## **Configuration Instruction**

# Integration of IPS Video Analytics on Cameras with a Milestone XProtect Video Management System

## Contents

1	Ove	erview	2
2	Met	tadata transmission	2
2	۲ <b>۱</b>	Overview of metadata in MAD	2
2	2.2	Overview of live metadata	4
3	Con	mpatibility	5
4	Inst	tallation	6
4	L <b>1</b>	Milestone XProtect	6
4	.2	IPS Analytics Module	6
4	.3	Components for the IPS Milestone Live Overlay	6
	-		-
5	Cor	nfigure the IPS components	9
5	5.1	Configure the IPS Analytics modules	9
5	5.2	Configure the IPS Analytics Streaming Service	9
	5.2.	.1 Required configuration steps	9
	5.2.	.2 Overview of the parameters	10
6	Cor	nfigure the Milestone System	14
6	5.1	Configure the XProtect Management Client	14
	6.1.	.1 Add cameras	14
	6.1.	.2 Configure IPS Video Analytics as metadata source	15
	6.1.	.3 Assign the metadata channels to the cameras	17
	6.1.	.4 Enable Analytics Events	18
	6.1.	.5 Add Analytics Events	19
	6.1.	.6 Add and configure Alarm Definitions	20
	6.1.	.7 Test the Analytics Events	21
	6.1.	.8 IPS overlay settings permission	22
	6.1.	.9 Specify rules for streaming on demand	24
	6.1.	.10 Configure rule for continuous recording of all cameras	27
6	).2 . 2	Configure IPS overlays in the Milestone XProtect Smart Client	
C	0.3	rime synchronization	29
7	Tes	st	29

#### 1 Overview

**IPS Video Analytics on Axis or Hikvision cameras** support MAD (Milestone Alert Data) packets that they send to Milestone XProtect system. These packets contain information on the event (alarm) and metadata (data for overlay of graphical elements and text into video images). If no additional modules are installed, only rectangles around alarm objects can be displayed.

By means of the **IPS Milestone Overlay Plugin** the display can be extended to **IPS Multi-Frame Overlays (+/- 3 sec)**. These overlays contain object rectangles, zones, vectors, traces, and text.

If the IPS Analytics Streaming Service is installed, additionally IPS Live Metadata are supported.

A Milestone XProtect Recording server is able to record these metadata.

#### 2 Metadata transmission

**Important note**: To ensure that the metadata correctly match with the video, time and date on the servers as well as on the cameras must be synchronized with an accuracy of +/- 100 msec.

The appropriate settings can be found at the following locations:

- on Axis cameras under System Options > Date & Time
- on Hikvision cameras under Configuration > System Settings > Time Settings

On the servers Windows manages the time synchronization.

#### 2.1 Overview of metadata in MAD

In case of an alarm, information on the alarm (event) is sent from AnalyticsManager to the Milestone Server.

If more than one alarm is triggered at the same time, for each alarm type a MAD block is sent separately.

If post-alarm images are configured, the MAD block is sent after the post-alarm images are completely stored. This causes an appropriate delay.

Type and contents of the metadata are configured in the camera's video analytics under **Global Parameters** | **VMS type**.

Configuration	Contents	Display
Milestone XProtect, Milestone overlay	Object rectangle (single frame)	Milestone XProtect Smart Client
Milestone XProtect, IPS overlay	Multi-frame overlay (+/- 3 sec): object rectangles, zones, vectors, traces, text	Milestone XProtect Smart Client + IPS Milestone Overlay Plugin
Milestone XProtect, Milestone + IPS overlay 1)		

The option Milestone + IPS overlay should be selected only when Milestone Clients are working partly with and partly without IPS Milestone Overlay Plugin.
 To avoid text info being doubly displayed, in the settings of the Smart Client under IPS overlay options one of the two overlays can be switched off.



#### Display of alarm objects in several images (Multi-frame overlay)



- 1) The IPS Milestone Overlay Plugin is required for displaying binary metadata
- --- Metadata
- · Events



#### 2.2 Overview of live metadata

The metadata type is configured in the IPS Analytics Streaming Service settings under 04. Milestone metadata | Milestone Metadata Type.

Configuration	Contents	Contained in	Required for the display
ONVIFMetadata	Object rectangles, text	IPS Live Metadata Stream	Milestone XProtect Smart Client
BinaryMetadata	Object rectangles, zones, vectors, traces, text	IPS Live Metadata Stream	Milestone XProtect Smart Client + IPS Smart Client Plug-in
ONVIF_And_Binary_Metadata 1)			

 The option ONVIF\_And\_Binary\_Metadata should be selected only when Milestone Clients are working partly with and partly without IPS Milestone Overlay Plugin.
 To avoid text info being doubly displayed, in the settings of the Smart Client under IPS overlay options one of the two overlays can be switched off.

#### Live alarm object display



- 1) The IPS Milestone Overlay Plugin is required for displaying live metadata
- 2) Depending on the configuration: ONVIF metadata, binary metadata or ONVIF and binary metadata
- ----- Video
- ––– Metadata
- · 🔶 Events

## 3 Compatibility

The following table shows the compatibility of IPS Video Analytics with Milestone XProtect systems:

IPS Video Analytics	Milestone XProtect	Supported Overlays	IPS Installation File
V7.0	Professional 2013 R2 Enterprise 2013 R2 Expert 2013 R2 Corporate 2013 R2 Corporate 2014	Multi-frame overlay (+/- 3 sec) 1)	Setup_mssc2013_plugin.exe
V8.0	Corporate 2016 R3 Corporate 2017 R1	Multi-frame overlay (+/- 3 sec)	Setup_mssc2016R2_plugin.exe
V9.0	Corporate 2017 R3 Corporate 2018 R1	Live metadata streaming, 2) Multi-frame overlay (+/- 3 sec)	Setup_mssc2017R3_plugin.exe
V10.0	2019 R1	Live metadata streaming, 2) Multi-frame overlay (+/- 3 sec)	Setup_MilestoneOverlayPlugin.exe
V11.0	2020 R1	Live metadata streaming, 2) Multi-frame overlay (+/- 3 sec)	Setup_MilestoneOverlayPlugin.exe

- 1) Overlay images in the period +/-3 seconds before or after the event.
- 2) If Live Metadata Streaming is disabled (option Use Milestone Metadata Server in the IPS Analytics Streaming Service settings is set to No), then the Multi-frame overlay (+/- 3 sec) can be used. The Multiframe overlay (+/- 3 sec) consists of overlay data, which are contained in the MAD block.

## 4 Installation

Install all required components according to the following sections.

### 4.1 Milestone XProtect

Install the Milestone XProtect system. For details, refer to the Milestone documentation.

#### 4.2 IPS Analytics Module

On the camera, install the **IPS Analytics module**. For the proceeding, refer to the document **Installation Instruction ACAP Analytics** or **Installation Instruction HEOP Analytics**.

#### 4.3 Components for the IPS Milestone Live Overlay

Download the IPS Milestone Overlay Package from the IPS web site.

The installation package is contained in the self-extracting file **Setup\_IPS\_Milestone\_Overlay\_Pack-age\_10.0.exe**. A signature secures this file against changes.

Check the signature **before** extracting the installation files. Perform the following steps:

- 1. Select the context command **Properties**.
- 2. Select the **Digital Signatures** tab.
- 3. Select the **Securiton GmbH** signature in the list.
- 4. Click on Details.
- 5. Check if the text **This digital signature is OK** is displayed.
- 6. Click on View Certificate.
- 7. Check the Issued to information: must be Securiton GmbH
- 8. Check the Issued by information: must be GlobalSign CodeSigning CA
- 9. Check the validity period.
- 10. If one or more of the checks fail, please contact the Securiton support.



Setup_IPS_Milesto	one_Overlay_Package_	10.0.exe Properties	
Security	Details	Previous Versions	
General	Compatibility	Digital Signatures	Digital Signature Details
		_	Constal A Local
Signature list			Advanced
Name of signer	r: Digest algorithm	Timestamp	Digital Signature Information
Securitor Cmb	L aba256	Diapetan 22 Oktober	This digital signature is OK.
Secontorr Cirilo	11 51182.30	Dienslag, 22. Oktobel	
			Signer information
			Name:
			Securiton GmbH
	_	Detaile	E-mail: Not available
		Details	
			Dienstag, 22. Oktober 2019 11:59:31
			View Certificate
			View Cel direate
			Countersignatures
			Name of signer: E-mail address: Timestamp
			GlobalSign TSA f Not available Dienstag, 22. Oktob
			Details
	OK	Cancel Apply	ОК
	ОК	Cancel Apply	СК
Certificate General Details C	ertification Path ate Information e is intended for the	following purpose(s):	
Certificate General Details C General Details C Certificat This certificat • Ensures s • Protects s • Refer to the co	ertification Path ate Information e is intended for the to software came from software software from alteration	following purpose(s): ware publisher after publication	
Certificate General Details C Certificat This certificat • Ensures s • Protects s * Refer to the certificat	OK ertification Path ate Information e is intended for the is software came from soft software from alteration ertification authority's sta	Cancel Apply	
Certificate General Details C Certific This certificat • Ensures s • Protects s * Refer to the co Issued to	OK ertification Path ate Information e is intended for the software came from soft software from alteration ertification authority's sto :: Securiton GmbH	following purpose(s): ware publisher after publication	
Certificate General Details C	OK ertification Path ate Information e is intended for the software came from soft software from alteration ertification authority's sta securiton GmbH g: GlobalSign CodeSignin	Cancel       Apply         Cancel       Apply         Image: Cancel       Apply         following purpose(s):	
Certificate General Details C This certificat • Ensures s • Protects s * Refer to the co Issued to Issued to Valid from	OK ertification Path ate Information e is intended for the to fortware came from soft software from alteration ertification authority's sto securiton GmbH c GlobalSign CodeSignin n 21. 11. 2018 to 2	Cancel       Apply         Cancel       Apply         following purpose(s):	
Certificate General Details C General Details C Finis certificat Ensures s Protects s Refer to the co Issued to Issued to Valid from Learn more about c	OK ertification Path ate Information e is intended for the software came from soft software from alteration ertification authority's sta :: Securiton GmbH r: GlobalSign CodeSignir n 21, 11, 2018 to 2 Install Certi ertificates	Cancel       Apply         Cancel       Apply         following purpose(s):          following purpose(s):          after publication          atement for details.          ng CA - SHA256 - G3          11. 11. 2021          ficate       Issuer Statement	

In order to unpack the installation files double-click Setup\_IPS\_Milestone\_Overlay\_Package\_10.0.exe.

When being asked "Do you want to allow the following program to make changes to this computer?" click **Yes**.

The dialog shown below opens.

Select the **Destination folder** (Browse button).

Click Extract.

IPS



For the functions of the individual components, refer to following table:

Component	Function
IPS Milestone Overlay Plugin	Displays IPS Overlays
IPS Analytics Streaming Server	Generates the Live Metadata Stream
IPS Service Manager	Used for configuration of the IPS Analytics Streaming Service

To install the individual components proceed as follows:

On each server on which a Milestone XProtect **Management Client** or a Milestone **Smart Client** is installed:

- 1. Exit the Milestone XProtect Client.
- 2. Install the IPS Milestone Overlay Plugin by running Setup\_MilestoneOverlayPlugin.exe.

Note: By means of the IPS Milestone Overlay Plugin, you can display the IPS Multi-frame overlay (+/-3 sec) (see also the section Compatibility). If you want to display the Live Overlay, you must additionally perform the following steps.

On each Milestone XProtect Recording server:

- To install the IPS Analytics Streaming Service run Setup\_AnalyticsStreamingServer.msi and follow the steps on the screen. Default directories are: Installation directory: C:\Programme (x86)\Securiton\VideoManager\AnalyticsStreamingServer Data directory: C:\Securiton\VideoManager\AnalyticsStreamingServer\
- 2. To install the IPS Service Manager run Setup\_ServiceManager.msi and follow the steps on the screen.

The default directory is C:\Programme (x86)\Securiton\VideoManager\ServiceManager\.

3. Restart the server.



## 5 Configure the IPS components

#### 5.1 Configure the IPS Analytics modules

Configure the IPS Analytics modules according to the document **Configuration Instruction IPS Analytics Applications**.

In the **Global Parameters** configuration of the IPS Analytics module in the **Connection to video man**agement system section the following parameters must be specified:

- Activate feature set to yes
- IP address (Milestone Management server)
- Port (port of the Milestone Management server, for events and metadata, e.g. 9091)
- Signal alarms
- Signal activity
- VMS type (Milestone XProtect, ...)

#### 5.2 Configure the IPS Analytics Streaming Service

Note: The steps described in this section are only required if you want to display the live overlay.

#### 5.2.1 Required configuration steps

#### To configure the IPS Analytics Streaming Service use the IPS Service Manager.

**Note**: As the **IPS Analytics Streaming Service** is used in different applications, the configuration also contains parameters that are not required for the live metadata streaming to a Milestone system.

At least, adapt the following parameters on each Milestone XProtect Recording Server (further adaptations as required):

- 1. Open the **IPS Service Manager** by double-clicking the **b** icon in the Windows info area (in the lower-right corner of your screen).
- 2. Select the Analytics Streaming Service.
- 3. Click Edit settings....
- 4. Under **01. Analytics Streaming Server settings** | **Remote Address** enter the IP address of the Milestone XProtect Management Server.
- 5. Adapt the **Remote Port**. **Note**: The same port must be specified in the Milestone XProtect system (see section **Activate Analytic Events**).
- 6. Set Enable Trigger On Activity Or Alarm to Yes, set Trigger Remote Alarm to Yes if required, and set Trigger Remote Activity to Yes if required.
- 7. Disable the SVG server by setting **Disable SVG Server** to **Yes**.
- Enable the standalone mode by setting Standalone Mode to Yes.
   In standalone mode live metadata are sent from IPS camera-based Analytics to a Milestone XProtect System.
- 9. Under **05. Camera metadata receiver** | **Camera List** enter data on each camera that belongs to the respective Recording Server. For notes on the parameters and for an example, refer to the end of the list in the next section.
- 10. Click **OK**. The **IPS Analytics Streaming Service** restarts automatically.
- 11. Exit the IPS Service Manager.

#### 5.2.2 Overview of the parameters

The following table contains a brief description on each parameter. Values that deviate from the default are shown in bold.

Parameter	Default	Description
01. Analytics Streaming Server settings		
File Version	10.0.0.0	Version of this XML file
Last Change	XX.XX.XXXX	Date of last change of this file
Management Server IP	127.0.0.1	IP address of the management server
Management Server Port	15008	Port for the communication with the IPS VideoManager Management
User Name	analytics1	User name for log-on to the Management
Password	*****	Password for log-on to the Management
Http User Name	admin	User name for the authentication at the HTTP-Server (for CGI commands or SVG)
Http User Password	*****	Password for the authentication at the HTTP-Server (for CGI commands or SVG)
Streaming Base Port	13000	For each video stream requested from the Device Server 4 port numbers are required. The port numbers start with the value defined in Streaming Base Port. If more than 1 stream is required, the Analytics Streaming Server allocates further ports.
Http Server Port	8088	HTTP Server Port of the Analytics Streaming Service; CGI receiving port
Http Bind Address	127.0.0.1	IP address to which the connection from the Manage- ment is bound; the Analytics Streaming Service acti- vates the receiving port at the specified IP address; if the IP address is 0.0.0.0, the Analytics Streaming Service receives on all network adapters.
Http Streaming Base Port	12000	Base Port used for streams requested from the VMS; SVG; 1 port per camera required.
Base Log File Max Size	10	The Log Base File is written once at the beginning of the logging process and remains unchanged as soon as it has reached the maximum size. Unit = megabytes.
Rolling Log File Max Size	5	If Rolling File 1 and Rolling File 2 are full, Rolling File 1 is deleted and Rolling File 2 is renamed as Rolling File 1. Rolling File 2 then is created anew and written. The latest entries always can be found in Rolling File 2. Unit = megabytes.
Remote Address	172.17.241.49	IP address of the Video Management System (VMS) which receives the TCP notifications
Remote Port	9091	Port number on which the Video Management System (VMS) listens to TCP notifications
Enable Trigger On Activity Or Alarm	No	If set to true TCP notifications are sent to the VMS
Trigger Remote Alarm	No	If set to <b>true</b> an alarm notification is sent to the VMS
Trigger Remote Activity	No	If set to <b>true</b> an activity notification is sent to the VMS
Remote VMS Type	Milestone Analyt- ics Events notifi-	TCP notification MAD notification, Milestone/IPS overlay MAD notification, Milestone overlay



	cation, Mile- stone/IPS overlay	MAD notification, IPS overlay Milestone Analytics Events notification, Milestone/IPS- overlay Milestone Analytics Events notification, Milestone over- lay Milestone Analytics Events notification, IPS overlay
Remote Metadata Frame Period	0	If this parameter is set to 0, each available metadata packet is sent; other values specify the time between 2 metadata packets; used only for connection to a Mile- stone system.
Remote Record Before Event	3	Recording period before an event; used only for connec- tion to a Milestone system.
Remote Record After Event	3	Recording period after an event; used only for connec- tion to a Milestone system.
Metadata Frame Rate	0	Frame rate when using SVG metadata reduction; 0 means "no reduction"
Disable SVG Server	Yes	If you set this parameter to Yes, the SVG server is disabled.
Standalone Mode	Yes	Set this parameter to Yes, in order that the <b>IPS Analyt-</b> ics Streaming Service can send live metadata from <b>IPS</b> camera-based Analytics to a Milestone XProtect sys- tem.
Set System Time	No	If you set this parameter to Yes, the time of the server on which the Analytics Streaming Service is installed, is set when a time command is received from the Manage- ment server. In standalone mode, this parameter has no meaning.
02. Video overlay		
Pre Alarm Objects	Yes	Include pre-alarm objects in the metadata stream.
Objects Without Updates	Yes	Include non-updated objects in the metadata stream.
Object Traces	Yes	Include object traces in the metadata stream.
Detection Zones	Yes	Include detection zones in the metadata stream.
Show Diagnostic Info	Yes	Include diagnostic info (analytics metadata like type of the analytics module, status,) in the metadata stream.
03. Milestone Analytics Event		
Username	admin	User name for Milestone Analytics Event
Password	*****	Password for Milestone Analytics Event
04. Milestone metadata		
Use Milestone Metadata Server	Yes	Set this parameter to Yes, in order to activate live Metadata streaming to a Milestone system. If it is set to No, the Multi-frame overlay (+/- 3 sec) can be used.
Milestone Metadata Server Port	52123	IPS Analytics Streaming Service port for metadata streaming to a Milestone system
Milestone Metadata Server Password	*****	Password used for requesting live metadata streams from the IPS Analytics Streaming Service
Milestone Metadata Type	BinaryMetadata	Type of the metadata sent from the IPS Analytics Streaming Service to the Milestone system: <b>OnvifMetadata</b> : object rectangles and text <b>BinaryMetadata</b> : object rectangles, text, zones, vectors, and traces; <b>IPS Milestone Overlay Plugin</b> required for



		display. Onvif_And_Binary_Metadata: both types
05. Camera metadata receiver		
Netterm User Name	admin	User name for communication with NetTerm (in stand- alone mode)
Netterm Password	*****	Password for communication with NetTerm (in stand- alone mode)
Accept Self Signed Certificate	Yes	If this parameter is set to Yes, the IPS Analytics Stream- ing Service accepts self-signed certificates for encrypted communication with the cameras. If it set to No the cer- tificates must be CA signed.
TIs Protocols	TIs TIs11 TIs12	Select which protocols are to be used for encrypted communication connections.
Camera List	(Collection)	Add all cameras from which the IPS Analytics Streaming Service is to receive metadata. Click the button. Click Add. Adapt the entries for the camera as follows: CameralP: enter the camera's IP address. CameraUID: assign a UID (unique identifier) for the camera. Start with 1900001 for the first camera; con- tinue with 1900002 for the second camera, etc. HttpPort: enter the number of the port on which the camera can be accessed (e.g. 80). HttpsPort: enter the number of the port on which the camera can be accessed via encrypted communication (e.g. 443). MetadataChannel: enter the number of the channel that you will configure in the Milestone system as metadata channel. Important note: the number must not be 0. MetadataOnRequest: set this parameter to False, if the metadata are to be delivered continuously. Set it to True, if the metadata are to be delivered from the camera only on request. Module: select the IPS Analytics Module, which is in- stalled in the camera. Password: password for authentication at the camera. UseHttps: set this parameter to True, if the communica- tion between the camera and the IPS Analytics Stream- ing Service is to be encrypted. Username: user name for authentication at the camera. VAModulePlatform: select the appropriate camera plat- form: Axis_ACAP or Hik_HEOP.

Camera (	Collection Editor	Intelligent	Video Analytics
Members:          ① AnalyticsStreamingServer.Camera         ① AnalyticsStreamingServer.Camera         ① AnalyticsStreamingServer.Camera         【 AnalyticsStreamingServer.Camera	AnalyticsStreamingSen	ver.Camera properties: 172.17.23.13 1900001 80 443 1 False ipsintrusion False root Axis_ACAP	

Example: Entries for a camera

#### Log Files

Log Base File	
Rolling File 1	
Rolling File 2	

The Log Base File is written once at the beginning of the logging process (and remains unchanged as soon as it has reached the maximum size).

If Rolling File 1 and Rolling File 2 are full, Rolling File 1 is deleted and Rolling File 2 is renamed as Rolling File 1. Rolling File 2 then is created anew and written.

The latest entries always can be found in Rolling File 2.

## 6 Configure the Milestone System

#### 6.1 Configure the XProtect Management Client

#### 6.1.1 Add cameras

**Note**: Configure a camera group before you start adding cameras (**Add Device Group...** context command under **Devices** | **Cameras**).

Add the Cameras as described in the following. The proceeding described is an example; Milestone offers different possibilities for this.

Prerequisite: a recording server is already configured.

- 1. Select the recording server.
- 2. Select Add Hardware....
- 3. Select the Manual option for hardware detection.
- 4. Click Next.
- 5. Click the Add button.
- 6. Enter User Name and Password.
- 7. Click Next.
- 8. Select the appropriate **driver** for the new camera.
- 9. Click Next.
- 10. Enter the camera's **IP address**.
- 11. Enter the **port**.
- 12. Under Hardware model leave auto-detect.
- 13. Click Next.
- 14. Activate the Add option.
- 15. Click Next.
- 16. Wait until the search for device-specific information has finished and click Next.
- 17. Click Next.
- 18. Select the **Camera group** to which the new camera is to belong.
- 19. Click Finish.

#### 6.1.2 Configure IPS Video Analytics as metadata source

Note: The steps described in this section are required only if you want to display the live overlay.

In the Milestone XProtect system, a metadata channel number must be assigned to each camera with IPS Video Analytics.

**Note**: In order to assign the metadata source to a metadata group, a metadata group must be created before performing the following steps (context command **Add Device Group** under **Devices** | **Metadata**).

To configure a camera as a metadata source

- 1. Select the recording server (under Servers | Recording Servers).
- 2. Select the **Add Hardware...** context command.
- 3. Select the Manual option for hardware detection.
- 4. Click Next.
- 5. Click the Add button.
- 6. In the User Name field, enter the MAC address of the PC on which the IPS Analytics Streaming Service is installed (= PC on which the XProtect Recording Server runs) without colons or other separating characters and enter the Password. The MAC address (physical PC address) can be found under the Network connection | Properties | Physical address. The password must correspond to the IPS Analytics Streaming Service setting 04. Milestone metadata | Milestone Metadata Server Password.
- 7. Click Next.
- 8. Under Milestone, select the MIP Driver.
- 9. Click Next.

Ado	l Hardware		_ <b>□</b> ×
Select which drivers to use when scanning for hardware. The more drivers selected, the slower the scanning.			
Canon   Hanwha   HikVision   Infinova   IQEye   JVC   LG Electronics   Milestone   Hisky IO module   Milestone Arcus Embedded Interconnect   Milestone XProtect Professional VMS Interconnect   Milestone XProtect VMS Interconnect   Milestone XProtect VMS Interconnect   Wilestone XProtect VMS Interconnect   Wilestone XProtect VMS Interconnect   Milestone XProtect VMS Interconnect   MIP Driver   Screen Recorder   Video Push Driver   Mobotix   ONVIF   Panasonic			Select All Clear All
Help	< Back	Next >	Cancel



10. Enter the **IP address** of the PC on which the **IPS Analytics Streaming Service** is installed, and the **Port** for the metadata (default is **52123**) and under **Hardware model** select the **MIP Driver**.

Note: If you want to use a different port, it must also be adapted in the IPS Analytics Streaming Service settings under 04. Milestone metadata | Milestone Metadata Server Port.

- 11. Click Next.
- 12. Make sure the **Add** option is activated and click **Next**.
- 13. Wait until the search for device-specific information has finished and click Next.
- 14. Click Next.
- 15. Select the **Camera group** to which the new camera is to belong.
- 16. Click Finish.
- 17. Save the changes.

**Important note**: If you want to add new (additional) metadata channels or if you change the metadata port number, you must perform the following steps:

- 1. Delete the current metadata device (MIP Driver).
- 2. Add a new metadata device.
- 3. Assign the new metadata channels to the cameras.

#### 6.1.3 Assign the metadata channels to the cameras

Note: The steps described in this section are required only if you want to display the live overlay.

To assign a metadata channel to a camera proceed as follows:

- 1. Select the recording server.
- 2. Select a video device.
- 3. Open the desired **camera**.
- 4. In the **Properties** section, select the **Client** tab.
- 5. Under **Related metadata**, click the button.

File Edit View Action Tools Help	
🖶 🍤 🕝 🗢 🛱	
Site Navigation 🚽 🕂 🗙	Recording Server 🗸 🕈 Properties 🗸 🖡
TESTFELD-XY - (13.1a)         Basics         Basics         Basics         Basics         Site Information         Site Information         Start Information         Renote Connect Services         Pailover Servers         Pailover Servers         Mobile Servers         Mobile Servers         Microphones         Speakers         Metadata         Motile Servers         Microphones         Speakers         Metadata         Smart Vall         View Groups         Smart Client Profiles         Management Client Profiles         Marix         Rules and Events         Notification Profiles         Analytics Events         Seneric Events	Clert settings Placeording Servers Placeord Placeording Servers Placeor
Roles	rtevnew 🗸 4 X
Basic Users	Live: 640x480 1KB
System Dashboard	
Current Tasks	
Site Navigation Federated Site Hierarchy	AVIS 201521 Nature of Course (1721
the Havigaton Presence cite (including)	AND F1357 Network Camera (1721-

- 6. In the Select devices dialog, open the desired metadata group.
- 7. Select the desired metadata channel.
- 8. Click the Add button.
- 9. Click **OK**.
- 10. Save the changes.

#### 6.1.4 Enable Analytics Events

- 1. In the Milestone XProtect Management Client select the Tools | Options menu item.
- 2. Select the Analytics Events tab.

-	Options								x
	General	Server Logs	Mail Server	AVI Generation	Network	Bookmark	User Settings	Evidence Lock	Access < >

- 3. Under Analytics Events set the Enabled option.
- 4. Enter the **Port** number where the events are accepted.
- 5. Under Security specify Events allowed from:
  - select the All network addresses option (if you are unsure which IP addresses to be used) or
  - Select **Specified network addresses** and **Import** the network addresses.
- 7. Click on **OK**.

Options						x
Evidence Lock	Access Control Settings	Analytics Events	Customer Dashboard	Event server	Generic Events	<>
- Analytics events	3					
Enabled						
Port:						
3031						
Security						
Events allowed	from:					
All network	addresses					
Specified n	etwork addresses:					
Addre	SS					
*						
l Ir	mport					
Help				ОК	Cancel	
					L	



## 6.1.5 Add Analytics Events

IPS AnalyticsManager supports 3 different Analytics Events:

- Activity (IPS-Analytics-Activity)
- Alarm (IPS-Analytics-Alarm)
- Sabotage (IPS-Analytics-Sabotage)

To configure the Milestone System to react to them, proceed as follows:

- 1. In the site navigation select Rules and Events | Analytics Events.
- 2. Select the context command Add New....
- 3. In the Name field enter IPS-Analytics-Activity (be sure to write it exactly in the given spelling).
- 4. Click on Save.
- 5. Create the IPS-Analytics-Alarm and IPS-Analytics-Sabotage analytic events in the same way.

File Edit View Action Tools Help			
🗟 🦻 🕝 🗢 🏥			
Site Navigation 🚽 🕈 🗙	Analytics Events 🚽 🕂	Properties	<b>→</b> ₽
Site Navigation       4         Site Navigation       4         TESTFELD-XY - (13.1a)       Basics         Excense Information       Excense Information         Site Information       Site Information         Statistic Connect Services       Servers         Servers       Servers         Mobile Servers       Cameras         Motile Servers       Cameras         Multice Servers       Seakers         Metadata       Seakers         Metadata       Seakers         Strant Client Profiles       Smart Client Profiles         Smart Wall       Searris         Strant Wall       Seat Exercise         Seat Exercis	Analytics Events Analytics Events IPS-Analytics-Activity IPS-Analytics-Sabotage	Properties           Name:         [IPS-Analytics-Activity           Description:         [IPS-Analytics-Activity	Test Event
Site Navigation Federated Site Hierarchy			
<b>\$</b>			

#### 6.1.6 Add and configure Alarm Definitions

An Analytics Event must be assigned to an Alarm Definition. To add and configure Alarm Definitions proceed as follows:

- 1. Under Alarms select Alarm Definitions.
- 2. Select the context command Add New....
  - Make sure the Alarm Definition is **enabled**.
  - Enter a Name, e.g. IPS Alarm Activity (Alarm when an activity event occurs).
  - Under Triggering event select Analytics Events and select IPS-Analytics-Activity.
  - Select All Cameras as the Source of the trigger.
  - Make further changes as required.
  - Click Save.
- 3. In the same way, create further Alarm Definitions for **IPS-Analytics-Alarm** and **IPS-Analytics-Sabotage**.

File Edit View Action Tools Help		
🗟 🍤 🕝 🗢 曲		
Site Navigation 🚽 🕂 🗙 Alarm Definitions 🚽 👎	Properties	👻 🤻
Mobile Servers 📃 🖃 🛃 Alarm Definitions	Alam definition	
E R Devices	Enable:	
Cameras		
Microphones	Name:	IPS Alarm Activity
Speakers	Instructions:	
Metadata		
Output		✓
	Trigger	
E Smart Wall		
🖓 View Groups	Inggenng event:	Analytics Events
😥 Smart Client Profiles		IPS-Analytics-Activity
Management Client Profiles		
Matrix	Sources:	All Cameras Select
Rules and Events	Activation period	
Time Bacting	Time profile:	Always
Notification Brofiles		
Viser-defined Events	O Event based:	Start: Select
Analytics Events		Stop: Select
Generic Events		
🗏 🐗 Security	Operator action required	
- Roles	Time limit:	1 minute V
Basic Users	Events triggered:	Select
System Dashboard		
Current Lasks	Other	
System Monitor Thresholds	Related cameras:	Select
Revidence Lock	Related map:	
Configuration Reports		
Server Logs	Initial alarm owner:	¥
Access Control	Initial alarm priority:	High 🗸
E Transact	Alarm category:	
Transaction sources	, tam outogoly:	
	Events triggered by alarm:	Select
Alarm Definitions	Auto-close alarm:	
Alarm Data Settings	Alarm assignable to Administrators:	
Sound Settings		
< III >		
Site Navigation Federated Site Hierarchy		



#### 6.1.7 Test the Analytics Events

- 1. In the Site Navigation select **Rules and Events** | **Analytics Events** and select the Analytics Event **IPS-Analytics-Activity**.
- 2. Click Test Event.
- 3. On the recording server select a camera and click OK.
- 4. Check the results in the Test Analytics Event dialog. Click OK.
- 5. Open the Milestone XProtect Smart Client.
- 6. Select the Alarm Manager tab.
- 7. Check if an appropriate event is available in the alarm list.
- 8. Double-click the event in order to check the event details.
- 9. Also, conduct the test for the analytics events **IPS-Analytics-Alarm** and **IPS-Analytics-Sabo-** tage.

File Edit View Action Tools Help			
🖥 🦻 🕝 🗢 🏥			
Site Navigation 🚽 🕈 🗙	🕻 Analytics Events 🔍 🖵 👎	Properties	
Site Navigation     9       Site Navigation     9       Basics     License Information       Estile Information     Site Information       Site Navigation     Site Information       Site Site Information     Site Navigation       Site Navigation     Site Information       Site Information     Site Information       Site Site Information     Site Navigation       Site Site Information     Site Navigation       Site Navigation     Site Navigation	Analytics Events  Analytics Events  Analytics Events  PS-Analytics-Alarm  IPS-Analytics-Sabotage	Properties           Name:         [PS-Analytics-Activity           Description:         [PS-Analytics-Activity	Test Event
Site Navigation Federated Site Hierarchy			

#### 6.1.8 IPS overlay settings permission

The IPS Video Analytics overlay consists of several components like alarm objects, detection zones, traces, vectors, or text. Each component can individually be switched on or off.

In order to specify which user is allowed to change the appropriate settings, follow the steps below.

#### 1. Create a new user

If not yet available, create a new user who shall have the permission to specify the overlay components. For instance, this can be a basic user.

- 1. For example, under **Security | Basic Users** select the **Create Basic User...** context command.
- 2. Enter a **User name**.
- 3. Enter the **Password** and confirm it.
- 4. Click OK.

#### 2. Add a role

- 1. Under Security | Roles select the Add role... context command.
- 2. Enter a Name for the role, e.g. UserManagers.
- 3. Click OK.

#### 3. Configure the role

**Note**: The settings described in the following can only be made, if the IPS Milestone Overlay Plugin is already installed.

To enable the permission to specify the overlay components, proceed as follows:

- 1. In the Site Navigation select Security | Roles.
- 2. Select the Role, e.g. UserManagers role.
- 3. Select the **MIP** tab.

👔 Info 🙀 Users and Groups 👔 Overall Security 💱 Device 🚭 PTZ 🍕 Speech	🙀 Remote Recordings 🔠 Smart Wall   🎈 External Events 🕼 View Group 🕕 Servers 🖾 Matrix 🌘 Alarms 🕼 Access Control 🔚 LPR 뵭 MIP
	Re Access Control 🔄 LPR

#### 4. Select IPS Overlay.

- 5. Adapt the **Security settings** for the IPS Overlay as desired:
  - Use IPS overlays: permission to enable IPS overlays and to select its components.
  - **Unveil privacy**: Permission to unveil privacy. **Note**: This setting is of no relevance for camera-based Analytics.

IPS tics

Intelligent Video Analytics

File Edit View Action Tools Help				
🗟 🦻 🕝 🗢 🏛				
Site Navigation 🚽 🕂 🗙	Roles 👻 🕂	Role Settings 🗸 🗸 🕂		
E D TESTFELD-XY - (13.1a)	Name	MIP configurations		
E Basics	👫 Administrators (Administrators have co			
E License Information	Notes the second			
Site Information	🔥 UserManagers			
Remote Connect Services				
Axis One-click Camera Con				
Servers				
Hecording Servers				
Failover Servers				
Mobile Servers				
Devices				
Microphonen				
Speakers				
Metadata				
Output				
E E Client				
Smart Wall				
📔 View Groups				
🚽 💀 Smart Client Profiles				
Management Client Profiles				
Matrix				
Rules and Events				
Rules				
- e Time Profiles				
Notification Profiles				
Vser-defined Events		Security settings for: IPS Overlay		
Analytics Events				
Generic Events				
Boles				
Basic Lleare				
System Dashboard				
Current Tasks				
	1			
Site Navigation Federated Site Hierarchy		🔄 View Group 🔲 Servers 📮 Matrix 🤵 Alarms 🎼 Access Control 🔚 LPF 🌸 MIP		
*				

## 4. Assign the role

- 1. Select the Users and groups tab.
- 2. Click the Add... button.
- 3. Select **Basic user**.
- 4. Activate the **Select** option for the appropriate **user**.
- 5. Click OK.

#### 6.1.9 Specify rules for streaming on demand

If you want to achieve that video images and the assigned metadata are transmitted or recorded only on demand, you must specify appropriate rules.

As examples, the following use cases are described:

- 1. Display and record video images
- 2. Display and record video images automatically in case of alarm

The respective rules are specified under **Rules and Events** | **Rules**. Select the **Add Rule** context command to open the **Manage Rule** wizard.

#### 6.1.9.1 Display video image and record it at the same time

## Note: For the camera, in the IPS Analytics Streaming Service under 05. Camera metadata receiver the parameter MetadataOnRequest must be set to True.

In order to request the video image only for the case it is displayed on at least one Milestone XProtect Smart Client, configure a rule as follows:

#### Step 1: Type of rule

- 1. Leave the rule type on Perform an action on <event>.
- 2. Edit the rule description:
  - Click the **event** link.
  - Under Events | Devices | Predefined Events select the Live Client Feed Requested events and click OK.
  - Click the link devices/recording server/management server.
  - Select the desired camera and click Add.
  - Click OK.
- 3. Click Next.

#### Step 2: Conditions

Click Next.

#### **Step 3: Actions**

- 1. Select the options Start recording on <devices> and Start feed on <devices>.
- 2. Click the link the device on which event occurred.
- 3. Activate the Select devices option and click OK.
- 4. Select the **camera** and click **Add**.
- 5. Select the **metadata channel** and click **Add**.
- 6. Click OK.
- 7. Click Next.

#### Step 4: Stop criteria

- 1. Leave the stop criterion on Perform stop action on <event> and leave the event Live Client Feed Terminated.
- 2. Click Next.

#### Step 5: Stop actions

- 1. Leave the stop action on stop recording immediately and stop feed immediately.
- 2. Click Finish.

Rule Information 👻 🕂
Name:
Display video image from camera 1
Description:
Display video image and record it at the same time
✓ Active
Definition:
Perform an action on Live Client Feed Requested
from AXIS P135/ Network Camera (1/2,1/,23,13) - Camera 1 the modified impediately and AVIS P1257 Network Camera (172,17,22,12) Camera 1 MIR Driver (172,17,241,46). Metadeta 1
and start feed on the device on which event occurred
Perform stop action on Live Client Feed Terminated
from AXIS P1357 Network Camera (172.17.23.13) - Camera 1
stop recording immediately
and stop reed initiaciately

#### 6.1.9.2 Display and record video image automatically in case of alarm

## Note: For the camera, in the IPS Analytics Streaming Service under 05. Camera metadata receiver the parameter MetadataOnRequest must be set to True.

In order to request the video image only for the case it is displayed on at least one Milestone XProtect Smart Client, configure a rule as follows:

#### Step 1: Type of rule

- 1. Leave the rule type on Perform an action on <event>.
- 2. Edit the rule description:
  - Click the event link.
  - Under Events | Analytics Events | Analytics Events select the IPS-Analytics-Alarm (Analytics Events) and click OK.
  - Click the link devices/recording server/management server.
  - Select the desired camera and click Add.
  - Click OK.
- 3. Click Next.

#### Step 2: Conditions

Click Next.

#### Step 3: Actions

- 1. Select the options Start recording on <devices> and Start feed on <devices>.
- 2. Click the recording device link.
- 3. In the Select devices and groups dialog activate the Select devices option and click OK.
- 4. Select the **camera** and click **Add**.
- 5. Select the metadata channel and click Add.
- 6. Click the second recording device link.
- 7. In the Select triggering devices dialog select the Select devices option and click OK.
- 8. Select the camera and click Add.
- 9. Select the **metadata channel** and click **Add**.
- 10. Click **OK**.
- 11. Click Next.

#### Step 4: Stop criteria

- 1. Under Select stop criteria, select Perform stop action on <event>.
- 2. Click the time link.
- 3. In the **Relative Time** dialog enter the time after which display and recording shall be stopped and click **OK**.
- 4. Click Next.

#### Step 5: Stop actions

- 1. Leave the stop action on stop recording immediately and stop feed immediately.
- 2. Click Finish.

F	Rule Information		
	Name		
	Name.		_
	Display and record video image from camera 1 in case of alarm		
	Description:		
	Display and record video image from camera 1 in case of alarm for a specified time period		
			-
	Definition:		
	Perform an action on IPS-Analytics-Alarm (Analytics Events)		_
	from AXIS P1357 Network Camera (172.17.23.13) - Camera 1		
	start recording immediately on AXIS P1357 Network Camera (172.17.23.13) - Camera 1, MIP Driver (172.17.241.46) - Metadata	1	
	and start feed on AXIS P1357 Network Camera (172.17.23.13) - Camera 1, MIP Driver (172.17.241.46) - Metadata 1		
	renorm accurate and the second		
	stop recording <b>miniculatery</b>		



#### 6.1.10 Configure rule for continuous recording of all cameras

#### Step 1: Type of rule

- 1. Select the rule type on Perform an action in a time interval.
- 2. Click Next.

#### **Step 2: Conditions**

Under Select conditions to apply select the Always option and click Next.

#### Step 3: Actions

- 1. Select the option Start recording on <devices>.
- 2. Click the recording device link.
- 3. In the Select devices and groups dialog activate the Select devices option and click OK.
- 4. Select All cameras and click Add.
- 5. Click OK.
- 6. Click Next.

#### Step 4: Stop criteria

- 1. Under Select stop criteria, select Perform stop action when time interval ends.
- 2. Click Next.

#### Step 5: Stop actions

Click Finish.

Rule Information	👻 👎
Name:	
Continuous recording of all cameras	
Description:	
Active	
Definition:	
Perform an action in a time interval	
start recording immediately on All cameras	
Perform an action when time interval ends	
stop recording immediately	



## 6.2 Configure IPS overlays in the Milestone XProtect Smart Client

To adapt the IPS Overlay Options in the Milestone XProtect Smart Client proceed as follows:

- 1. Launch the Milestone XProtect Smart Client.
- 2. Click and select Settings.

15/10/2019 14:15:41 📃		×	
+ 6	9	~	
Setun		≎	Settings
Setup		-	Toggle theme
		₽	Toggle simplified or advanced mode

- 3. Select IPSOverlay Options.
- 4. Enable or disable the display of the overlays and configure which objects you want to see.

<b>\$</b>	Settings	_		x
Application	✓ Enable overlays			
	✓ Show Detection Zones			
Panes	✓ Show PreAlarm Objects			
Functions	✓ Show Sleeping Objects			
Timeline	Show Object Traces			
Export	🗹 Draw Text Inserts 9 🔶 [Font size]			
	Show Hidden Overlays			
Smart map	Unveil Privacy			
Joystick				
Keyboard				
Access Control				
Alarm				
IPSOverlay Options				
Advanced				
Language				
Help			Clo	se

#### 6.3 Time synchronization

To ensure that the metadata correctly match with the video, time and date on the servers as well as on the cameras must be synchronized with an accuracy of +/- 100 msec.

The appropriate settings can be found at the following locations:

- on Axis cameras under System Options > Date & Time
- on Hikvision cameras under **Configuration** > **System Settings** > **Time Settings**

On the servers Windows manages the time synchronization.

#### 7 Test

Besides the installation and configuration described above the following prerequisites must be fulfilled for testing the live metadata overlays:

- 1. In the camera the appropriate IPS Analytics module must be installed, licensed, and launched (see the instructions Installation-Instruction\_ACAP-Analytics\_Vx.x\_R0x\_en or Installation-Instruction\_HEOP-Analytics\_Vx.x\_R0x\_en).
- 2. The Analytics module must be configured (see Configuration-Instruction\_CB-Analytics\_Vx.x\_R0x\_en).
- 3. In the Milestone XProtect system, the cameras and metadata channels must be configured.

In order to test the live metadata, switch a camera image to a Smart Client view.

Check if every type of overlay you selected (like detection zones, pre-alarm objects, traces, ...), is displayed.

Copyright © 2020 Securiton GmbH. IPS and the IPS logo are registered trademarks of Securiton GmbH.

Securiton GmbH has included the information contained in this manual to the best of its knowledge. Content of this documentation exclusively serves information purposes and may be changed without prior notice. Securiton GmbH accepts no responsibility for damage or accidents, which occur as a consequence of information, which has been given regarding devices or components not manufactured by itself. Securiton GmbH accepts no responsibility for changes or modifications, which have not been explicitly authorised by Securiton GmbH.