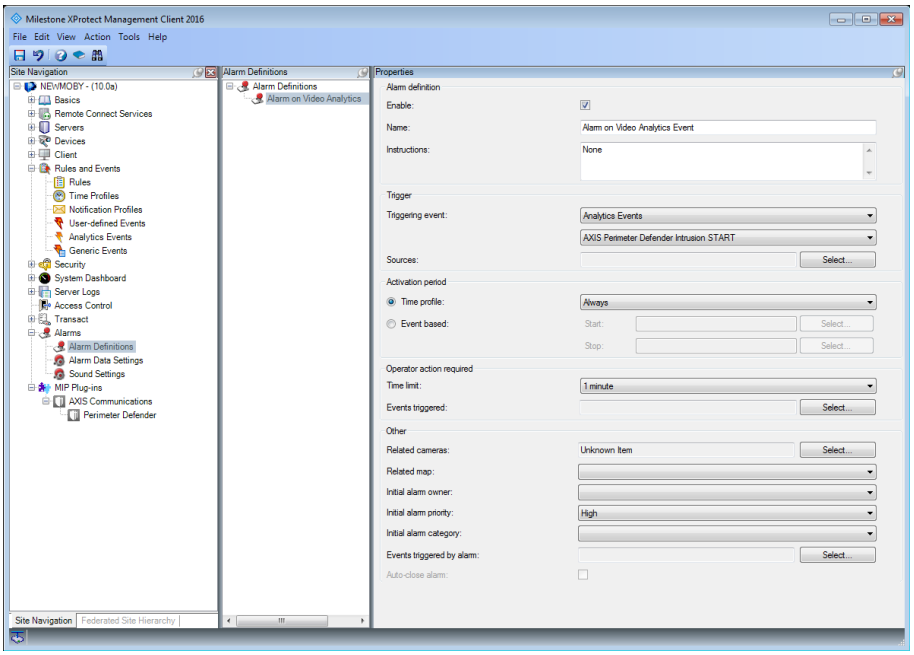


4. Type a name with the following syntax: "AXIS Perimeter_Defender <ScenarioName> <START/STOP>", where <ScenarioName> is the name of the scenario as defined AXIS Perimeter Defender, and START/STOP is one of the following values: "START" or "STOP".

   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-3 START". If you want the rule to trigger for all scenarios, type "ALL" as <ScenarioName>.

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.



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

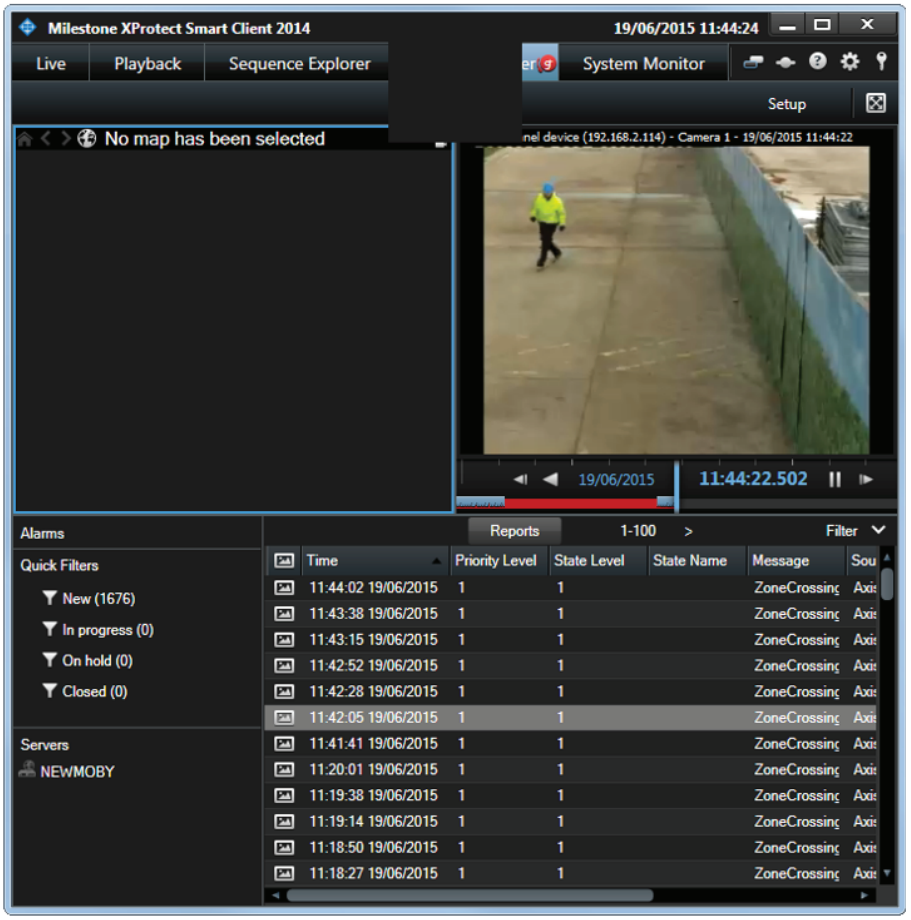
How to use the Smart Client

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

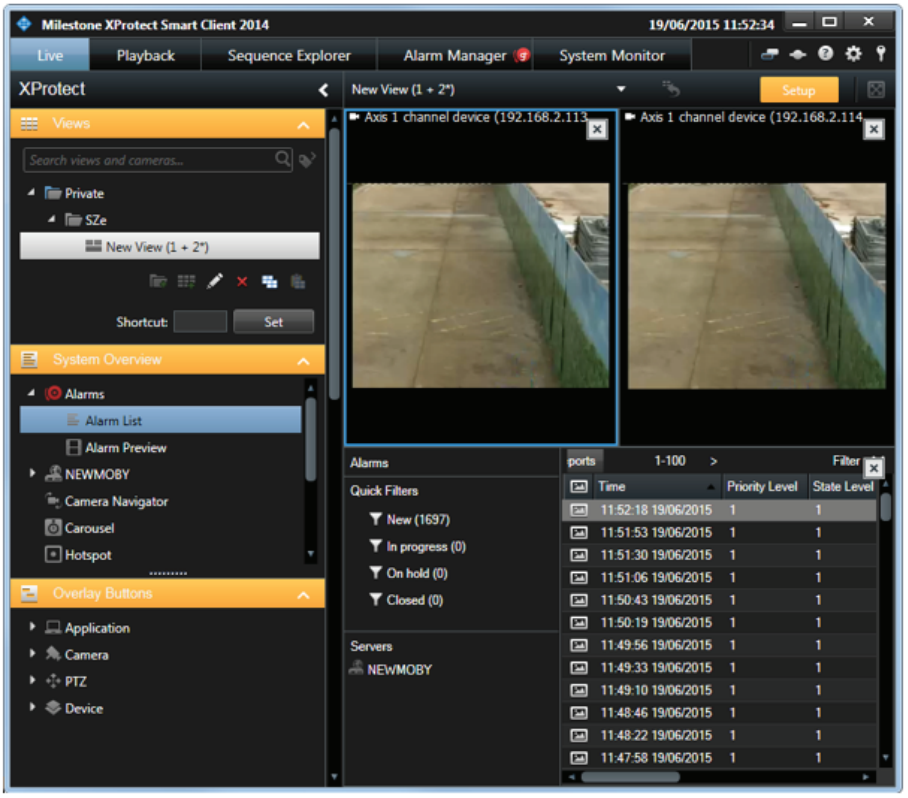
To view all alarms, go to **Alarm Manager**.

Alarms, events, bookmarks, and metadata



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.

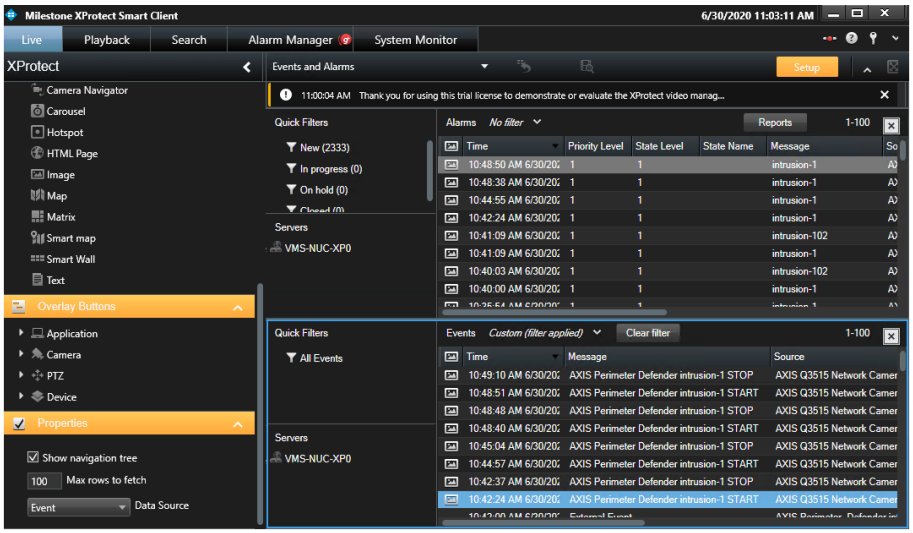


If you are not interested in alarm reception in the Smart Client, you can deactivate the automatic triggering of alarms by the AXIS Perimeter Defender Metadata Bridge by using the Configuration Tool. See *Software installation on the host running the XProtect Recording Server on page 12*.

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**:



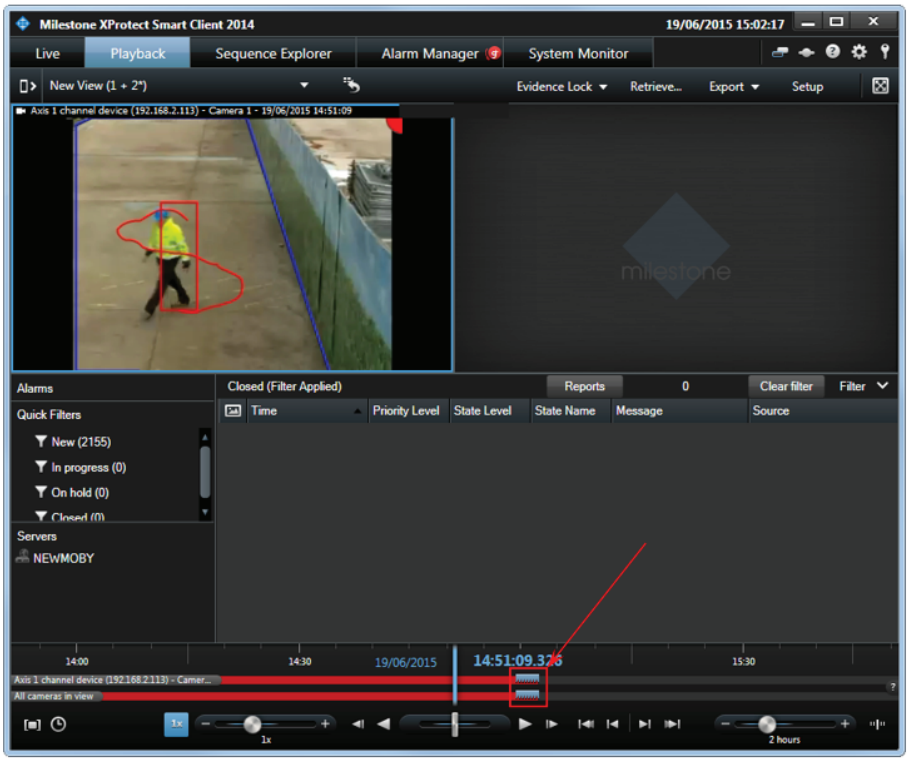
5. The events triggered by AXIS Perimeter Defender show up in the corresponding tile when you commute back from the **Setup** mode.
6. You can also switch from alarms to user-defined events in the **Alarm Manager** tab, by following the same procedure.

About bookmarks

Important

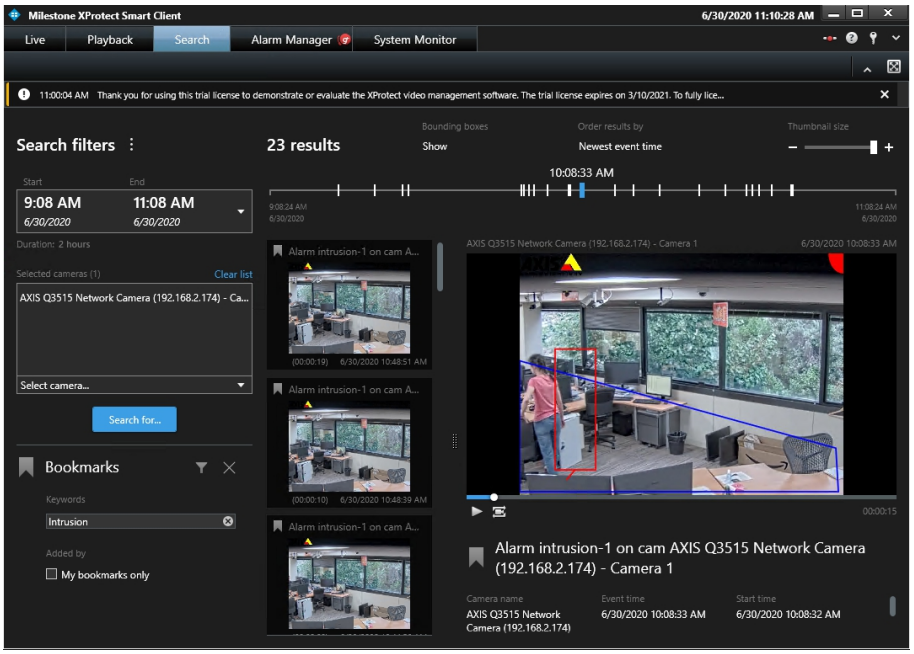
Bookmarks are only available in XProtect Corporate/Expert/Professional+.

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.



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

Bookmarks can also be used to search for sequences in the **Search** tab.



1. Open the **Search** 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 "Intrusionr".
5. The corresponding bookmarked sequences are shown in the center pane and on the timeline.
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

Starting from XProtect 2017R1, 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. For XProtect releases before 2017R1, an additional step is required to associate a metadata stream with the corresponding video stream. This step is described in *Manually associate a metadata stream and a video stream on page 63*.

Typically, metadata looks like in the image below.

1. The upper right corner of the image contains a colored spot. The color indicates the alarm status:
   - Red, if AXIS Perimeter Defender is running and an alarm is triggering for the camera (in the 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)
   - Yellow, if AXIS Perimeter Defender is in error state. This situation requires to use the AXIS Perimeter Defender Setup Tool to check the Video Analytics Configuration. Usually this happens when the video source

feeding a server that has changed the aspect ratio with respect to the one used to calibrate. In this case, AXIS Perimeter Defender can't run and the calibration needs to be redone.

- Gray, during a short period (30–60 seconds) after AXIS Perimeter Defender has been started. During this phase AXIS Perimeter Defender is initializing and can't 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 the ground relative to the scenario(s) defined on the camera are shown in blue.
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.

Fix "skew" in metadata display

Sometimes the metadata shown on top of a video stream in the Smart Client looks “skewed” or incorrectly sized. A quick comparison with the same metadata shown in the AXIS Perimeter Defender Setup Tool helps confirm that something is wrong.

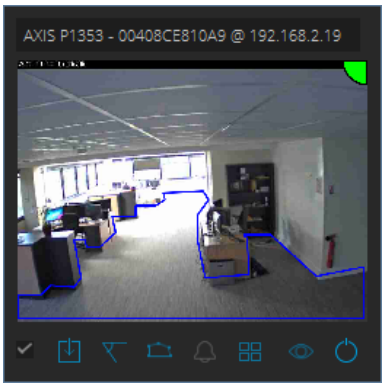


Image with metadata in AXIS Perimeter Defender Setup Tool

Alarms, events, bookmarks, and metadata

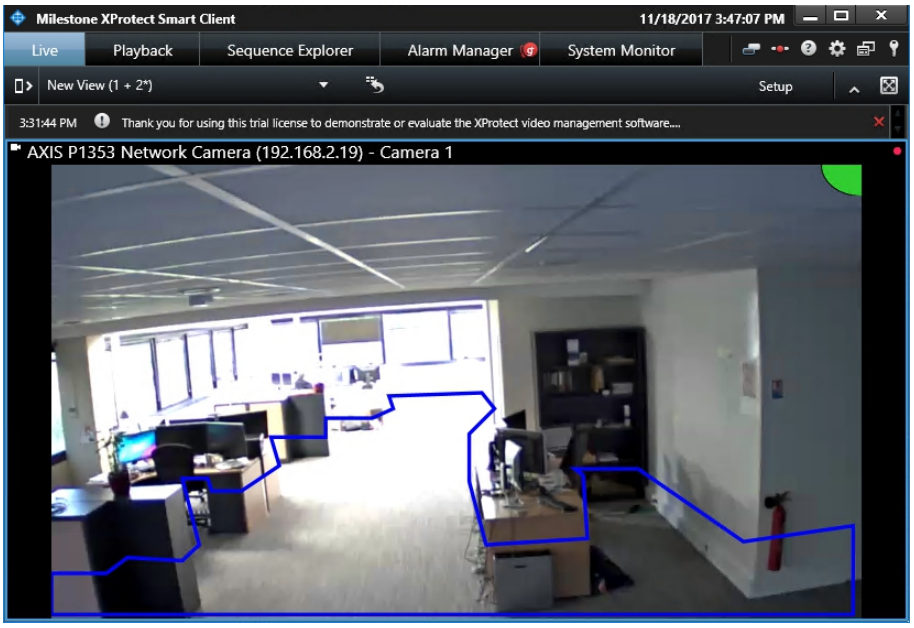


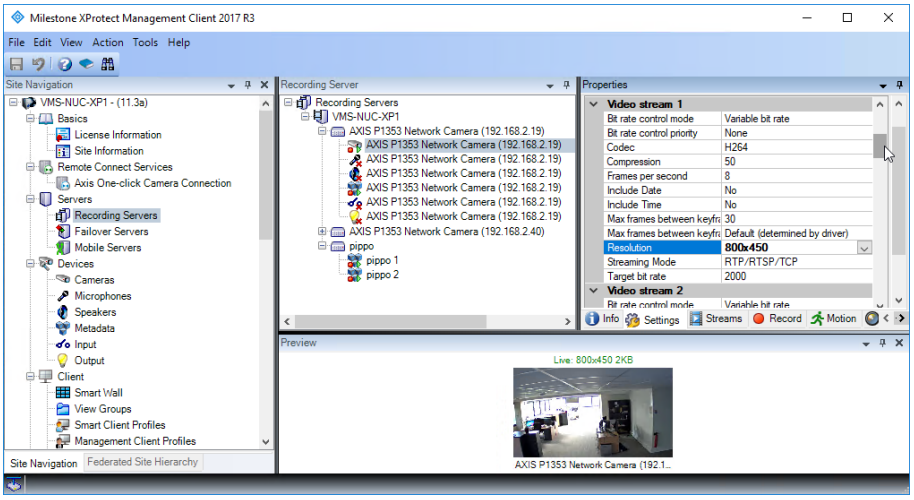
Image with metadata in the Smart Client

In the image from the AXIS Perimeter Defender Setup Tool, the metadata is correctly shown, while in the image from the Smart Client the metadata is skewed and doesn't match the image. This problem occurs when the XProtect Recording Server requests a video stream whose aspect ratio is different from the one analyzed by AXIS Perimeter Defender on the camera.

To solve this issue, you have to modify the video stream resolution in the Management Client and set an aspect ratio that matches the one analyzed by AXIS Perimeter Defender.

1. In AXIS Perimeter Defender Setup Tool, hover the video source name above the video stream to show a tooltip including the aspect ratio of the analyzed video stream.

2. In XProtect Management Client, select the corresponding camera and open the **Settings** tab.



3. Among the available video stream resolutions, select one with the same aspect ratio as the video stream analyzed by AXIS Perimeter Defender, for example 800x600 or 640x480.

4. Save the modification.

5. The Smart Client immediately uses the new resolution and the metadata is shown correctly on top of the video stream.

Fix desynchronization in metadata playback display

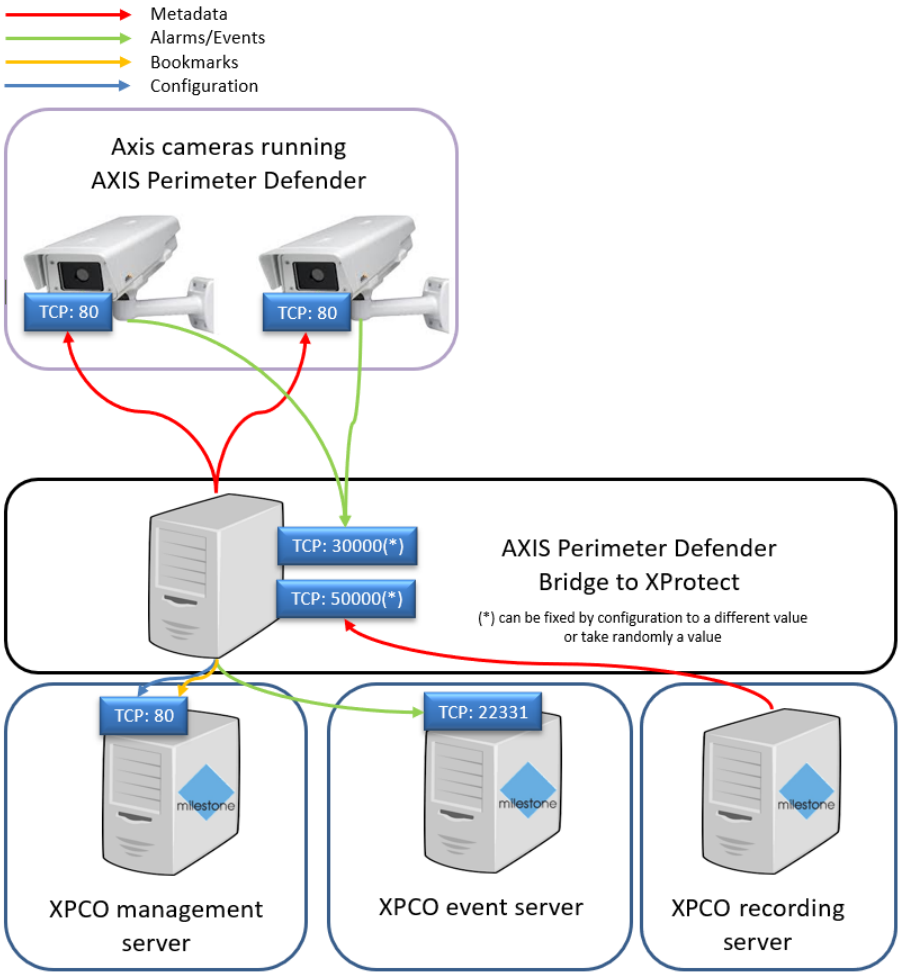
Sometimes the metadata looks desynchronized when played by the Smart Client. Typical signs is that the bounding boxes surrounding actors are ahead of or behind the actors. To minimize this issue:

1. Install, configure, and use an NTP time server (not the standard Windows time synchronization feature) to provide time to all the involved video sources (cameras/encoders), servers (AXIS Perimeter Defender servers and Milestone servers), and players (PC where the Smart Client is used).
2. Make sure all devices are set to use the same NTP server, that their time zone is correctly set, and that the daylight saving is activated coherently on all of them.
3. Check that all cameras and servers have the same time, with a maximum drift of 250 ms from each other.
4. In the Management Client, go to **MIP Plug-ins > AXIS Communications > Perimeter Defender bridges** and select the bridge.
5. Select the **Alarm & Metadata Configuration** tab.
6. Select **Servers/cameras use NTP for time synchronization**.
7. Save the settings.

Advanced configuration

Network communication

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 APD Bridge is shown as a separate server, but can be installed on the XPCO host as well.
- The APD 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 APD Bridge connects to AXIS Perimeter Defender and retrieves the metadata stream. It then implements a 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 APD Bridge stores its configuration in the XPCO Management Server.

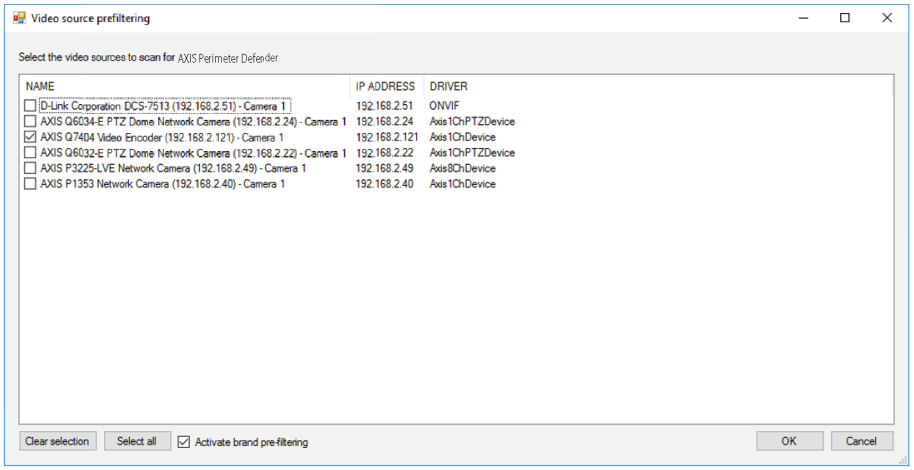
Add new video sources to the system

When you add a new video source, you first need to 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.

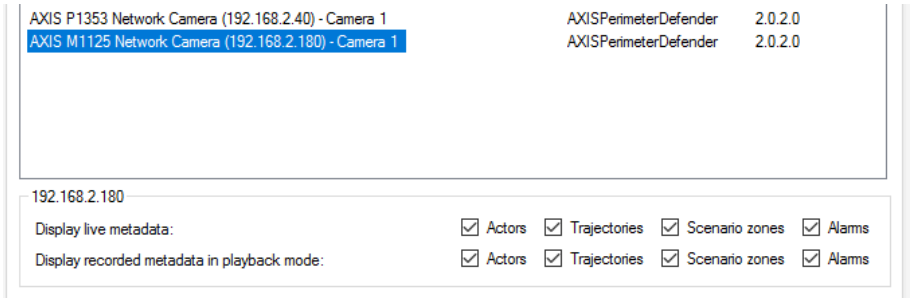
In the following instructions, the video source "AXIS Q7404 Video Encoder (192.168.2.121) – Camera 1" has recently been added to the system.

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

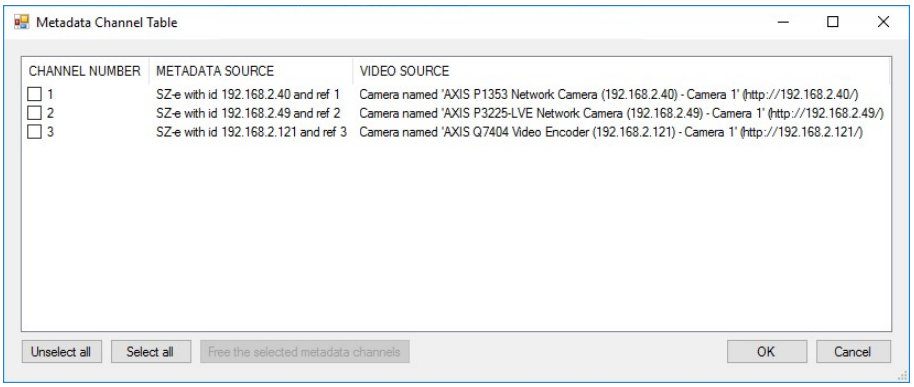
1. Configure the AXIS Perimeter Defender installed on the device and start the application.
2. In the **AXIS Perimeter Defender cameras** tab, click **Scan new cameras** and, if the pre-selection steps is chosen, make sure that the new devices are selected.

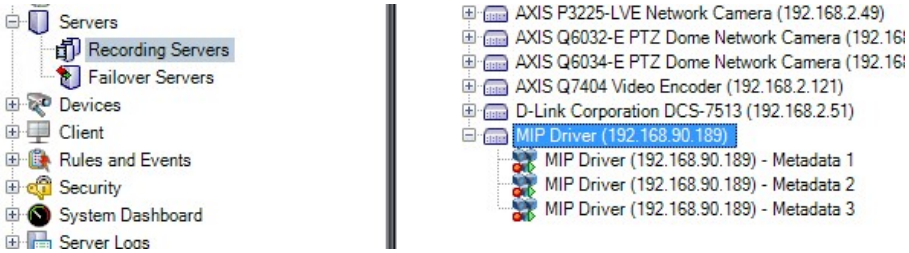


3. When the scan has finished, select the new devices one by one and select the **Display live metadata** and **Display recorded metadata in playback mode** options.



4. In the **Alarm & Metadata Configuration** tab, click **Generate user-defined events** if you plan to use them, and then press CTRL+S to save the configuration.
5. Consider if you need to replace the MIP Driver device within the XProtect system. See *Increase the number of channels of the MIP Driver on page 55*.
6. In the **Alarm & Metadata Configuration** tab, click **Display metadata channels** to display the channel table. Make sure that the metadata channel associated to the new device is enabled on the MIP Driver device.



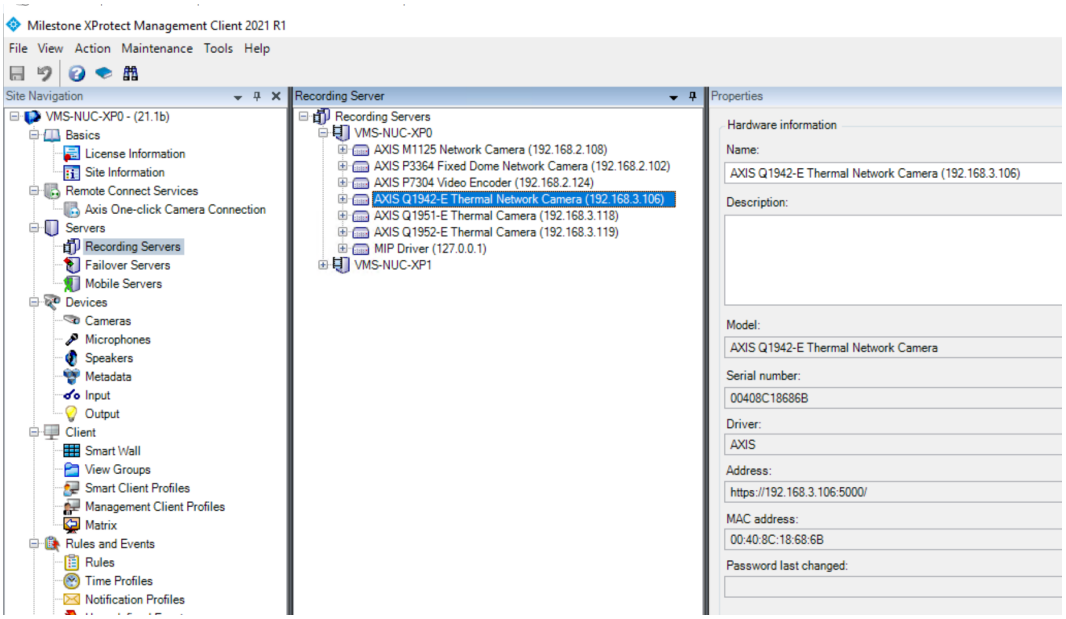


Add HTTPS devices to the system

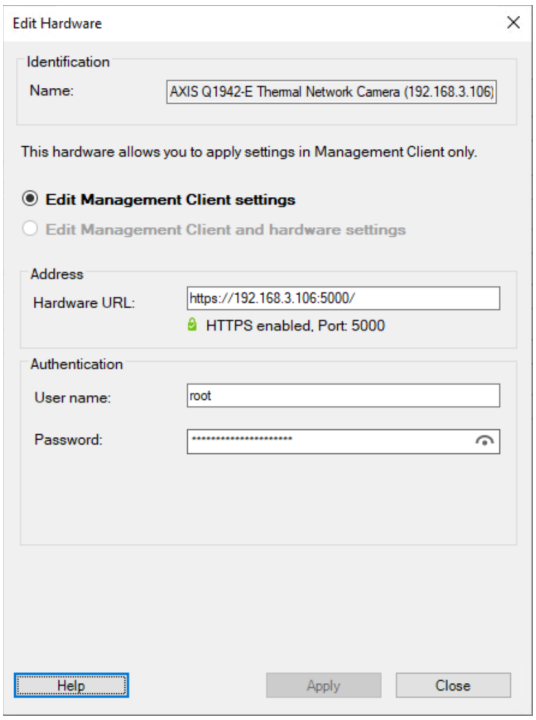
To make it possible for the bridge to reach AXIS Perimeter Defender on devices that are configured in HTTPS-only mode (no HTTP), you need to follow these instructions when you add the devices to the VMS.

1. Add the device to the VMS.
2. Under the corresponding recording server, click the device and check that the URL format in **Address** corresponds to: `https://<IP_or_hostname>:<https_port>`.

   The `<https_port>` can be missing if the device uses the default port (443).



3. Right-click the device and click **Edit hardware**.
4. If the URL in **Hardware URL** is incorrect, update it.

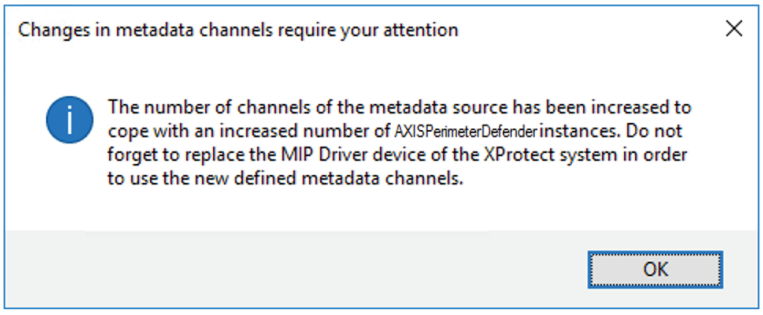


5. Click **Close**.
6. Go back to the plugin page on the **AXIS Perimeter Defender cameras** tab, and press F5 to reload the configuration.
7. Do a new scan and proceed according to the instructions in *Add new video sources to the system on page 52*.

Increase the number of channels of the MIP Driver

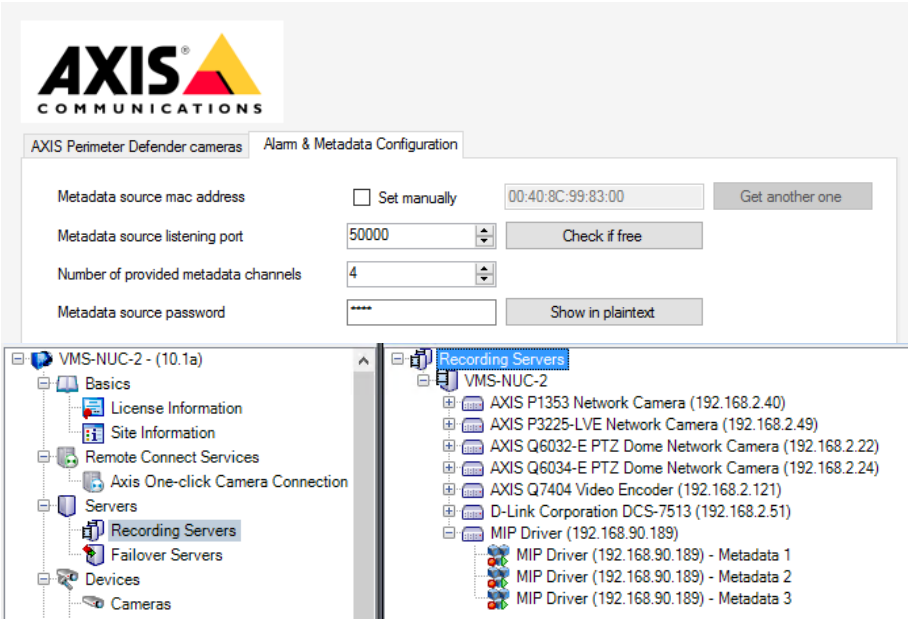
The MIP Driver device that sends the metadata streams to XProtect must be replaced if the number of channels it presented when added to XProtect the very first time is smaller than the number of AXIS Perimeter Defender instances sending metadata to XProtect.

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.

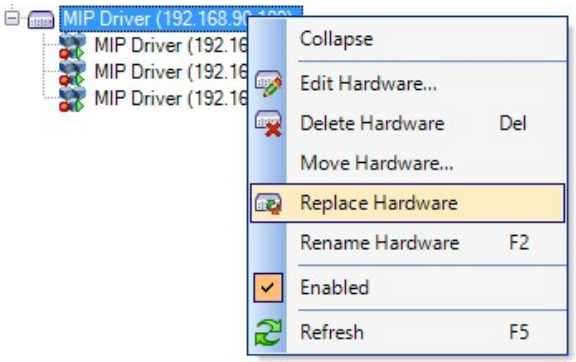


In this example, the MIP Driver device must be replaced in order to obtain the 4 metadata channels provided by the metadata source.

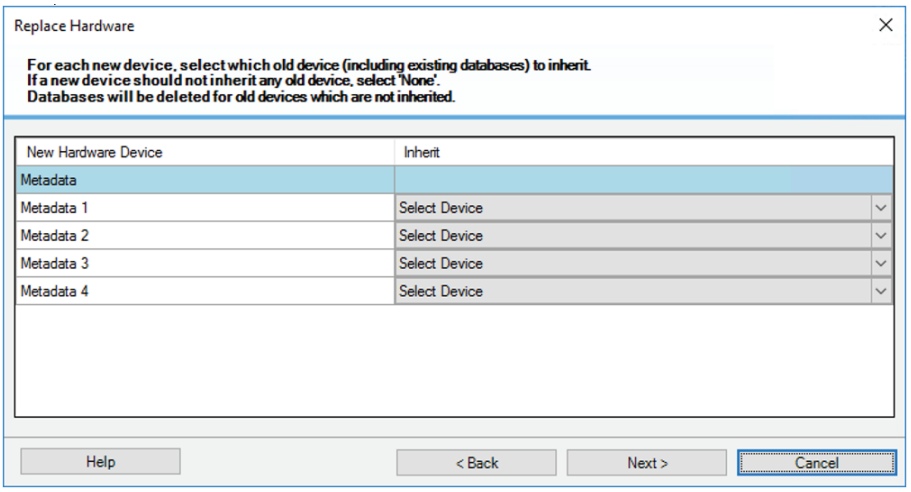
Select one of the following options:

- 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**.

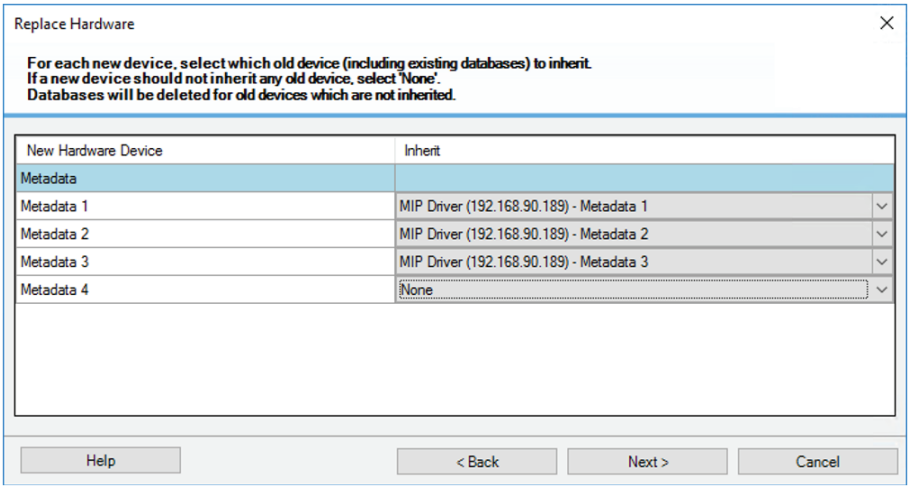


2. Click **Next**.
3. Check the information. If nothing has changed, click **Next**.

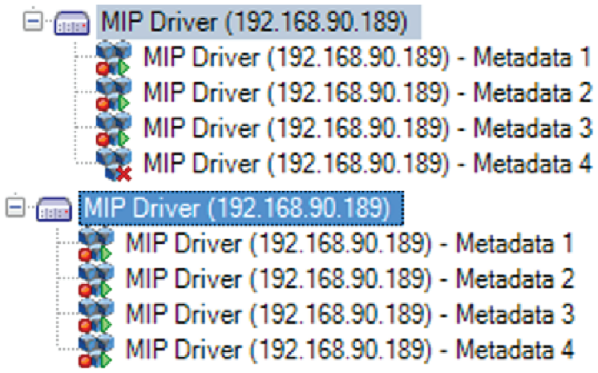


This window presents all the metadata channels provided by the metadata source, in this example four metadata channels.

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.



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



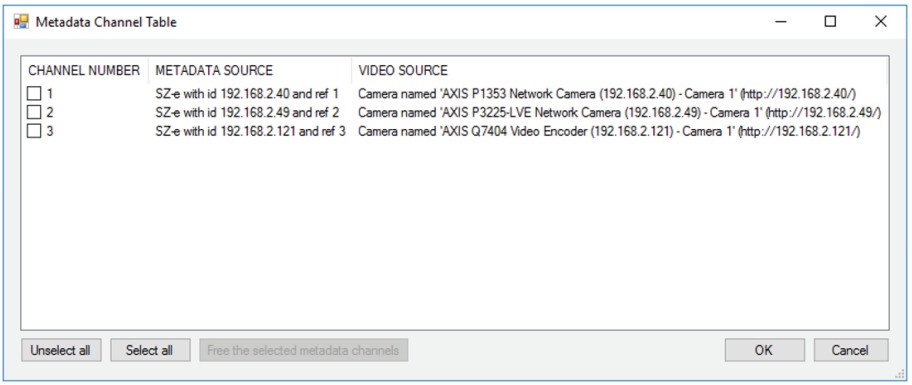
Remove video sources from the bridge configuration

Note

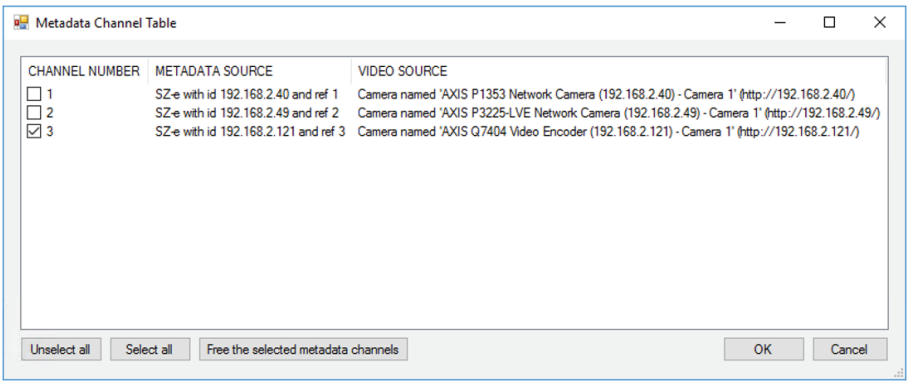
This section is only valid for XProtect Corporate/Expert.

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

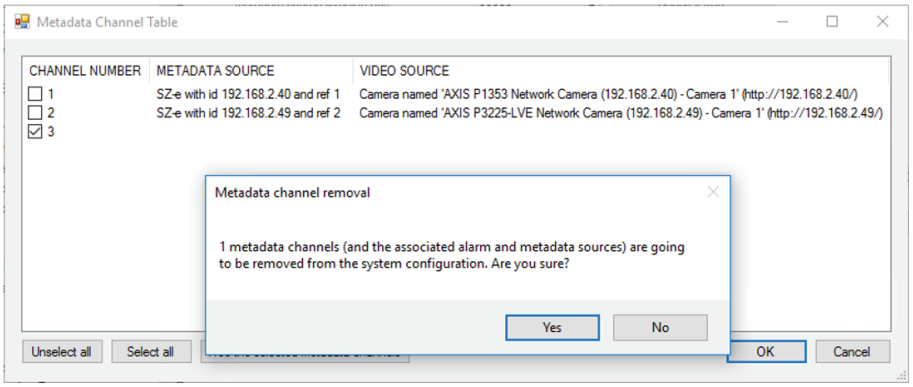
1. Click **Display metadata channel**.



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**.



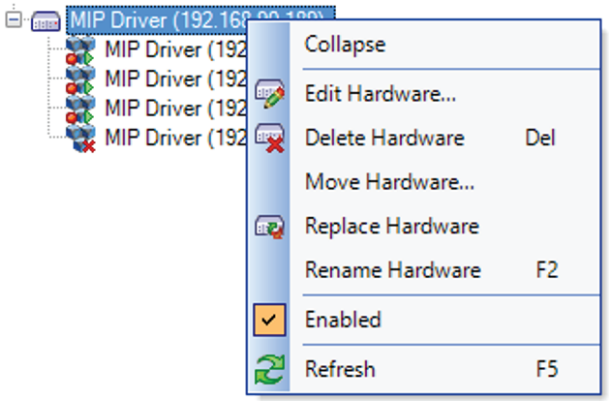
3. Click **OK** and then click **Yes**.



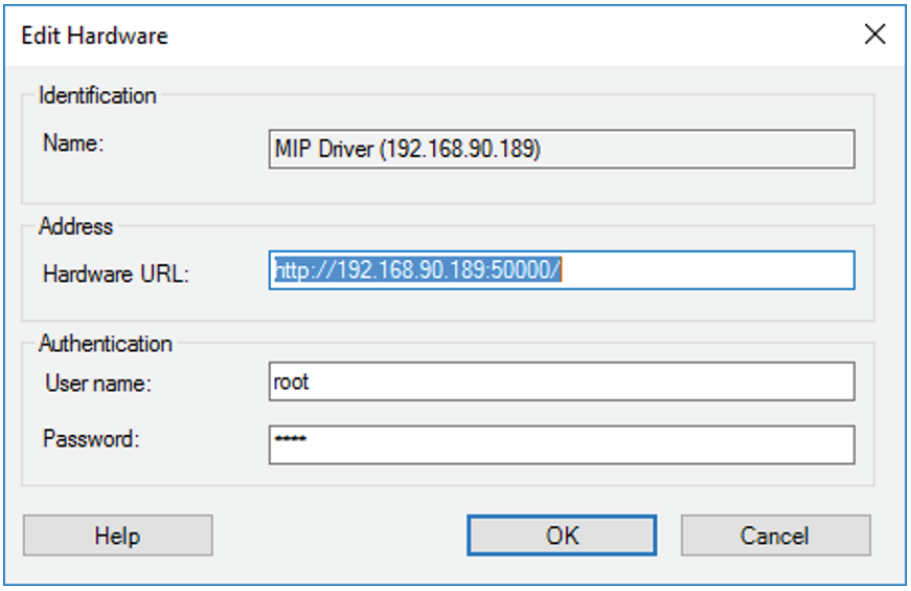
Change the IP address of the bridge server

To change the IP address of the host where the bridge is installed:

1. Change the IP address of the host at Operative System level.
2. Reboot the host.
3. 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**.



- 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.

Change the IP address of an Axis device

To change the IP address of an Axis device where AXIS Perimeter Defender is installed:

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.
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.

Enable metadata export when exporting video footage

When you export video sequences with AXIS Perimeter Defender metadata on top, metadata is automatically exported along the video sequence and is automatically replied on top of the exported video sequence.

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.

Upgrade the software to a newer version

When a new version of the APD Bridge to Milestone XProtect software is released, consider upgrading your existing installation to the new version. Before you decide:

- Check the release notes of the new version to see if the upgrade is worthwhile (for example, if the new release fixes bugs that you encountered or introduces interesting new functionality).
- Make sure that the new release is compatible with your existing systems. Check:
  - The version of the AXIS Perimeter Defender software you are currently using. Does the new version of the Milestone Bridge still support them?
  - The version and the type of the XProtect software you are using: does the new version of the Milestone Bridge still support them?
  - The software prerequisites introduced by the new version of the Milestone Bridge: does your currently installed system fulfil those prerequisites? If not, can you upgrade these prerequisites as well?

Once you verified that you can safely proceed to the software upgrade, follow these steps to upgrade the software:

1. Uninstall the old version of the software through the Windows Control Panel, in **Programs and Features**. The existing configuration of your system will be left in place.
2. Install the new version, as described in *Installation and first configuration steps on page 9*.
3. At the first run, the AXIS Perimeter Defender MIP Plugin retrieves the old configuration. Convert it to the format of the new software so you retrieve the same configuration that you had before.
4. Perform a complete set of checks (alarms, bookmarks, metadata, and so on) to be sure that your system behaves as expected (and consistently with how it was configured before).

Important

When you upgrade, make sure to upgrade all instances of the MIP Plugins (both in the Management Client and the Smart Client) and the APD Bridges at the same time.

Set alarm reception parameters in specific situations

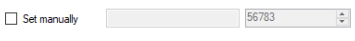
The APD Bridge triggers two tasks to receive alarms from AXIS Perimeter Defender:

- At start-up, it opens a listening TCP/IP socket on all the IPv4 addresses of the host, on a specific port.
- At start-up, and then periodically (every hour) it programs the AXIS Perimeter Defender applications to send alarms to a specific IPv4 address of its host, on the specific port it is listening on.

In simple situations corresponding to simple network topologies, you can configure the bridge in "automatic mode" to handle these steps automatically. In automatic mode the operator does not need to configure anything. To activate "automatic mode", leave the check box **Set manually** in the **Alarm & Metadata Configuration** tab of the AXIS Perimeter Defender MIP Plugin clear.

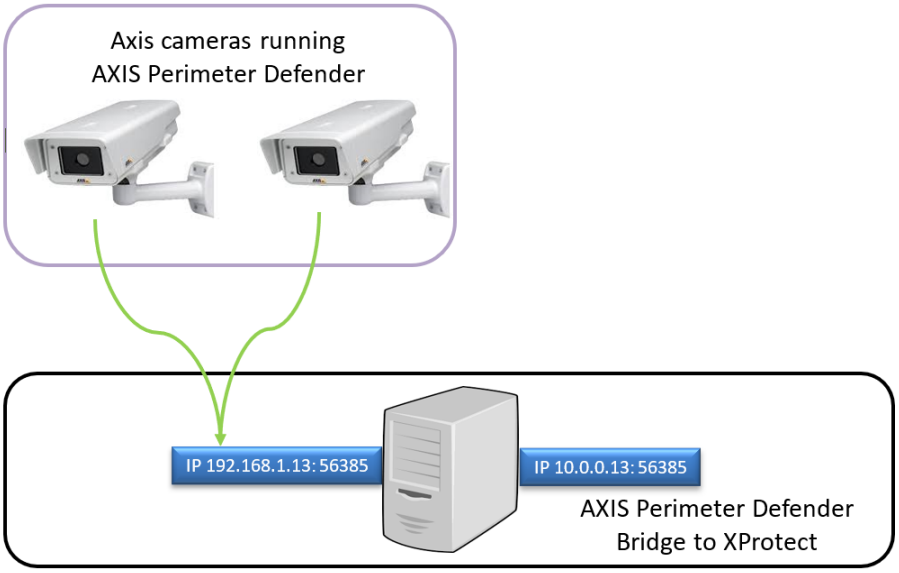
When the automatic mode is active:

- The APD Bridge autonomously chooses a listening port that is free (that is, no other application is listening on it) on the host. The chosen port randomly changes at each restart of the APD Bridge, that is, it is not constant across restarts. The chosen port is displayed by the MIP Plugin in the port dialog near the **Set manually** checkbox (56783 in the image):



- The APD Bridge opens a TCP/IP listening socket on that port and on all the IPv4 interfaces of the host it is running on.
- For each device with AXIS Perimeter Defender (configured to be used as source of alarms) the APD Bridge detects the IPv4 network interface - among all the available ones – that routes to the camera, and sets the corresponding AXIS Perimeter Defender to use it, in association with the chosen port, as destination for the alarms.

Advanced configuration



A general network topology compatible with the automatic mode.

The illustrated example shows:

- The host where the APD Bridge runs has two public IPv4 network interfaces, 192.168.1.13 (used to connect it to all the cameras running AXIS Perimeter Defender) and 10.0.0.13 (used to connect it to all the servers running AXIS Perimeter Defender).
- At start-up, the APD Bridge finds the free (on all its interfaces) listening port 56385 and opens a listening socket on this port and on all its IPv4 interfaces. This port can change at the next restart of the APD Bridge service.
- The APD Bridge sets all the AXIS Perimeter Defender instances to send alarms to tcp://192.168.1.13:56385 and all the AXIS Perimeter Defender servers to send alarms to tcp://10.0.0.13:56385

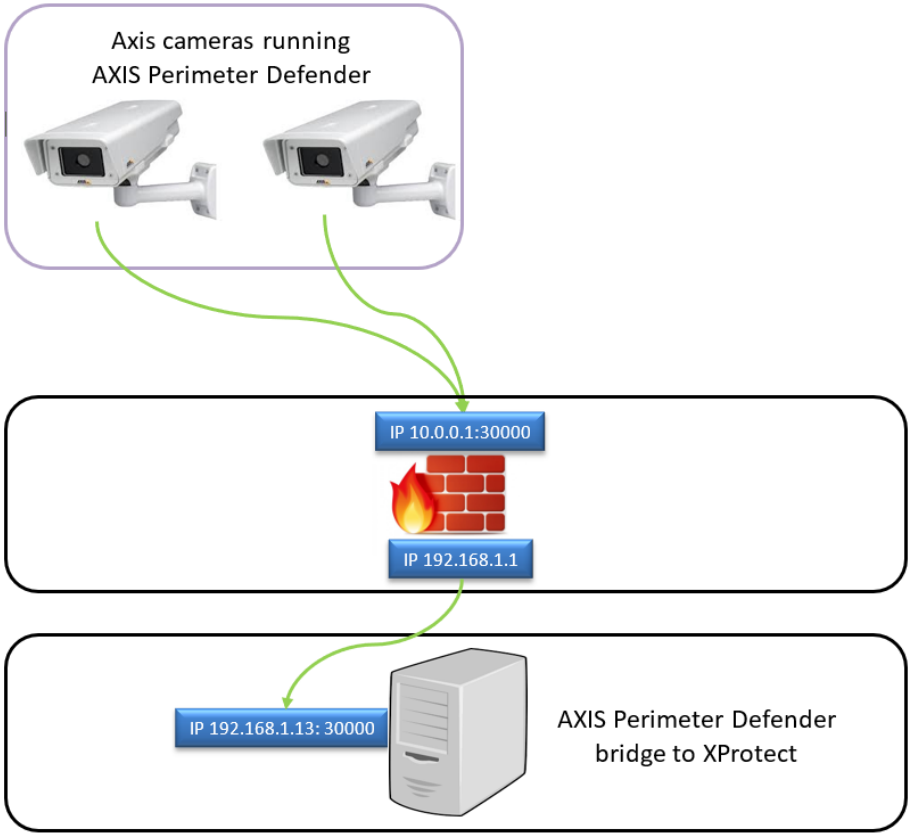
There are two situations in which the automatic mode cannot be used:

- If the listening port is not allowed to change across restarts of the application (for example, for firewall or port redirection reasons).
- If the auto-detection of the destination IPv4 interface can't work, like, for example, in a NAT scenario (when the bridge would assume that the IPv4 interface of the host is the one to use by AXIS Perimeter Defender to send alarms, whilst this would not work as the one to use is the public IP address of the NAT device).

In these situations, you must deactivate the automatic mode and manually specify:

- The listening port that the APD Bridge should use to receive the alarms. It is the user responsibility to make sure that this port is free (and will be always free in the future) on all the IPv4 interfaces of the APD Bridge host.
- The IP address that AXIS Perimeter Defender should use to send alarms to the Bridge. In NAT scenarios this usually corresponds to the external IP address of the device implementing the NAT (a firewall or a router).
- The appropriate port redirection in the NAT front-end (the firewall/router).

Advanced configuration



A typical NAT situation

The illustrated example shows:

- The firewall/router implementing the NAT hides the APD Bridge behind a "public" address 10.0.0.1.
- AXIS Perimeter Defender cameras have connectivity to the IP address 10.0.0.1 of the router (for example, they have IP addresses in the network 10.0.0.1/24).
- The APD Bridge has an IPv4 address 192.168.1.13, which is not reachable directly from the cameras.
- In this case, the user selects the checkbox **Set manually** and enters the parameters like in the following image:

- The user adds a redirection rule in its firewall/router from tcp://10.0.0.1:30000 to tcp://192.168.1.13:30000. It is not possible to have different port numbers on the firewall and on the APD Bridge, so choose one which is free on both the firewall/router and the APD Bridge host.

With these settings, the APD Bridge:

- at start-up, opens a listening socket on all its IPv4 interfaces on the given port 30000.
- at start-up and then every hour, it sets tcp://10.0.0.1:30000 as the destination for the alarms for all the AXIS Perimeter Defender instances.

This way, when AXIS Perimeter Defender triggers an alarm, it sends the TCP/IP notification to tcp://10.0.0.1:30000, the firewall/router receives it and redirects the message to tcp://192.168.1.13:30000 where the APD Bridge receives and processes it.

Manually associate a metadata stream and a video stream

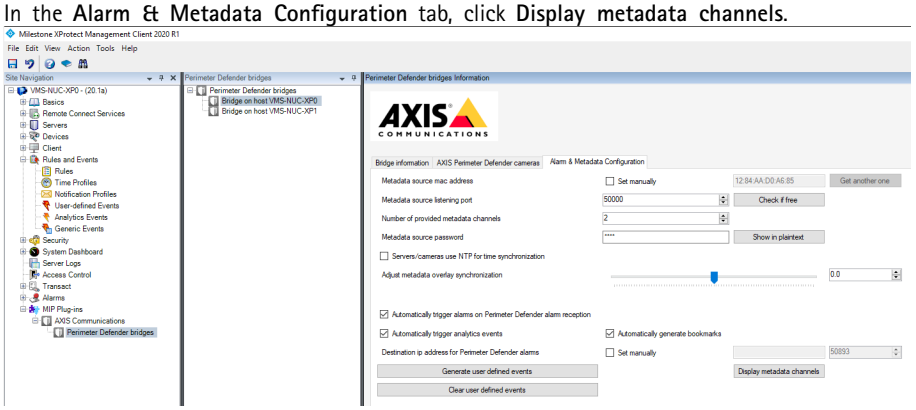
Note

This instruction is only needed for XProtect versions up to 2016R3. In XProtect version 2017R1 and later, the association is done automatically.

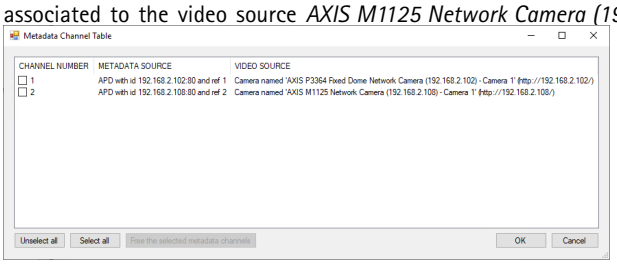
To associate a metadata stream to a video stream (so that the metadata is displayed on top of the video stream):

1. In the Management Client, navigate to **MIP Plugins > AXIS Communications > Perimeter Defender bridges** and select the APD Bridge that you want to configure.

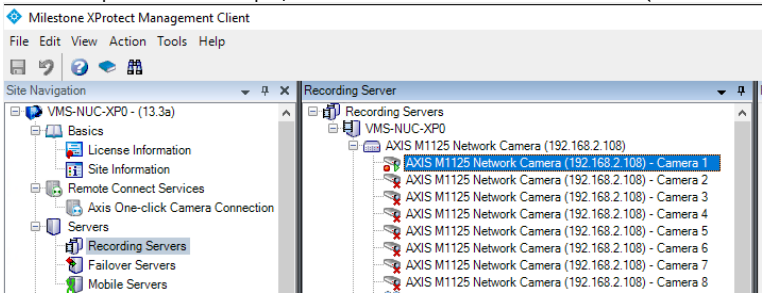
2. In the **Alarm & Metadata Configuration** tab, click **Display metadata channels**.



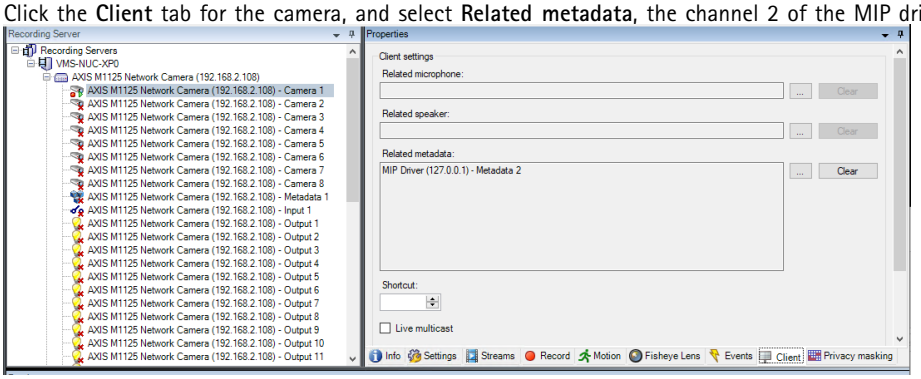
3. Note the channel number for the relevant video source. In this example, the metadata channel associated to the video source *AXIS M1125 Network Camera (192.168.2.108) – Camera 1* is 2.



4. Select the video stream that you want to associate to the metadata channel in **Servers > Recording servers**. Don't select the hardware device but the video streams on which you want the metadata to show up. In this example, select *AXIS M1125 Network Camera (192.168.2.108) – Camera 1*.



5. Click the **Client** tab for the camera, and select **Related metadata**, the channel 2 of the MIP driver.



6. Save the configuration.

7. Repeat for every camera that has an AXIS Perimeter Defender associated metadata stream.

Important

To see the metadata on top of the corresponding video streams, you have to restart the Smart Client.

Change log settings

Each application (APD Bridge, APD Bridge Configuration Tool, Management Client MIP Plugin, and Smart Client MIP Plugin) has its own independent log settings that specify:

- The maximum number of log files that the application keeps on disk.
- The maximum size of the log files.
- The log file position (directory and filename) on disk.
- The log verbosity level.

The standard parameters for each application are:

- Each application keeps at most 10 log files on disk. Each file grows to its maximum size (see below). It's then closed and a new one is used. If there are already 10 log files on disk, the oldest one is deleted.
- The APD Bridge and the AXIS Perimeter Defender Bridge Configuration Tool can append log to their current log file until it reaches 10 MB.
- The Management Client MIP Plugin and the Smart Client MIP Plugin can append log to their current log file until it reaches 100 kB.

As a result, the maximum amount of disk space that can be take by default by each application is:

- 10*10 MB = 100 MB for the APD Bridge and the AXIS Perimeter Defender Bridge Configuration Tool
- 10*100 kB = 1 MB for the Management Client and the Smart Client MIP Plugins

You can change these settings in the log settings files. You can find them:

- For the APD Bridge, in "C:\Program Files (x86)\Axis Communications\AXIS Perimeter Defender Bridge to Milestone XProtect\Alarm and Metadata Bridge\APD.Milestone.MetadataBridge.exe.config"
- For the AXIS Perimeter Defender Bridge Configuration Tool, in "C:\Program Files (x86)\Axis Communications\AXIS Perimeter Defender Bridge to Milestone XProtect\Bridge Configuration Tool\APD.Milestone.BridgeConfigurationTool.exe.config"
- For both the Management Client MIP Plugin and the Smart Client MIP Plugin, in "C:\AXISlogs\AXIS Perimeter Defender Bridge to Milestone XProtect\AXIS-APD-MIPPlugin.log.config". This file is common to both plugins, so if you change the log settings for one plugin it will automatically change for the other one as well.

In the log settings files, the part that needs to be modified is this:

```
<log4net>
    <appender name="MainAppender" type="log4net.Appender.RollingFileAppender">
      <file type="log4net.Util.PatternString" value="%env{SystemDrive}\AXISlogs\AXIS Perimeter Defender Bridge to Milestone
XProtect\%property{application_name}\AXIS_MIP_Plugin.log" />
      <encoding value="utf-8" />
      <appendToFile value="true" />
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="10" />
      <maximumFileSize value="100KB" />
      <staticLogFileName value="true" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%date %-5level [%-3thread] - %message%newline" />
        <header value="%date [START OF A NEW RUN] [Release %property{release_number}]----------------------------------------
---%newline" type="log4net.Util.PatternString" />
        <footer value="%date [END OF RUN] ------------------------------------------------------------------------------------
---%newline" type="log4net.Util.PatternString" />
      </layout>
    </appender>
    <root>
      <level value="INFO" />
      <appender-ref ref="MainAppender" />
    </root>
  </log4net>
```

The most important settings, and the only ones we advise you to change, are:

- **maxSizeRollBackups**: it specifies the maximum number of log files to keep.
- **maximumFileSize**: it specifies the maximum size of each file. The format is a number followed by a space unit like KB (kilobytes), MB (megabytes), GB (gigabytes).

Note

You don't have to restart the application for changes to be implemented.

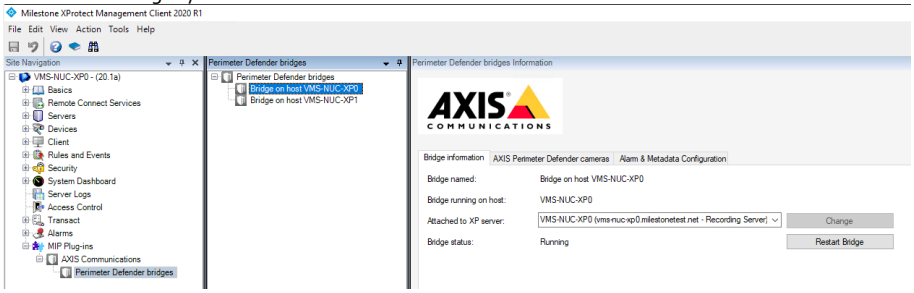
Attach an APD Bridge to a different XP server

If needed, you can change which XP server an APD Bridge is attached to. If you detach an Alarm and APD Bridge from one server to attach it to another, it can have consequences to the bridge configuration:

- If the APD Bridge is detached from a Recording Server to be attached to a Management Server, the configuration is kept, untouched.
- If, on the other hand, the APD Bridge is detached from the Management Server to be attached to a Recording Server, the video devices that are not directly attached to the destination Recording Server will be removed from the configuration.

To change the attached server:

1. Select the bridge you want to attach to a different server.



2. In the **Bridge information** tab, select the new server in **Attached to XP server**.
3. Click **Change**.
4. Review the analysis of the impact the change will have. The analysis checks:
   - The number of video devices that will be removed from the bridge configuration because they are not attached to the new recording server.
   - If there is a MIP Driver device that is compatible with the destination server (that is, directly attached to it if it's a Recording Server, or attached to any Recording Server if the destination server is a Management Server.

5. If you accept the impact, click **Confirm change**.

   Otherwise, select the original server in the list.

Install silently from the command prompt

To install the application from the command prompt, run the file *AXIS_Perimeter_Defender_Bridge_to_Milestone_XProtect.exe*. When you install from the command prompt, you can use parameters to customize the installation.

Installation options:

- silent – without graphical interface
- unattended – no user input requested
- partial – skip certain features

Parameters:

- `/exenoui /qn` – installs silently and unattended
- `skip_mip_plugin_installation=true` – skips the installation of the MIP Plugins
- `skip_bridge_installation=true` – skips the installation of the Alarm & Metadata Bridge.

If you choose to install silently and unattended, and the installation requires a reboot, it is performed without notification. The installation finishes silently at the next user logon.

User manual
AXIS Perimeter Defender with Milestone VMS

Ver. M11.2
Date: February 2023
Part no. T10071930