MAKE THE
WORLD SEE

Milestone Systems

ONVIF drivers

Version 1.23 / June 2024

milestone

Contents

Copyright, trademarks, and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file `3rd_party_software_terms_and_conditions.txt` located in your Milestone system installation folder.

Introduction and scope

About this document

This information in this document is in accordance with the latest released version of the ONVIF driver.

You can download the latest Device Pack release from here:

https://www.milestonesys.com/support/software/device-packs/

What is ONVIF?

ONVIF® is a leading and well-recognized industry forum whose mission is to provide and promote standardized interfaces for effective interoperability of IP-based physical security products.
[1]

When products that conform to the same ONVIF profile are used together, systems designers and end users know that they can easily design and use a system where products will seamlessly communicate and integrate.

For detailed information about ONVIF, the organization and their full scope, check: https://www.onvif.org/

Milestone ONVIF drivers

Milestone is currently conformant with ONVIF profiles S, T, G and M (see also ONVIF conformance on page 8) and has created standard drivers to facilitate the integration of compliant devices into XProtect. Conformance for Profile Q is no longer maintained as it is deprecated from 2022 onwards. Some functionality related to Profile Q might still be available in XProtect.

This Driver Overview document defines the settings, features, events, and profiles that ONVIF and ONVIF16 channel driver support. There are in details which settings are dynamic, how drivers handle the events, what is necessary to be set up in order some functionalities to work.

Milestone constantly updates and adds new functionality to our ONVIF drivers, making sure that they are compliant with the most recent official ONVIF specifications.

A device fully compliant to ONVIF profiles S, T, G or M will likely work with Milestone XProtect, and be able to send and receive video, audio, metadata and configuration data – however it will not necessarily be directly supported by Milestone Technical Support.

In case of any issues, please note Milestone Technical Support services cover only the devices our driver teams have worked to test directly. For more information, please check the Supported Device list.

[1] **® ONVIF is a trademark of Onvif, Inc.**

ONVIF conformance

ONVIF conformance

Milestone Systems XProtect product line is conformant with the following ONVIF specification profiles:

- Supported profiles: S, T, G, M
- ONVIF Client Test Tool Version: 22.06 rev.4624
- Test date: 2022-08-03

Note: Not all XProtect products support all ONVIF Profiles. Refer to the table:

	Essential+	Express+	Professional+	Expert	Corporate
Profile S	✓	✓	✓	✓	✓
Profile T			✓	✓	✓
Profile G			✓	✓	✓
Profile M			✓	✓	✓

ONVIF supported features

Profile S & T

- Video streaming (JPEG, MPEG4, H.264, H.265)
  - RTSP/TCP
  - RTSP/UDP unicast
  - RTSP/UDP multicast
  - RTSP over HTTP
  - RTSP over HTTPS
  - JPEG snapshot
- Audio streaming (G.711, G.726, AAC)
- Audio backchannel (G.711, G.726, AAC)

- Metadata Streaming
- Image properties (Brightness, Saturation, Sharpness, White Balance)
- Relay outputs
- Digital inputs
- Events (PullPoint subscription)
- PTZ
- Auxiliary commands
- OSD (Date and Time)
- Digest authentication
- WSSE authentication

Profile G

- Recording search
- Recording replay/retrieve

Profile M

- Enable/Disable Analytics
- Configure Metadata streaming
- Receive Metadata

Profile Q

- Network configuration (IP, mask, gateway)
- User management (List users, create user, delete user)
- Password management (Change password)
- Transition from Factory Default state to Operational state

Not Profile specific

- Firmware update

ONVIF16 driver

ONVIF16 driver

Important: As of Device Pack 13.3a, the ONVIF16 driver has been moved to Legacy Device Pack 3.0.

The ONVIF16 driver is obsolete and is limited to 16 video/audio channels. The driver has the same settings and specifications as the generic ONVIF driver. The following sections describe the generic ONVIF driver. If there are other differences between the two drivers, except for the number of channels, they will be explicitly stated. The ONVIF Driver supports devices with up to 512 video/audio channels.

Definitions

Definitions

Definitions

Transparent PTZ - Functionality that allows a client to send a PTZ protocol command (e.g. Pelco D) to a receiver (camera, encoder) which sends it transparently to a PTZ device through serial connection. The receiver of the Transparent PTZ command does not need to understand the data it receives, it only needs to transfer the payload through the serial connection to the final receiver.

Edge Storage - Functionality that allows a client to retrieve a recording locally stored on the device. This remote recording either with higher quality than the streamed received during Live Streaming or missing data in periods of no connection to the device. For more information see Milestone Edge Storage White Paper.

Standard references

Standard References

The ONVIF driver relies on functionality from the following specifications:

Name	Version	Link
ONVIF Core	19.12	https://www.onvif.org/specs/core/ONVIF-Core-Specification.pdf
ONVIF Streaming	19.12	https://www.onvif.org/specs/stream/ONVIF-Streaming-Spec.pdf
Device IO	19.06	https://www.onvif.org/specs/srv/io/ONVIF-DeviceIo-Service-Spec.pdf
Imaging	19.06	https://www.onvif.org/specs/srv/img/ONVIF-Imaging-Service-Spec.pdf
Media	19.12	https://www.onvif.org/specs/srv/media/ONVIF-Media-Service-Spec.pdf
Media 2	19.12	https://www.onvif.org/specs/srv/media/ONVIF-Media2-Service-Spec.pdf
PTZ	18.12	https://www.onvif.org/specs/srv/ptz/ONVIF-PTZ-Service-Spec.pdf
Recording Search	18.12	https://www.onvif.org/specs/srv/rsrch/ONVIF-RecordingSearch-Service-Spec.pdf
Replay Control	17.06	https://www.onvif.org/specs/srv/replay/ONVIF-ReplayControl-Service-Spec.pdf

References to these specifications further in this document should be considered with the version specified here.

The ONVIF driver uses these services:

Name	Version	WSDL
Device	19.12	https://www.onvif.org/ver10/device/wsdl/devicemgmt.wsdl

Name	Version	WSDL
Media	19.06	https://www.onvif.org/ver10/media/wsdl/media.wsdl
Media 2	19.06	https://www.onvif.org/ver20/media/wsdl/media.wsdl
Imaging	19.06	https://www.onvif.org/ver20/imaging/wsdl/imaging.wsdl
Event	19.06	https://www.onvif.org/ver10/events/wsdl/event.wsdl
Device IO	19.12	https://www.onvif.org/ver10/deviceio.wsdl
PTZ	17.06	https://www.onvif.org/ver20/ptz/wsdl/ptz.wsdl
Recording Search	2.4.2	https://www.onvif.org/ver10/search.wsdl
Replay Control	18.06	https://www.onvif.org/ver10/replay.wsdl

References to these services further in this document should be considered with the version specified here.

Driver settings

Hardware information

The hardware information is placed under the device tab containing basic information for the device. For one device there is only one hardware information as follows:

Setting name	Description	Value taken from device
Name	Manufacturer name, model name and device IP	✓
Description	--	×
Model	Manufacturer name and model name	✓
Version	Firmware version	✓
Serial number	Device serial number	✓
Driver	Loaded device driver: • ONVIF Conformant Device • ONVIF Conformant Devices (2-16 channels))	×
Address	IP address	✓
MAC address	Device MAC address	✓

Most of the hardware settings are dynamic and depend on device information.

If there is a new firmware uploaded on the device, a procedure of “Replace hardware” or “Remove then add the device in Management Client” is necessary in order to be up to date and working as expected.

Removing a device in Management Client will delete all its saved recordings.

General device settings

The global settings for the device are settings that should be set once for all channels and streams. They are placed under the device item in “Settings” tab. When global settings change, major functionalities change as well. The following table contains the device’s general settings:

Setting name	Possible values	Value taken from device	Default value
Model name	Manufacturer name and model name	✓	--
HTTPS enabled	No Yes	×	No
HTTPS port	[1,65535]	✓	443
HTTPS Validate Certificate	No Yes	×	No
HTTPS Validate Hostname	No Yes	×	No
Media Service	Media 1 Media 2	✓	Media 2 service - if device supports it, else Media 1 service. See Media service on page 25

Media Service should be changed only if there are known compatibility issues with the device with the default Media Service

Changing the Media Service requires a Recording Server restart afterwards.

When changing Media Service from Media 2 to Media 1, make sure to not have a codec set to H.265. Media 1 does not support H.265 and when using it some devices incorrectly report the current codec.

HTTPS

General

To enable HTTPS the “Https enable” setting must be set to “Yes”. When HTTPS is enabled all functionalities that the ONVIF driver supports will work on HTTPS:

- Video*
- Audio IN*
- Metadata*

- PTZ
- Video Edge Storage*
- Audio Edge Storage*
- Metadata Edge Storage*
- Pull Point Events
- Aux commands
- Digital Inputs
- Relay Outputs

The HTTPS port will be read from the device when possible. If the device does not respond to GetNetworkProtocols or does not return a HTTPS port, the default value of 443 will be used. When changing the HTTPS port in the Management Client the driver will try to also set the port on the device. Some devices deny changing the port through the SetNetworkProtocols command. In this case no error is displayed, and the only signs of that failure are that the HTTPS stops working and failure of the SetNetworkProtocols command in Wireshark. In these situations, the user must ensure that the port set in the Management Client and the one used by the device are equal. This is done usually by changing the HTTPS port on the device's web page.

HTTPS must be enabled on the device as well (usually through the device's Web Page).

If the option "HTTPS Validate Certificate" is enabled the ONVIF driver will check the validity of the certificate of the device when HTTPS connection is being established. If the certificate cannot be verified (is expired or the certificate chain does not lead a trusted root) the connection will be dropped, and no communication will be done with the device. For information on how to work with certificates see HTTPS Certificates on page 17.

If the option "HTTPS Validate Hostname" is enabled the ONVIF driver will check if the hostname it's connecting to matches the ones the certificate is issued to.

For Video, Audio IN, Metadata, Video Edge Storage, Audio Edge Storage and Metadata Edge Storage to be over HTTPS their streaming method must be changed to RTP/RTSP/HTTP/TCP.

Audio OUT does not support HTTPS. The ONVIF specification and the document from Apple for RTSP over HTTP does not specify how the Audio Backchannel should be sent and as such there is no standard way of sending audio backchannel data to the device over HTTP or HTTPS.

ONVIF commands over HTTPS

When HTTPS is enabled all ONVIF SOAP requests will be transferred over HTTPS. These include all commands for setting and retrieving settings, PTZ, Pull Point Events, Aux commands, Digital Inputs and Relay Outputs.

Media over HTTPS

The ONVIF driver uses RTSP over HTTP in order to receive securely media data from the device. For RTSP over HTTPS to work, the "Https enable" setting must be set to "Yes" and the streaming method must be set to either

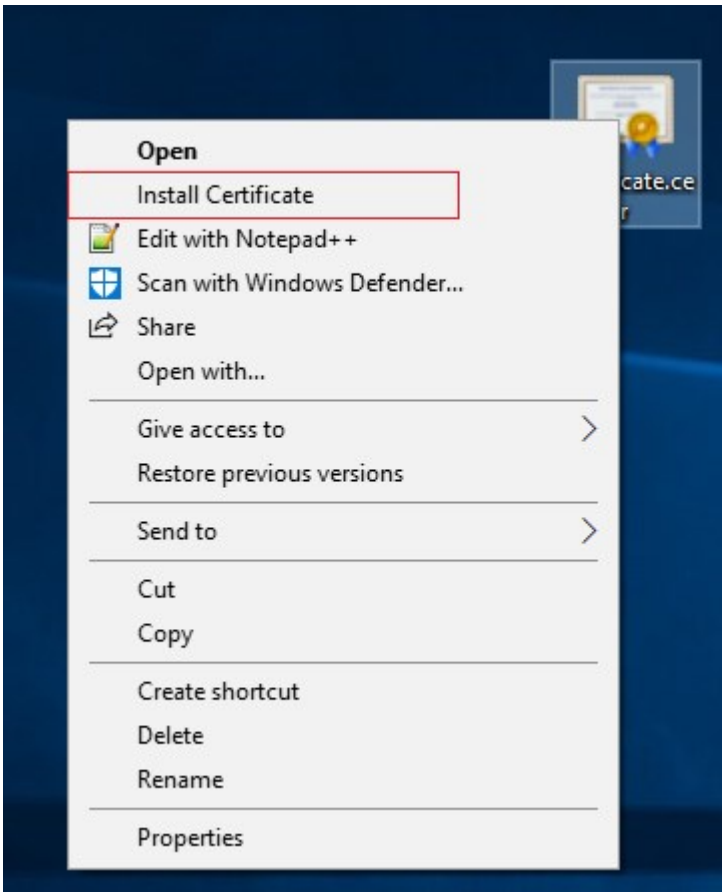
RTP/RTSP/HTTP/TCP or HTTP snapshot. If streaming mode is set to a value other than RTP/RTSP/HTTP/TCP or HTTP snapshot, streaming will work but without encryption. All ONVIF requests to the device will be on HTTPS, but the video, audio or metadata will be on RTSP.

HTTPS Certificates

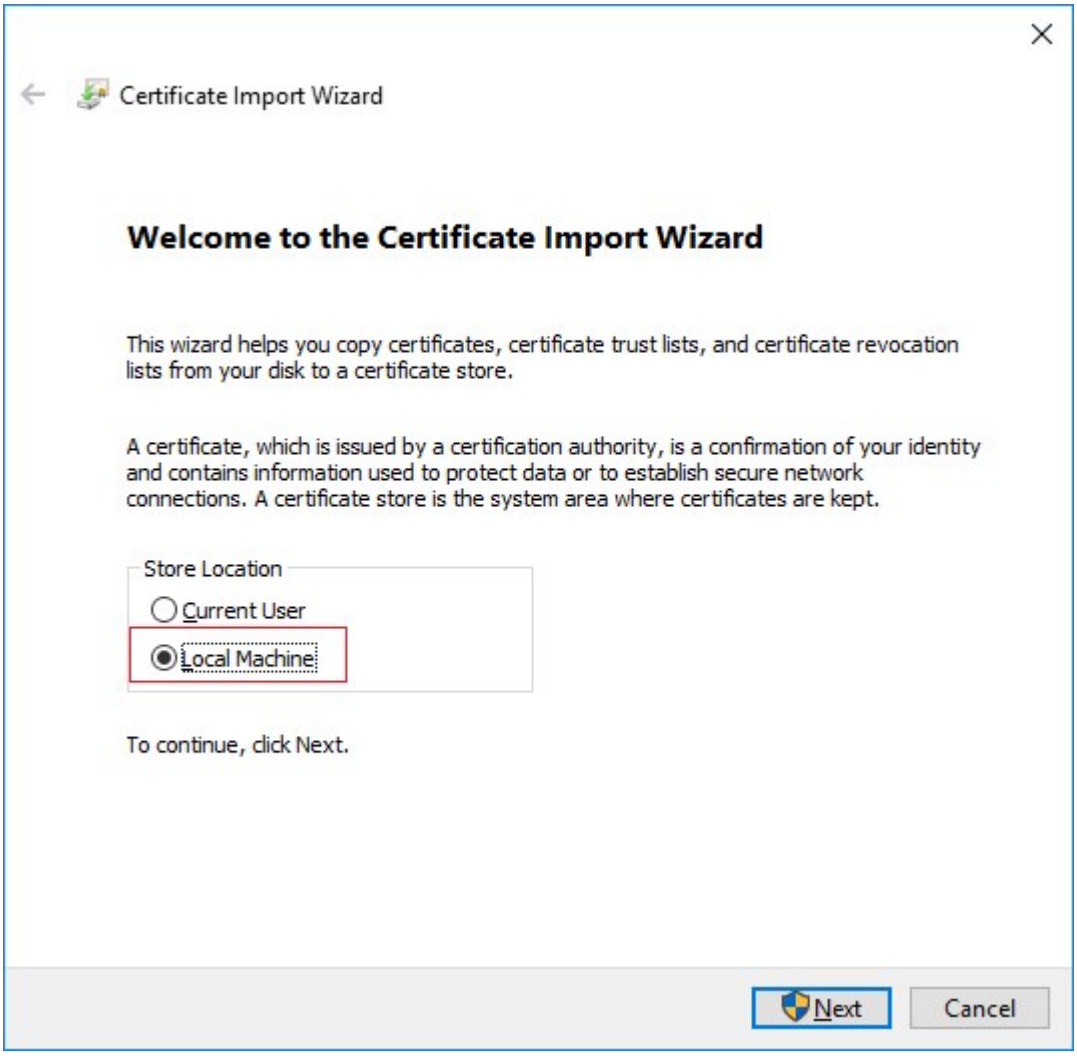
The ONVIF driver supports self-signed and authority-signed certificates. If an authority-signed certificate is used on the device and this certificate is not signed by a root CA, the device's certificate root must be installed on the recording server for the ONVIF driver to be able to validate the certificate chain.

Here is how to install a certificate in the Windows Certificate Store

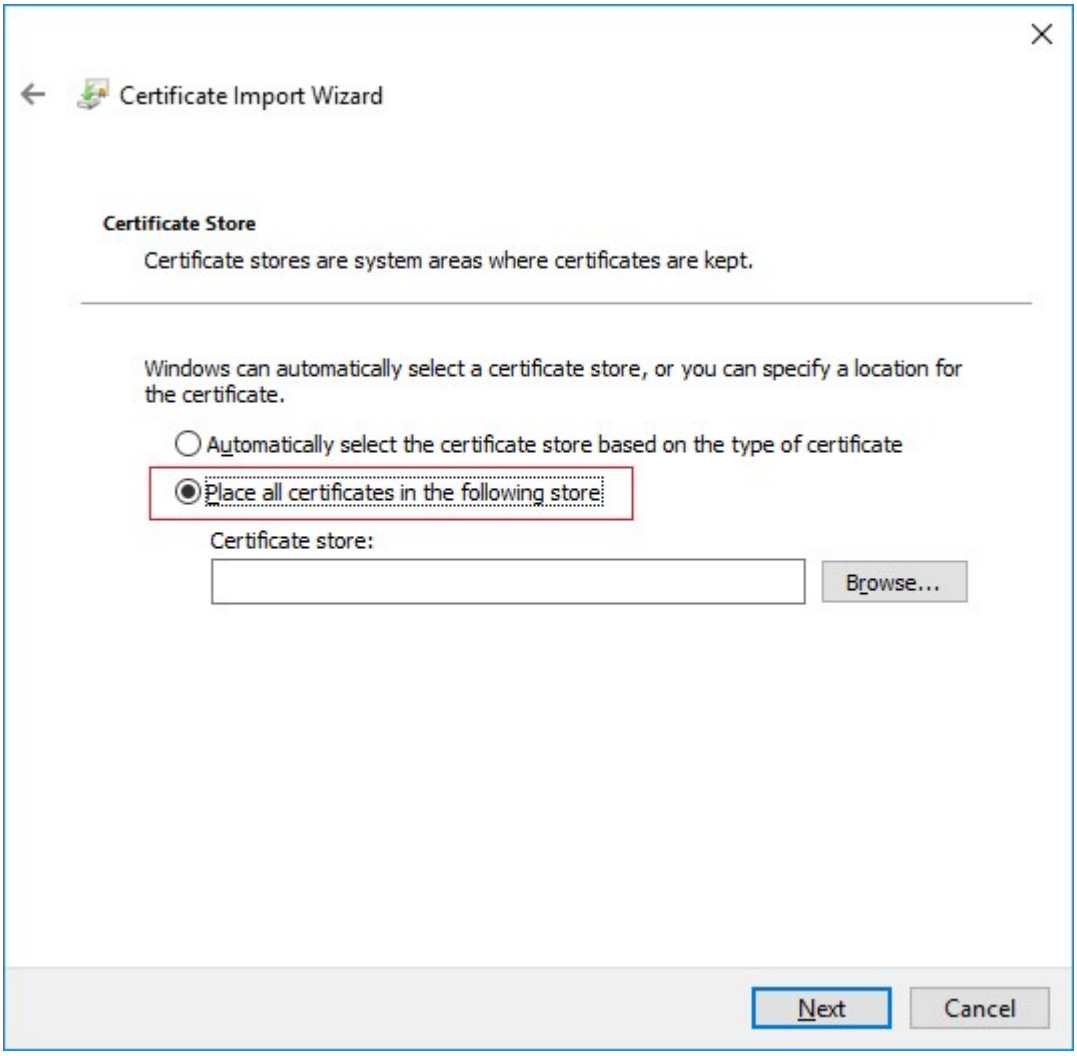
Copy the certificate to the Recording Server machine. Right Click on the Certificate and choose "Install Certificate"



On the "Certificate Import Wizard" choose to install the certificate in the store of the "Local Machine". Installation in this store is needed as the Recording Server runs under the user "NETWORK SERVICE" and can only access its user's Certificate Store or the store of the Local Machine.

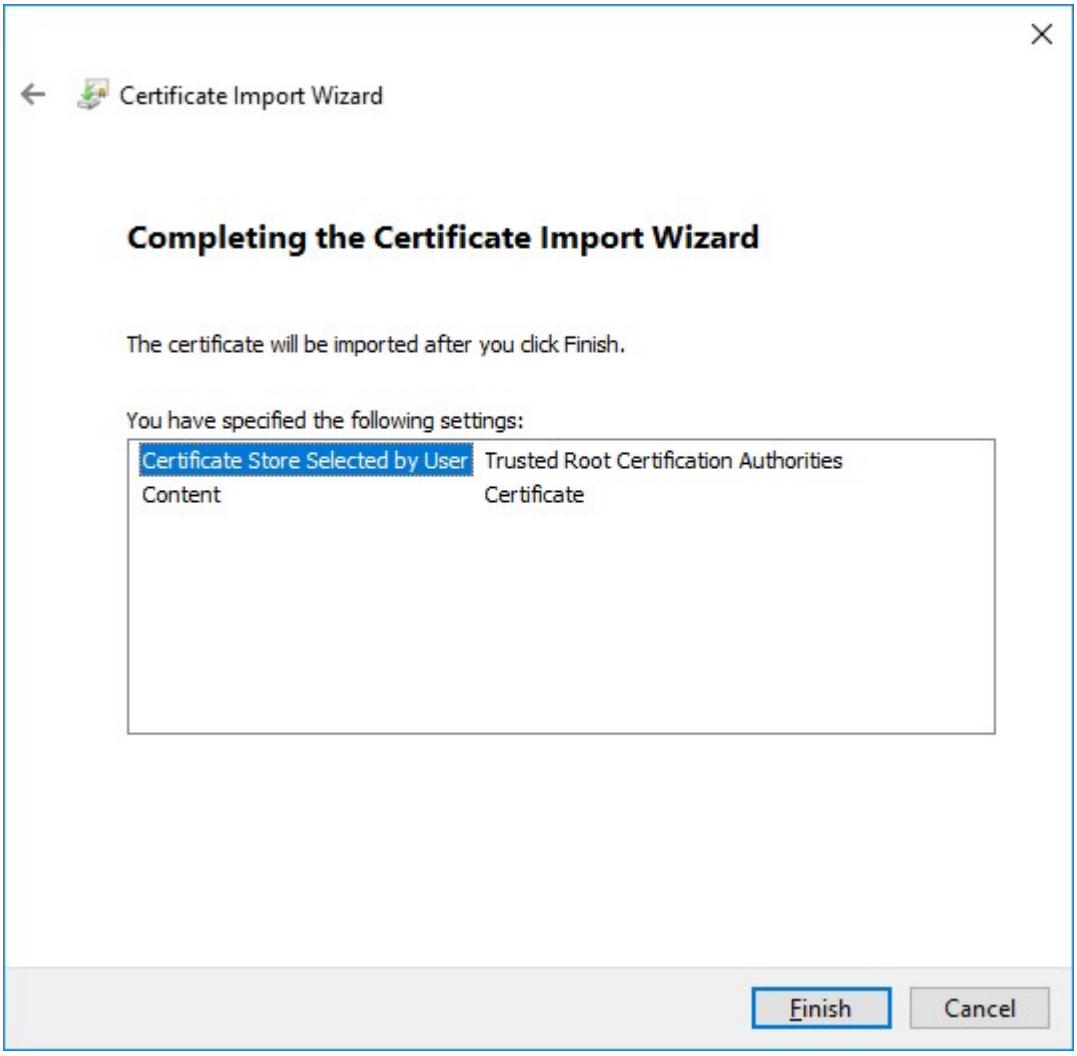


Choose to manually select the store in which the certificate will be installed.

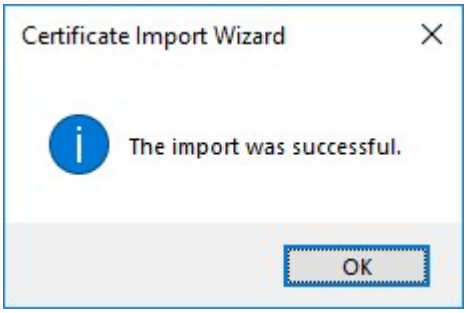


Click “Browse” button and select the “Trusted Root Certification Authorities”

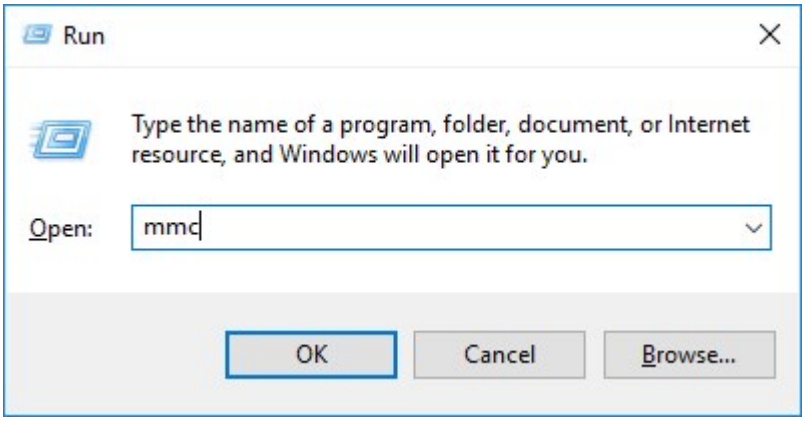
Click Finish on the “Completing the Certificate Wizard” dialog.



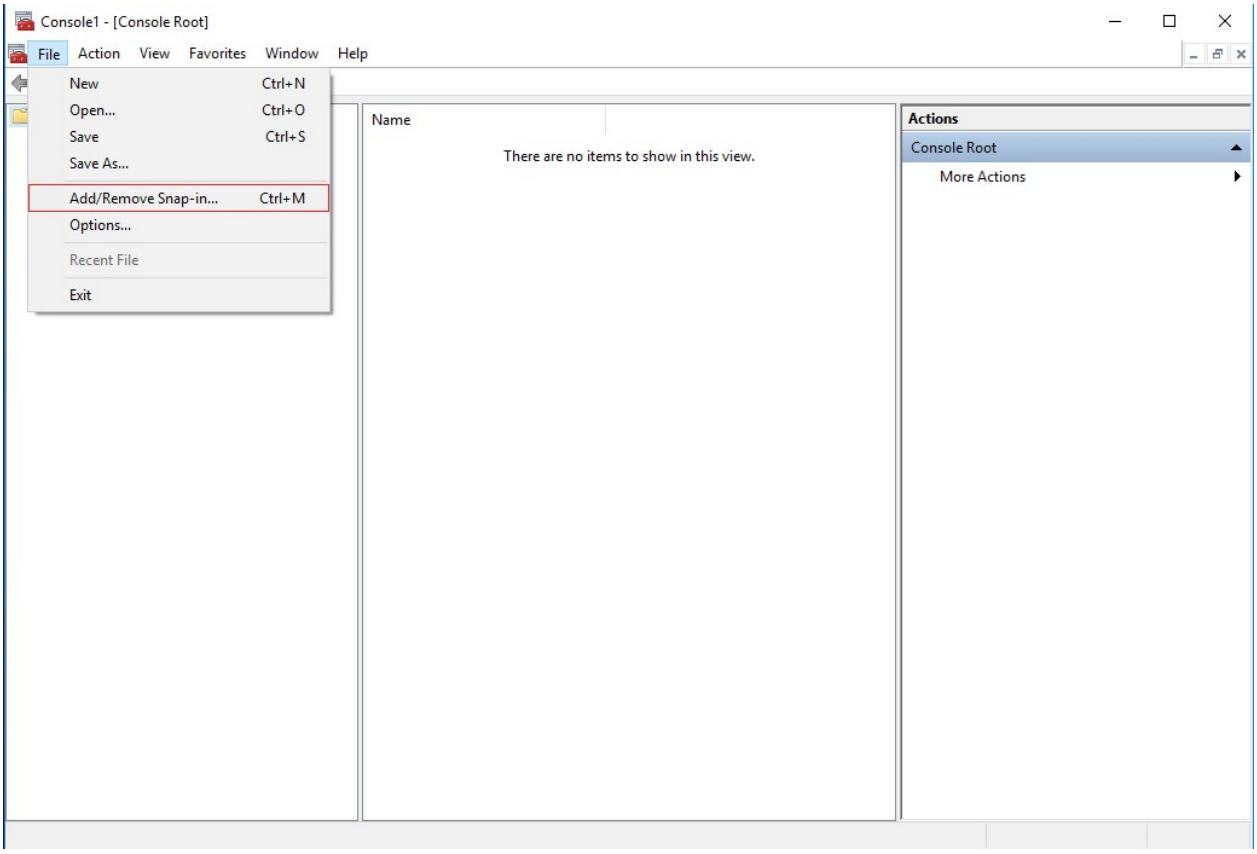
You will receive a confirmation dialog of successful import.



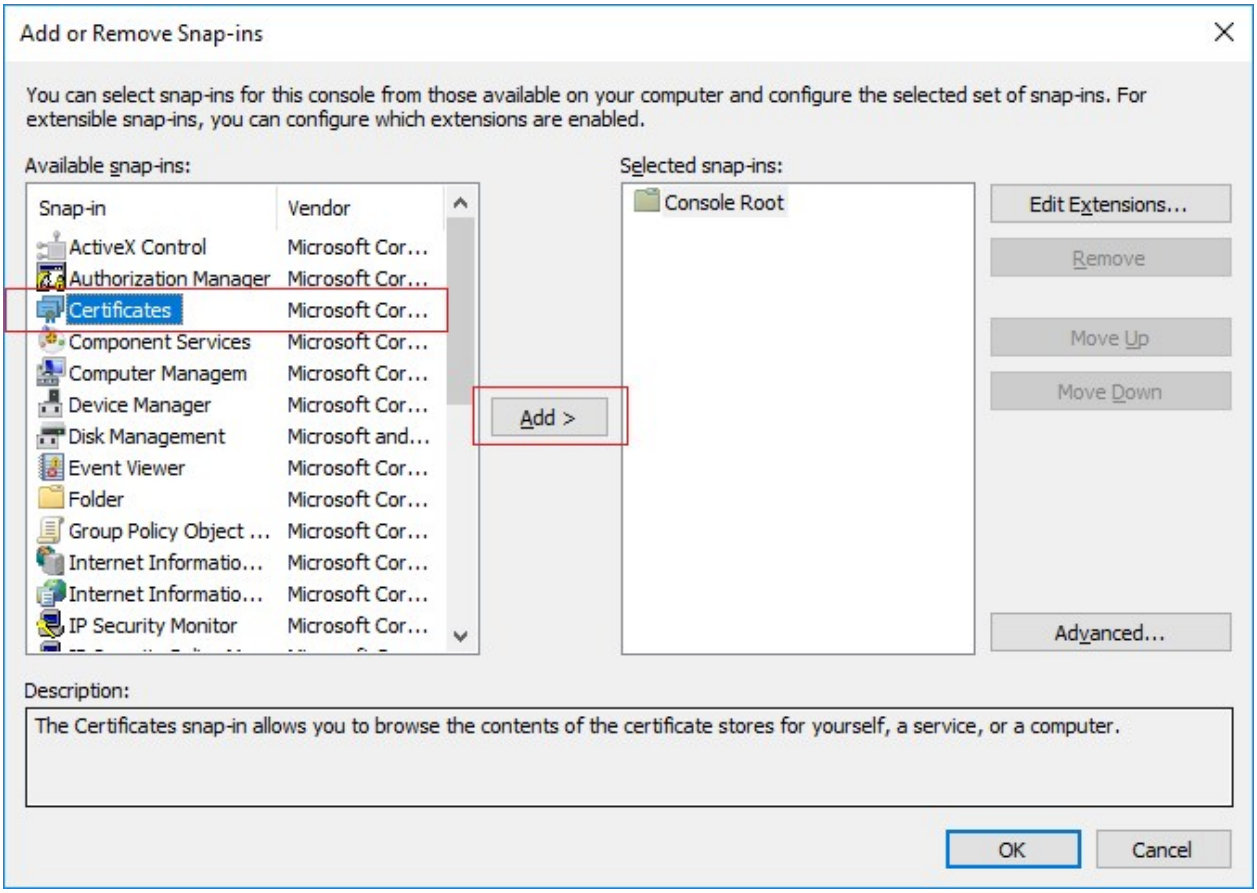
To verify that the certificate is imported start the Microsoft Management Console.



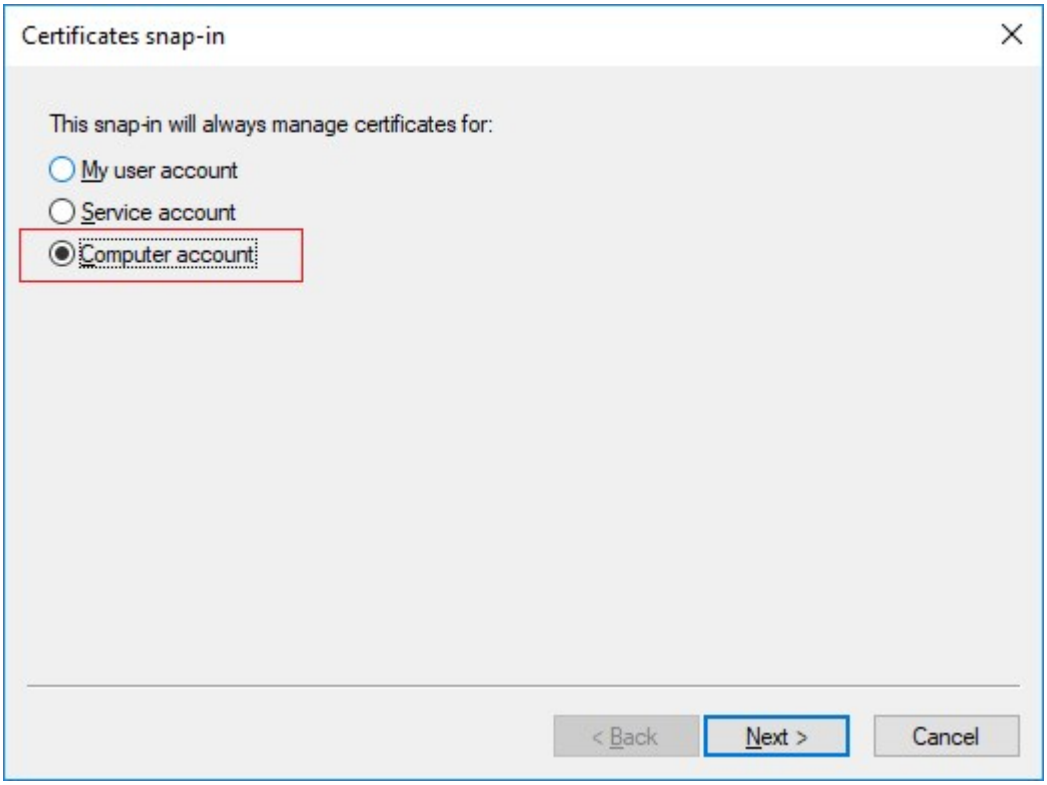
In the Microsoft Management Console from the File menu select “Add/Remove Snap-in...”



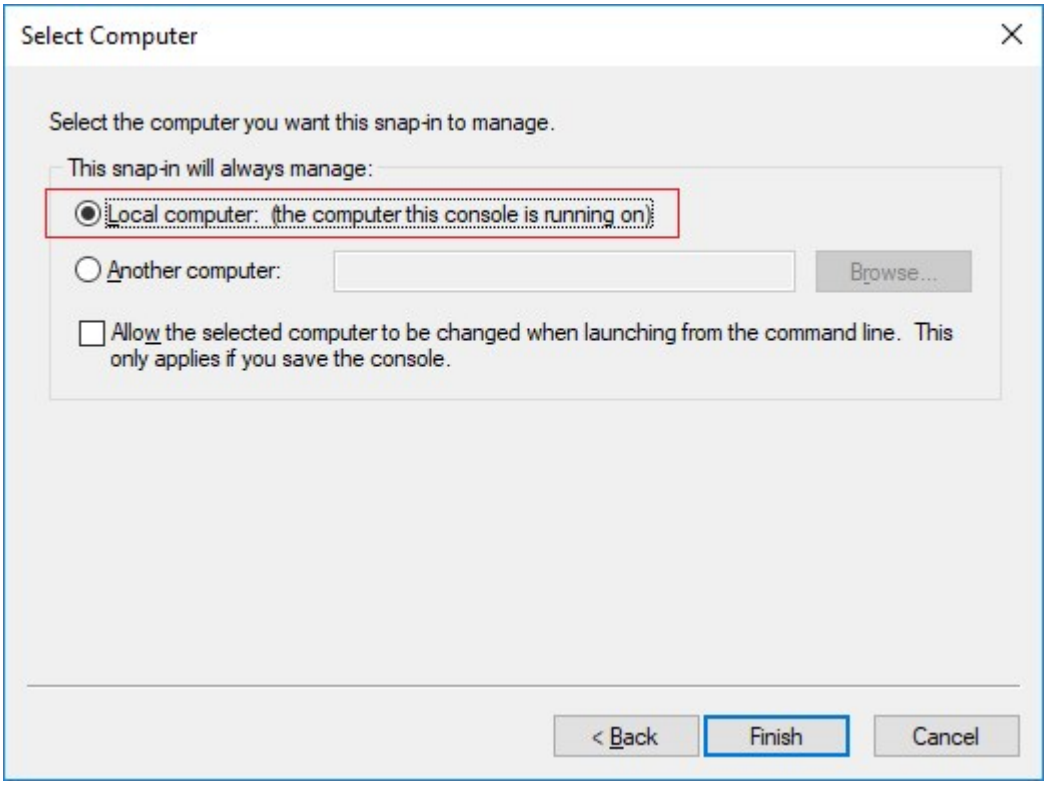
Select the “Certificates” snap-in and click the “Add” button.



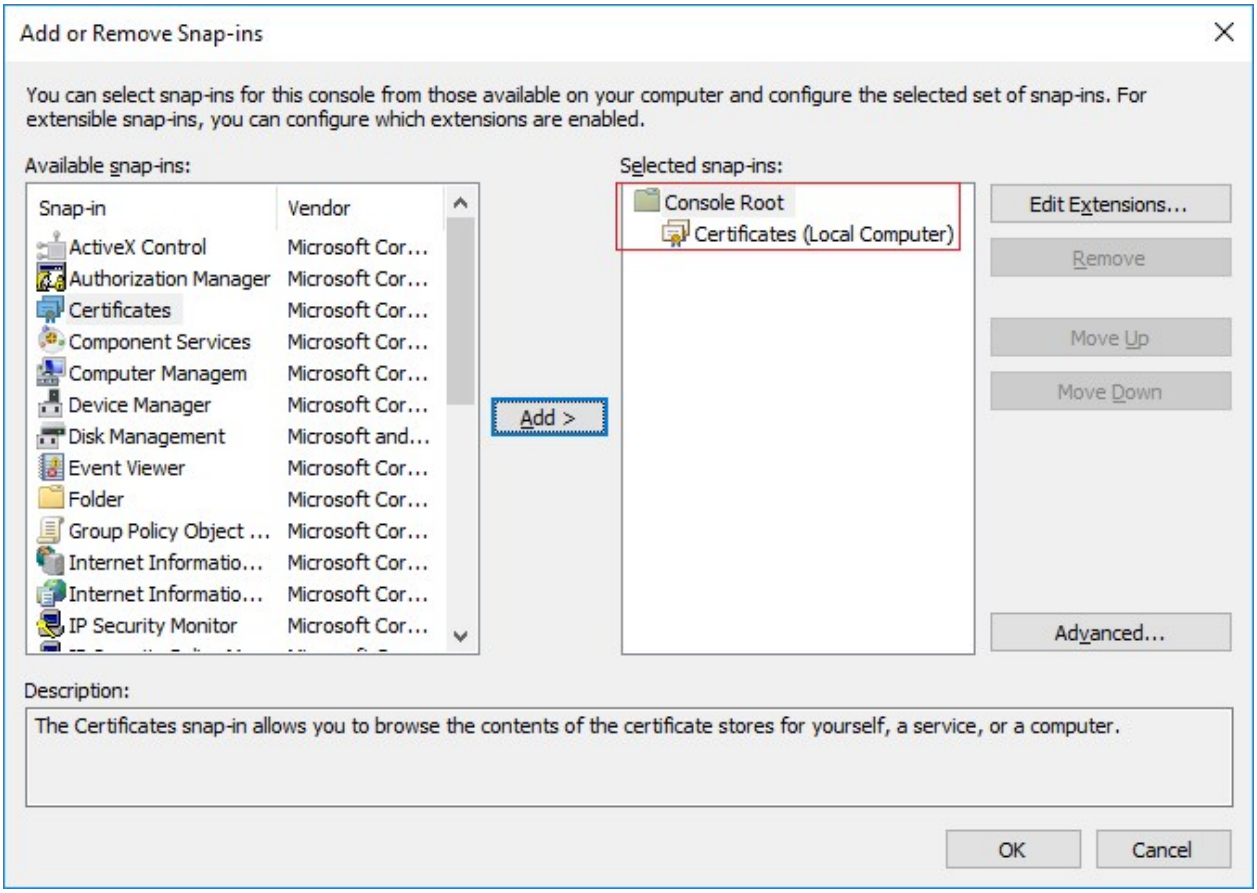
Select the snap-in to manage the certificate for the “Computer account”.



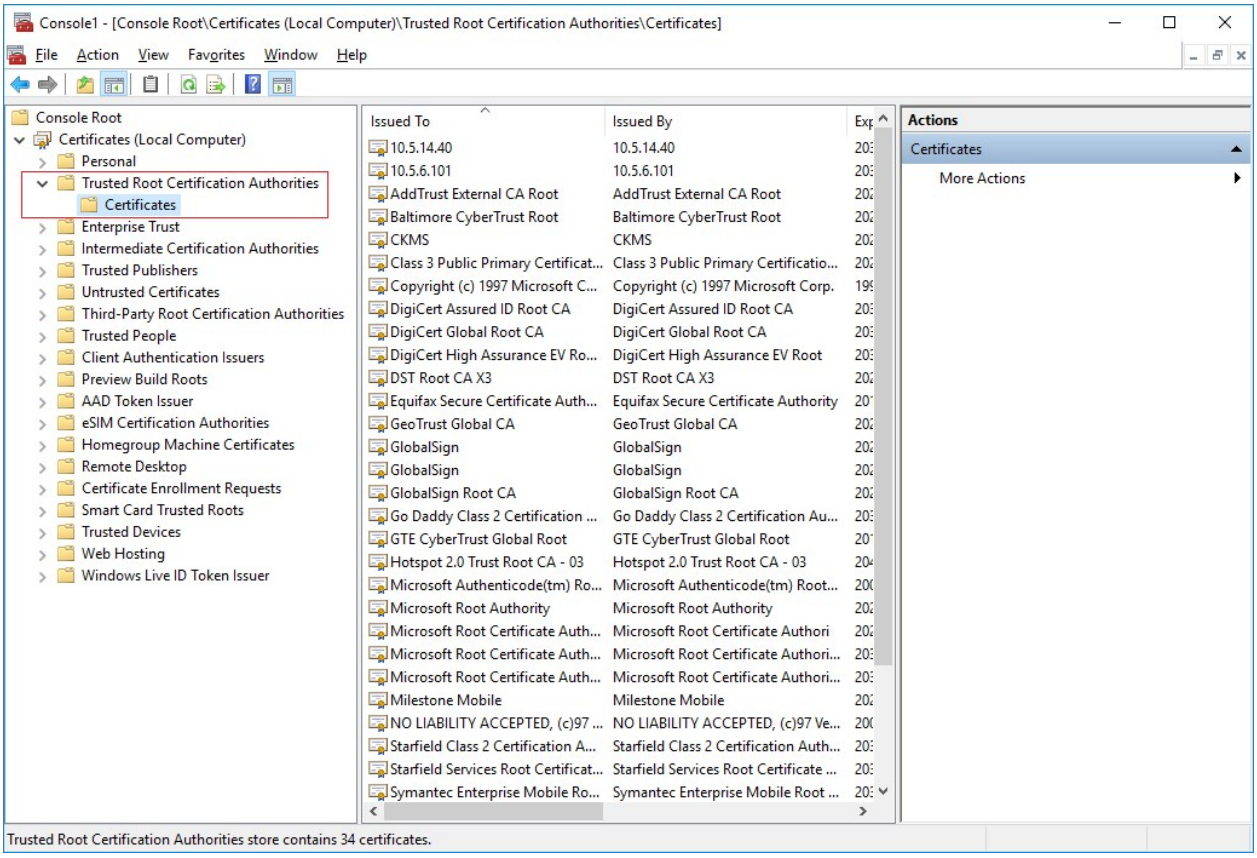
Select “Local computer” on the next step.



Click OK after the snap-in has been added.



Verify that the certificate is listed in the center view of the “Trusted Root Certification Authorities” subtree.



Media service

There are two types of media services the driver supports. The Media 1 service (profile S) and Media 2 service (profile T). Some of the devices support both media services.

- If the device supports only Media 1 service (ver10), only this will be in use.
- If the device supports both media services (ver10 and ver20), Media 2 service will be in use by default. If the user wants to use Media 1 service, it can be selected in the drop-down menu followed by recording server restart. Otherwise, the driver will continue using Media 2 service.
- If the device supports only Media 2 service (ver20), the driver will use this.
- If the device does not support DeviceIO service, the Media 2 service will be unavailable.

If the device supports both media services and it is added in the Management Client with a Device Pack which supports only Media 1 service, only Media 1 service will be available. With Device Pack upgrade (DP 9.5) which supports both services, still the Media 1 service will be in use. To switch the setting to Media 2 Service must be changed manually which requires a Recording Server restart afterwards.

Video settings

The general video settings are video settings per device channel. If a device supports more than one channel, those settings can be configured different for each channel. In the Management Client they are placed on “Settings” tab. For devices with one channel, there is only one general settings section. If the configuration is changed, it will be applied on all video streams (profiles) for that channel. For multi-channel devices, there are video general settings for each channel separately.

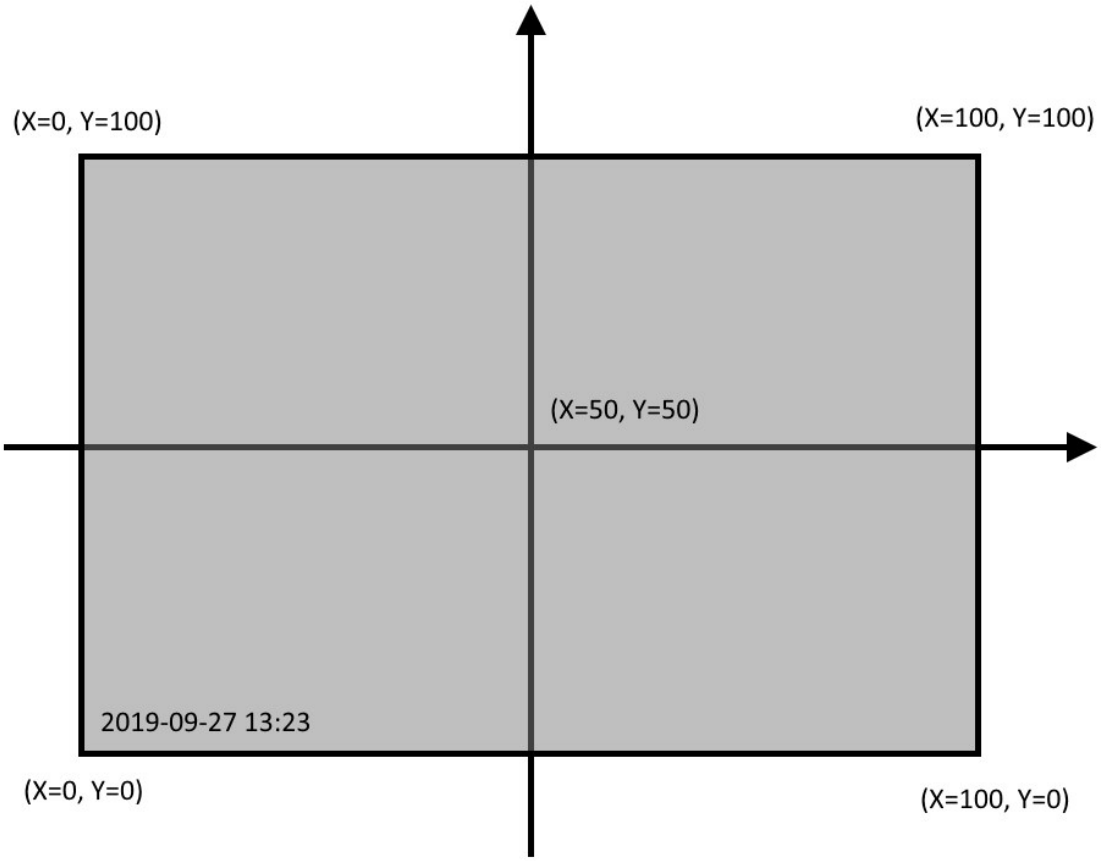
Setting name	Possible values	Value taken from device	Default value
Brightness	[0,100]	✓	50
Contrast	[0,100]	✓	50
Saturation	[0,100]	✓	50
Sharpness	[0,100]	✓	50
White Balance Mode	Auto Manual	✓	Auto
White Balance Cb Gain	[0,100]	✓	50
White Balance Cr Gain	[0,100]	✓	50
OSD Date And Time	Disabled Up Left Up Right Down Left Down Right Custom	✓	Disabled
OSD Date And Time X	[0, 100]	✓	0
OSD Date And Time Y	[0, 100]	✓	0
PTZ Zoom Step	[0, 100]		10

Setting name	Possible values	Value taken from device	Default value
PTZ send zoom parameter	Always When Changed		Always

If the device does not support white balance, the settings for White Balance will not be displayed. If White Balance Mode is Manual, “White Balance Cb Gain” and “White Balance Cr Gain” are available. If White Balance Mode is AUTO, “White Balance Cb Gain” and “White Balance Cr Gain” values do not have impact on the setup.

If the device does not support OSD that displays the date and time, the settings “OSD Date and Time”, “OSD Date and Time X” and “OSD Date and Time Y” will not be displayed. Support for Date and Time OSD was added in Device Pack 10.6. Some of the positions for “OSD Date and Time” might not be available. This depends on the values the device supports.

When “Custom” is available and selected for “OSD Date and Time” the “OSD Date And Time X” and “OSD Date and Time Y” control the position of the OSD on the video. The values correspond to the following positions:



PTZ Zoom Step can be used to control how much a camera should zoom when performing a RelativeMove zoom – e.g., single click on the PTZ Overlay Zoom buttons or zooming via the mouse scroll wheel. The default value is 10, i.e., 1/10th of the maximum zoom range of the device. Behaviour between different devices may vary.

A special value of 0 can be set to replace the use of RelativeMove command with a ContinuousMove command. This can be used on devices that have too much movement even on the lowest value of 1.

PTZ send zoom parameter [Always/When changed] – this setting is introduced as a workaround to accommodate some devices that do not handle the ContinuousMove command properly. The setting controls when to include the optional Zoom element in a ContinuousMove command. According to section 5.3.3. ContinuousMove of the ONVIF™ PTZ Service Specification it can be omitted without affecting the current Zoom movement (if any).

When this setting is set to "Always", the Zoom parameter will always be included in the ContinuousMove command, even when there is no change in the Zoom movement since the last ContinuousMove command (i.e., repeating the last sent value).

When the setting is set to "When changed", the Zoom parameter is only included if a change has occurred in the Zoom movement since the last ContinuousMove command, and omitted if there is no change.

RTP/RTSP/HTTP/TCP Video stream settings

The number of video streams is the number of supported profiles. Each video stream has its own settings section. This gives the opportunity, different video streams to have different setup.

Setting name	Possible values in driver	Value from device	Affected features or Important notes
Media profile (name)	None Default value: --	✓	The profile name is taken from the device. There is a different video stream representing each of the profiles. Profile 1 is the Video stream 01, the second profile is Video stream 02, etc. If the device supports 5 profiles, there will be 5 available video streams. The max number of Profiles in the driver is 40.
Codec	• JPEG • MPEG4 Simple Profile • MPEG4 Advanced Simple Profile	✓	The available codecs can be different per Profile, they are taken dynamically from the device. Some of the values may not be listed in the drop-down menu, if the device does not support it. Example:

Setting name	Possible values in driver	Value from device	Affected features or Important notes
	• H264 Baseline Profile • H264 Main Profile • H264 Extended Profile • H264 High Profile • H265 Main Profile • H265 Main 10 Profile Default value: One of the supported codecs		The device has 2 profiles. Profile 1 support all types of H264 (baseline, main, extended and high) and H265 main codec. The Profile 2 support JPEG, H264 main and H265 main.
Frames per second	[0.00028, 30.0] Default value: 8.0 Usually, it is half of the max limit.	✓	The min is always 0.00028. The max limit is taken from the device. It can be different than 30, and for each code or profile.
Keep Alive type	• Default • None • RTCP • OPTIONS Default value: Default (Options)	×	This setting can be used when streaming mode is RTP/UDP, RTP/RTSP/TCP and RTP MULTICAST, otherwise it has no impact on the streaming.
Max. frames between keyframes	[1-1000] Default value: 1	✓	The max and minimum frames between key frames are taken from the device. For different devices, the range is different.

Setting name	Possible values in driver	Value from device	Affected features or Important notes
Max. frames between keyframes mode	• Default (determined by driver) • Custom Default value: Default		
Maximum bit rate (kbit/s)	[0,2147483647] Default value: 10000	✓	
Multicast address	none Default value: The same as the one from the device.	✓	Dynamically taken from the device. If the device does not support multicast setting, multicast settings will not be shown in the product.
Multicast force PIM-SSM	• Yes • No Default value: No	×	Source-Specific Multicast (SSM) -identify a set of multicast hosts not only by group address but also by source. A SSM group, called a channel, is identified as (S, G), where S is the source address and G is the group address. The value is always “No”. Can be changed manually in the product. When value is “Yes”, the driver forces the IP to be part of the SSM group.
Multicast port	[0,65535] Default value: 0	✓	Dynamically taken from the device.
Multicast time to live	[0,255] Default value: 5	✓	Dynamically taken from the device.
Quality	[0,100] Default value: 50	✓	A high value means higher quality. Dynamically taken from the device.

Setting name	Possible values in driver	Value from device	Affected features or Important notes
Resolution	All possible values are taken dynamically from device Default value: 640x480	✓	The resolution is taken dynamically every time from the device. If the device has new resolutions in the next firmware, the device should be replaced/re-added with the same one. The purpose is to regenerate the xml with the new resolution values.
Streaming mode	• RTP/UDP • RTP/RTSP/TCP • RTP/RTSP/HTTP/TCP • HTTP snapshot or HTTP/TCP snapshot • RTP/UDP multicast Default value: RTP/UDP	×	The streaming mode will always have "RTP/UDP" and "RTP/RTSP/HTTP/TCP" in the list. If the profile can stream JPEG, in the streaming mode list "HTTP snapshot" will be included. The other values depend on the device. If the device supports them, they will be in the list.

Audio IN/OUT

The ONVIF driver supports Audio IN and Audio OUT.

For the audio channel to work, there needs to be an Audio Encoder configuration available in the Media Profiles returned as response to GetProfiles.

Or if such is not available, GetAudioEncoderConfigurations must return at least one configuration, then ONVIF Driver will try to add it to the media profile using AddConfiguration or AddAudioEncoderConfiguration.

For the Audio Source – the behaviour is the same, if such is not available, GetAudioSourceConfigurations must return at least one configuration, then ONVIF Driver will try to add it to the media profile using AddConfiguration or AddAudioSourceConfiguration.

Setting name	Possible values	Value taken from device	Affected features or Important notes
AUDIO IN			
Codec	Combination of [Codec / Bitrate / Samplerate] Default value: The first configured from the dropdown list Supported codecs by the ONVIF driver are: • G711 on sample rate 8kHz • G711 on bitrate 64kbps • G726 on bitrates 16, 24, 32, 40kbps • AAC		Dynamically taken from the device. In the list only valid combinations of codec, bitrate and sample rate will be visible. If a specific combination is supported by the device but not by the Driver/VMS it will not be listed. When starting the Driver/Recording Server if the device is currently set to an unsupported combination, it will be changed to one for the supported list (usually the first in the list).
Streaming method	• RTP/UDP • RTP/TCP • RTP/RTSP/TCP • RTP/RTSP/HTTP/TCP • RTP/UDP multicast Default value: RTP/UDP	✓	The streaming audio method will always have "RTP/UDP" and "RTP/RTSP/HTTP/TCP" in the list. The other values depend on the device. If the device supports them they will be listed. The Streaming method list is the same as video streaming methods without "HTTP snapshot" value.
Multicast address	-- Default value: the same as the one from device.	✓	Dynamically taken from the device. If the device does not support multicast for audio, multicast settings for audio will not be shown in the product.
Multicast	[0,65535]	✓	Dynamically taken from the device.

Setting name	Possible values	Value taken from device	Affected features or Important notes
port	Default value: 0		
AUDIO OUT			
Buffer size	• 0 • 200 • 400 • 600 • 800 • 1000 • 1200 • 1400 Default value: 0	×	The values in the drop-down menu are defined as different buffer sizes. Packets that are buffered before the audio is sent to the device. Increasing the buffer might help with playback on some devices but will also increase the latency of the audio. Increase only if you experience problems with choppy audio. The default of 0 (zero) means no buffering and packets are sent as soon as they are generated.
Codec	Combination of [Codec / Bitrate / Samplerate] Default value: The first configured from the dropdown list Supported codecs by the ONVIF driver are: • G711 on sample rate 8kHz • G711 on bitrate 64kbps • G726 on bitrates 16, 24, 32, 40kbps • AAC	✓	Dynamically taken from the device.

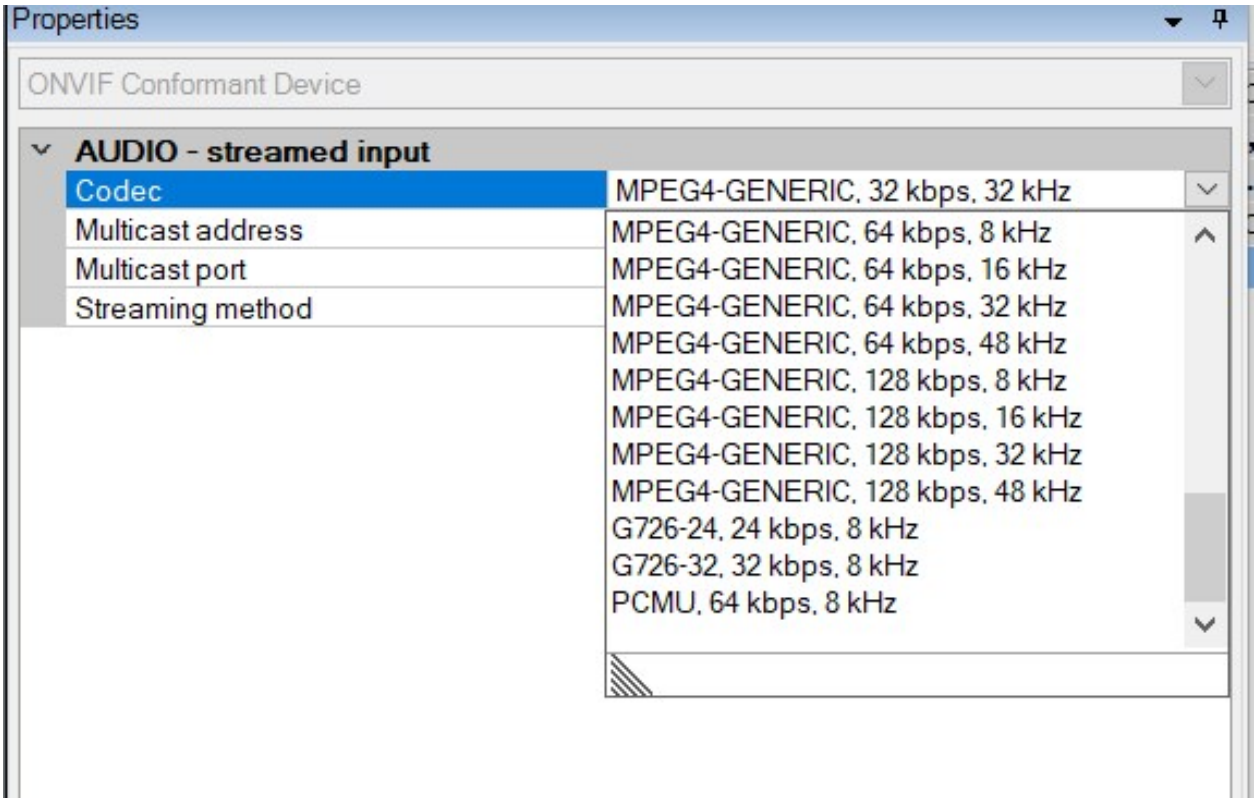
Setting name	Possible values	Value taken from device	Affected features or Important notes
Streaming method	• RTP/UDP • RTP/RTSP/TCP Default value: RTP/UDP	✓	If device support RTP/UDP and RTP/RTSP/TCP they will always be available.

Audio Out does not support multicast streaming. The ONVIF Streaming specification does not specify using multicast streaming for Audio Backchannel.

Audio Out does not support RTSP over HTTP streaming (RTP/RTSP/HTTP/TCP

Some ONVIF devices do not fully comply with the ONVIF Specification for Audio Out codec selection. In such cases selecting the Audio Out codec in the settings might not work and the codec used will be the same as selected for Audio In. For more information see Audio Backchannel codec selection on page 88

The names of the codec combinations for Audio In might be different between the different devices. The ONVIF Driver is using the Audio Codec name as specified by the device. Different devices refer to the codecs with different aliases. For example, AAC / MPEG4-GENERIC / MP4A-LATM or G.711 / PCMU.



Retrieval of remote recordings (Edge storage)

The ONVIF driver supports retrieval of remote recordings from a device (edge storage) using ONVIF Profile G. The communication protocol for Edge Storage is always RTSP. When the device is configured to live stream on RTP/RTSP/HTTP/TCP, the protocol for retrieval of recordings will be RTSP over HTTP, otherwise it will be RTSP. When RTSP over HTTP is selected and HTTPS is enabled the retrieval will be done using RTSP over HTTPS.

The ONVIF driver exposes the edge storage functionality only if the device implements ONVIF Profile G. For the driver to enable edge storage, there is a requirement that the device must fulfil.

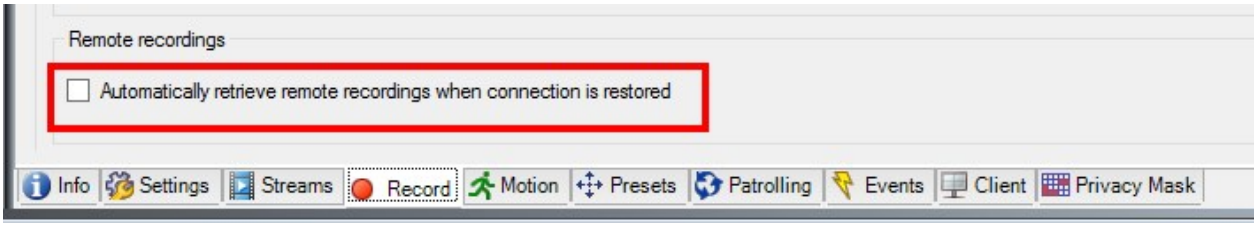
The device must implement the following ONVIF services:

- Recording
- Replay
- Search
- Media or Media2 (if the device has any on-board media sources)
- DeviceIO (if Media2 service is supported)

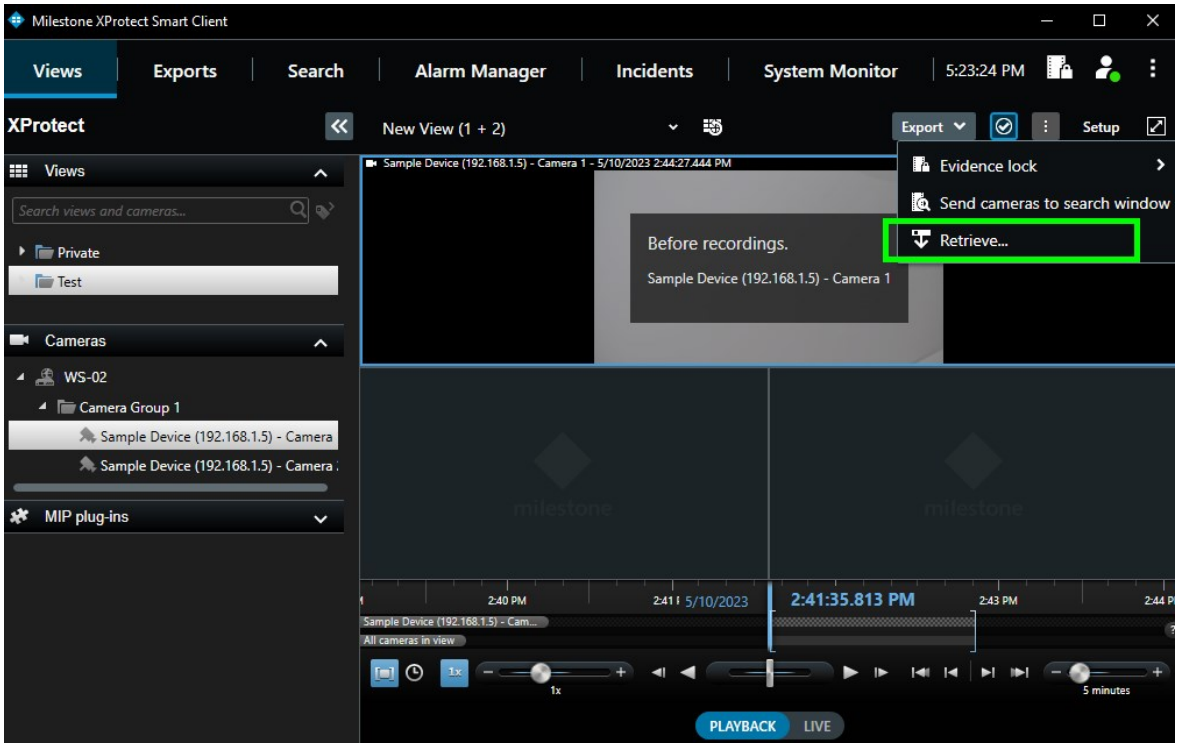
Currently the ONVIF driver needs Media or Media2 service for Edge Storage support. And if Media2 service is available the ONVIF driver needs DeviceIO service. If these services are not available Edge Storage will not be supported.

While the device is added in the Management Client, the driver will retrieve all services that the device supports. If all the mentioned services are implemented, the Edge Storage functionality will be available in XProtect. The automatic retrieving in Management Client will be available as well as the “Retrieve” button in the Smart Client.

- Management Client



- Smart Client

- 

If one of these does not show in the Management Client or the Smart Client, then this means that Edge Storage is not available and therefore some of the important services are not implemented by the device firmware.

The retrieval of Video, Audio and Metadata is done in three steps. When a retrieval of specific time interval is requested first a video recording is searched for and then retrieved. After that is complete, audio is searched for and retrieved. Then last, metadata recording is searched for and retrieved.

For more information on Edge Storage see Milestone Edge Storage White Paper.

Video Edge Storage

The ONVIF driver supports retrieving recordings from the device with the following codecs: JPEG, MPEG4, H.264, and H.265. The ONVIF driver supports retrieval of edge storage video from multichannel video devices (multiple video sources) as well as retrieval from single channel devices. For the details of the edge storage retrieval flow see Edge Storage retrieval workflow on page 83 and

for technical requirements a multichannel device needs to fulfil see Requirements for Edge Storage on Multichannel devices. on page 84Requirements for Edge Storage on Multichannel devices. on page 84

Audio Edge Storage

The ONVIF driver supports retrieval of remote audio recordings with the following audio codecs: G.711, G.726, and AAC. This is applicable for single channel and multichannel devices. Support for single channel audio edge storage is available since XProtect Corporate 2018 R1* and Device Pack 9.6. Multichannel audio edge storage is

available since Device Pack 9.7. For more technical information see Edge Storage retrieval workflow on page 83 and Requirements for Edge Storage on Multichannel devices. on page 84Requirements for Edge Storage on Multichannel devices. on page 84

XProtect Corporate 2018 R1 comes with Device Pack 9.5, so for support of audio edge storage an update of the Device Pack to version 9.6 or newer is required.

Metadata Edge Storage

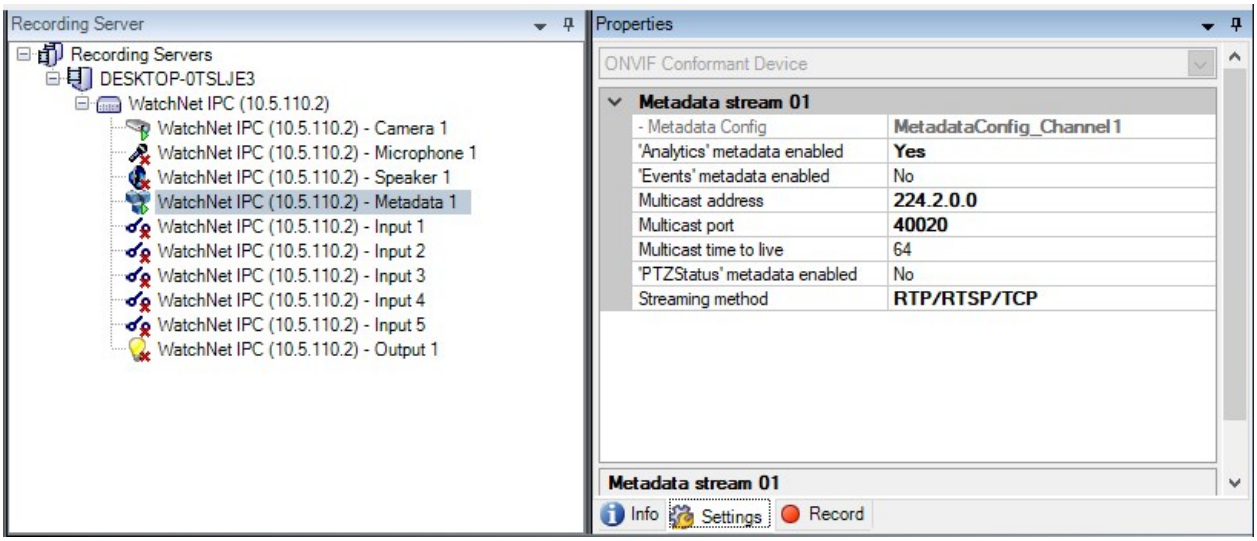
The ONVIF driver supports retrieval of remote metadata recordings from device's storage. Metadata Edge Storage is supported from XProtect 2019 R1 or later and Device Pack 10.8 or later.

Metadata

ONVIF and ONVIF16 drivers support Metadata Bounding Boxes for devices that report Metadata support. The device needs to implement Media Service and/or Media2 Service.

A device with Metadata support will have at least one Metadata Configuration returned in the result of 'GetMetadataConfigurations' request. The first configuration from the returned list is used for all media profiles that **do not** have one already assigned.

There is a Metadata channel corresponding to each video channel. Each Metadata channel can be started or stopped individually and has a single Metadata stream with configurable settings in Management Client:



For the metadata channel to show up, there needs to be a Metadata configuration available in the Media Profiles returned as response to GetProfiles.

Or if such is not available, GetMetadataConfigurations must return at least one configuration, then ONVIF Driver will try to add it to the media profile using AddConfiguration or AddMetadataConfiguration.

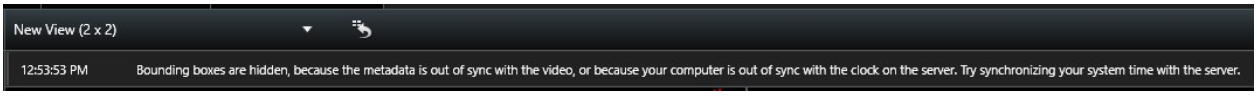
Setting name	Possible values	Value taken from device	Affected features or Important notes
- Metadata Config	Name of the Metadata configuration being used.	✓	Read-only parameter, used for information purposes.
Streaming method	• RTP/UDP • RTP/RTSP/TCP • RTP/RTSP/HTTP/TCP • RTP/UDP multicast Default value: RTP/UDP	×	The streaming method will always have "RTP/UDP" and "RTP/RTSP/HTTP/TCP" in the list. The other values depend on the device. If the device supports them, they will be listed. The streaming method list is the same as video streaming methods without "HTTP snapshot" value.
Multicast address	-- Default value: the same as the one from device.	✓	Dynamically taken from the device. If the device does not support multicast for metadata, multicast settings for metadata will not be shown in the product. The value will be used only when “RTP/UDP multicast” method is selected.
Multicast TTL	[0,255] Default value: 0	✓	Dynamically taken from the device. The value will be used only when “RTP/UDP multicast” method is selected.
Multicast port	[0,65535] Default value: 0	✓	Dynamically taken from the device. The value will be used only when “RTP/UDP multicast” method is selected.
✓	[Yes, No] Default value: No	✓	Dynamically taken from the device. Enable analytics metadata streaming.
'Events' metadata enabled	[Yes, No] Default value: No	✓	Dynamically taken from the device. Enable events metadata streaming.

Setting name	Possible values	Value taken from device	Affected features or Important notes
'PTZStatus' metadata enabled	[Yes, No] Default value: No	✓	Dynamically taken from the device. Enable PTZ status metadata streaming.

✓
Sometimes devices report having multicast settings for Metadata but do not actually support multicast streaming of Metadata.

In order to successfully receive and show Metadata Bounding Boxes, the following requirements might need to be fulfilled:

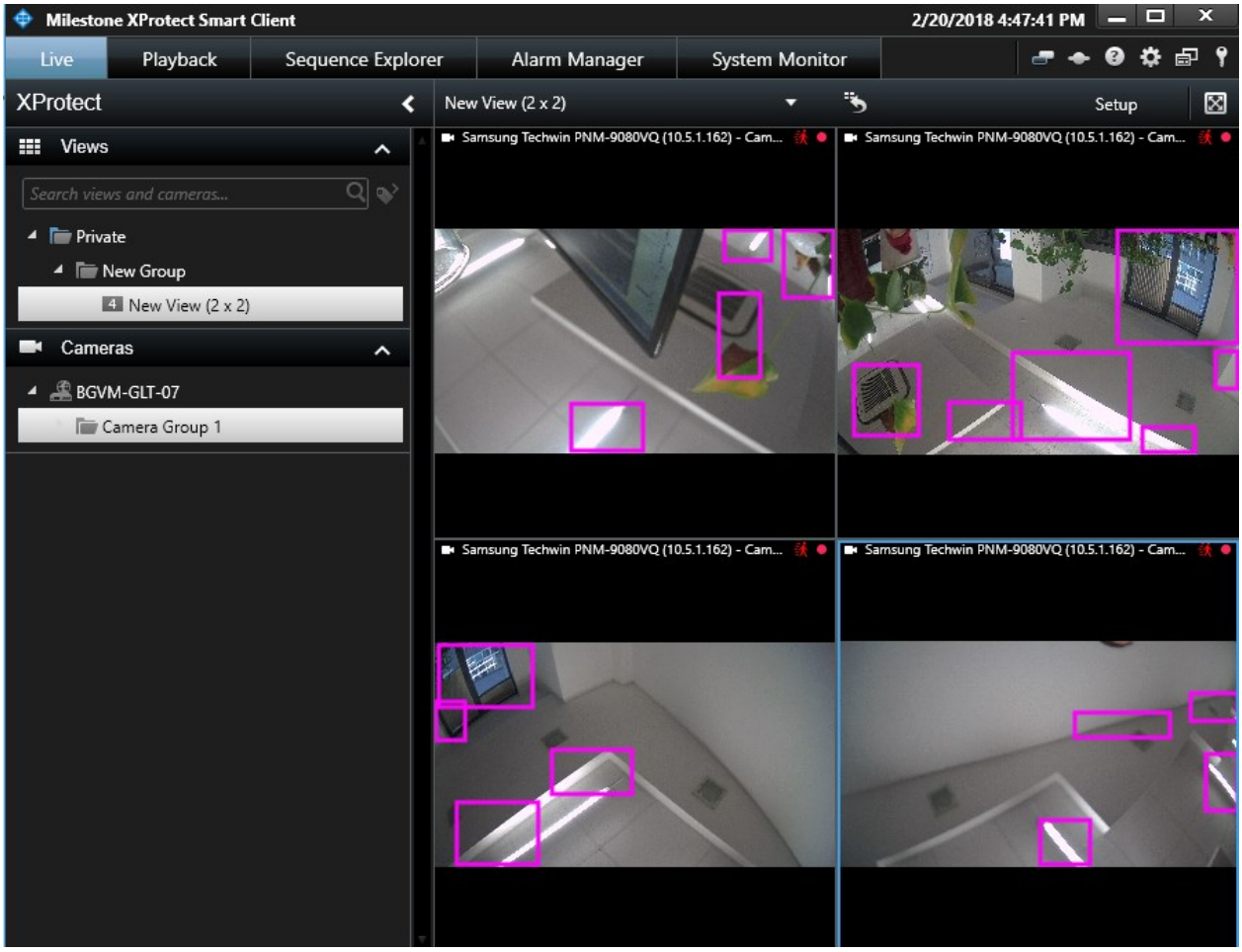
- Date/Time settings on the device and RS should be synchronized. Failure to do so will result in the following message in Smart Client:



“Bounding boxes are hidden, because the metadata is out of sync with the video, or because your computer is out of sync with the clock on the server. Try synchronizing your system time with the server.”

- Video Analytics functionality might need to be enabled from the device’s web page

Metadata Bounding Boxes appear in Smart Client in the following way:



Currently the ONVIF driver supports handling metadata in whole finished XMLs. The ONVIF Streaming Specification states in section '5.1.2.1.1 RTP for Metadata stream" that there is no limitation on the size of the XML document, and it can be continuously appended with new data. The specification recommends closing the XML and starting new one at most at 1 second intervals. Due to the specifics of the internal handing in XProtect, it will not parse an XML document that is not complete and closed. This means that some analytic events might get processed too late and in the specific case of bounding boxes - not displayed at all. As the data is parsed late, the timestamp of the bounding box will be too far in the past and will be skipped as invalid. Due to this limitation, we recommend when sending the metadata to close the XML as soon as possible. In best case scenario to have the whole XML in one RTP packet.

Relay outputs

The ONVIF driver supports activation of the Relay Outputs of an ONVIF device. The Relay Outputs can be activated manually or by a rule.

The ONVIF driver allows the user to configure the output by setting the Trigger Time and Idle State.

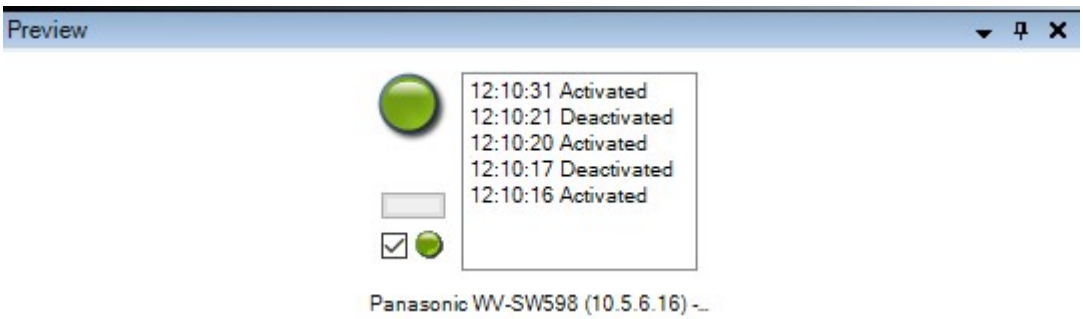
The ONVIF driver controls the mode (Bistable or Monostable) based on the requested action, support from device and Trigger Time.

There are two ways the ONVIF driver can activate an output of an ONVIF device:

1. Trigger – short term activation and then deactivation of the output. Usually controlled by the device, if it supports Monostable mode. The idea here is for ONVIF driver to activate the output and set the activation time and then the device to deactivate itself after the time has passed. One example of such usage is triggering opening of a door. When specific event happens, the ONVIF driver activates the output, the door unlocks and after the set timeout passes (2-3 seconds) the ONVIF device deactivates the output itself and the door locks again. If the ONVIF device does not support Monostable mode, the ONVIF driver will try to simulate this by using Bistable mode and sending both an activation and deactivation command. The timeout between activation and deactivation is controlled by the "Output Trigger Time (msec)" setting of the Output.
2. Activate – long term activation and deactivation of the output. This is activation of the output without a specified timeout. On event the ONVIF driver activates the output and then on another event it deactivates the output. For this type, Bistable mode is used. One example of such usage is starting an alarm speaker.

Setting name	Possible values	Value taken from device	Default value
Idle output state	Open, Closed	✓	Open
Output Trigger Time (msec)	[100,15000]	×	500

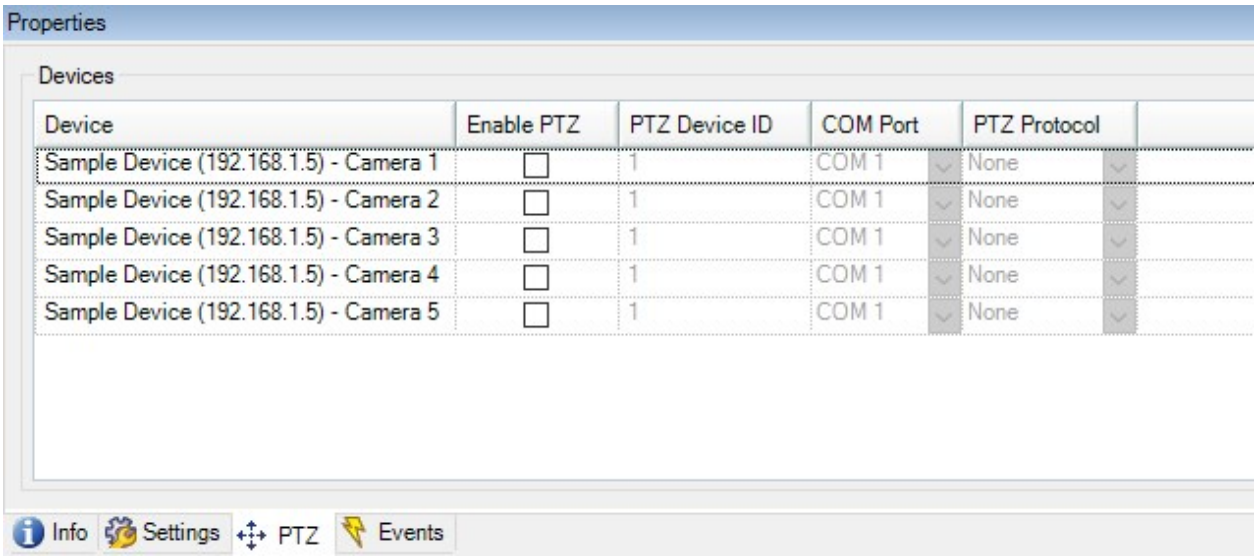
The checkbox and button in the Preview section of the Output can be used to test both modes of operation. The button starts Trigger mode, and the checkbox activates the output on check and deactivates the output on un-check. The green dot shows the current state of the output.



PTZ

PTZ

The ONVIF driver supports PTZ functionality only if the device supports it as well. Currently PTZ must be enabled manually in the PTZ section in the properties window in the Management Client.



When PTZ is enabled, devices that support PTZ will have PTZ, otherwise the PTZ will not work. The “Preset” and “Patrolling” tab will appear under each channel properties.

The ONVIF driver supports these absolute translation spaces used in AbsoluteMove command:

- http://www.onvif.org/ver10/tptz/PanTiltSpaces/PositionGenericSpace
- http://www.onvif.org/ver10/tptz/ZoomSpaces/PositionGenericSpace
- http://www.onvif.org/ver10/tptz/PanTiltSpaces/SphericalPositionSpaceDegrees

The ONVIF driver supports these relative translation spaces used in ContinousMove command:

- http://www.onvif.org/ver10/tptz/PanTiltSpaces/VelocityGenericSpace
- http://www.onvif.org/ver10/tptz/ZoomSpaces/VelocityGenericSpace
- http://www.onvif.org/ver10/tptz/PanTiltSpaces/TranslationSpaceFov

Note: The SphericalPositionSpaceDegrees is supported since Device Pack 10.6

Presets

There are two types of PTZ which determine the presets:

- Relative. When the PTZ Protocol is set to relative, presets must be taken from the device. They cannot be created manually by the user.
- Absolute. When the PTZ is set on absolute, presets can be created manually or they can be taken from the device.

Home position

Home position is a specific pre-defined preset/command. This operation moves the PTZ unit to its home position. The ONVIF driver sends the GotoHomePosition command when the user requests the home preset. Not all devices might support Home Position.

Center Click

The center click is a conditional command. The ONVIF driver will support it only if the device supports the optional translation space - http://www.onvif.org/ver10/tptz/PanTiltSpaces/TranslationSpaceFov.

See https://www.onvif.org/specs/srv/ptz/ONVIF-PTZ-Service-Spec-v1712.pdf (Section A.3.2 Pan/Tilt Translation Space in FOV).

Area Zoom

The Are Zoom use the PTZ Move Commands for Click-to-Move and Drag-to-Zoom. The ONVIF driver will support it only if the device supports the optional translation space. See https://www.onvif.org/specs/srv/ptz/ONVIF-PTZ-Service-Spec-v1712.pdf (Section A.3.2 Pan/Tilt Translation Space in FOV).

For more details how Area Zoom is implemented see Area zoom implementation on page 93.

ONVIF PTZ Configurations

If an ONVIF PTZ device is missing the PTZ Configuration for the first Media Profile on every Video Channel, the ONVIF Driver will try to add a Configuration to that Profile. The method GetCompatibleConfiguration will be called to get a suitable configuration, then that will be added to the Media Profile. In cases when this fails, GetConfigurations will be called and the first PTZ configuration in the list will be added to the Media Profile.

Aux

Auxiliary

This section describes how the driver manages auxiliary commands, such as an infrared (IR) lamp, a heater, a wiper or a washer. There are two possible options for using Aux commands – Aux Commands in the Device Service and Aux Commands in the PTZ Service.

```
<GetServicesResponse xmlns="http://www.onvif.org/ver10/device/wsdl">
  <Service>
    <Namespace>http://www.onvif.org/ver10/device/wsdl</Namespace>
    <XAddr>http://172.32.1.12:1081/onvif/device_service</XAddr>
    <Capabilities>
      <Capabilities>
        <Network ZeroConfiguration="true" NTP="1"/>
        <Security HttpDigest="true" MaxUserNameLength="60" MaxPasswordLength="20"/>
        <System DiscoveryBye="true"/>

          <Misc AuxiliaryCommands="tt:Wiper|On tt:Wiper|Off tt:Washer|On
tt:Washer|Off tt:WashingProcedure|On tt:WashingProcedure|Off tt:IRLamp|On
tt:IRLamp|Off tt:IRLamp|Auto"/>

      </Capabilities>
    </Capabilities>
    ...
  </Service>
  ...
</GetServicesResponse>
```

Aux Commands in the Device Service are retrieved using the commands GetServices or GetServiceCapabilities.

When Aux Commands are detected in the Device Service capabilities, they are sent using the SendAuxiliaryCommand on user request.

Note: Aux Commands from the Device Service are supported in the ONVIF driver since Device Pack 10.3.

Note: Aux Commands in the PTZ Service have higher priority. This means that if the device has PTZ Service, Aux commands will be used from that service.

For PTZ Aux commands to be recognized by the driver, the PTZ must be enabled in the Management Client. On the first PTZ command no matter which one, the GetNode request is sent to the device. The Response contains all auxiliary commands that are supported by the device.

```
<env:Body>
  <tptz:GetNodeResponse>
    <tptz:PTZNode token="PTZNODETOKEN">
```

```
        ...
        <tt:AuxiliaryCommands>tt:Wiper|On</tt:AuxiliaryCommands>
        <tt:AuxiliaryCommands>tt:Wiper|Off</tt:AuxiliaryCommands>
      </tptz:PTZNode>
    </tptz:GetNodeResponse>
  </env:Body>
```

The maximum auxiliary commands that the driver can support are 8. For each auxiliary there are three buttons assigned – “Aux N on”, “Aux N off” and “Aux N on while pressing”. In the example above, “Wiper|On” and “Wiper|Off” will be assigned to Aux 1 On button and Aux 1 Off button in the Smart Client and are counted as one auxiliary command.

Types of commands that the driver accepts are assigned to the Aux buttons in the Smart Client:

Auxiliary commands	**Example**	✓	✓
AuxiliaryData | On	Wiper|On	Button -> Aux 1 on Button -> Aux 1 off Button -> Aux 1 on while pressing	Wiper|On Wiper|Off Wiper|On and Wiper|Off
AuxiliaryData | Off	Wiper|Off	Button -> Aux 1 on Button -> Aux 1 off Button -> Aux 1 on while pressing	Wiper|On Wiper|Off Wiper|On and Wiper|Off
AuxiliaryData	Defog	Button -> Aux 1 on Button -> Aux 1 on while pressing	Defog Defog
AuxiliaryData | Auto	Wiper|Auto	Button -> Aux 1 on Button -> Aux 1 on while pressing	Wiper|Auto Wiper|Auto

If command contains symbol “|” followed by “On” or “Off” (e.g., “Wiper|On” or e.g. “Wiper|Off”) 2 buttons will be mapped (“Aux 1 On” and “Aux 1 Off”)

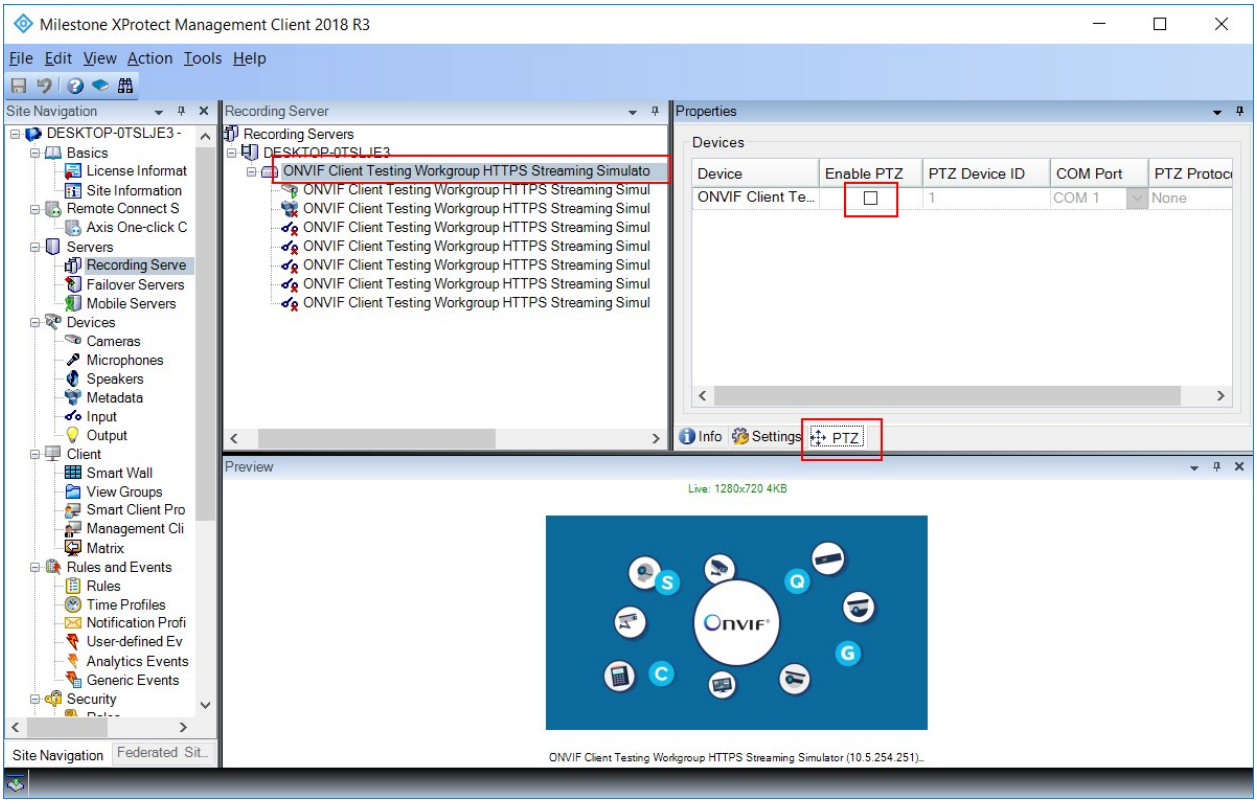
If command does not contain symbol “|” (e.g., “Defog”) only one button will be mapped (“Aux 1 On”). The Aux Off button will not be mapped.

If command contains symbol “|” and something different than “On” and “Off” (e.g., “Wiper|Auto”) only one button will be mapped (“Aux 1 On”). The Aux Off button will not be mapped.

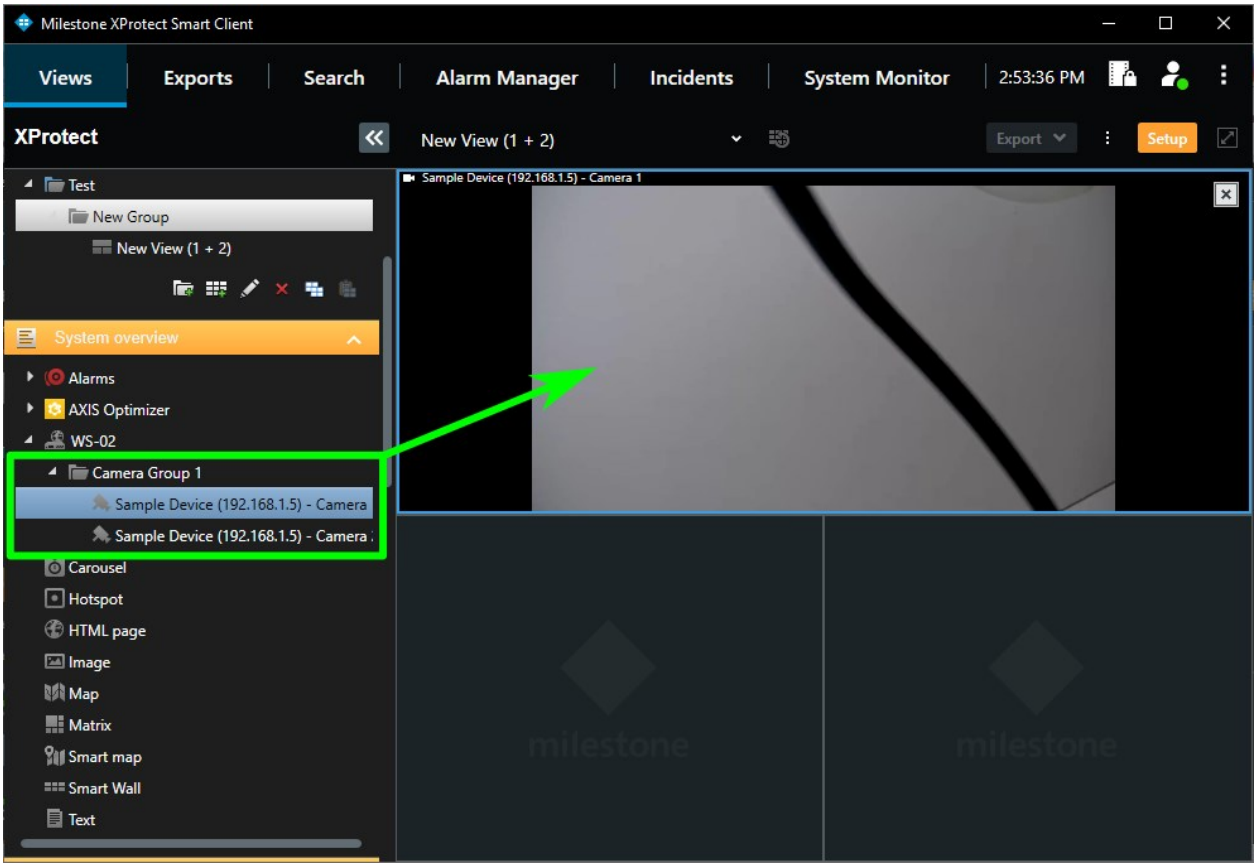
Buttons that are not mapped (e.g., “Aux 1 Off” when Auxiliary command is “Wiper|Auto”), when pressed will not send command to the device.

Setup of Aux buttons in the Smart Client

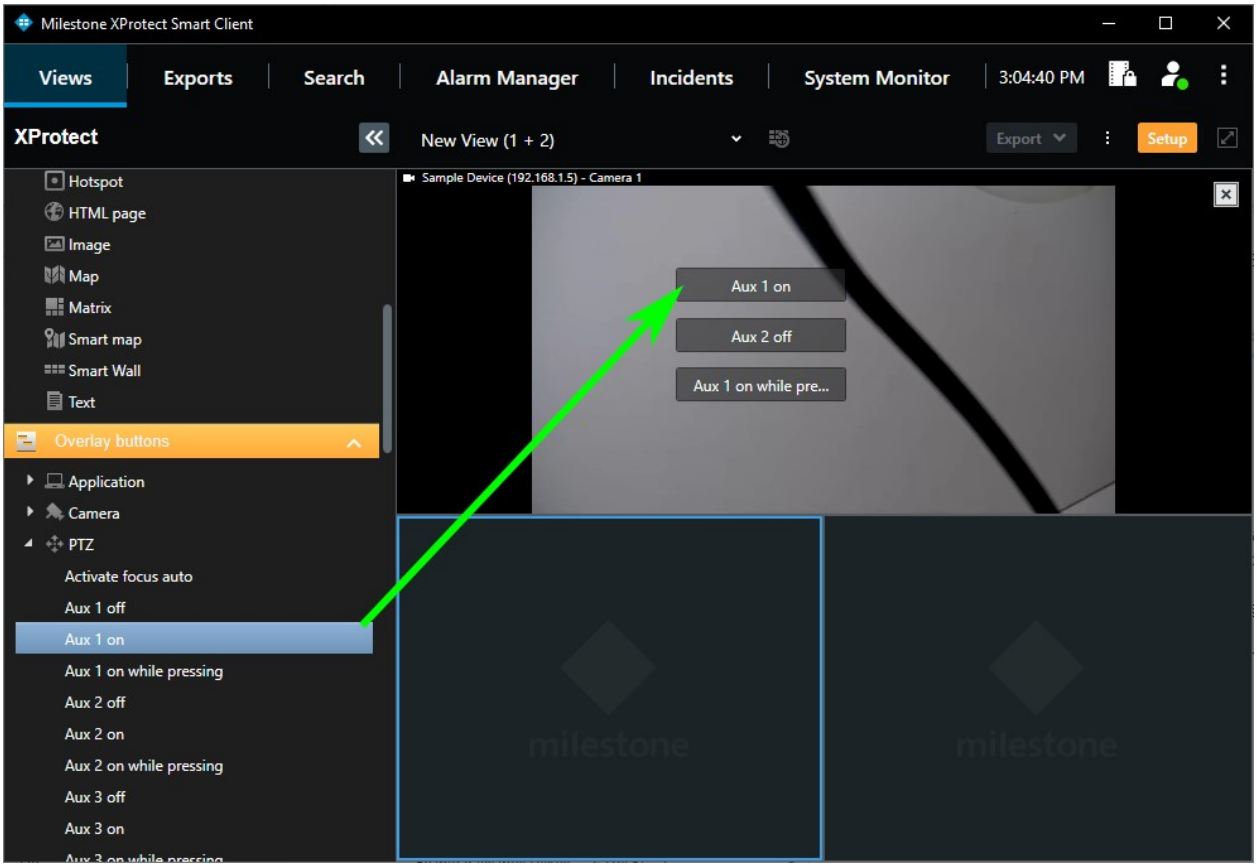
- When the camera is added in the Management Client and if it’s PTZ you must enable PTZ manually in the Management Client. If the device supports Device Service Aux Commands, there is no need to enable the PTZ option in Management Client.



- If the Smart Client is already running, and PTZ is enabled after that, it should be restarted for the PTZ setting to be activated and available
- In the Smart Client, under “Setup” mode, first of all the device must be selected from “System Overview” menu and dragged and dropped in one of the views



- The AUX buttons/commands can be found under “Overlay Buttons” in the PTZ section and can be added by dragging and dropping in the same view area



- Maximum 8 Aux commands are supported, but not all the representing buttons would be working. It depends on how many auxiliary commands the device supports. (i.e. if the device has wiper and washer, then Aux 1 and Aux 2 buttons will work. In the example above only the first Aux button will work because the device only supports the Wiper command.)
- There are 3 kinds of button in Smart client per each command:
- “Aux On” ->send only one command “On” (e.g., “Wiper|On”)
- “Aux Off” -> send only one command “Off” (e.g., “Wiper|Off”)
- “Aux on while pressing” ->when the button is pressed the command “On” is send only once and when the button is released the command “Off” is sent only once. While the button is kept pressed no commands are sent
- Aux Buttons can be renamed to correspond to functionality:


Sample Device (192.168.1.5) - Camera 1
IR Lamp

Events

Events

When events are enabled in the Management Client, the driver creates a pull point subscription and starts sending PullMessagesRequests periodically (every 5 seconds by default) looking for a PullMessagesResponse with notification messages. The notification messages contain information representing that an event occurred, otherwise they are empty. So, for the driver to recognize that an event occurred, the driver must match the message from PullMessagesResponse with some already predefined filters. They are described in the following sections for every event that our current ONVIF driver implementation supports.

The PullMessagesResponse that the driver receives must contain some of the following data, not all of them are required:

- The driver explicitly checks for PropertyOperation = “Changed”. All Notification messages with status “Changed” will be detected by the driver. Therefore, messages with PropertyOperation = “Changed” must be send only if event status is changed, otherwise there will be a lot of unnecessary triggered events. Notification messages that do not have this value are ignored.
- The message topic must be the same or similar in order to match the Topics filter list below for each event. (i.e., If Topic description is Motion as predefine filter in the driver, then Topic category in the received response must contain either/or: Motion, MotionAlarm, **Something**MotionAlarm or MotionAlarm**Something**).
- The Source must contain Name and Value attributes. Name must have the exact match with the description in the Name categories listed (i.e., If Name is InputToken as predefine filter in driver, then Name category in the response must contain InputToken). The Value category needs to refer to the type of the value and not the value itself. (i.e. (negation) means “false”, “off”, “inactive”).

The value types can be:

Value types	Meaning
(VSToken)	String token of a Video Source (i.e., “VideoSourceToken”)
(inputToken)	String token of a Digital Input (i.e., “InputToken”)
(negation)	“true”/”false”; “on”/"off"; “up”/"down"; “high”/"low", “active”/"inactive”, ”1”/"0", “Triggered”/”Normal”
(input)	String which contains number (zero-based index)

Value types	Meaning
(inputNumber)	String which contains number (one-based index)
(source)	String which contains number (zero -based index)
(int)	Number
(window)	Window number
(AEConfToken)	String token of an Audio Encoder Configuration
io	String
(dateTime)	Date and time as string

- Data must follow the same logic as the Source category above in terms of Name and Value.
- Key must follow the same logic as the Source category above in terms of Name and Value.

The next description presents an example of PullMessagesResponse:

```
  <env:Body>
    <tev:PullMessagesResponse>
      <tev:CurrentTime>2017-08-29T09:30:25Z</tev:CurrentTime>
      <tev:TerminationTime>2017-08-30T21:43:45Z</tev:TerminationTime>
      <wsnt:NotificationMessage>

<wsnt:
TopicDialect="http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet">tns1:RuleEngine
/CellMotionDetector/Motion</wsnt:Topic>

        <wsnt:Message>

          <tt:Message UtcTime="2017-08-29T09:30:25Z" PropertyOperation="Changed">
 <tt:Source>

              <tt:SimpleItem Name="VideoSourceConfigurationToken"
Value="VideoSourceToken"/>
              <tt:SimpleItem Name="VideoAnalyticsConfigurationToken"
Value="VideoAnalyticsToken"/>
              <tt:SimpleItem Name="Rule" Value="MyMotionDetectorRule"/>
            </tt:Source>
```

```
          <tt:Data>

            <tt:SimpleItem Name="IsMotion" Value="false"/>
          </tt:Data>
        </tt:Message>
      </wsnt:Message>
    </wsnt:NotificationMessage>
  </tev:PullMessagesResponse>
</env:Body>
```

There are one Topic, PropertyOperation with status “Changed”, three sources and one Data. Each Response can contain more than one Source and more than one Data inputs. The driver requirements for proper match are described for each event below.

Note: After successful creation of a pull point subscription the ONVIF driver will send SetSynchronizationPoint command in order to retrieve the current state of all events.

Inputs

Only one match (one row) is enough for the driver to handle the event. For input event, there are a lot of variations for different vendors. Each Response can contain more than one Source and more than one Data inputs (i.e., 2 rows in the table has two datasets, which means that both will have to correspond to the information in the response).

In the Management Client there are two events:

- Driver events: “Input Rising event” and “Input Falling event”.
- Rule events: “Input Activated” and “Input Deactivated”.

Topic	Source 1		Data 1		Key		Data 2	
	Name	Value	Name	Value	Name	Value	Name	Value
DigitalInput	InputToken	(inputToken)	LogicalState	(negation)				
DigitalInput	DigitalInputToken	(inputToken)	LogicalState	(negation)				

Topic	Source 1		Data 1		Key		Data 2	
DigitalInput	Index	(input)	Level	(negation)				
VivoDigitalInput	Index	(input)	Level	(negation)				
IO/Change/Port	*read the note		port	(input)			flank	(negation)
	Token	(inputNumber)	flank	(negation)				
IO/State/Port	app	io	state	(negation)	port	(input)		
AlarmIn	AlarmInToken	(inputToken)	State	(negation)				
BinaryInput	BinaryInputToken	(inputToken)	State	(negation)				
UserAlarm	AlarmID	(inputNumber)	LogicalState	(negation)				
IO/Port			port	(inputNumber)			state	(negation)
IO/Port	port	(input)	state	(negation)				
DigitalInput	DigitalInputToken	(inputToken)	State	(negation)				
AuxIn	Token	(inputToken)	Value	(negation)				
Trigger/Relay	RelayInputToken	(inputToken)	LogicalState	(negation)				

The ONVIF driver checks the data value for any of the predefined negative values and depending on the result triggers “Rising” or “Falling” event. If the Data field is missing the event will still be triggered but may not be turned off. In this case there is only “Rising” event, without a “Falling” event.

An empty “Name” in “Source” is a problem for multi-input devices, but it is still possible for single input devices. This is not good practice.

Motion

In the Management Client there are two events:

- Driver events: “Motion Started (HW)” and “Motion Stopped (HW)”.
- Rule events: “Motion Started (HW)” and “Motion Stopped (HW)”.

The driver can signal in which window the motion is detected. The maximum window sources can be 8. The indexation starts from 0.

Topic	Source 1		Data 1		Source 2		Data 2	
	Name	Value	Name	Value	Name	Value	Name	Value
MotionAlarm	Source	(VSTOken)	State	(negation)	Window	(window)		
MotionAlarm	Source	(VSTOken)	State	(negation)			ID	(window)
MotionAlarm	Source	(VSTOken)	State	(negation)				
MotionDetection	window	(window)	motion	(negation)				

Topic	Source 1		Data 1		Source 2		Data 2	
MotionAlarm	VideoSourceToken	(VSToken)	State	(negation)				
Motion	VideoSourceConfigurationToken	(VSToken)	Level	(negation)	MotionWindowIndex	(window)		
Motion	VideoSourceToken	(VSToken)	Level	(negation)	MotionWindowIndex	(window)		
MotionDetection	region	(window)	motion	(negation)				
VideoSource/MotionAlarm	VideoSourceConfigurationToken	(VSToken)	IsMotion	(negation)	VMDRegionToken	(window)		
CellMotionDetector	VideoSourceConfigurationToken	(VSToken)	IsMotion	(negation)				
VideoMotion/Zone_Motion	Zone	(window)	Value	(negation)				
MotionDetected	VideoSourceToken	(VSToken)						
VideoSource/MotionAlarm	Source	(VSToken)	State	(negation)				
AdaptiveMotion/	token	(VST	Valu	(neg				

Topic	Source 1		Data 1		Source 2		Data 2	
Triggered		oke n)	e	atio n)				
DirectionalMotion/Triggered	token	(VST oke n)	Valu e	(neg atio n)				

Tampering

In the Management Client there are three events.

For devices which have only one state the following event should be used:

- Driver event: “Tampering”.
- Rule event: “Tampering”.

For devices which have a start and stop state the following events should be used:

- Driver event: “Tampering Started” and “Tampering Stopped”.
- Rule event: “Tampering Start” and “Tampering Stop”.

Topic	Source 1		Source 2		Data 1	
	Name	Value	Name	Val ue	Name	Value
VideoSource/GlobalSceneChange	VideoSource	(VSTok en)	RuleNa me		State	(negati on)
VideoSource/ImageTooDark	VideoSource	(VSTok en)	RuleNa me		State	(negati on)
VideoSource/ImageTooBlurry	VideoSource	(VSTok en)	RuleNa me		State	(negati on)
VideoSource/ImageTooBr	VideoSource	(VSTok	RuleNa		State	(negati

Topic	Source 1		Source 2		Data 1	
ight		en)	me			on)
Tampering					tamper ing	(negati on)
SignalToo	VideoSourceToken	(VSTok en)			State	(negati on)
VideoSource/GlobalScene Change	VideoSourceConfigToken	(VSTok en)			State	(negati on)
VideoSource/GlobalScene Change	VideoSourceConfiguratio nToken	(VSTok en)			State	(negati on)
Tampering	VideoSourceConfiguratio nToken	(VSTok en)			Level	(negati on)
Tampering	VideoSourceToken	(VSTok en)			Level	(negati on)
Tamper	VideoSourceConfiguratio nToken	(VSTok en)			IsTamp er	(negati on)
Tampered	VideoSourceConfiguratio n	(VSTok en)			Tampe red	(negati on)
TamperingDetection	VideoSourceToken	(VSTok en)			State	(negati on)
Tampering	VideoSourceConfiguratio nToken	(VSTok en)			detecte d	(negati on)
CameraSabotage/Trigger ed	VideoSourceConfiguratio nToken	(VSTok en)			Value	(negati on)
CameraSabotage/Trigger ed	Source	(VSTok en)			Value	(negati on)

Video Loss

In the Management Client there are two events:

- Driver events: “Video Loss” and “Video Resumed”.
- Rule events: “Video Loss” and “Video Resumed”.

Topic	Source 1		Source 2		Data 1	
	Name	Value	Name	Value	Name	Value
VideoSource/SignalLoss	VideoSource	(VSToken)	RuleName		State	(negation)
SignalLoss	Source	(VSToken)			State	(negation)
SignalLoss	VideoSourceToken	(VSToken)			State	(negation)
VideoLoss	VideoSourceConfigurationToken	(VSToken)			Level	(negation)
SignalLoss	VideoSource	(VSToken)			State	(negation)

Illegal Access

In the Management Client there is one event:

- Driver event: “Illegal Access”.
- Rule event: “Illegal Access”.

Only one requirement is defined in the driver for Illegal Access event. The Topic in PullMessageResponse must contain the word “IllegalAccess”. The Data and the Key are not checked.

Detect Sound

In the Management Client there is one event:

- Driver event: “Audio passing”.
- Rule event: “Audio Passing”.

Topic	Source 1		Data 1		Data 2	
	Name	Value	Name	Value	Name	Value
DetectedSound	AudioSourceConfigurationToken	AudioSrcConfToken	isSoundDetected	(negation)	UTCTime	(dateTime)
AudioDetection	AudioSourceToken	AudioSrcToken	State	(negation)		
Trigger/VolAlarm	Source	<none>	Level	(negation)		
Audio/DetectedSound	Source	(AudioSrcToken)	State	(negation)		
AudioDetection	token	(AudioSrcToken)	Value	(negation)		

Line Crossed

In the Management Client there is one event:

- Driver event: “Line cross started”.
- Rule event: “Tripwire”.

Topic	Source 1		Source 2		Data 1		Key		Data 2	
	Name	Value	Name	Value	Name	Value	Name	Value	Name	Value

Topic	Source 1		Source 2		Data 1		Key		Data 2	
Crossed	VideoSourceConfigurationToken	(VSToken)			ObjectId	(id)				
Crossed	VideoSourceConfigurationToken	(VSToken)					ObjectId	(id)		
Crossed	VideoSourceConfigurationToken	(VSToken)	Rule	(window)	ObjectId	(id)				
PerimeterIntrusionLine	Source	(VSToken)								
Crossed	VideoSource	(VSToken)	RuleName	(window)	ObjectId	(id)			State	(negation)
Crossed	token	(VSToken)			Value	(negation)				

Defocus

In the Management Client there are two events:

- Device events: “Defocus Start” and “Defocus Stop”.
- Rule events: “Defocus Start” and “Defocus Stop”.

When Defocus is triggered, the Tampering event in the driver is triggered as well.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
ImageToo	Source	(VSToken)	State	(negation)

Scene Change

In the Management Client there are two events:

- Device events: “Scene change Start” and “Scene change Stop”.
- Rule events: “Scene change” and “Scene Change Stop”.

When Scene Change is triggered, the Tampering event in the driver is triggered as well.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
GlobalSceneChange	Source	(VSToken)	State	(negation)
SceneDetector/Changed	VideoSourceConfigurationToken	(VSToken)	isSceneChanging	(negation)

Intrusion Detector

In the Management Client there are two events:

- Device events: “Intrusion detection Start” and “Intrusion detection Stop”.
- Rule events: “Intrusion started” and “Intrusion stopped”.

Topic	Source 1		Source 2		Data 1	
	Name	Value	Name	Value	Name	Value
ObjectsInside	VideoSourceConfigurationToken	(VSToken)	Rule	(window)	IsInside	(negation)
PerimeterIntrusionZone	Source	(VSToken)				

Topic	Source 1		Source 2		Data 1	
IntrusionStarted	Source	(VSToken)			Rule	(window)
IntrusionEnded	Source	(VSToken)			Rule	(window)
RuleEngine/FieldDetector/ObjectsInside	token	(VSToken)			Value	(negation)
RuleEngine/FieldDetector/ObjectsInside	VideoSource	(VSToken)	RuleName	(window)	Inside	(negation)

Abandoned Detector

In the Management Client there are two events:

- Device events: “Abandoned object started on camera” and “Abandoned object stopped on camera”.
- Rule events: “Abandoned object event started” and “Abandoned object event stopped”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
ObjectsAbandoned	VideoSourceConfigurationToken	(VSToken)	IsAbandon	(negation)
ObjectIsLeft	token	(VSToken)	Value	(negation)
ObjectsAbandoned	VideoSourceConfigurationToken	(VSToken)		

Missing Detector

In the Management Client there are two events:

- Device events: “Object removal started on camera” and “Object removal stopped on camera”.
- Rule events: “Object removal event started” and “Object removal event stopped”.

Topic	Source 1		Source 2		Data 1	
	Name	Value			Name	Value
ObjectsMissing	VideoSourceConfigurationToken	(VSToken)				
ObjectsMissing	VideoSourceConfigurationToken	(VSToken)			IsMissing	(negation)
ObjectIsRemoved	token	(VSToken)			Value	(negation)
ObjectRemoval	token	(VSToken)			Value	(negation)
ObjectRemoval	VideoSourceConfigurationToken	(VSToken)	VideoAnalyticsConfigurationToken		Value	(negation)

Loitering Detector

In the Management Client there are two events:

- Device events: “Loitering detection started on camera” and “Loitering detection stopped on camera”.
- Rule events: “Loitering detection event started” and “Loitering detection event stopped”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
ObjectIsLoitering	VideoSourceConfigurationToken	(VSToken)	IsLoitering	(negation)
ObjectIsLoitering	token	(VSToken)	Value	(negation)
LoiteringDetection	VideoSourceConfigurationToken	(VSToken)	Value	(negation)

Face

In the Management Client there are two events:

- Device events: “Face appeared on camera” and “Face disappeared on camera”.
- Rule events: “Face Appearing” and “Face Disappearing”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
ObjectDetector/Face	VideoSourceToken	(VSToken)	IsFaceDetection	(negation)
FaceDetector/Face	token	(VSToken)	Value	(negation)

Object counting

In the Management Client there is one event:

- Driver event: “Object counting event started”.
- Rule event: “Object counting event started”.

Topic	Source 1		Data	
	Name	Value	Name	Value
CountAggregation/Counter	VideoSourceConfigurationToken	(VSToken)		
CountAggregation/Counter	VideoSource	(VSToken)		
ObjectCounting/CountExceeded	token	(VSToken)		
ObjectCounting/CountExceeded	VideoSourceConfigurationToken	(VSToken)	Value	(negation)

Temperature

In the Management Client there are two events:

- Device events: “Temperature detection started on camera” and “Temperature detection stopped on camera”.
- Rule events: “Temperature Detection Started” and “Temperature Detection Stopped”.

Topic	Source 1		Data 1		
	Name	Value	Name	Value	
SceneTemperature	VideoSourceConfigurationToken	(VSToken)	IsTemperatureAlarm	(negation)	
SceneTemperature	VideoSourceToken	(VSToken)	IsTemperatureAlarm	(negation)	
RadiometricAlarm	Source	(VSToken)	Active	(negation)	
RadiometryAlarm	VideoSource	(VSToken)	State	(negation)	

Fire

In the Management Client there are two events:

- Device events: “Fire detection started on camera” and “Fire detection stopped on camera”.
- Rule events: “Fire Detection Started event” and “Fire Detection Stopped event”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
FireAlarm	VideoSourceConfigurationToken	(VSToken)	IsFireAlarm	(negation)
FireAlarm	VideoSourceToken	(VSToken)	State	(negation)

IP Conflict

In the Management Client there are two events:

- Device events: “IP conflict started on camera” and “IP conflict stopped on camera”.
- Rule events: “IP conflict start event" and “IP conflict stop event”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
IPConflict	VideoSourceConfigurationToken	(VSToken)	IsIPConfig	(negation)

Recordings Available

In the Management Client there is one event:

- Driver event: “Recordings Available Event”.
- Rule event: “Recordings Available Event”.

Topic	Source 1		Data 1		Data 2	
	Name	Value	Name	Value	Name	Value
RecordingsAvailable	VideoSourceToken	(VSToken)	StartTime	(dateTime)	EndTime	(dateTime)

The Recordings Available event should be raised when there is available recording to be retrieved from the device. This can trigger our recording server to retrieve missing parts of video for some period of time or for the period of time sent in the response.

SD Card Mounted

In the Management Client there are two events:

- Device events: “SD Card Mounted” and “SD Card Removed”.
- Rule events: “SD Card Mounted” and “SD Card Removed”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
SmartSD	Source	(VSToken)	Level	(negation)

SD Card error

In the Management Client there is one event:

- Driver event: “SD Card Error”.
- Rule event: “SD Card Error”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
HardwareFailure/StorageFailure	Token	(source)	Failed	(negation)
HardwareFailure/HardDiskError	HardDiskNo	(source)		
HardwareFailure/HardDiskFull	HardDiskNo	(source)		

Brute Force Attack

In the Management Client there is one event:

- Driver event: “Brute Force Attack”.
- Rule event: “Brute Force Attack”.

Topic	Source 1	
	Name	Value
BruteForceAttack	Source	<none>

Cyber Attack

In the Management Client there is one event:

- Driver event: “Cyber Attack”.
- Rule event: “Cyber Attack”.

Topic	Source 1	
	Name	Value
CyberAttack	Source	<none>

Quarantine

In the Management Client there is one event:

- Driver event: “Quarantine”.
- Rule event: “Quarantine”.

Topic	Source 1	
	Name	Value
Quarantine	Source	<none>

Auto Tracker

In the Management Client there are two events:

- Driver events: “Auto Tracker started on camera” and “Auto Tracker stopped on camera”.
- Rule events: “Auto tracker event started” and “Auto tracker event stopped”.

Topic	Source 1		Data 1	
	Name	Value	Name	Value
SmartTracking	Source	(VSToken)	tracking	(negation)

Crowd Detection

In the Management Client there are two events:

- Driver events: “Crowd Detection Rising event on camera X, window X” and “Crowd Detection falling on camera X, window X”.
- Rule events: “Crowd Detection Rising event” and “Crowd Detection Falling event”.

Topic	Source 1		Data 1		Source 2	
	Name	Value	Name	Value	Name	Value
ObjectIsCrowd	VideoSourceConfigurationToken	(VSToken)	IsCrowd	(negation)	Rule	(window)
CrowdDetector/Crowded	token	(VSToken)	Value	(negation)		

Running Detection

In the Management Client there are two events:

- Driver events: “Running Detection Rising event on camera X, window X” and “Running Detection falling on camera X, window X”.
- Rule events: “Running Detection Rising event” and “Running Detection Falling event”.

Topic	Source 1		Data 1		Source 2	
	Name	Value	Name	Value	Name	Value
ObjectIsRunning	VideoSourceConfigurationToken	(VSToken)	IsRunning	(negation)	Rule	(window)

Stopped Vehicle Detection

In the Management Client there are two events:

- Driver events: “Stopped vehicle event started” and “Stopped vehicle event stopped”.
- Rule events: “Stopped vehicle event started” and “Stopped vehicle event stopped”.

Topic	Source 1		Source 2		Data 1	
	Name	Value	Name	Value	Name	Value
StoppedVehicle	VideoSourceConfigurationToken	(VSToken)	VideoAnalyticsConfigurationToken		Value	(negation)

Dynamic events

Overview of dynamic events

When a device is added to the Recording Server with the ONVIF Driver, from DP 11.9 or later, the driver reads all device events with the help of GetEventProperties request and adds all events, that are not described in the previous section (9.0), as dynamic events.

Implementation Specifics

Each event description from the response of GetEventProperties is matched against the currently implemented events and if there is a match with existing scheme the event is discarded. All other events have their topic generated form the event description XML tree and are then added to the corresponding device type based on the following rule: if the topic value has “Audio” it is moved to the “Audio In” events, if it has “Device” and any one of the following: “Output”, “Relay” or “Input” it is moved to the “Input” events, anything else is added to the "Video" events. Based on the event properties types the dynamic event could have different behaviour. If there is a property with type Boolean, the event will be with Rising/Falling after its name. If there is a property with type Integer, the event will have Event Index property (Window option) in MA. All event properties with type Token will be checked against the assigned device (Video, Audio, Input) Token, i.e., for video device the tokens used for matching will be VideoSoureTokens.

When an event is received from the device PullMessagesResponse it is first matched against the already defined in the previous section events, if there is no match a search based on the event topic is performed in the dynamic event list. If this search is successful, based on the provide event info for the event Sources the driver determines the device channel, event window and current state. The channel is determined as described in the previous paragraph: first the driver checks the token in the corresponding token list (Video, Audio, I/O), if there is no such token the driver checks in the device configuration tokens and if there is no match again the channel is defaulted to 0.

Windowed events have an extra check to determine which window has triggered the event. If the event description has an Integer type this is considered as window number and in the event check it is converted to correspond to the event window with zero base indexing, i.e., an event has a Source with name Index and type Integer, when matching – this field will be used as zero-based event/window index.

The event state is checked only if the event has a property with type Boolean. If the event reports active/triggered state the “rising” event will be triggered, if the event reports inactive state the “falling” event will be triggered.

Limitations

ONVIF is a standard used by many manufacturers and each one has its own defined version of a certain event and based on types alone it is difficult to recognize what a certain field is used for. In some cases, an integer field could be used for “percentage of certainty”, and this will be considered by the driver as an event number, causing improper matching of the event. In other cases, the event might not provide a source token, but a

channel number (most likely for I/Os), this will again cause the driver to recognize it as window and this might lead to missing an event triggered from another channel. For example, A face recognition event reports “percent match” as an integer value, this will lead to using the percentage information as window number.

Types duplication: Because the driver implementation relies on types provided in the event description, there might be cases where type duplication might occur. For example, there might be several source fields that have Integer type, and this could lead to mismatching an event index, or there might be several ReferenceToken fields that might not correspond to the channel/device triggering the event and this could also lead to false channel matching.

Some devices might report the same event with different rule names to distinguish between different areas and with the current implementation in the driver this cannot be reflected, and different rule names will trigger the same event.

Factory default state

Overview of the factory default state

Conformance with Profile Q is no longer maintained as it is deprecated from 2022 onwards. Some functionality related to Profile Q might still be available in XProtect.

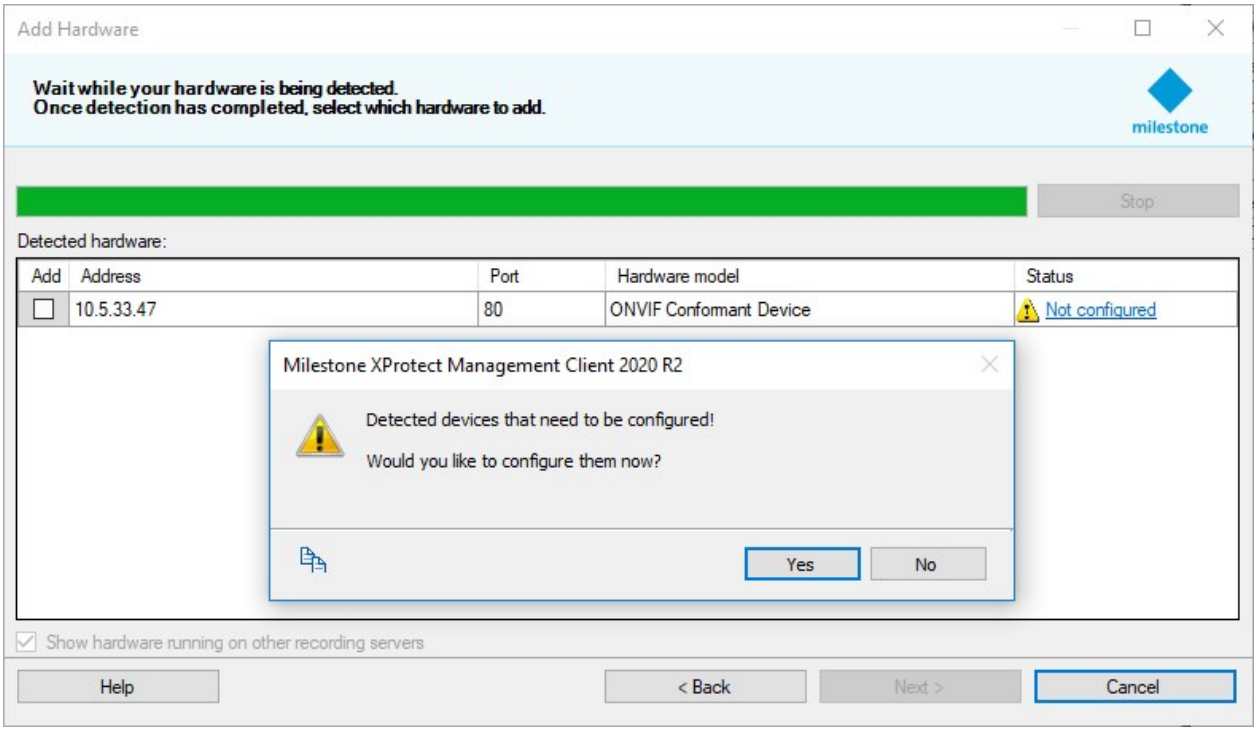
Profile Q conformant devices are in the Factory Default State when first connected to a network. This state is intended for initial configuration, and the device should be deployed only in Operational State.

The ONVIF driver supports Factory Default State detection for profile Q conformant devices and can also transition devices to the Operational State.

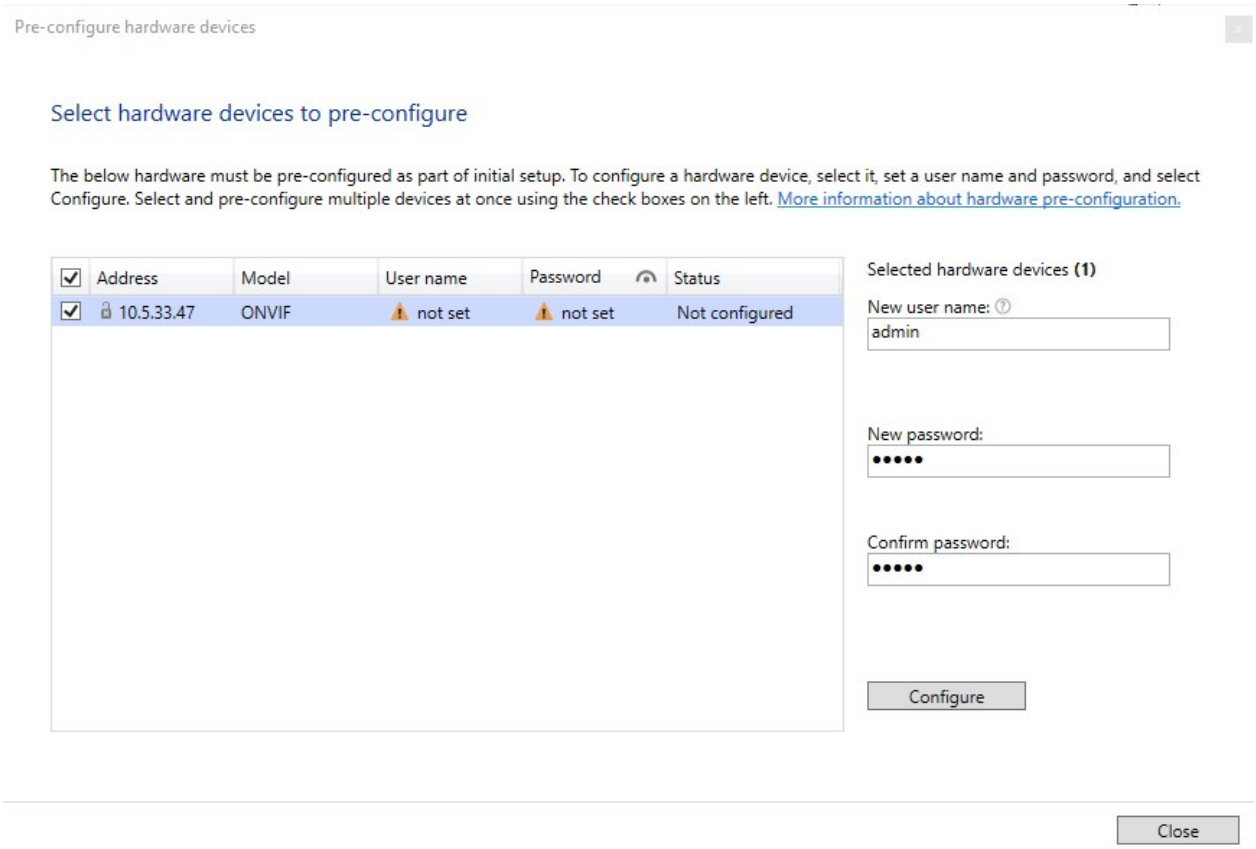
Factory Default State detection and initial configuration are supported as of Device Pack version 11.1 and XProtect version 2020 R3.

Detecting Factory Default State

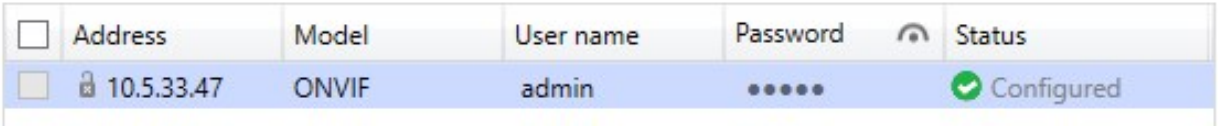
While a device is being added to a Recording Server, the driver will attempt to determine whether the device is in Factory Default State. If so, the VMS will prevent the user from adding the device, and will prompt them to perform an initial configuration procedure on the device:



The user will have the opportunity to configure the device with administrator credentials in order to transition to Operational State:



Upon clicking “Configure”, the device will be configured into Operational State:



Once the device is in Operational State, and the pre-configuration dialog is closed, it can be added to the Recording Server as usual:

Technical details

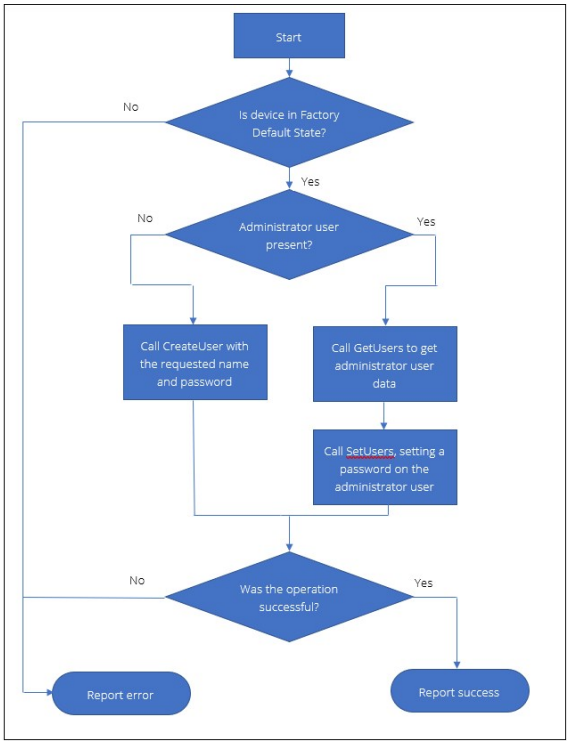
The driver will consider a device to be in Factory Default State if the following conditions hold true:

- A successful call to GetUsers with empty credentials
- And either:
    - No users were returned by GetUsers, or
    - One user was returned, having UserLevel of Administrator

In the case where an administrator user already exists on the device, its name will be forwarded to the VMS, allowing the VMS operator to set a password on the existing administrator user.

Transitioning to Operational State

The ONVIF driver can transition a device in Factory Default State to Operational State. It will follow the steps outlined below:



Firmware update

Overview of firmware update

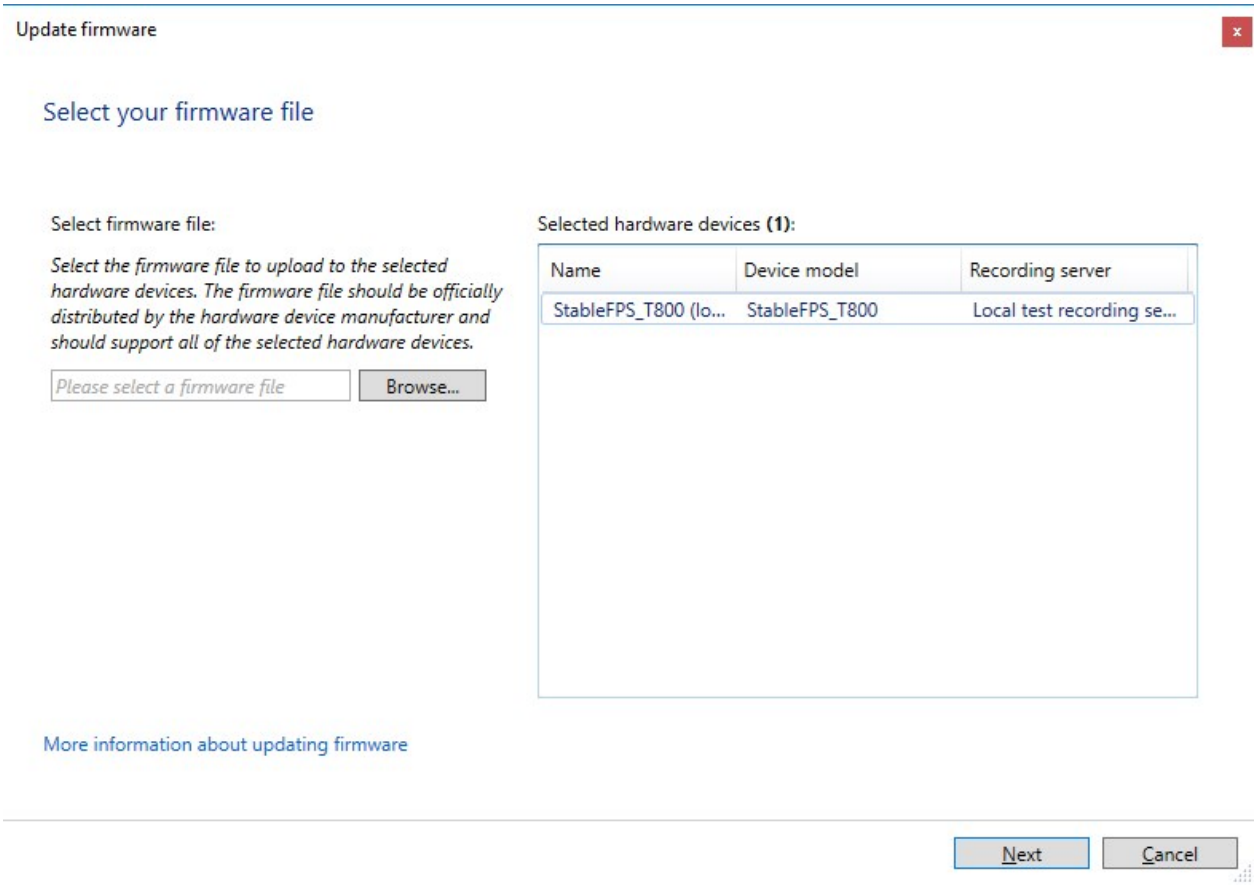
ONVIF devices support firmware update via two mechanisms: update via MTOM using the UpgradeSystemFirmware command, and update via HTTP POST using the StartFirmwareUpgrade command. As of Device Pack version 11.2 and XProtect 2021 R1, firmware update is supported via the latter HTTP POST mechanism.

Detecting firmware update support

Firmware update support is determined by examining the HttpFirmwareUpgrade capability in the System category inside the response returned by the GetServiceCapabilities command. The “Update firmware” wizard in the VMS will only be available for device which report support for HttpFirmwareUpgrade.

Updating firmware

The user may initiate a firmware update on a supported ONVIF device via the Management Client. A right click on a hardware entry in the Recording Servers tree will show a context menu containing the “Update firmware...” item. Upon clicking the item, the “Update firmware” wizard will appear.



Using the wizard, the user can select a firmware image to update the device with. A series of preparatory steps will take place, distributing the file around the VMS, after which the ONVIF driver will be invoked and the firmware upload to the device will begin. The steps are outlined below:

1. Call the StartFirmwareUpgrade command. From the response message, three values are expected:
    1. **UploadUri** – the URL to which the firmware image will be sent to
    2. **UploadDelay** – the amount of time to wait before beginning the HTTP POST request
    3. **ExpectedDownTime** – the duration for which the device expects to be unavailable for after the upload is complete
2. Wait for the duration specified in **UploadDelay**
3. Upload the firmware image to the URL specified in **UploadUri** using an HTTP POST request.
4. The HTTP response code is examined. Unless it's 200 OK, the driver will report a network error at this point and terminate the update process.

5. Wait for the duration of time specified in **ExpectedDownTime**, while attempting reconnection to the device every 30 seconds. The reconnection sequence is as follows:
    1. Call the GetServices command. If it succeeds, move to the next step.
    2. Call the GetDeviceInformation command. If it succeeds, report success. If the reported firmware version is unchanged from the one reported when the update procedure began, report a warning instead.
    3. In case of failure in any of the steps, attempt reconnection again in 30 seconds.
6. Perform a final reconnection attempt. If it fails, report a failure, otherwise, report success or warning according to the same rules as specified in 5b.

FAQ

Which ONVIF Profiles does the ONVIF driver support?

Conformance with Profile Q is no longer maintained as it is deprecated from 2022 onwards. Some functionality related to Profile Q might still be available in XProtect.

The ONVIF driver supports ONVIF Profile S, Profile T, Profile G and Profile Q.

Is JPEG/MJPEG codec a must for a device to work with the ONVIF driver?

The ONVIF Specification requires a compliant device to support JPEG/MJPEG.

ONVIF Profile S, Media1 service – see https://www.onvif.org/specs/srv/media/ONVIF-Media-Service-Spec-v1706.pdf

Section 5.1

"In order to ensure interoperability between client and device, this standard mandates the following codec profiles:

• An ONVIF compliant device shall support JPEG QVGA"

ONVIF Profile T, Media2 service – see https://www.onvif.org/wp-content/uploads/2017/12/ONVIF_Profile_T_Specification_RC_v1-3.pdf

Section 7.19 JPEG Snapshot

7.19.3 Function List for Devices

JPEG Snapshot		Device MANDATORY
Function	**Service**	**Requirement**
GetSnapshotUri	Media 2	M

However, the ONVIF driver is not strict on these requirements and can work with devices not supporting JPEG/MJPEG.

Is G.711 codec a must for a device to work with the ONVIF driver?

ONVIF Specification requires a compliant device to support G.711.

ONVIF Profile S, Media1 service – see https://www.onvif.org/specs/srv/media/ONVIF-Media-Service-Spec-v1706.pdf

Section 5.1

“In order to ensure interoperability between client and device, this standard mandates the following codec profiles:

• An ONVIF compliant device shall support G.711µ Law (Simplex-Camera Microphone Only, 1ch) [ITU-T G.711] if the device supports audio.”

However, the ONVIF driver is not strict on these requirements and can work with devices not supporting G.711.

Does the ONVIF driver support Transparent PTZ?

No, the ONVIF driver does not support Transparent PTZ (see section Definitions on page 11.Definitions on page 11) as the ONVIF Specification does not define functionality that can be used for that.

Does the ONVIF driver support License Plate Recognition (LPR) or Automatic Number-Plate Recognition (ANPR)?

No, currently the ONVIF driver does not support receiving LPR and ANPR data from an ONVIF device through metadata or events. However, XProtect supports LPR through additional add-on that does LPR analytics on the video received.

Does the ONVIF driver support B-frames?

The ONVIF driver and XProtect do not support B-frames.

Does the ONVIF driver support HLS?

No, HLS (HTTP Live Streaming – Apple specification RFC8216) is not part of the ONVIF Specification.

Does the ONVIF driver support MP4 or MKV containers?

No, the ONVIF Specification defines media streaming only using RTSP and RTP. See ONVIF Streaming Spec, Section 4 and Section 5.

Why the ONVIF driver does not send PTZ Stop command?

There are two ways in ONVIF to stop Continuous PTZ movement:

- Using Stop command
- Using ContinuousMove command with velocity set to zero.

The ONVIF driver uses the second option. This is perfectly OK as specified in the PTZ Service specification:

Section 5.3.3 ContinuousMove

“A device shall stop movement in a particular axis (Pan, Tilt, or Zoom) when zero is sent as the ContinuousMove parameter for that axis. Stopping shall have the same effect independent of the velocity space referenced. This command has the same effect on a continuous move as the stop command specified in section 5.3.5.”

Does the ONVIF driver work with Audio only devices?

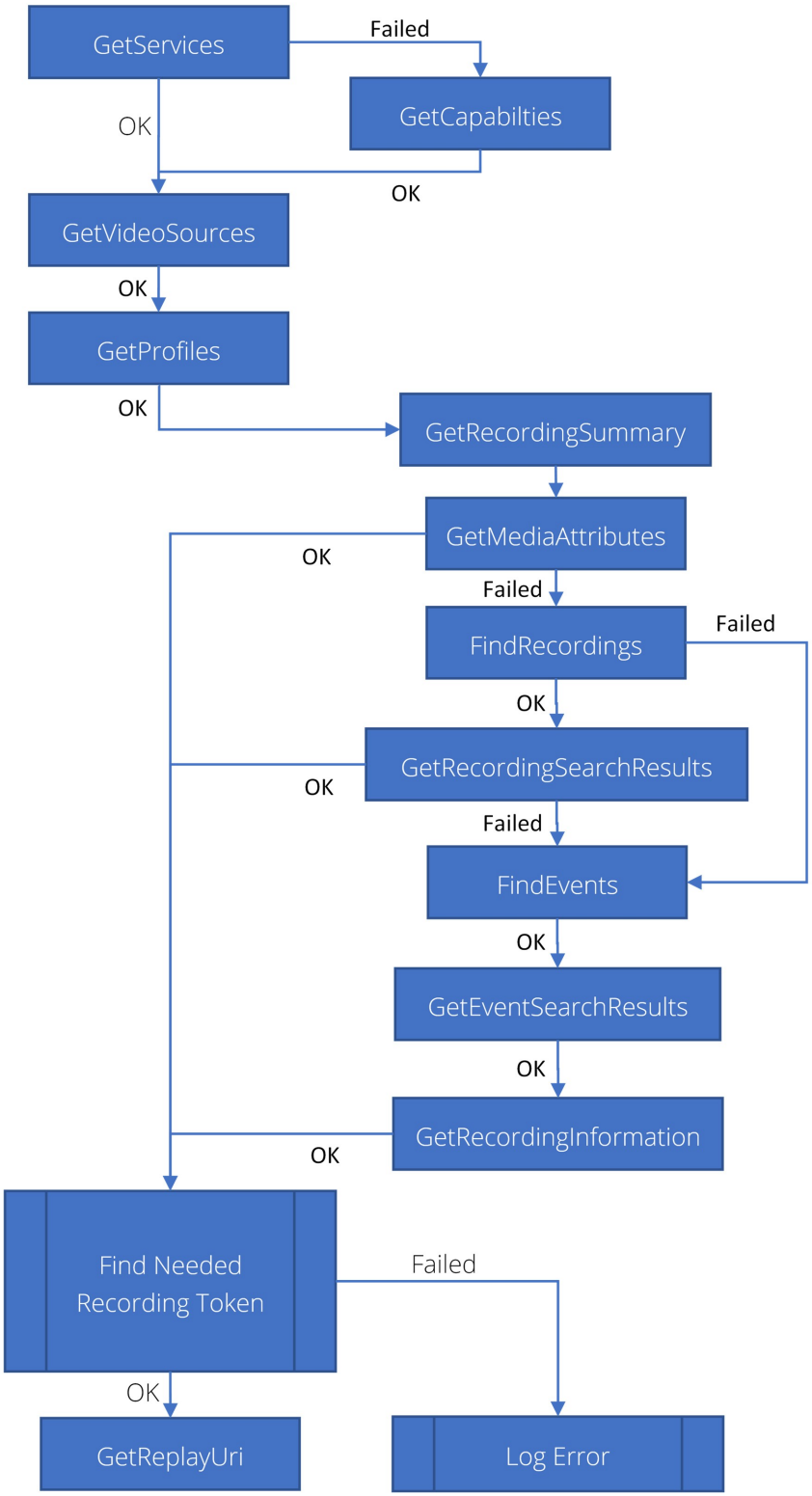
Audio only devices have only Audio In/Out channels and do not have Video channels/sources. The ONVIF driver does work with such devices.

Does the ONVIF driver work with devices behind NAT and when port forwarding is used?

Yes, the ONVIF driver can work with devices that are behind NAT but it depends on the configuration of the device. See Configuration of devices behind NAT and port forwarding on page 89.

Technical section

Edge Storage retrieval workflow



Requirements for Edge Storage on Multichannel devices.

For maximum compatibility, the ONVIF driver requests to get all available recordings on the device, the driver does not ask the device to do complex filtering. The filtering is done in the driver.

In addition to the list of recording retrieved using the ONVIF Search Service, additional information is retrieved using the ONVIF Recording Service and ONVIF Media Service. To find a specific recording the ONVIF driver several methods from the ONVIF Search Service (see the workflow diagram in Edge Storage retrieval workflow on page 83) and matches them with information retrieved from the ONVIF Media Service (Media1 for Profile S, Media2 and DeviceIO for Profile T) see Figure 1. Example retrieval of information about Video recording on page 86Figure 1. Example retrieval of information about Video recording on page 86.

FindRecordings is called with RecordingInformationFilter having value of:

- For Video: boolean(//Track[TrackType = "Video"])
- For Audio: boolean(//Track[TrackType = "Audio"])

As a fallback if GetRecordingJobs fails or doesn't return the needed information the SourceId field of the RecordingInformation structure will be checked if it matches the token of the needed Video/Audio source or if it matches the MediaProfile tokens of all profiles containing our needed Video/Audio source. By the ONVIF specification this is not the intended usage of the SourceId field but some ONVIF Profile G devices use it as a holder for the token of the Video/Audio source.

For reference of used functions see:

Table 1. Used functions for Edge Storage retrieval

GetServices		**https://www.onvif.org/ver10/device/wsdl/devicemgmt.wsdl**
GetCapabilities		https://www.onvif.org/ver10/device/wsdl/devicemgmt.wsdl
GetVideoSources	Profile S	https://www.onvif.org/ver10/media/wsdl/media.wsdl
	Profile T	https://www.onvif.org/ver10/deviceio.wsdl
GetAudioSources	Profile S	https://www.onvif.org/ver10/media/wsdl/media.wsdl
	Profile T	https://www.onvif.org/ver10/deviceio.wsdl
GetProfiles	Profile S	https://www.onvif.org/ver10/media/wsdl/media.wsdl
	Profile T	https://www.onvif.org/ver20/media/wsdl/media.wsdl

GetServices	**https://www.onvif.org/ver10/device/wsdl/devicemgmt.wsdl**
GetRecordingSummary	https://www.onvif.org/ver10/search.wsdl
GetMediaAttributes	https://www.onvif.org/ver10/search.wsdl
FindRecordings	https://www.onvif.org/ver10/search.wsdl
GetRecordingSearchResults	https://www.onvif.org/ver10/search.wsdl
FindEvents	https://www.onvif.org/ver10/search.wsdl
GetEventSearchResults	https://www.onvif.org/ver10/search.wsdl
GetRecordingInformation	https://www.onvif.org/ver10/search.wsdl
GetRecordingJobs	https://www.onvif.org/ver10/recording.wsdl
GetReplayUri	https://www.onvif.org/ver10/replay.wsdl

Figure 1. Example retrieval of information about Video recording

Edge Storage Retrieval and RTSP/RTP timestamps

For XProtect to correctly place the received Video/Audio/Metadata data on the timeline, the ONVIF driver needs to receive exact wall-clock time for every frame. There are couple mechanisms with which this can be accomplished.

One way is for the device to send a “Range” parameter with a “clock” value in the response to the RTSP PLAY command. This value is specifying the wall-clock time of the first frame in the stream. Then based on that time and the RTP timestamps the ONVIF driver can calculate the wall-clock times of every frame.

The second and preferred way is to follow the ONVIF Streaming specification and use the 0xABAC extension for the RTP packets. Every first RTP packet of every frame should have the 0xABAC extension as specified in the ONVIF Streaming specification, Section 6.3 “RTP header extension”.

If both methods are used the ONVIF driver will respect the 0xABAC extension with higher priority.

RTSP PLAY command “Range” parameter

When initiating playback of a recording from the device, the ONVIF Driver adds a “Range” parameter with the needed start time of the stream. Below is an example of the command with the parameters.

PLAY rtsp://10.5.2.49:554/rtsp_tunnel RTSP/1.0

Session: 12342512568a5f8

CSeq: 4

User-Agent: CmRtspClient Unknown

Range: clock=20200227T081350.000Z-

Require: onvif-replay

Rate-Control: no

Authorization: Digest username="service", realm="Please log in with a valid username", nonce="7daf7249134b343866e87d085b967491", algorithm="MD5", uri="rtsp://10.5.2.49:554/rtsp_tunnel", response="ff558f784bb8f35f204e2a18c93442e6"

The start time of the requested recording is given with the parameter: Range: clock=20200227T081350.123Z format as defined in RFC2326 and is absolute time.

The ONVIF driver also requests the device to not do any rate control of the stream with the parameter Rate-Control: no . This means that the device can stream the recording as fast as possible.

RTP timestamps and 0xABAC extension

In order to provide accurate recorded frames (Video/Audio/Metadata), the device must set absolute wall-clock timestamp for each packet with the same RTP timestamp. This is achieved using an RTP header extension 0xABAC containing a NTP timestamp. This timestamp shall increase monotonically over successive packets within a single RTP stream.

The replay mechanism uses the extension ID 0xABAC for the replay extension.

NTP timestamps are represented as a 64-bit fixed-point number, in

seconds relative to 0000 UT on 1 January 1900. The integer part is

in the first 32 bits and the fraction part in the last 32 bits, as

shown in the following diagram.

```
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Integer Part                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Fraction Part               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

See section 4 in https://tools.ietf.org/html/rfc958

And section 2 in https://www.eecis.udel.edu/~mills/time.html

Audio Backchannel codec selection

Selection of the codec to be used for the Audio Backchannel stream is done in a different way than all the other stream types. The ONVIF device does not have a current audio backchannel codec configuration and only lists all the supported ones using GetAudioDecoderConfigurationOptions. There is no SetAudioDecodecConfiguration in the ONVIF Specifications as there is for Audio In – SetAudioEncoderConfiguration. The selection of the codec is done in the RTSP. This is done by having multiple rtpmap for the Audio Backchannel track.

Section ”5.3.2 Connection setup for a bi- directional connection” of the ONVIF Streaming Specification states:

” The server shall list all supported decoding codecs as own media section and the client

chooses which one is used. The payload type and the encoded bitstream shall be matched

with one of the a=rtpmap fields provided by the server so that the server can properly

determine the audio decoder.”

Section ”5.3.2.3” of the ONVIF Streaming Specification gives an example of SDP with multple Audio Backchannel codecs supported:

v=0

o= 2890842807 IN IP4 192.168.0.1

s=RTSP Session with audiobackchannel

m=video 0 RTP/AVP 26

a=control:rtsp://192.168.0.1/video

a=recvonly

m=audio 0 RTP/AVP 0

a=control:rtsp://192.168.0.1/audio

a=recvonly

m=audio 0 RTP/AVP 0 97 98 99 100

a=control:rtsp://192.168.0.1/audioback

a=rtpmap:0 PCMU/8000

a=rtpmap:97 G726-16/8000

a=rtpmap:98 G726-24/8000

a=rtpmap:99 G726-32/8000

a=rtpmap:100 G726-40/8000

a=sendonly

Based on this SDP the ONVIF driver will select the needed codec, encode the audio stream, and send the RTP audio packets with the payload type of the codec. For example, if the user has selected "G726, 32kbps, 8kHz", the ONVIF driver will encode the audio using the G.726 codec in 32 kbps and set the payload type of the RTP packets sent to 99.

Unfortunately, a lot of ONVIF devices do not follow this convention and will list in the SDP only one codec for the Audio Backchannel track. This usually is also the codec of the Audio In track. In these cases, the ONVIF driver will ignore the user's selection and will use the codec stated in the SDP. Also, if for some reason the codec selected by the user does not exist in the codec list in the SDP, then the ONVIF Driver will select the first supported audio codec.

Configuration of devices behind NAT and port forwarding

For the ONVIF driver it does not matter if it is connecting directly to a device or through a NAT. One exception is the GetStreamUri command. When a device is behind a NAT it usually does not know this so when it is sending the URL for connecting to a media stream, the device sends it with its own IP address and the port on which it is listening. When such device is behind a NAT, the IP address and port through which the media stream is accessible from outside may be different.

The ONVIF driver ignores the IP address returned in the GetStreamUri response and always uses the IP address with which the device was added in XProtect. The RTSP, HTTP or HTTPS port returned in GetStreamUri is handled differently. If the port is not explicitly specified, the ONVIF driver will use the default port for the protocol. In the case of RTSP this will be 554. For HTTP this will be the port with which the device was added in XProtect (might be different from 80). For HTTPS, the port that is specified in the device settings in XProtect will be used. When the port is explicitly specified in the URL returned in GetStreamUri response, the ONVIF driver will always use that port.

For example, if the device is added with port 8081, but GetStreamUri response returns the URL as follows:

http://192.168.10.50:80/stream1

the ONVIF driver will try to connect on port 80 instead of port 8081.

Here are some possible scenarios for setting up the ONVIF driver to work with devices behind NAT.

Currently it is not possible to use UDP streaming with devices behind NAT (RTP/UDP and RTP/UDP multicast).

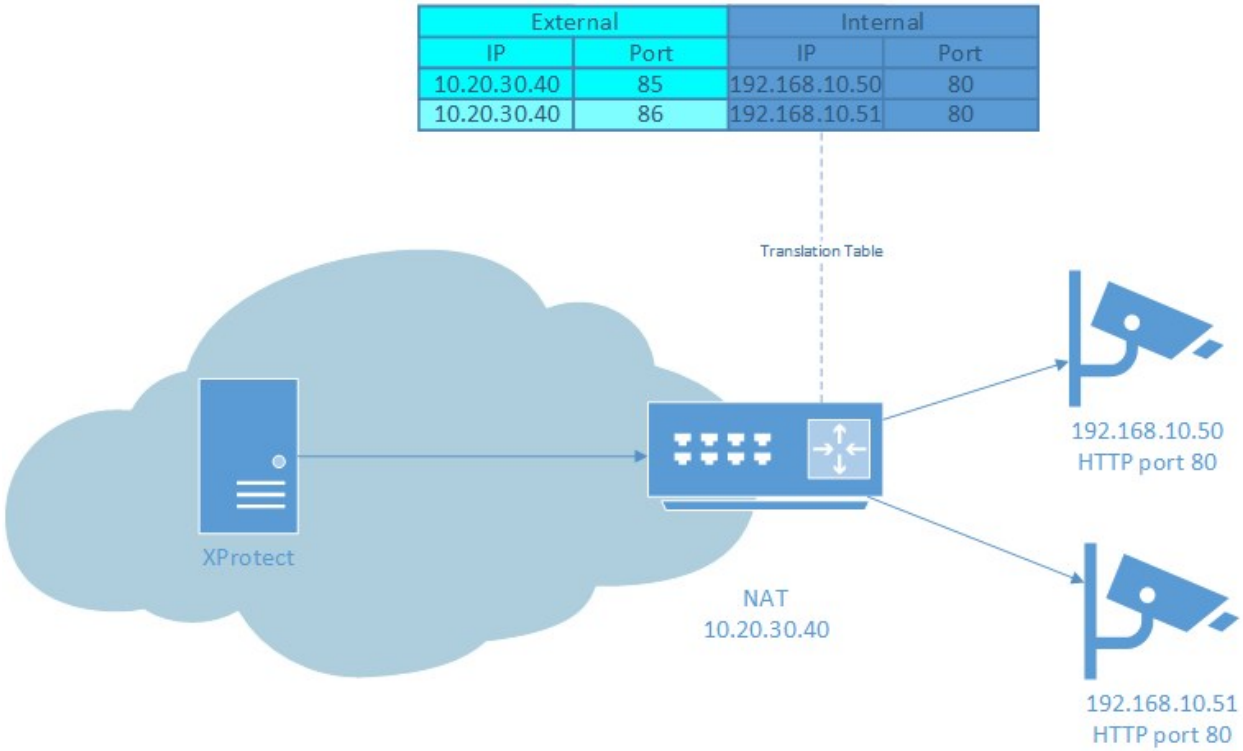
Scenario 1: Unsecure, easy setup, everything over HTTP

Streaming Mode: RTP/RTSP/HTTP/TCP

HTTPS: OFF

Device on default port 80.

Forward any port from outside to port 80 on device.



This will work on most devices and is the easiest to setup. This will not work when the HTTP port on the device is different from the default port 80 and the forwarded port is different from it. Also, this will not work on devices that explicitly state the HTTP port in the URL even if it is the default port 80. For the above cases use Scenario 1A.

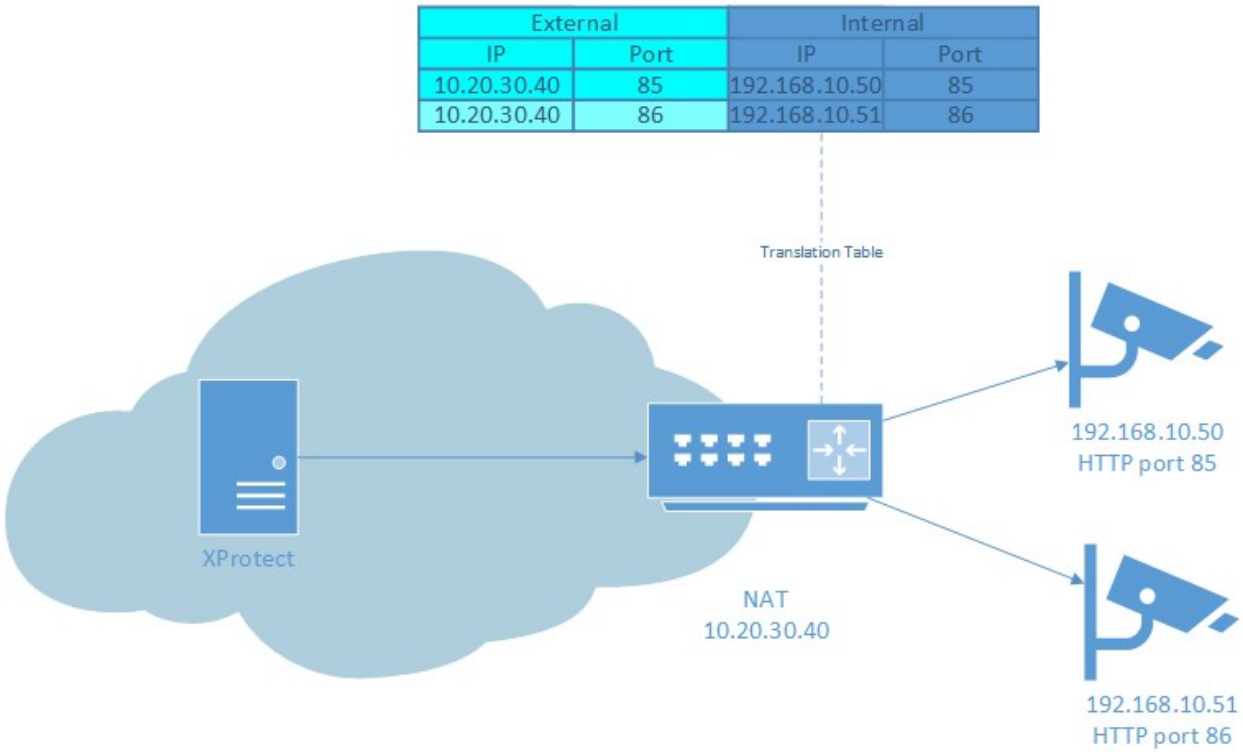
Scenario 1A: Unsecure, medium setup, everything over HTTP

Streaming Mode: RTP/RTSP/HTTP/TCP

HTTPS: OFF

Device HTTP port must be set to forwarded port.

Forward same port number as HTTP port on device.



This will work on all devices that support RTSP over HTTP streaming. One inconvenience is that the HTTP port on all devices must be changed to a unique value.

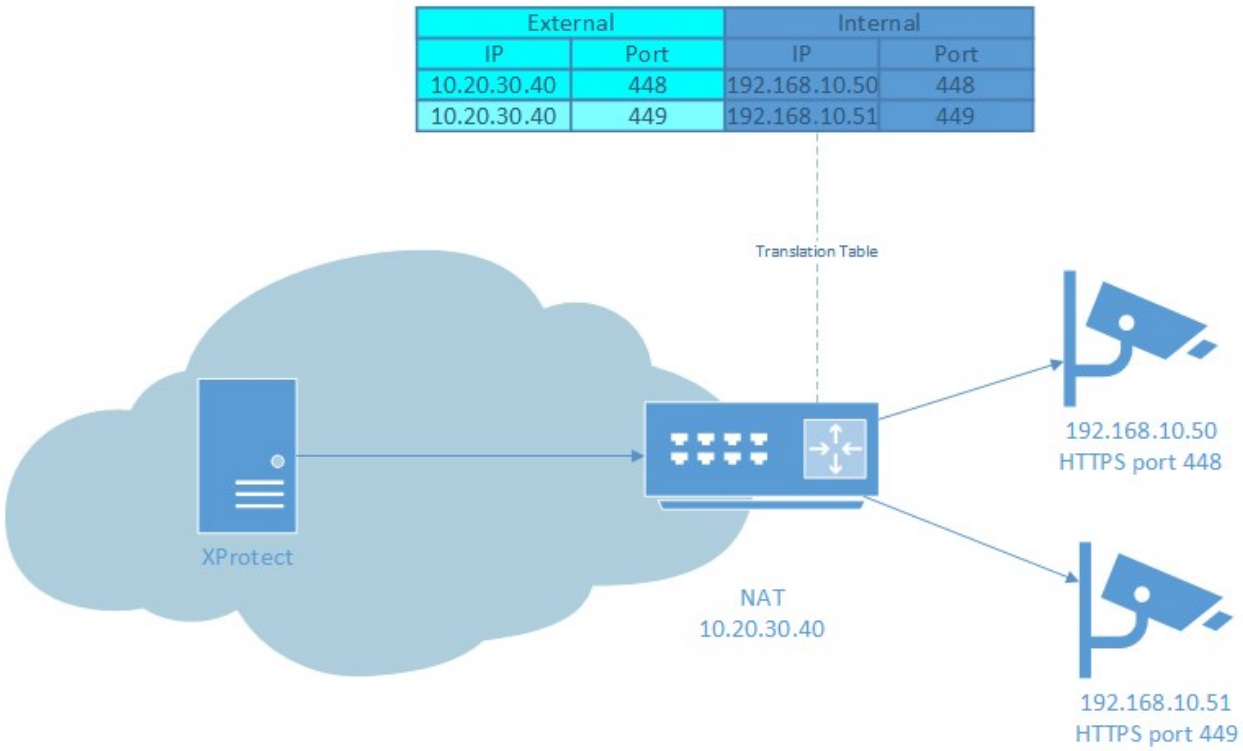
Scenario 2: Secure, everything over HTTPS

Streaming Mode: RTP/RTSP/HTTP/TCP

HTTPS: ON

Device HTTPS port must be set to forwarded port.

Forward same port number as HTTPS port on device.



This is the most robust and secure way of adding devices behind NAT in XProtect.

For more information about HTTPS and Media over HTTPS refer to section HTTPS on page 15.

Scenario 3: Unsecure, HTTP and RTSP

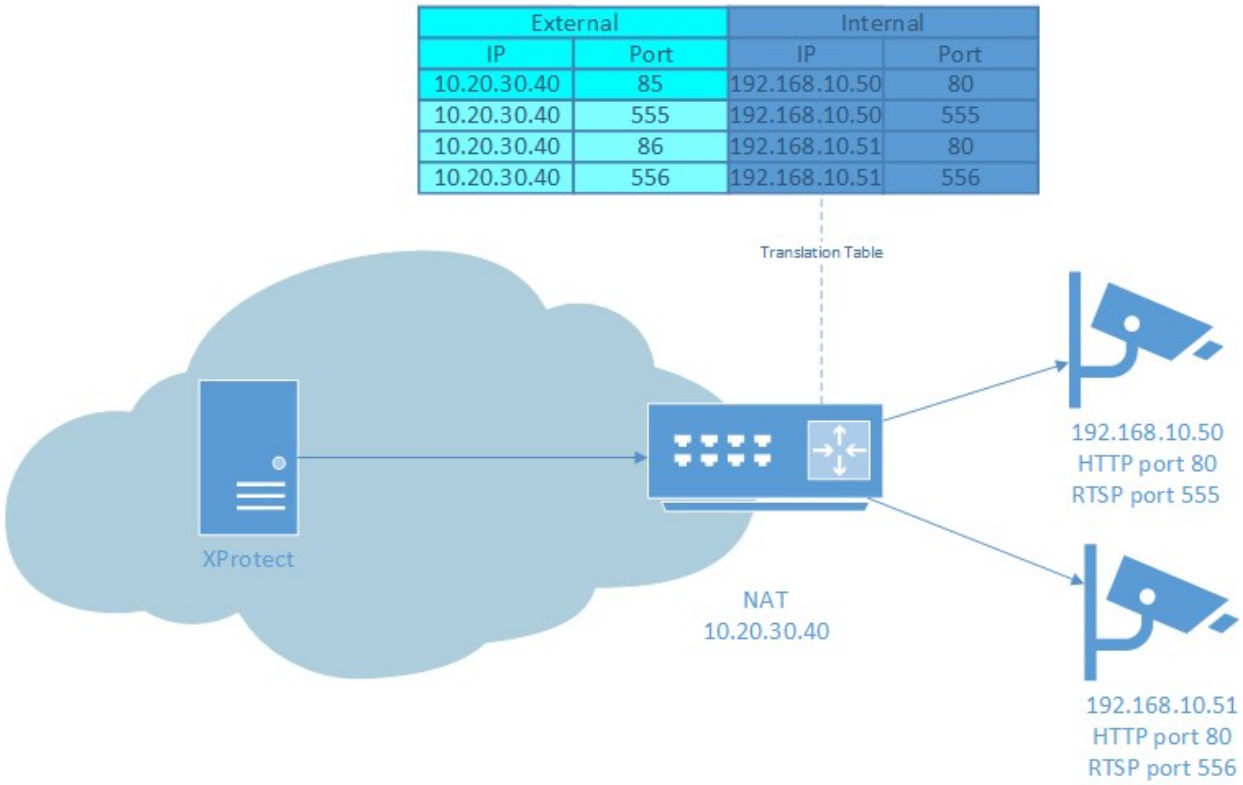
Streaming Mode: RTSP/RTP/TCP

HTTPS: OFF

Device RTSP port must be set to forwarded port.

Forward same port number as RTSP port on device.

Forward any port number to device HTTP port.

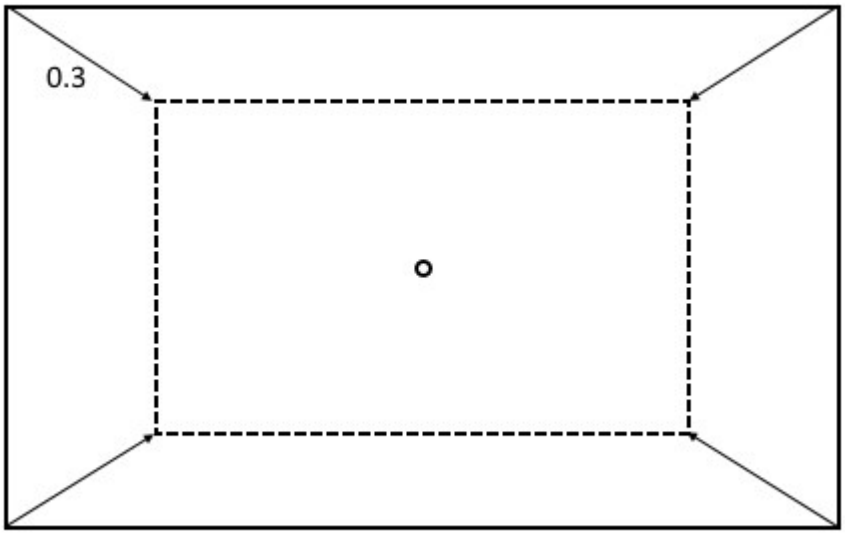


Area zoom implementation

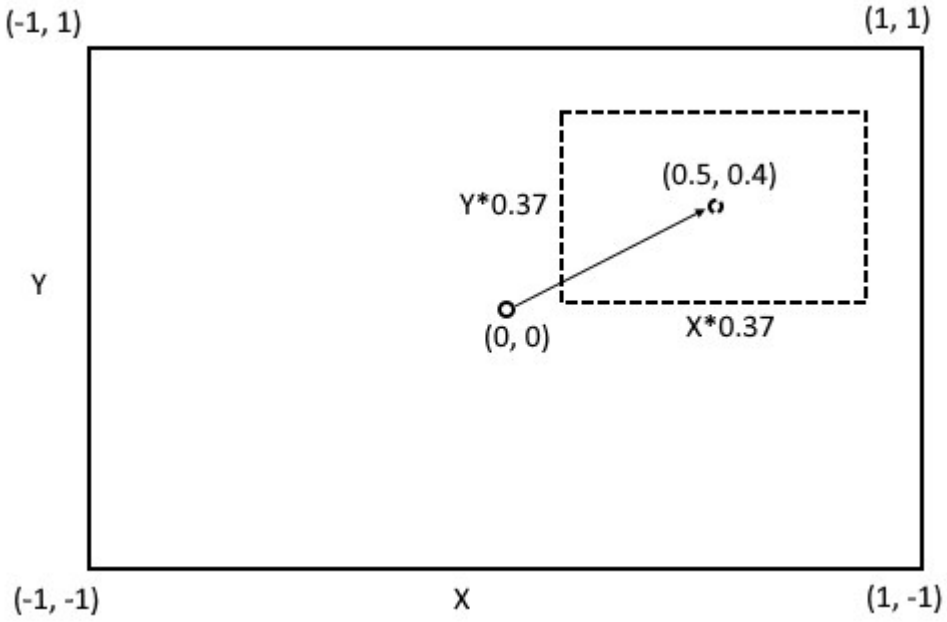
Area zoom is implemented via PTZ commands: PTZ Click-to-Move and Drag-to-Zoom. For Click-to-Move is used tag PanTilt in space PanTiltSpase/TranslationSpaceFov. For Drag-to-Zoom is used tag Zoom in space ZoomSpace/TranslateSpaceFov.

Zoom Translation Space in FOV

The Relative Zoom Translation Space in FOV is introduced to simplify the navigation and zooming with dome cameras in graphical user interfaces. When the user wants to zoom in relative to the current camera view, the user requests a movement with respect to the current FOV.



If a user wants to zoom in on a certain position in the current camera view, the Relative Zoom Translation in FOV can be combined with Relative Pan/Tilt Translation in FOV. This combination achieves the Area Zoom functionality.



The Zoom factor is the relation between the target and current view. The orientation of the target view (horizontal or vertical) determines which of the two dimensions (width or height) is used to calculate the zoom factor.

For example, if the target view is oriented horizontally (width > height), the zoom factor is based on the relation between the target view's width and the current view's width:

zoomfactor = targetview(width)/currentview(width)

If the target view is oriented vertically (height > width), then it is the height that is used:

zoomfactor = targetview(height)/current(height)

A value of 0.5 means the target view's width or height is half in relation to the current view's width or height, and an object in the target view is twice as big compared to the same object in the current view. A value of 1.0 means that the target view's width or height is the same as the current view's width or height and thus Zoom is not necessary.

Values below 1.0 specify Zoom In, values above 1.0 specify Zoom Out. (Please note that the Zoom Out values are specified only for completeness of the specification, and in XProtect it is not possible to perform Zoom Out via Area Zoom).

The following XML illustrates Area Zoom command for the transformation pictured above:

```
<tptz:RelativeMove>
 <tptz:ProfileToken>defaultPrimary</tptz:ProfileToken>
  <tptz:Translation>
   <tt:PanTilt xsi:type="tt:Vector2D" x="0.5" y="0.4"
        space="http://www.onvif.org/ver10/tptz/PanTiltSpaces/TranslationSpaceFov"/>
   <tt:Zoom xsi:type="tt:Vector1D" x="0.37"
  space="http://www.milestonesys.com/ver10/tptz/ZoomSpaces/TranslationSpaceFov"/>
  </tptz:Translation>
  <tptz:Speed>
   <tt:PanTilt xsi:type="tt:Vector2D" x="1" y="1"/>
   <tt:Zoom xsi:type="tt:Vector1D" x="1"/>
  </tptz:Speed>
</tptz:RelativeMove>
```

If a device supports the Zoom Translation Space in FOV, it must specify it in the SupportedPTZSpaces field in the GetNodeResponse and GetNodesReponse commands.

The proposed range for this relative direction space ranges from 0 to plus infinity. The relative direction space is defined as follows.

```
<tt:RelativeZoomTranslationSpace>
 <tt:SpaceURI>
  http://www.milestonesys.com/ver10/tptz/ZoomSpaces/TranslationSpaceFov
```

```
  </tt:SpaceURI>
  <tt:XRange>
    <tt:Min>0</tt:Min>
    <tt:Max>INF<tt:Max>
  </tt:XRange>
</tt:RelativeZoomTranslationSpace>
```

Change history

Document version

Ver.	Date	Section	Description	Author	
1.0	February 2018		ONVIF/ONVIF16 driver overview	Magdalena Filcheva Georgi Yanev Maxim Zapryanov Gabriela Tzanova Reem Rady	
1.1	March 2018		Edge storage for multichannel devices Info about Aux Buttons renaming	Maxim Zapryanov	
1.2	March 2018	Video Edge Storage on page 36 Audio Edge Storage on page 36 Requirements for Edge Storage on Multichannel devices. on page 84	Minor modifications.	Joanna Zdunek	
1.3	May 2018	Requirements for Edge Storage on Multichannel devices. on page 84	Add information about alternative fallback method for linking a recording to a Video/Audio source.	Maxim Zapryanov	
		Definitions on page 11	Add information about		

Ver.	Date	Section	Description	Author	
		Does the ONVIF driver support Transparent PTZ? on page 80	Transparent PTZ.		
		Does the ONVIF driver support License Plate Recognition (LPR) or Automatic Number-Plate Recognition (ANPR)? on page 80	Add question about LPR/ANPR.		
		Does the ONVIF driver support B-frames? on page 80	Add question about B-frames.		
		HTTPS on page 15	Reorganize section. Add clarification for Audio OUT (audio backchannel) over HTTPS.		
		Audio Edge Storage on page 36	Add information for version requirements for Audio Edge Storage		
		Auxiliary on page 44	Additional information about types of commands that the driver accepts and assigned to the buttons in Smart Client	Magdalena Filcheva	
		Events on page 50	Type of event's negation		
		Line Crossed on page 59	Add new schema for Line crossed event		
		Intrusion Detector on page 61	Add new schema for Field detector event		

Ver.	Date	Section	Description	Author	
1.4	August 2018	RTP/RTSP/HTTP/TCP Video stream settings on page 28	Clarify multicast address setting	Magdalena Filcheva	
			Specify the default value and streaming method for Keep alive type setting		
		Audio IN/OUT on page 31	Add new value for audio bitrate (48 kbps)		
		Events on page 50	The value type (source) add and describe		
		Object counting on page 64	Add event “Object counting”		
		Recordings Available on page 66	Add event “Recordings Available”		
		SD Card error on page 67	Add event “SD Card error”		
		General device settings on page 14	Add “HTTPS Validate Certificate” and “HTTPS Validate Hostname” options	Maxim Zapryanov	
		HTTPS Certificates on page 17	Add new section for HTTPS Certificates		
1.5	January 2019	Tampering on page 56	Add new schema for Tampering event	Magdalena Filcheva	
		SD Card Mounted on page 66	Add new event SD Card Mounted		

Ver.	Date	Section	Description	Author	
			Fix grammar	Maxim Zapryanov	
		Standard References on page 12	Add new section “Introduction”		
		Does the ONVIF driver support HLS? on page 80	Add question about HLS.		
		Does the ONVIF driver support MP4 or MKV containers? on page 80	Add question about supported containers.		
		Metadata on page 37	Add requirements for metadata channel to be shown in Management Client		
		Metadata on page 37	Add note about handling of metadata in streaming XMLs		
		Audio IN/OUT on page 31	Add note about Audio Out for multicast streaming and RTSP over HTTP.		
		Relay outputs on page 40	Add section for Relay outputs		
1.6	July 2019	Detect Sound on page 58	Detect Sound Event New attribute values for the Source No more valid note: “The ONVIF driver cannot detect which audio source is triggering the event.”	Magdalena Filcheva	
		Media service on page	Add a note about Media Service		

Ver.	Date	Section	Description	Author	
		25	and older Device Packs		

Ver.	Date	Section	Description	Author	
		HTTPS on page 15	HTTPS port is now read from the device when possible.	Maxim Zapryanov	
		HTTPS on page 15	Add information about usage of “HTTPS Validate Certificate” and “HTTPS Validate Hostname” options.		
		Auxiliary on page 44	Add information Aux Commands in the Device Service (Available in ONVIF driver in Device Pack 10.3) Also add clarifications and fix inconsistencies in the text		
		Retrieval of remote recordings (Edge storage) on page 35	Add clarification about needed ONVIF services for Edge Storage support		
		ONVIF conformance on page 8	Update with information about certification with latest ONVIF Client Test Tool 18.12 rev.2606		
		Metadata on page 37	Update screenshot of metadata settings		
		Detect Sound on page 58	Detect Sound Event – add new scheme		
		What is ONVIF? on page 7	New Introduction and scope. What is ONVIF? And Milestone ONVIF drivers	Magdalena Filcheva	
		Brute Force Attack on page 67	Add event “Brute Force Attack”		
		Cyber Attack on page 68	Add event “Cyber Attack”		

Ver.	Date	Section	Description	Author	
		Quarantine on page 68	Add event “Quarantine”		
		Audio IN/OUT on page 31	Splitting Audio IN/OUT settings in two different sections		
		Metadata on page 37	Add new metadata stream settings ‘PTZStatus’, ‘Events‘, ‘Analytics‘.		
		Tampering on page 56	Add new schema for Tampering		
		Detect Sound on page 58	Extend the "Trigger/VolAlarm" schema with Data 1		
		Line Crossed on page 59	Add new schema for Line Crossed		
		Temperature on page 64	Add new schema for Temperature		
		Temperature on page 64	Add new schema for Fire		
1.7	November 2019	Metadata on page 37	Changed default values for streaming method to RTP/UDP	Magdalena Filcheva	
		Audio IN/OUT on page 31	Add new “Buffer size” setting for Audio Out		
		Why the ONVIF driver does not send PTZ Stop command? on page 80	Add FAQ about PTZ Stop command	Maxim Zapryanov	
		Standard References on page 12	Update references to used specifications		

Ver.	Date	Section	Description	Author	
		Events on page 50	Add note about SetSynchronizationPoint		
		Video settings on page 26	OSD – add settings and description		
		PTZ on page 42	Add information about the supported PTZ spaces		
1.7.1	November 2019	Temperature on page 64	Add new thermal events	Magdalena Filcheva	
1.8	March 2020	Standard References on page 12	Update to ONVIF Service Specification 19.12	Maxim Zapryanov	
		ONVIF conformance on page 8	Update with information about conformance with Profiles S, T, G and Q		
		Metadata Edge Storage on page 37	Add information about Metadata Edge Storage support		
		Video Edge Storage on page 36	H.265 video edge storage support	Margarit Nikolov	
		Retrieval of remote recordings (Edge storage) on page 35	Add section explaining handling of timestamps during Edge Retrieval	Georgi Georgiev	
1.8.1	April 2020	Milestone ONVIF drivers on page 7 Which ONVIF Profiles does the ONVIF driver support? on page 79	Update with Profiles S, T, G and Q	Maxim Zapryanov	
		What is ONVIF? on	Add information about ONVIF		

Ver.	Date	Section	Description	Author	
		page 7	trademark		
1.9	June 2020	Edge Storage retrieval workflow on page 83	Update Edge retrieval diagram to show that the result of GetRecordingSummary is ignored	Gabriela Tzanova	
		Audio IN/OUT on page 31 Audio Backchannel codec selection on page 88	Update Audio Out section and add new section explaining the backchannel codec selection process.	Maxim Zapryanov	
		Auto Tracker on page 68	Add event “Auto Tracker”	Gabriela Tzanova	
1.10	August 2020	Overview of the factory default state on page 73	Add information about Factory Default state and Profile Q	Maxim Harizanov	
1.11	November 2020	Overview of firmware update on page 76	Add new section for firmware upgrade functionality	Maxim Harizanov	
		Intrusion Detector on page 61	Rename “Field Detector” to “Intrusion Detector” and add two new schemas for detection – IntrusionStarted and IntrusionEnded	Maxim Zapryanov	
		Crowd Detection on page 69 Running Detection on page 69	CrowdDetection and RunningDetection events are added with Vivotek schema	Dayana Hristova	
		Home position on page 43	Add information about the command used for home position	Maxim Zapryanov	

Ver.	Date	Section	Description	Author	
1.12	December 2020	Detecting firmware update support on page 76	Add information about when to use Tampering Start and Tampering End events instead of just Tampering event	Magdalena Filcheva	
		Audio IN/OUT on page 31	Change Audio In settings of Encoding and bitrate to a combined setting of Codec/Bitrate/Samplerate	Maxim Zapryanov	
1.13	February 2021	Does the ONVIF driver work with devices behind NAT and when port forwarding is used? on page 81 Configuration of devices behind NAT and port forwarding on page 89	Add new FAQ about devices behind NAT and add new section describing the different possible scenarios	Maxim Zapryanov	
1.14	August 2021	Line Crossed on page 59 Intrusion Detector on page 61 Crowd Detection on page 69 Running Detection on page 69	Added new Source column for Intrusion and Line Crossed events to reflect the added windowed schema for Vivotek Changed Crowd and Running detection event window parameter	Georgi Yanev	
		Motion on page 54 Detect Sound on page 58 Line Crossed on page 59	Added Vicon special events support for Motion Detection, Sound Detection, Line crossed, Intrusion, Abandon Detection, Missing Detector, Loitering, Face Detection, Object Count and	Dayana Hristova	

Ver.	Date	Section	Description	Author	
		Intrusion Detector on page 61 Abandoned Detector on page 62 Missing Detector on page 62 Loitering Detector on page 63 Face on page 64 Object counting on page 64 Crowd Detection on page 69	Crowd Detection		
		Motion on page 54 Detect Sound on page 58 Missing Detector on page 62 Object counting on page 64	Added Pelco special events support for Adaptive Motion/Directional Motion, Audio Detection, Object Removed and Object Count	Dayana Hristova	
		Audio IN/OUT on page 31	Audio Encoder configuration is added by the driver, if there is at least one in the camera, but there isn't any associated with the Media Profiles.	Dayana Hristova	
			Fix references to Management Client	Maxim Zapryanov	
1.15	August 2021	Video settings on page 26	Updated Video Settings with PTZ Zoom Step setting description	Gabriela Tzanova	

Ver.	Date	Section	Description	Author
		Video settings on page 26	Add information about PTZ Zoom Step value of zero	Maxim Zapryanov
	September 2021	Audio IN/OUT on page 31	Added supported by ONVIF driver codecs for Audio In and Audio Out	Dayana Hristova
	October 2021	Missing Detector on page 62 Loitering Detector on page 63 Object counting on page 64 Stopped Vehicle Detection on page 70	Added New Pelco events for Object Missing, Loitering, Object Counting, Stopped Vehicle	Georgi Yanev
1.16	December 2021	Overview of dynamic events on page 71	Added new section “Dynamic events“ after the Events section effectively moving all following sections with one move index forward.	Georgi Yanev
		Home position on page 43	Clarify PTZ Home Position support by devices.	Maxim Zapryanov
		Tampering on page 56 Video Loss on page 58	Added ONVIF Specification Tampering schemes for “GlobalSceneChange” / “ImageTooDark” / “ImageTooBlurry” / “ImageTooBright” Added ONVIF Specification VideoLoss scheme for “SignalLoss”	Georgi Yanev

Ver.	Date	Section	Description	Author
		ONVIF conformance on page 8	Add Profile M	Maxim Zapryanov
		Area Zoom on page 43 Area zoom implementation on page 93	Area Zoom Area zoom implementation	Georgi Georgiev
1.17	May 2022	General device settings on page 14	Add note about switching to Media 1 and H.265 codec	Maxim Zapryanov
1.18	August 2022	Audio IN/OUT on page 31	Added supported by ONVIF driver codecs for Audio In and Audio Out	Iliyan Ruykov
	October 2022	ONVIF PTZ Configurations on page 43	Add section about ONVIF PTZ Configurations	Maxim Zapryanov
	November 2022	ONVIF16 driver on page 10	Update information on ONVIF Driver and multichannel devices	Maxim Zapryanov
1.19	April 2023	Does the ONVIF driver support B-frames? on page 80	Updated information on support of B-frames in XProtect and ONVIF driver	Gabriela Tzanova
1.20	May 2023	Retrieval of remote recordings (Edge storage) on page 35 PTZ on page 42 Setup of Aux buttons in the Smart Client on page 46	Updated screenshots	Petko Petrov
1.21	July 2023	Does the ONVIF driver	Updated information on support	Gabriela Tzanova

Ver.	Date	Section	Description	Author
		support B-frames? on page 80	of B-frames in XProtect and the ONVIF driver	
	August 2023	Milestone ONVIF drivers on page 7 ONVIF conformance on page 8	Update language around ONVIF conformance	Maxim Zapryanov
	November 2023	Video settings on page 26	Add information about new general setting “PTZ send zoom parameter”	Gabriela Tzanova
1.22	December 2023	Area zoom implementation on page 93	Add more details to the “Zoom Translation Space in FOV” section. Change in the proposed space URI name.	Gabriela Tzanova
1.23	June 2024	Overview of the factory default state on page 73 Which ONVIF Profiles does the ONVIF driver support? on page 79	Added disclaimer for Profile Q support	Gabriela Tzanova
1.24	September 2024	About this document on page 7 ONVIF16 driver on page 10	Added new section “About this document”. Updated information about the availability of ONVIF16 driver	Gabriela Tzanova

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.