

ONVIF Device Manager



User Guide

1. Introduction

1.1 Intended Use

ONVIF Device Manager is a software application used to administrate network video servers and cameras within CCTV systems. The User Guide describes the product installation, video encoder, network and analytics configuration, the software update and troubleshooting. Thus, the document is intended for the personnel responsible for administrating CCTV systems and separate network video surveillance devices with the help of ONVIF Device Manager.

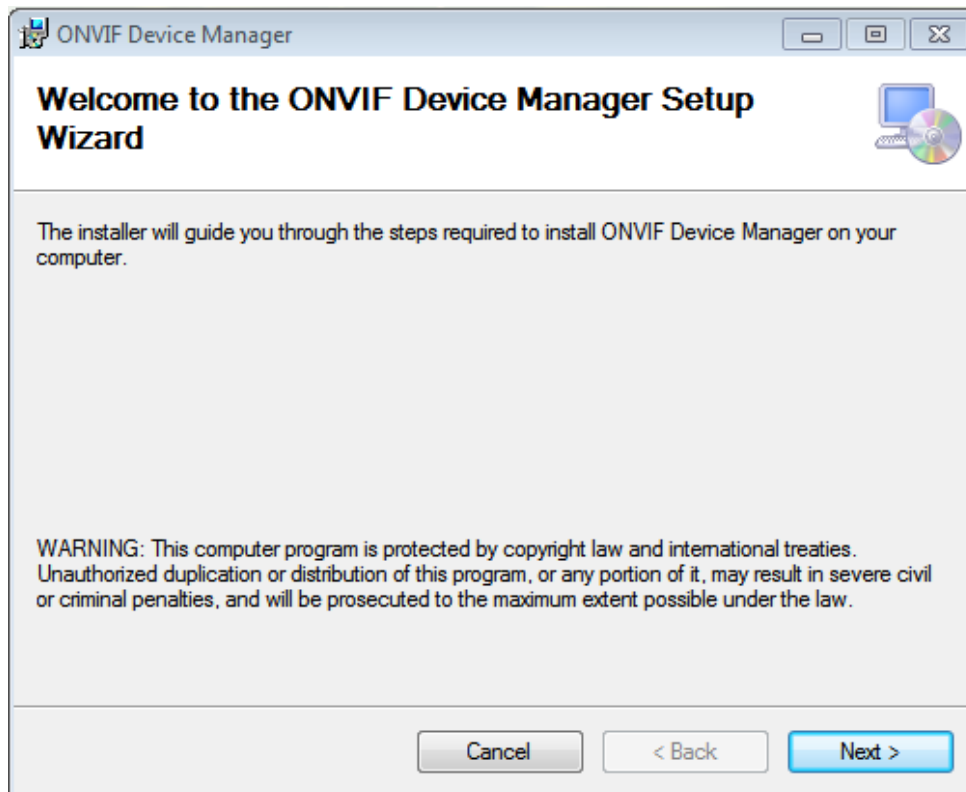
1.2 System Requirements

- Windows XP SP3 operation system (or higher; Windows 7 recommended)
- Microsoft .NET Framework 4
- 1 Gb RAM (2 Gb recommended)
- 40 Mb of free drive space

2. Installing and Getting Started

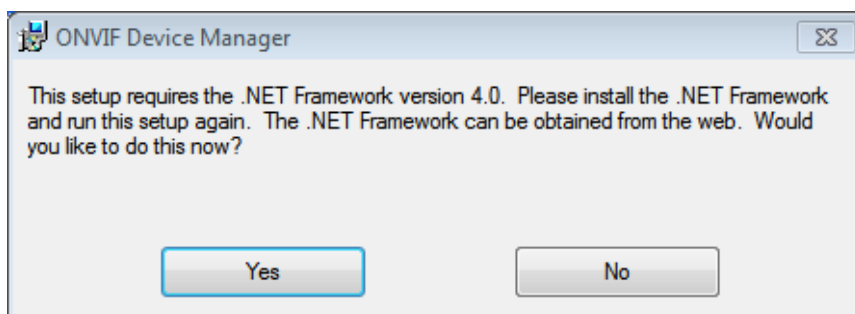
2.1 ONVIF Device Manager Setup

1. Download [onvifdm.msi](http://synesis.ru/ru/surveillance/downloads) setup-file from Synesis or SourceForge (<http://sourceforge.net/projects/onvifdm/>) web site.



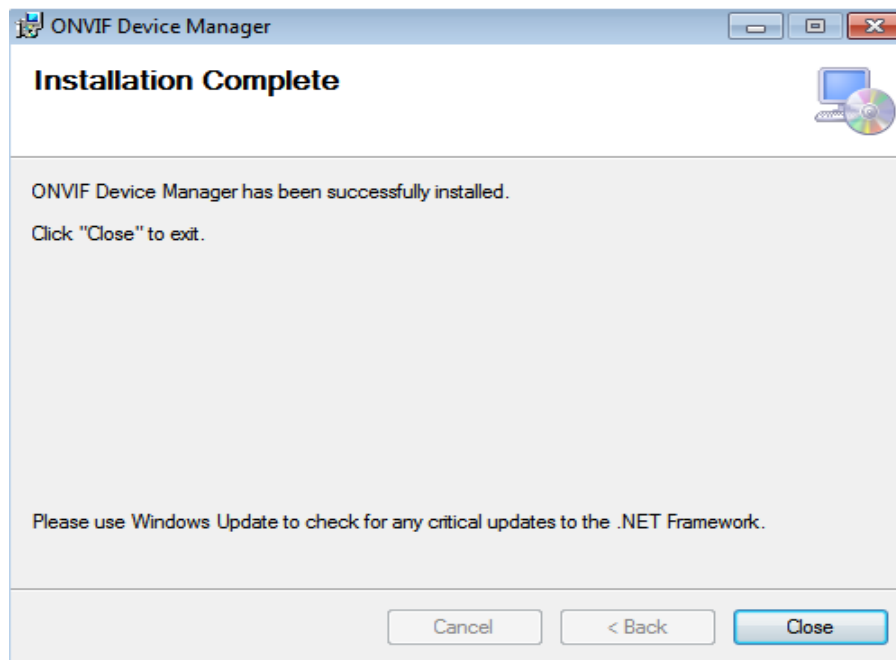
2. Run onvifdm.msi.

Setup Wizard will check if Microsoft .NET Framework 4 is installed to the computer. If it is absent, the following message is displayed.



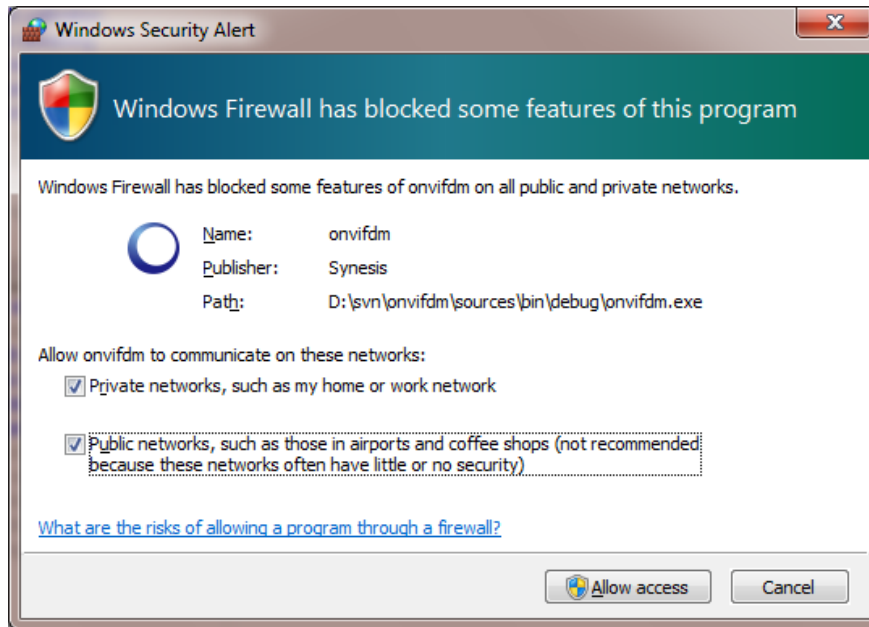
3. Click Yes. You will be redirected to <http://www.microsoft.com/>.

4. Download *dotNetFx40_Full_setup.exe* and install .NET Framework according to the setup instructions.
5. After Microsoft .NET Framework 4 setup run *onvifdm.msi* again.
6. Windows User Account Control may ask for the permission to continue the installation. Click Yes.
7. To complete ONVIF Device Manager installation process, click *Close*.




2.2 Starting ONVIF Device Manager

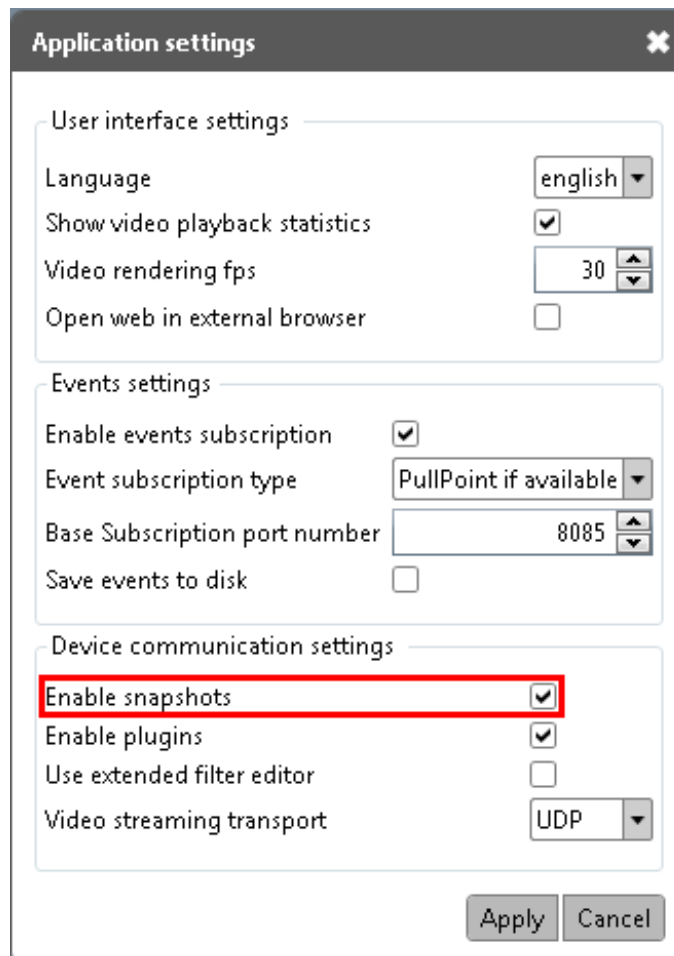
1. Launch ONVIF Device Manager from the desktop or *Start* menu.
2. During the first launch, Windows Firewall may ask for the permission to open access to the network for onvifdm.exe. Click *Allow access*.



3. After ONVIF Device Manager has been launched, your device is automatically detected and displayed at the end of the device list on the left. If the device has not been detected automatically, check the connection and click *Refresh*.



4. To make sure the device is selected correctly, check live video snapshots from the active video channels. If the snapshots are not displayed, check *Enable snapshots* in *Application Settings* ( button).



The screenshot shows the 'Application settings' dialog box with three sections: 'User interface settings', 'Events settings', and 'Device communication settings'. The 'Enable snapshots' checkbox in the 'Device communication settings' section is highlighted with a red rectangle.

Section	Setting	Value
User interface settings	Language	english
	Show video playback statistics	<input checked="" type="checkbox"/>
	Video rendering fps	30
	Open web in external browser	<input type="checkbox"/>
Events settings	Enable events subscription	<input checked="" type="checkbox"/>
	Event subscription type	PullPoint if available
	Base Subscription port number	8085
	Save events to disk	<input type="checkbox"/>
Device communication settings	Enable snapshots	<input checked="" type="checkbox"/>
	Enable plugins	<input checked="" type="checkbox"/>
	Use extended filter editor	<input type="checkbox"/>
	Video streaming transport	UDP

Buttons: Apply, Cancel

3. Application Configuration

3.1 Video Server Identification

1. Click on the device.
2. Select *Identification* at the top of the menu list.
3. Check that *Device ID* value coincides with its serial number.
4. Fill in *Name* and *Location* fields.
5. Click *Apply*. Your settings are saved.



Identification tab contains URI parameter necessary for connecting the device to a video management system.

The screenshot displays the configuration page for device MB-2. On the left, there is a menu with options: Identification (highlighted in red), Time settings, Maintenance, Network settings, User management, Certificates, System log, Relays, Web page, and Events. Below the menu is a 'NVT' section with a 'Refresh' button and a video source label 'VIDEO_SOURCE_0: CH-A-H264'. A live video feed is visible at the bottom left. The main 'Identification' tab on the right contains the following fields:

Name	MB-2
Location	country/undefined; city/undefined
Manufacturer	Synesis
Model	MB-2
Hardware	1.0.6
Firmware	1287.5700
Device ID	000000000000000DF
IP address	192.168.3.55, 169.254.223.135
MAC address	CC-EE-99-66-EE-11
ONVIF version	2.20
URI:	https://192.168.3.55/onvif/device_service

At the bottom right of the Identification tab, there are 'Apply' and 'Cancel' buttons.

3.2 Time Settings

For correct functioning of access management system, it is necessary to synchronize the time on the device and on the user's computer. If the device is equipped with a real-time clock with independent power supply, the time is synchronized automatically.

For video servers and cameras not equipped with an RTC-clock or independent power supply, it is necessary to select *Synchronize with NTP server* option. Otherwise, in case of power cut the time on the device is reset, and it is impossible to access the device from the PC.

Time settings

Current time 18:23:40 22.08.2012 (Local)

Time zone:

std-4 ...

Automatically adjust for daylight saving time changes.

Time settings:

Synchronize with NTP server

Please go to [Network settings link](#) to set up NTP servers

Apply Cancel

3.3 Network Settings

Select Network Setting from the device menu. By default, the settings are the following.

Network settings

DHCP:	<input type="text" value="On"/>	
IP Address:	<input type="text" value="192.168.3.55"/>	
Subnet mask:	<input type="text" value="255.255.248.0"/>	
Default gateway:	<input type="text" value="192.168.1.2"/>	
<hr/>		
Host name:	<input type="text" value="DHCP"/> <input type="text" value="MB-2-00DF"/>	
DNS:	<input type="text" value="DHCP"/> <input type="text" value="8.8.8.8"/>	
NTP servers:	<input type="text" value="Manual"/> <input type="text" value="0.pool.ntp.org; 1.pool.ntp.org; 2.pool"/>	
<hr/>		
HTTP ports:	<input type="text" value="Enable"/> <input type="text" value="80"/>	
HTTPS ports:	<input type="text" value="Enable"/> <input type="text" value="443"/>	
RTSP ports:	<input type="text" value="Enable"/> <input type="text" value="554"/>	
<hr/>		
Enable zero config:	<input checked="" type="checkbox"/> <input type="text" value="169.254.223.135"/>	
ONVIF discovery mode:	<input type="text" value="Discoverable"/>	
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

3.3.1 Settings for a Network with DHCP Server

Nowadays, most networks are equipped with a DHCP server which automatically assigns an IP-address to devices connected. In this case fields *IP Address*, *Subnet Mask* and *Default Gateway* are filled automatically and uneditable.

1. *Host name*, *DNS* and *NTP servers* can either be received from DHCP or entered manually. Select the option you need.
2. After all the settings are selected, click *Apply*.
3. Wait until the device reboots.

3.3.2 Settings for a Network without DHCP Server

If the network has no DHCP server, the device IP address is determined automatically via ZeroConf protocol (*Enable zero config* option is checked by default).

1. In **computer's** network settings select *Receive IP address automatically*. (If a static IP address is selected, the video server will not be shown in the device list as belonging to another network).
2. In order to assign the device a static IP address (eg., in a network without DHCP server), select *Off* in *DHCP* dropdown. After that fields *IP address*, *Subnet mask* and *Default gateway* are possible to edit manually.
3. Fill in fields *Host name*, *DNS* and *NTP* servers manually.
4. Specify other settings and click *Apply*.
5. Wait until the device reboots.

3.3.3 Discovering device in a network

To make device function without being discovered in the network, select *non discoverable* option as *ONVIF discovery mode*.

To make it visible in the list select *discoverable*.

3.3.4 Additional Settings

In most cases a video analytical device is connected to a local network and has a local IP address. In order to get access to the device beyond the local network, or to connect it directly to the Internet, the following settings are necessary.

1. Go to *Web page* to *Network* tab.
2. Check *Enable NAT traversing*.
3. Enter Global IP address.
4. Specify NAT ports and click *Apply*.

The screenshot shows the 'Web page' interface with the 'Network' tab selected. The URL bar displays 'https://192.168.3.55/params/nat.cgi'. The 'Network' section includes a checked checkbox for 'Enable NAT traversing', a 'Global IP address' field with the value '172.16.1.2', and a 'NAT port mapping' section with fields for 'HTTP port' (80), 'HTTPS port' (443), 'RTSP port' (554), and 'FTP port' (21). At the bottom, there are 'Apply' and 'Cancel' buttons.

3.4 User Management

ONVIF Device Manager supports the following types of users.

Anonymous user is not registered in the system and, therefore, can have unlimited access only to those devices from the list where no users from other categories ("user", "operator", "administrator") are registered. On the devices with at least one abovementioned user, anonymous user has right only to view time settings.

Administrator has access to **all** application sections and features, the rights to reboot the device, reset the settings and update the firmware, create other users with different access rights.



The first user on the device must be created as Administrator.

For the differences in Operator's and User's access rights (by default), consult the table on the following page.

CHANGE – the right to change current and create new settings.

VIEW – the settings are not hidden, but it is not permitted to change and create them.

HIDDEN – Certain settings or even the whole section is hidden.

Application section or feature	Operator	User
Identification	VIEW	HIDDEN
Time Settings	VIEW	VIEW
Maintenance		
Configuration backup	HIDDEN	HIDDEN
Configuration restore	HIDDEN	HIDDEN
Soft factory reset	HIDDEN	HIDDEN
Hard factory reset	HIDDEN	HIDDEN
Device Reboot	CHANGE	HIDDEN
Firmware update	HIDDEN	HIDDEN
Network Settings	VIEW	VIEW
Users	HIDDEN	HIDDEN
Certificates	VIEW	VIEW
System Log	HIDDEN	HIDDEN
Relays Settings	CHANGE	VIEW
Web Page	CHANGE	
Events (including filter management)	CHANGE	CHANGE
Live Video (including rtsp-link)	CHANGE	CHANGE
Video Streaming	CHANGE	VIEW
Analytics		
Object tracking	CHANGE	VIEW
Depth calibration	CHANGE	VIEW
Service detectors	CHANGE	VIEW
Antishaker	CHANGE	VIEW
Annotation settings	CHANGE	VIEW
Rules	CHANGE	VIEW
Metadata	CHANGE	VIEW
Profiles	CHANGE	VIEW
Settings (Kipod Server)	CHANGE	VIEW

3.4.1 Creating Users

1. To create a new user go to *User management* tab and click *Create*.

The screenshot shows the 'User management' interface. At the top, there are buttons for 'Policies: Backup', 'Restore', and 'Edit'. Below that, a 'Users:' section lists three users:

Name:	Password:	Role:
Mr.White		Administrator
Mr.Black		Operator
Mr.Gray		User

At the bottom right, there are buttons for 'Create', 'Modify', and 'Delete'. The 'Create' button is highlighted with a red box.

2. In the next window specify User name, password (2 times), and his role in the system (administrator, operator or user). Click *Apply*.

The screenshot shows the 'User management' interface with the user creation form. The fields are:

- Name: Mr. White
- Password: 123456
- Repeat password: 123456
- Role: Administrator (dropdown menu)

At the bottom right, there are buttons for 'Apply' and 'Cancel'. The 'Apply' button is highlighted with a red box.



The first user on the device must be created as Administrator.

The following message is displayed, and the user is added to the list.

The screenshot shows a success message in the 'User management' interface:

i User has been created successfully. Please notice that it may affect security aspects and device will be inaccessible in current session.

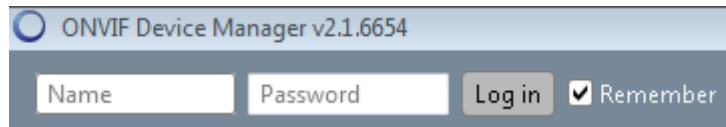
At the bottom right, there is a 'Close' button.

To edit user data, use *Modify* button.

To delete a user, click *Delete*.

3.4.2 Login

1. After launching ONVIF Device Manager, enter user name and password in the corresponding fields at the left upper corner of the window.



ONVIF Device Manager v2.1.6654

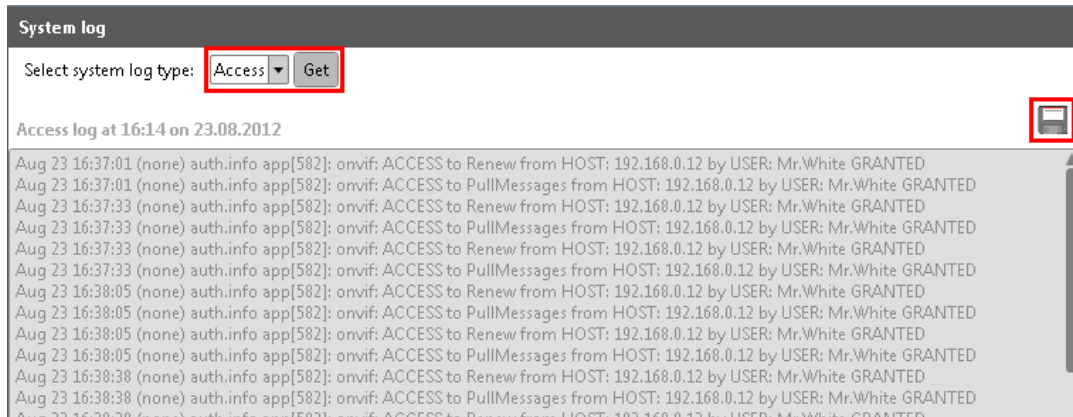
Name Password Log in Remember

2. To remember login and password for the next application launch, check *Remember* before logging in.

3.4.3 Viewing Device User Data

Administrator can view the data about device users.

1. Open *System Log* tab.
2. Select *Access* as log type and click *Get*.



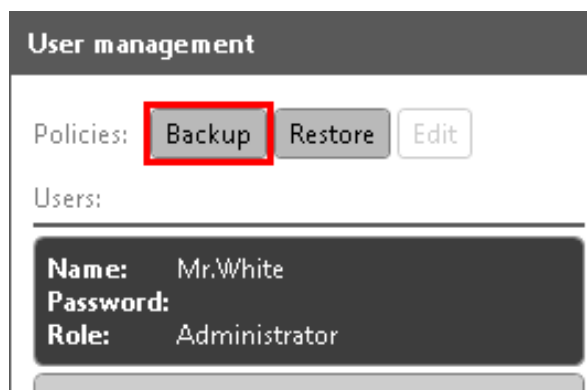
3. To save the log to a separate file use *Save* button at the right corner.

3.4.4 Changing Default User Settings

The list of rights assigned to each user category is possible to edit. For this purpose, device settings are saved in a text file containing program code. The file is edited and imported back to the system.

We strongly recommend that this operation is fulfilled by qualified personnel or our customer service specialists.

1. In order to save the current user settings to a file, go to *User Management* tab.
2. Click *Backup* in *Policy* section. File save dialogue will open to save the current settings to a .txt file.



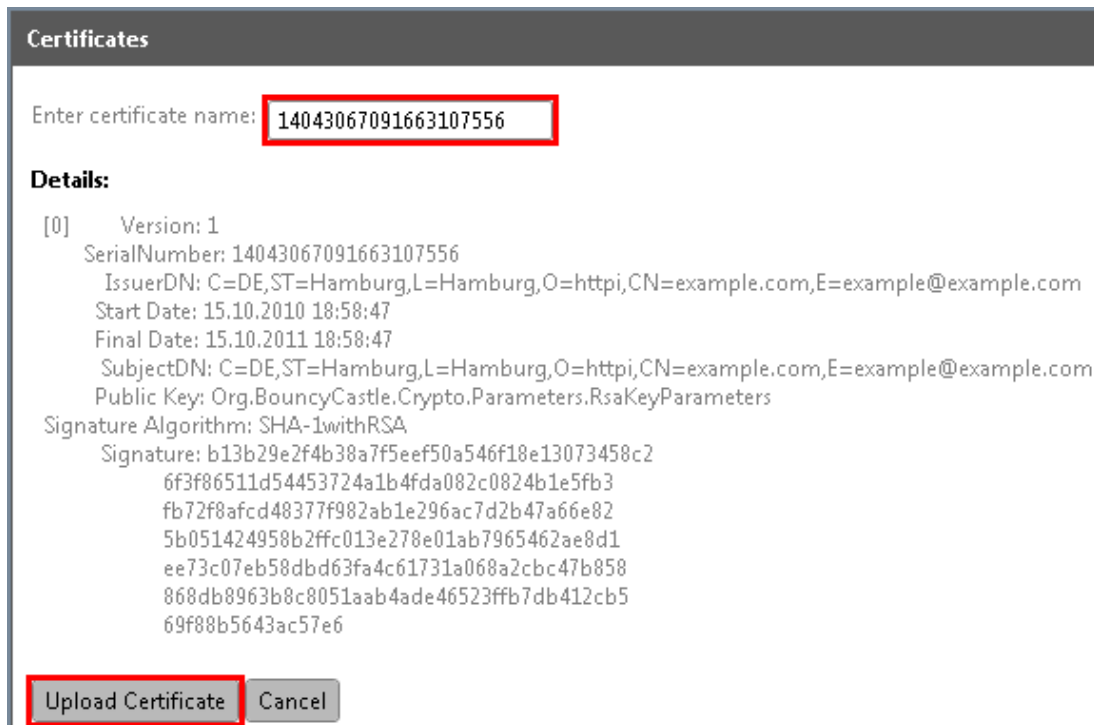
3. Edit the file the way you need.
4. In order to upload the edited file, click Restore and select the file on your hard drive.

3.5 Certificates

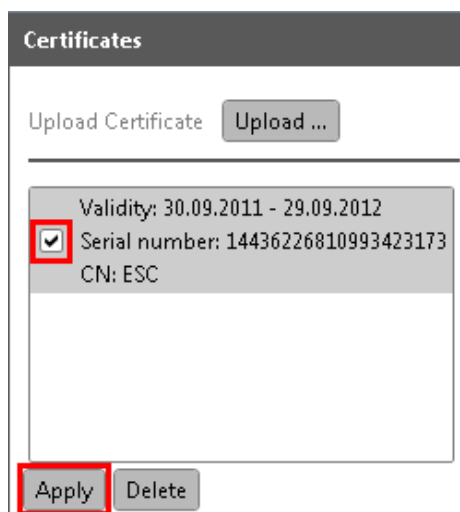
Safety certificates allow you to transfer data via a safe connection.

3.5.1 Certificate Upload

1. To upload a certificate click *Upload*.
2. Select the certificate file from your hard drive (.pem).
3. Enter certificate name and click *Upload Certificate*.



4. Check the certificate and click *Apply*.



5. For the correct functioning of the certificate, go to *Network Settings* and enable HTTPS protocole.

6. Click *Apply* to save the settings.

Network settings

DHCP:	<input type="text" value="Off"/>
IP Address:	<input type="text" value="192.168.0.48"/>
Subnet mask:	<input type="text" value="255.255.248.0"/>
Default gateway:	<input type="text" value="192.168.1.2"/>
<hr/>	
Host name:	<input type="text" value="Manual"/> <input type="text" value="MB-2-00DF"/>
DNS:	<input type="text" value="Manual"/> <input type="text" value="192.168.1.8; 192.168.1.16"/>
NTP servers:	<input type="text" value="Manual"/> <input type="text" value="0.pool.ntp.org; 1.pool.ntp.org; 2.pool"/>
<hr/>	
HTTP ports:	<input type="text" value="Enable"/> <input type="text" value="80"/>
HTTPS ports:	<input type="text" value="Enable"/> <input type="text" value="443"/>
RTSP ports:	<input type="text" value="Enable"/> <input type="text" value="554"/>
<hr/>	
Enable zero config:	<input checked="" type="checkbox"/> <input type="text" value="169.254.17.148"/>
ONVIF discovery mode:	<input type="text" value="Discoverable"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

3.5.2 Deleting a Certificate

1. Disable HTTPS protocols in network settings.
2. In *Certificates* tab check the certificate and click *Delete*.

3.6 Relays Settings (optionally)

Relays tab contains information on all the relays connected to the device.

The screenshot shows the 'Relays' configuration window. On the left, under 'Digital outputs (relays)', there is a list with 'RELAY0' selected and 'RELAY1' below it. On the right, under 'Relay options:', the 'Relay token' is set to 'RELAY_0'. The 'Relay mode' is a dropdown menu set to 'Bistable'. The 'Relay idle state' is a dropdown menu set to 'open'. The 'Delay time' is a text input field containing '30'. Below these fields is a 'Set' button. At the bottom, under 'Relay state:', there are two buttons: 'Activate' and 'Deactivate'.

To configure a relay, perform the following actions:


1. Select a relay from the list on the left.
2. Set relay mode, idle state and delay time.
3. Click *Set*.

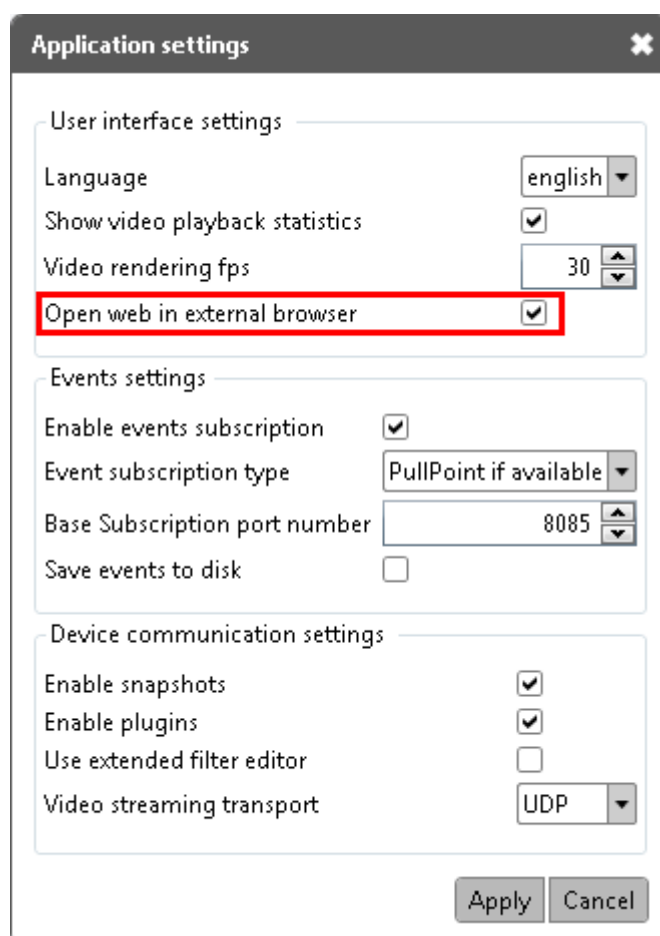
To activate or deactivate the relay use the corresponding button.

3.7 Web Page

The appearance and functionality of the web page depends on the device connected and its manufacturing company. For this reason, this section cannot be described within the current document.

Functionalities of devices by Synesis represented on the web page are described in relevant sections of the User Guide.

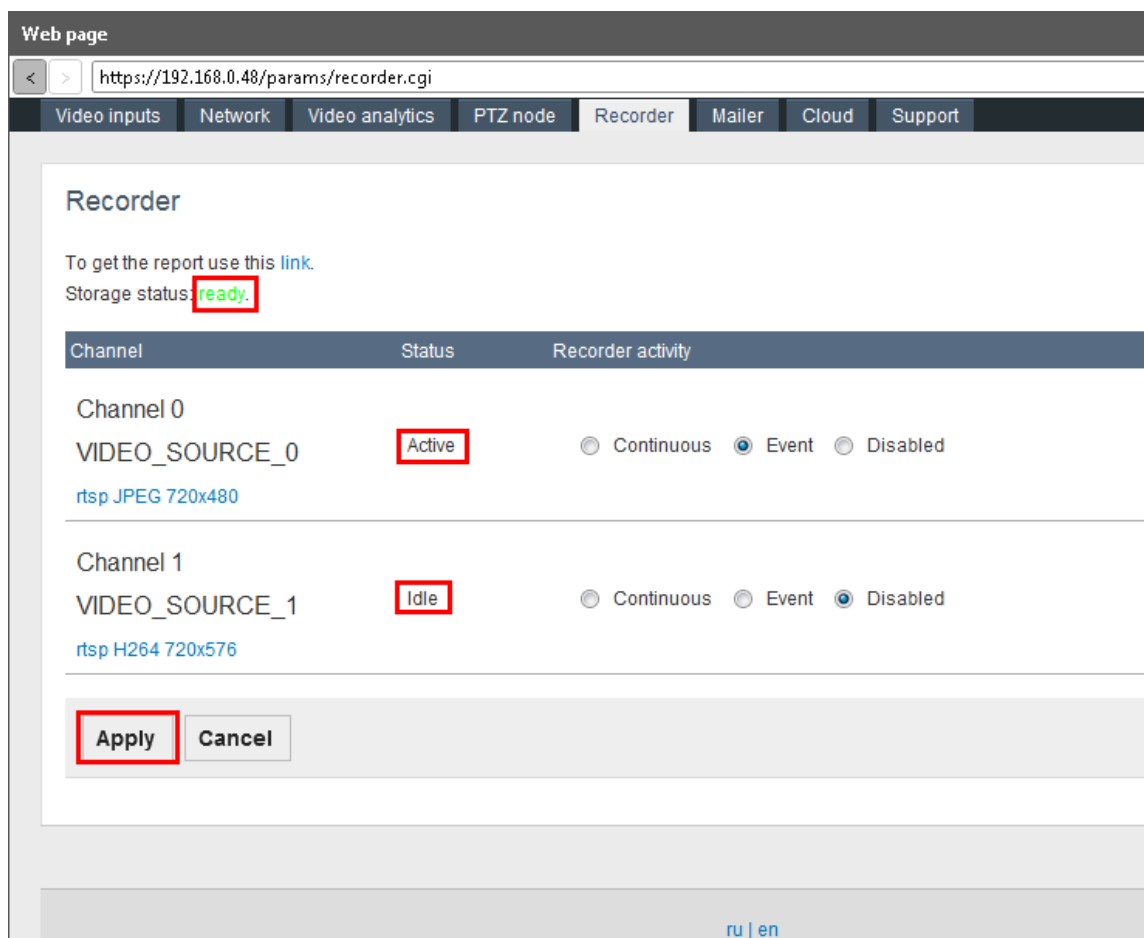
To open the web page in a separate browser, check *Open web in external browser* in *Application settings* ( button).



3.8 Recording to a Removable Storage Device

3.8.1 Recording Settings

1. Go to *Web page* to *Recorder* tab.



2. Connect a USB storage device to the video server and wait until its status changes to *Ready*.

3. Select *recorder activity* type for each video channel: *Continuous* or *Event*.

Continuous recording is performed in continuous mode regardless to video analytics events. When the removable storage memory is full, the oldest recordings are removed automatically, releasing space for the newer ones.

Event recording is triggered by a video analytics rule, pre- and post-recording time comprising 10 seconds.

4. If one of the channels does not require recording, select *Disabled* in *Recorder activity*.

5. Click *Apply* to save the settings.

3.8.2 Recorder Report

To get the recorder report, use the link in the upper line.

The screenshot shows a web browser window with the URL `https://192.168.3.80/params/show_report.cgi?lang=en`. The interface has a navigation bar with tabs: Video inputs, Network, Video analytics, PTZ node, Recorder, Mailer, and Support. The 'Recorder' tab is active, displaying the 'Recorder Report' page. The page is divided into two sections: 'Content' and 'Archive'.

Content Section:

Record	Part
CONTINUOUS_RECORD_VIDEO_SOURCE_0	2012 08 24

Archive Section:

Record	Part	Track	Data
CONTINUOUS_RECORD_VIDEO_SOURCE_0	2012_08_24_15_42_42	SNAPSHOT001	2012_08_24_15_42_44_SNAPSHOT001_PART_0.jpeg 2012_08_24_15_42_59_SNAPSHOT001_PART_1.jpeg 2012_08_24_15_43_15_SNAPSHOT001_PART_2.jpeg 2012_08_24_15_43_36_SNAPSHOT001_PART_3.jpeg

At the bottom of the page, there is a language selector: `ru | en`.

3.8.3 Sending Recording Notifications

The system allows sending notifications about the recording to an e-mail specified.

1. To configure notification sending, go to *Mailer* tab in Web page.
2. Specify SMTP server name, user name and password (the same as for sender's e-mail), mail sender and recipient.
3. To save the settings, click *Apply*.

The screenshot shows the 'Mailer' configuration page in the web interface. The URL is `https://192.168.3.80/params/mailer.cgi`. The 'Mailer' tab is active. The configuration fields are as follows:


- SMTP server: `smtp://smtp.example.com`
- User name: `admin`
- Password: `•••••`
- Mail sender: `admin@example.com`
- Mail recipient: `<user@example.com>`

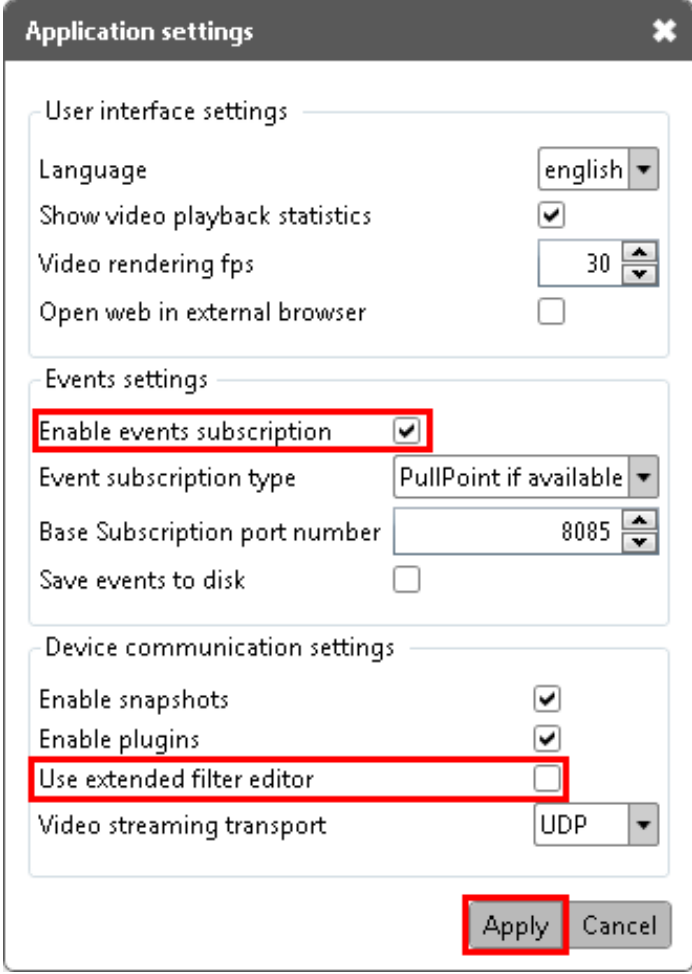
At the bottom of the form, there are two buttons: 'Apply' (highlighted with a red box) and 'Cancel'. At the very bottom of the page, there is a language selector: `ru | en`.

3.9 Events

3.9.1 Section Settings

This section allows viewing all the events registered by the device in text mode.

1. To enable *Events* section on the device, check *Enable events subscription* in Application settings (checked by default). To access Application Settings, click .




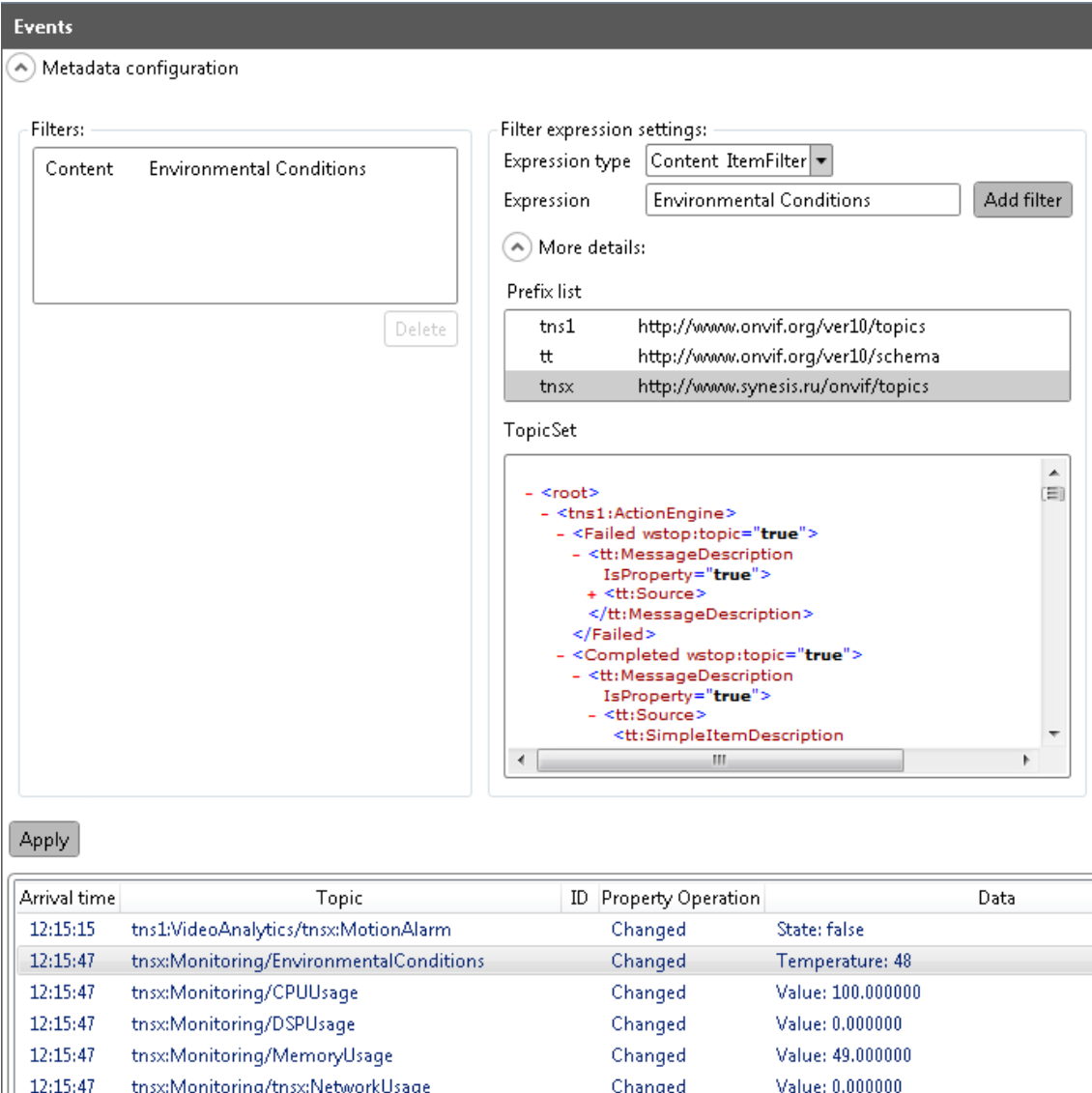
The screenshot shows the 'Application settings' dialog box. It is divided into three sections: 'User interface settings', 'Events settings', and 'Device communication settings'. In the 'Events settings' section, the 'Enable events subscription' checkbox is checked and highlighted with a red box. Below it, the 'Event subscription type' dropdown is set to 'PullPoint if available'. The 'Base Subscription port number' is set to 8085. In the 'Device communication settings' section, the 'Use extended filter editor' checkbox is unchecked and highlighted with a red box. At the bottom right, the 'Apply' button is highlighted with a red box, and the 'Cancel' button is visible next to it.

2. From the dropdown select event subscription type. By default *PullPoint if available* is selected.
3. Selecting *Only Base Subscription*, specify port number.
4. To save the settings, click *Apply*.

3.9.2 Metadata Configuration

To optimize separate events search, the application supports *Metadata Configuration*.

1. In *filter expression settings* select *expression type* and enter the *expression* to create a filter.
2. Click *Add filter*. The filter will appear in the filters list on the left.
3. To specify the filter details unfold *More details* section.
4. In *Prefix list* only those prefixes are available which are used in the current .xml document. In order to be able to create prefixes manually, check *Use extended filter editor* in Application Settings (, see the previous picture).



Arrival time	Topic	ID	Property	Operation	Data
12:15:15	tns1:VideoAnalytics/tnsx:MotionAlarm		Changed	State: false	
12:15:47	tnsx:Monitoring/EnvironmentalConditions		Changed	Temperature: 48	
12:15:47	tnsx:Monitoring/CPUUsage		Changed	Value: 100.000000	
12:15:47	tnsx:Monitoring/DSPUsage		Changed	Value: 0.000000	
12:15:47	tnsx:Monitoring/MemoryUsage		Changed	Value: 49.000000	
12:15:47	tnsx:Monitoring/tnsx:NetworkUsage		Changed	Value: 0.000000	

For detailed filter management rules consult ONVIF specification <http://www.onvif.org/specs/core/ONVIF-Core-Specification-v220.pdf>, chapters 9.5.5 and 9.7.3.

4. Managing video

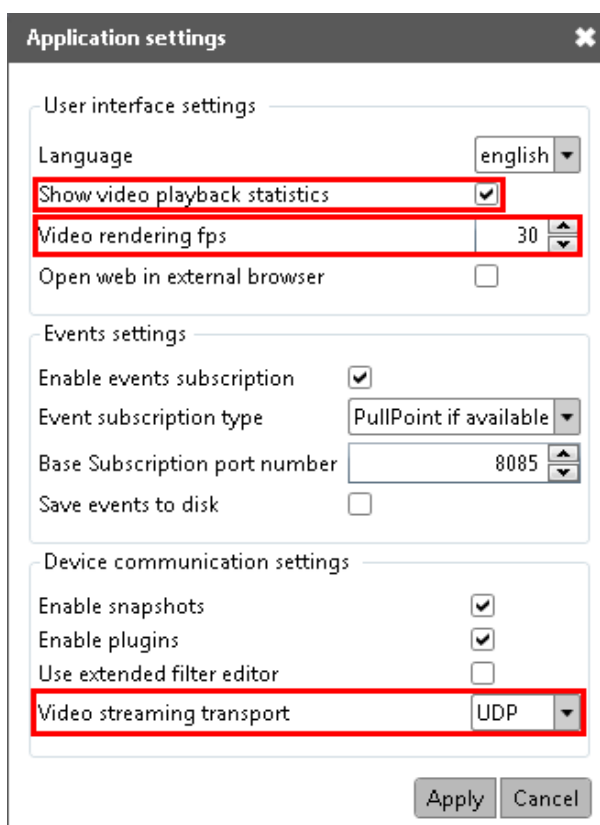
4.1 Application Settings

The application provides several video transmission settings, common to all the devices connected.

1. Check *Show video playback statistics* to display this parameter within the video frame (frame per second frequency for rendering and decoding).



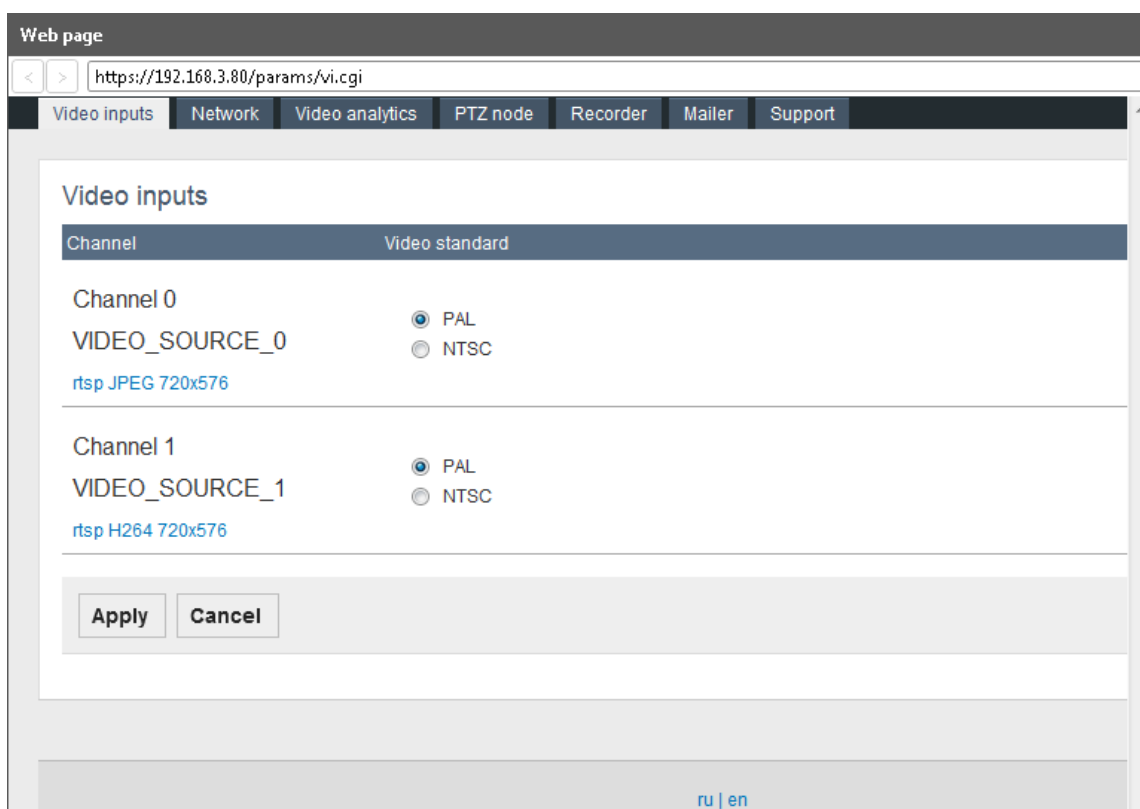
2. In order to enable this option, check it in Application settings (🔧 button).
3. Set *Video rendering fps*.
4. From the dropdown select *Video streaming transport*. This parameter denotes, via which protocol ONVIF Device Manager receives video stream from network video transmitter (NVT).
5. Set the necessary values and click *Apply*.



4.2 Additional Settings (optionally)

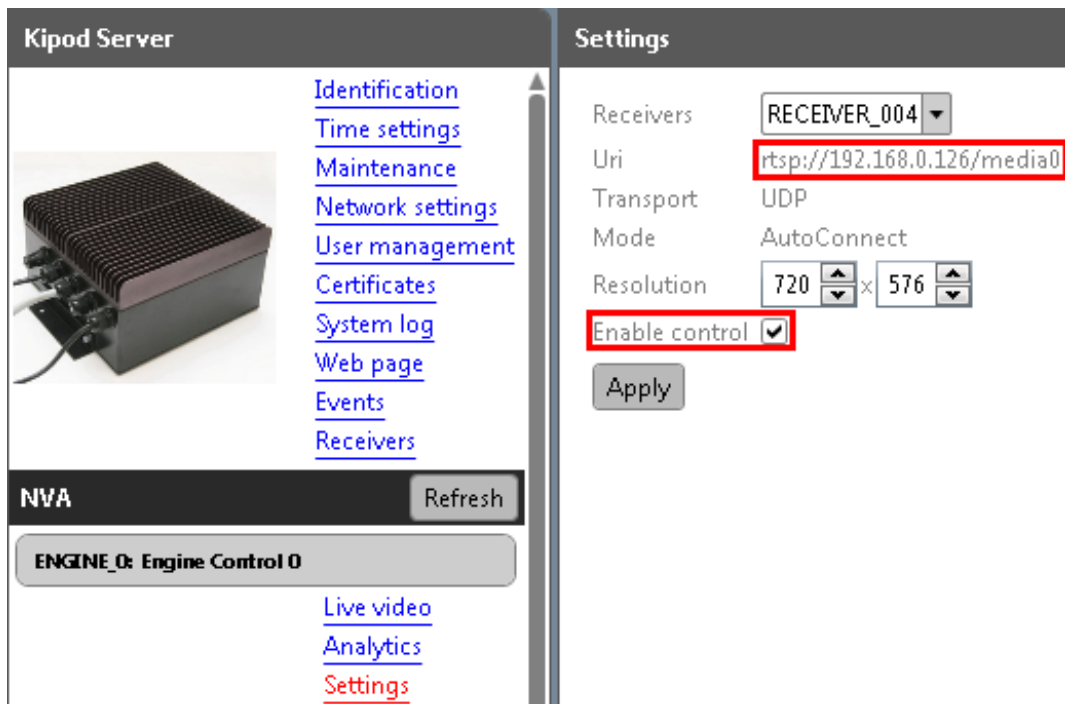
The application allows choosing video standard for each channel. For better video reception quality, the standard on the channel and on the video camera should coincide. For example, the camera transmits analogue video via NTSC. For correct video reception, it is necessary to set NTSC video standard on the receiving channel.

1. To configure video channels, go to Web page, Video inputs tab.
2. Select video standard for each channel (PAL or NTSC) and select Apply.



4.3 Channel Configuration (optionally)

1. Go to *Settings* of the selected video channel.



2. Select the receiver from the dropdown.
3. In Uri-field paste rtsp-link to the video, copied from the network device transmitting or processing live video (IP-camera, video-encoder).
4. Specify video resolution.
5. Check *Enable control*.
6. Click *Apply*.
7. Go to *Live video* section.

Here you can see the video, the link to which you have specified.

4.4 Video Streaming (optionally)

This section allows you to configure the following parameters of displaying video:

Encoder and resolution (pixels) of the video (selected in the dropdown).

Frame rate (frame per second) denotes how many frames per second are captured by the video camera connected to the device. This parameter is uneditable and shown just for information.

Encoding interval (number of frames) denotes at which rate the frames coming from the camera are encoded. For example, when encoding interval comprises 25, it means that 1 frame from 25 captured per second is encoded and transmitted to the user. The maximum value reduces the load to the channel, but may cause skipping information from the frames that were not encoded. Reducing encoding interval will increase the frequency of picture update, as well as the load to the channel. The parameter is set with the help of slider bar.

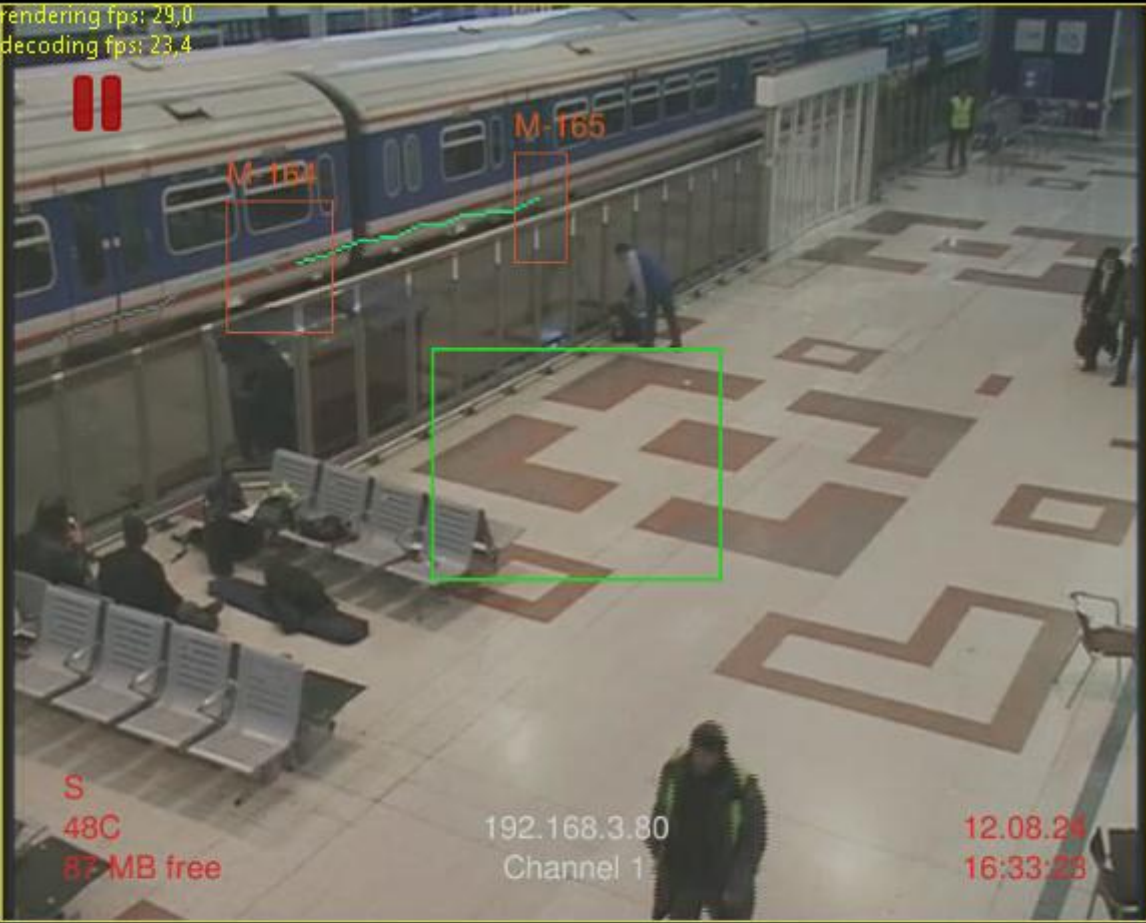
Bitrate limit (kbps) is the amount of information required to play one second of video. The less the bitrate is, the less the final video file size will be. But when the bitrate is considerably reduced, the program will have to use stronger compression algorithms, which reduces video quality, too. The value is entered manually or with the help of spin box.

Quality is the parameter which enables to reduce the load to the channel by means of reducing the picture definition. The parameter is set with the help of slider bar: the left most position corresponds to the highest picture definition, the right most to the lowest load to the video channel.

GOV length is possible to edit only in case the encoder is H264. This parameter denotes the length of picture group between the two key frames. The higher this value is, the less is the load to the network, but the quality of the video is affected. The value is entered manually or with the help of spin box.

Video streaming

rendering fps: 29,0
decoding fps: 23,4



S
48C
87 MB free

192.168.3.80
Channel 1

12.08.24
16:33:23

Encoder and resolution(pixels)

Frame rate, fps

Encoding interval

Bitrate limit, kbps

Quality

GOV length

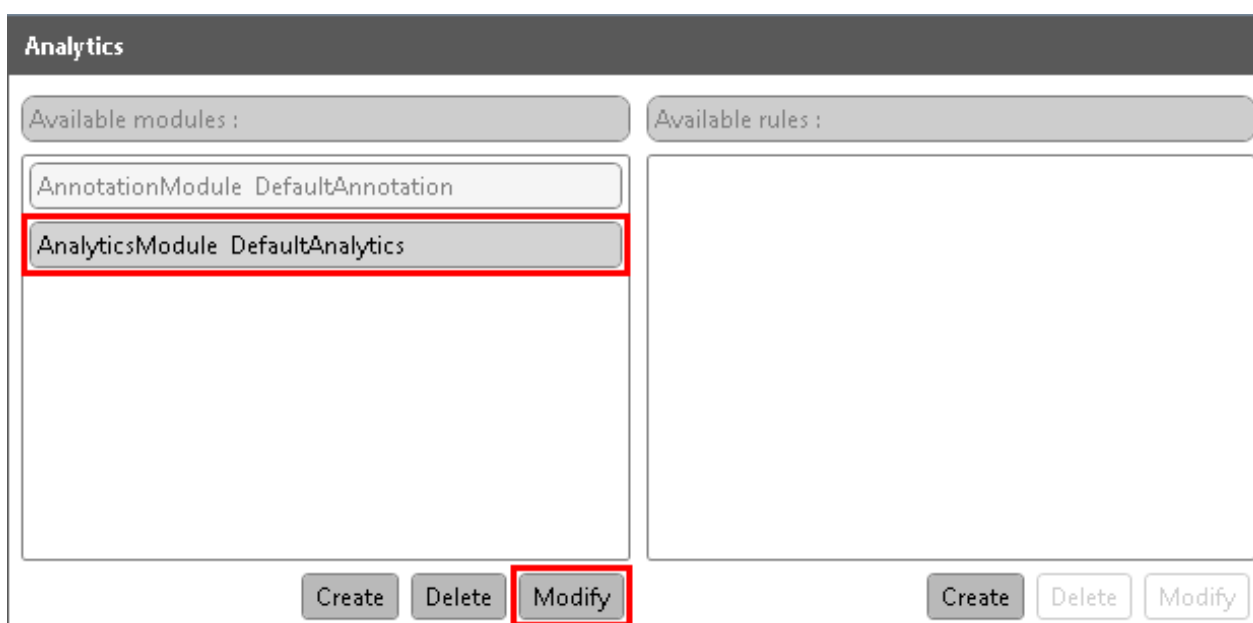
Set the necessary values and click *Apply*.

5. Video analytics Configuration

5.1 Default Annotation and Analytics Configuration.

ONVIF Device Manager has default annotation and analytics settings and is ready to use with any device. It is possible to view the settings with a double-click on *Annotation Module Default Annotation* and *Analytics Module Default Analytics* respectively.

To modify analytics module, click on *Analytics Module Default Analytics* and then click *Modify*.



5.2 Object Tracker Configuration

The screenshot displays the 'Analytics' configuration window for an ONVIF device. The 'Object tracker' tab is active. The video feed shows a street scene with a blue van. A red rectangle is drawn around the van, and green lines connect its corners to a central point, forming a polygon. The interface includes a top menu with 'Object tracker', 'Depth calibration', 'Tampering detectors', and 'Antishaker'. Below the video feed, there are controls for 'Enable object tracker' (checked), 'Contrast sensitivity', and 'Displacement sensitivity'. At the bottom, there are 'Apply' and 'Cancel' buttons.

1. Specify the region where object tracking should be applied. For this, move the sides of the red rectangle by dragging its corners with the mouse left button.
2. In order to create additional corners, double click on one of rectangle sides in any place. Holding mouse left button, move the new point to the necessary position until a new polygon corner is formed. The same way create other polygon corners.
3. Position the polygon so that its borders correspond to the tracking region.

4. Check *Enable object tracker* to make other parameters editable.
5. Set necessary *contrast sensitivity* by moving the slider. This value denotes how contrastive an object should be to be detected against the background. For example, at high contrast sensitivity a person in dark clothes is more likely to be detected against dark background.
6. By moving the slider, set *displacement sensitivity*. It denotes which distance a person or vehicle should cover in the video to be detected as a moving object. At high displacement sensitivity, a short distance is enough for detection.
7. Video analytics can be configured to track only objects moving in a certain direction. For this, select the directions you need at the octangular figure on the left. The selected directions turn gray after a mouse click.
8. To select all the directions at once, use *All* button. *None* button deselects everything.
9. To save the settings click *Apply*.

5.3 Depth Calibration

Calibration allows relating object sizes in the video with their real sizes. ONVIF Device Manager supports two types of calibration.

5.3.1 Height Calibration

This calibration type requires specifying the following parameters:

- Camera matrix format
- Focal length, mm
- Marker real height, cm

1. Open *Depth calibration* tab in *Analytics* section.
2. Select *Height Marker* calibration type.
3. Select an object in the video that has equal height at its different parts (eg., a fence). It is important to measure the height from the ground.
4. Set both markers against objects of the same height (see the picture). Marker height can be changed by dragging its upper and lower points (the cursor assuming the form of a vertical arrow).



5. To move the marker, drag it to the necessary position with the mouse left button.
6. Fill in the necessary fields under the video: from the dropdown select matrix format, specify focal length and height of the real object related to the markers.
7. Save the settings by clicking *Apply*.

5.3.2 2D-Calibration

Does not require specifying matrix format and camera focal length. For this calibration type it is necessary to specify height and width of the real object (mm) shown in the video at different distance from the camera. The easiest way is calibration by a person's picture.

1. Select *2D-marker*.
2. The person stands within camera view in the background. The first 2D-marker should be positioned in such a way that vertically it corresponded to the person's height and horizontally to the space he takes.
3. The first 2D-marker remains in the same position. The person moves to the foreground within camera view and stands in the same position as the first time. Place the second marker the same way as the first.
4. Fill in the parameters under the video: real object width and height (mm).
5. Save the settings by clicking *Apply*.



5.4 Настройка сервисных детекторов

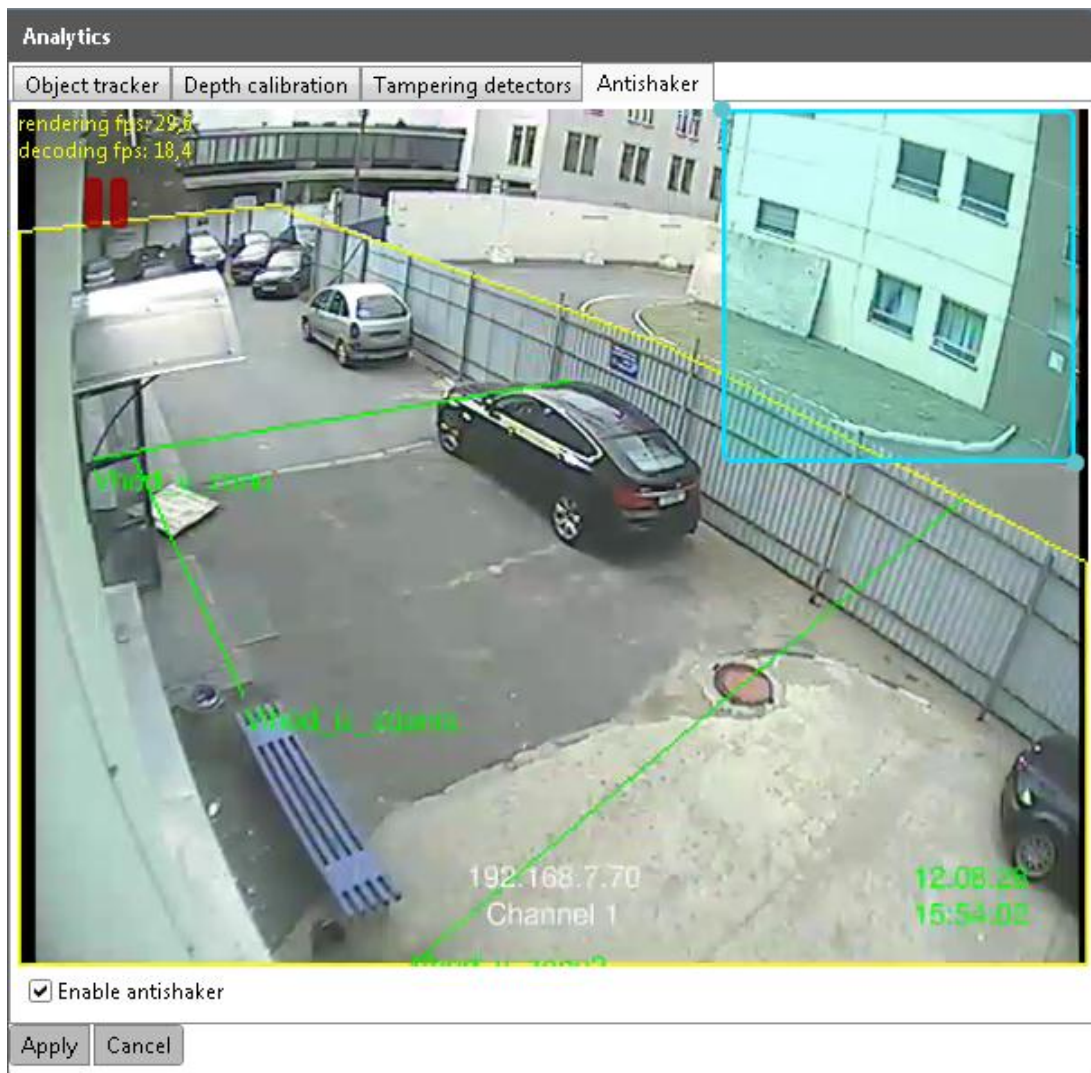
1. Go to *Tampering detectors* tab in *Analytics* section.
2. Check situations that require automatic notification.
 - Camera redirected
 - Camera obstructed
 - Image too dark
 - Image too blurry
 - Image too bright
 - Image too noisy



3. Save the settings by clicking *Apply*.

5.5 Antishaker Settings

1. In *Antishaker* tab check *Enable Antishaker*.
2. In the video select a region containing typical scene elements against which the camera should be stabilized (road, columns, fence). For this, holding left mouse button move the blue rectangle corner points until it is reduced to a needed size.
3. Some moving elements like large vehicles and shaking trees can be present in antihaker zone. But it is highly recommended to exclude elements certainly not suitable for stabilization, like black video frame or the sky.



4. Save the settings by clicking *Apply*.

5.6 Annotation Settings

1. In *Analytics* tab in *Available modules* section select *Annotation Module Default Annotation* and click *Modify*.
2. In annotation window select elements to show in the video.
 - Annotate moving rects
 - Annotate speed
 - Annotate time stamp
 - Annotate system information
 - Annotate channel name
 - Annotate tracking
 - Annotate user region
 - Annotation rules
 - Annotate calibration results



3. To save the settings, click *Apply*.

5.7 Configuring Analytics in Text Format

Alongside with the described ways of configuring analytics and annotation, the application provides an alternative way of configuring with disabled video plugins.

This way is used to configure analytics on devices by certain manufacturers, like Axis, or in case it is necessary to configure parameters absent in video plugin.

1. In order to enable this way of configuration, uncheck *Enable pugins* in Application settings (🔧 button).
2. Go to *Analytics* tab of the selected channel.
3. Check necessary options and set exact number values in the relevant fields.
4. Annotation and Rules are configured the same way with disabled plugins.

Analytics

UseObjectTracker

MaxObjectArea

MinObjectArea

MaxObjectSpeed

DisplacementSensitivity

StabilizationTime

ContrastSensitivity

UseAntishaker

ShiftOutputPicture

CameraRedirected

CameraObstructed

ImageTooDark

ImageTooBlurry

ImageTooBright

ImageTooNoisy

AntishakerCrop

XOffs

YOffs

CropWidth

CropHeight

MarkerCalibration

CombinedMarkerCalibration

CombinedMarkers

UserRegion

Rose

Points

Points

Points

Points

Points

Points

Points

Apply Cancel

5.8 Additional Video Analytics Settings

Besides configuration in manual or text format, the application supports analytics configuration via the file containing program code.



It is strongly recommended that this type of configuration is performed by specially trained personnel, as incorrectly changed parameters can damage the system.

1. Go to Web page to video analytics tab.
2. In *Extended parameters* section download the source file of each channel by clicking *Download*. The file is saved to your hard drive.
3. Edit the file the way you need and save the changes.
4. Click *Browse* on the relevant channel and select the edited file from the hard drive. Click *Apply*. The status will change from *Default* to *Changed*.
5. To remove the edited file from the system and restore the default settings, click *Delete*.

Web page

http://192.168.0.48/params/va.cgi

Video inputs Network **Video analytics** PTZ node Recorder Mailer Cloud Support

Video analytics

Activation

The device will restart after activating.

Status	License
Activated	

Browse... Apply Delete

Extended parameters

Channel	File	Status
Channel 0 VIDEO_SOURCE_0 rtsp H264 720x576	C:\Users\loksana.nesterov Browse...	Apply Changed Download Delete
Channel 1 VIDEO_SOURCE_1	Browse...	Apply Default Download Delete

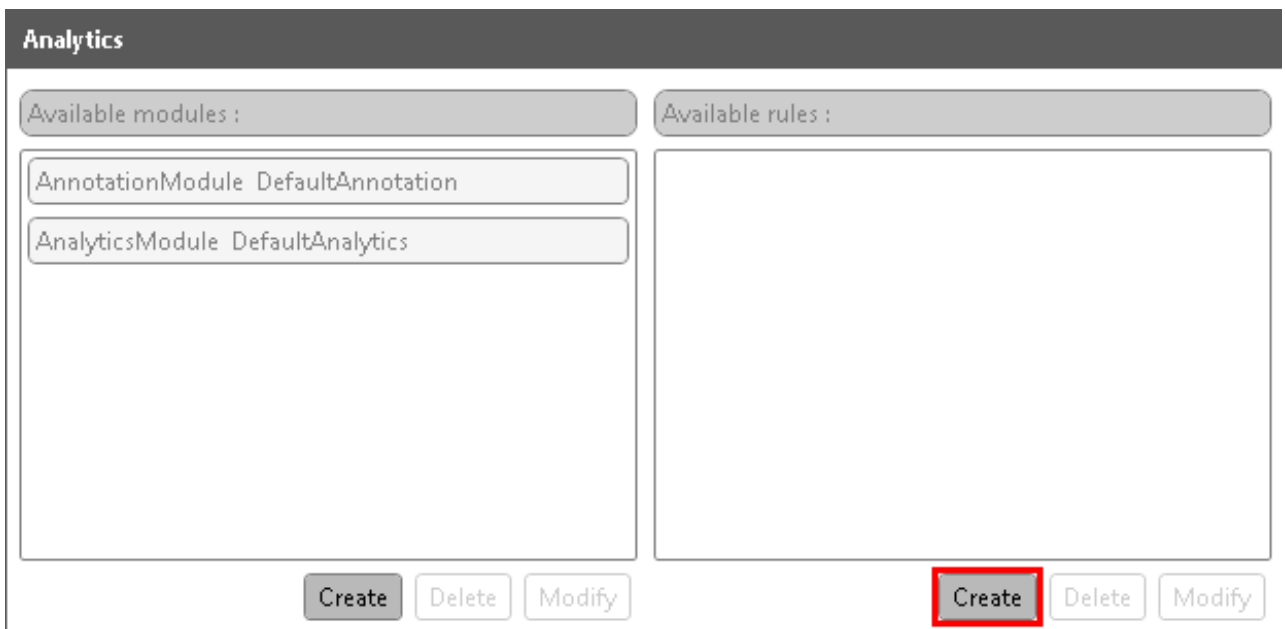
ru | en

6. Video Analytics Rules

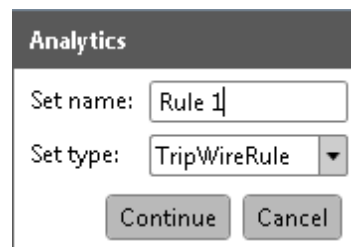
6.1 Tripwire Rule

A tripwire rule means defining a tripwire in tracking zone, crossing which in one or both directions is regarded as an alarm event. For example, the tripwire is drawn in the driveway to the yard. An event is generated each time a person or vehicle come into the yard.

1. Go to *Analytics* tab of the selected video channel.
2. Click *Create* in *Available Rules* section.



3. In the next window specify the rule name.
4. In *Type* dropdown select *Trip Wire Rule*.

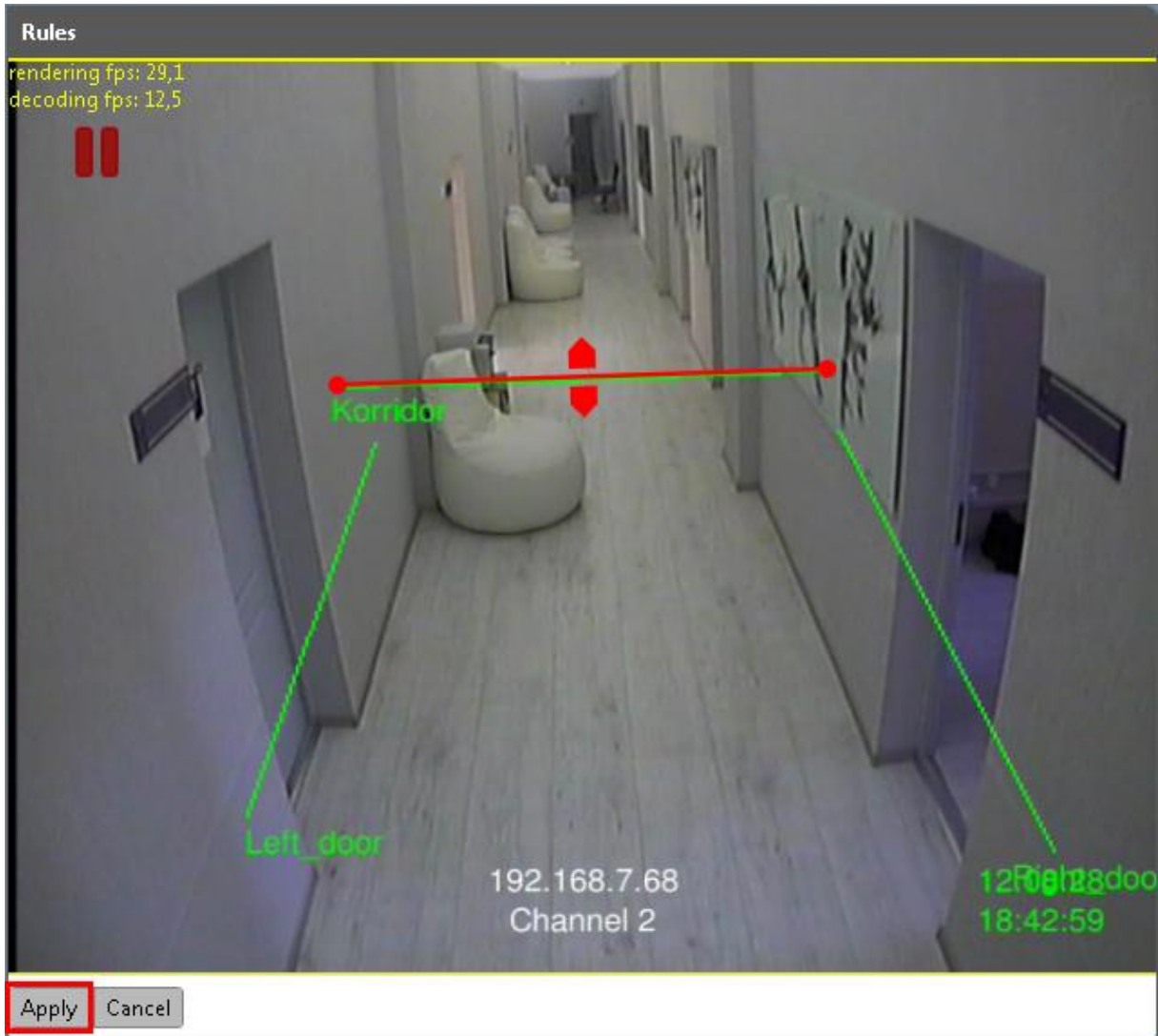


5. Click *Continue*.

A video frame will open with a red line in the center of the screen. Here you can define the rule settings.

6. Move the line by dragging its end points until it reaches necessary length and position.

- Define in which directions crossing the line is meaningful. For this purpose, click on one of the arrows in the middle of the line. When crossing the line in this direction, an alarm event is created. When both directions are selected (two arrows are marked), the event is registered in all the cases of crossing the line.



- To save the settings, click *Apply*.

6.2 Region Rule

A region rule enables you to set a region and allow or forbid certain actions inside it. Depending on the settings, an alarm event is generated each time the rule is violated.

1. To create a region rule go to *Analytics* tab of the relevant channel.
2. Click *Create* in *Available rules* section.
3. In the next window specify the rule name.

4. In *Type* dropdown select *Region Rule*. Click *Continue*.

The video frame will open, where you can define the rule settings.

5. In the center of the frame there is a red rectangle. You can change its size and shape by dragging its corner points with the left mouse button until it covers the rule region (if the rule region is tetragonal by shape).
6. In order to add another corner (in case the rule region has the form of a polygon with five or more corners), double click on one of its sides in any place to form a new point. Drag it to form a new corner of the polygon.
7. Create other polygon corners and align its sides with the borders of the rule region (see the picture below).
8. Under the video check the options the analytics should react to in the rule region.
9. *Motion* tracks moving within the region.
10. *Loitering* means someone's walking around a place during a certain time, or insignificant moving at a low speed. In order to detect such behaviour, check *Loitering* and specify its time.
11. To detect running within the region, select *Speeding over...* with specifying speed and time.
12. To generate an event when an object was abandoned within the rule region check *Abandoned item*.
13. Save the settings by clicking *Apply*.

Rules

Rendering fps: 29,6
Decoding fps: 23,3

S
45C
103 MB free

192.168.0.8
Channel 1

12.08.29
15:00:37

Motion

Loitering s

Speeding over km/h during s

Abandoned item

Apply Cancel

7. PTZ-Camera Control

ONVIF Device Manager is optimized to control a Pan-Tilt-Zoom camera. While connecting the camera, follow the manufacturer's instructions. The correctly connected camera is displayed in the device list.

7.1 Common Settings

1. Go to Web page to PTZ Node.
2. Default *PTZ Speed* including *Pan min*, *Pan max*, *Tilt min* and *Tilt max* correspond to PelcoD standard.

Change the settings, if necessary.

3. Specify PTZ-node address for each channel (number value). Zero value is also an address, it does not mean absence of device.
4. To save the settings, click *Apply*.

The screenshot shows a web browser window with the URL `https://192.168.0.48/params/ptz.cgi`. The page has several tabs: Video inputs, Network, Video analytics, PTZ node (selected), Recorder, Mailer, Cloud, and Support. The main content area is titled "PTZ node" and contains the following settings:

- PTZ speed: 4800
- Pan min: 0
- Pan max: 35999
- Pan mirror neg
- Tilt min: 0
- Tilt max: 35999
- Tilt mirror neg

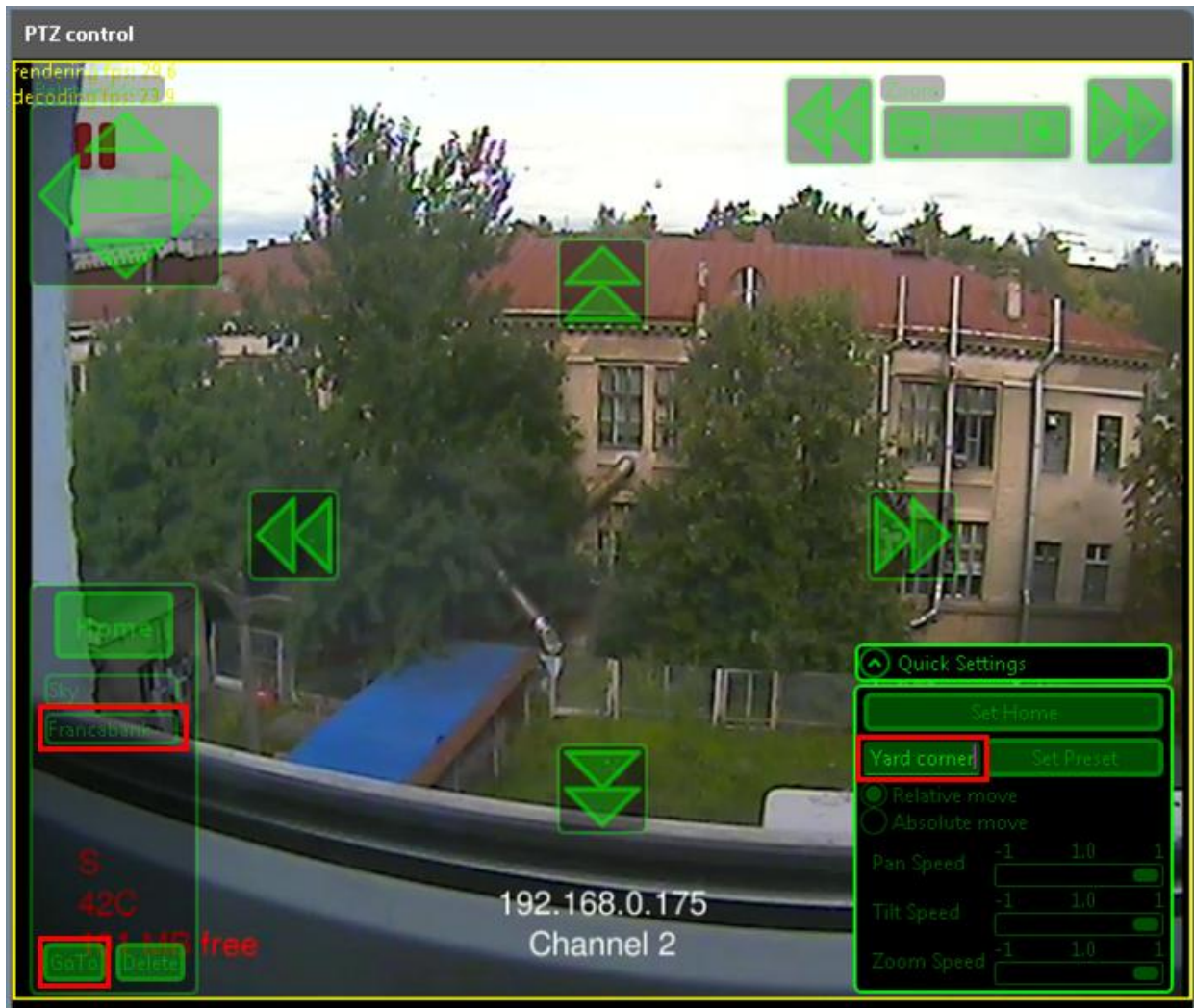
Below the settings is a table with two columns: "Channel" and "PTZ node address".

Channel	PTZ node address
Channel 0 VIDEO_SOURCE_0 rtsp H264 720x576	0
Channel 1 VIDEO_SOURCE_1	1

At the bottom of the page, there are two buttons: "Apply" and "Cancel". The "Apply" button is highlighted with a red box.

7.2 Camera Movement Settings

1. Open *PTZ control* tab.



2. Adjust camera position with the help of arrow buttons in the center of the screen and zoom buttons at the right top corner. This view will be used as home position.
3. Open *Quick Settings* section in the right lower corner of the screen.
4. Click *Set Home*.

The camera will turn back to this position each time you click *Home* in the left part of the screen.

5. The same way set additional camera position. In *Quick Settings* section enter the name of the camera new position and click *Set Preset*. The preset is displayed in the list in the left part of the screen.
6. In order to set the camera in preset position, select it in the list and click *Go to*. The camera will automatically turn to this position.

7. In *Quick Settings* section set *tilt*, *pan* and *zoom speed*.
8. Select camera move type: *relative* or *absolute*. For absolute move the exact final position is specified, for the relative - the final position is calculated basing on the current camera position.

8. Profiles Management

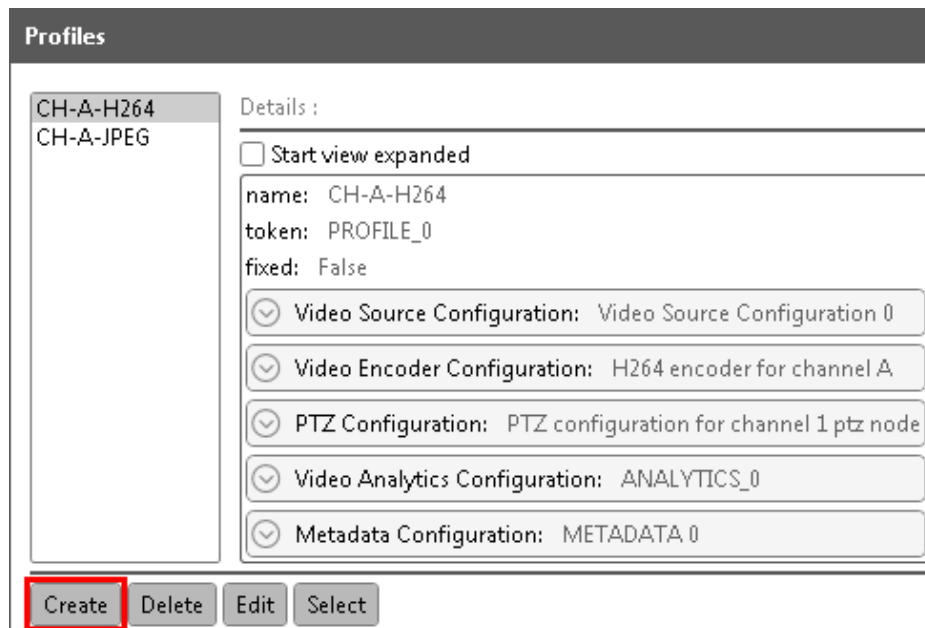
Profile is a complex of the following settings:

- Video Source Configuration
- Video Encoder Configuration
- PTZ Configuration
- Video Analytics Configuration
- Metadata Configuration

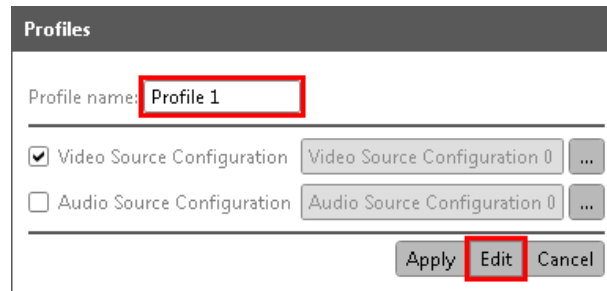
The application allows creating profiles of different configuration, eg., a profile without video analytics, only transmitting video, or a profile supporting PTZ configuration for a separate camera. Disabling unused functions helps unload video transmission channel. To change configuration, it is enough to select another profile without changing the settings manually.

By default there are two profiles for H264 and JPEG encoders.

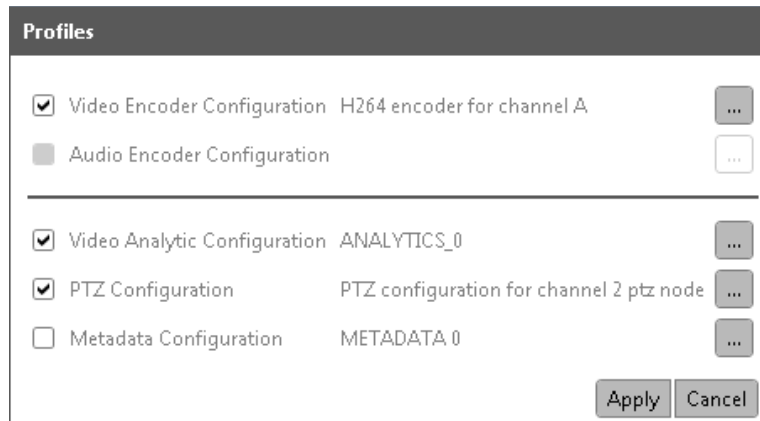
1. To create a new profile, click *Create* in *Profiles* tab.



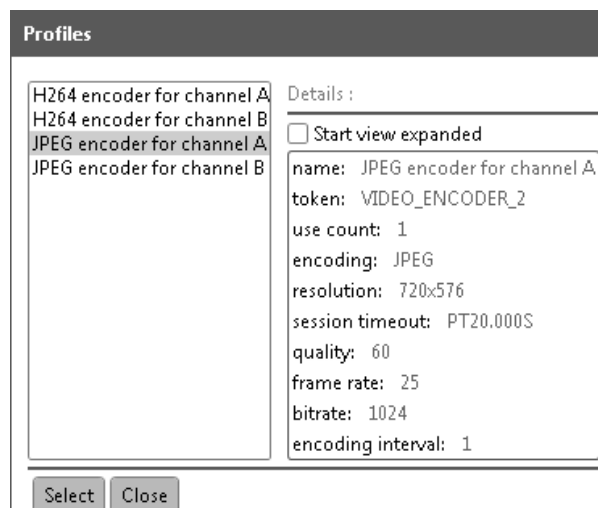
2. In the next window specify the profile name and check audio and/or video source configuration.
3. Configuration of the checked source will be included in the profile. Uncheck audio configuration to reduce the load to the channel (eg., in case your device does not transmit audio).



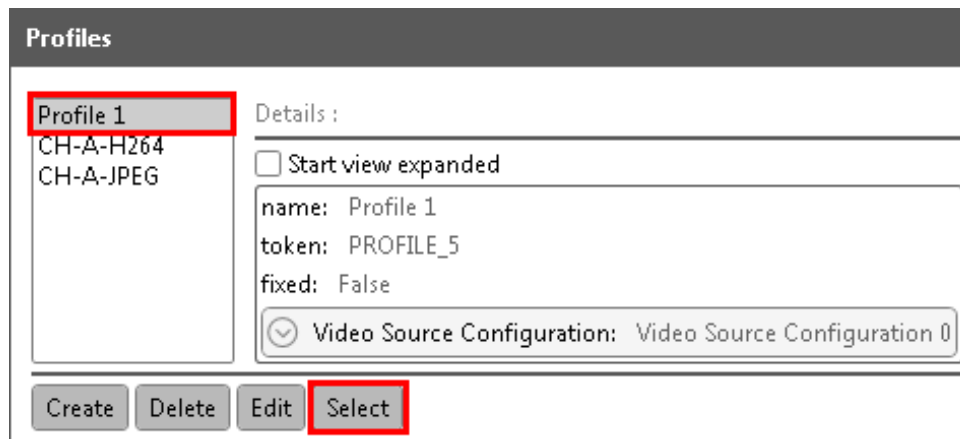
4. To continue profile configuration click *Edit*.
5. In the next window check profile components you need.



6. In the right column default configuration is described. To view and change default configuration settings, click on the gray button in the corresponding line.
7. In the left window highlight a setting and click *Select*. The details will show in the window on the left.



8. The same way select and configure other profile components. Click *Apply*.
9. After the profile settings are configured, select it in the list on the left.



All the profile components will appear in the configured channel menu.

10. To delete a profile from the list, highlight it and click *Delete*.

9. Metadata

Metadata is text information associated with a video analytics event.

To view it, open *Metadata* tab of the relevant channel.

In *Metadata details* you can view detailed information on the selected metadata fragment.

The screenshot shows the ONVIF Device Manager interface. On the left, there is a sidebar with navigation links for a device named 'Склад, Вход в офис'. The main area is titled 'Metadata' and shows 'Metadata details' expanded. The XML metadata is displayed as follows:

```

- <tt:MetadataStream>
- <tt:Event>
- <wsnt:NotificationMessage>
  <wsnt:Topic Dialect="http://docs.oasis-open.org/wsn/t-
  1/TopicExpression/Concrete">tns1:RuleEngine/LineDetector/tnsx:Object</wsnt:Topic>
- <wsnt:Message>
- <tt:Message UtcTime="1970-01-01T00:36:12Z" PropertyOperation="Initialized">
- <tt:Source>
  <tt:SimpleItem Name="Rule" Value="Vorota"/>
  <tt:SimpleItem Name="VideoAnalyticsConfigurationToken" Value="ANALYTICS_0"/>
  <tt:SimpleItem Name="VideoSourceConfigurationToken"
  Value="VIDEO_SOURCE_CONFIG_0"/>
</tt:Source>
- <tt:Key>
  <tt:SimpleItem Name="ObjectId" Value="85"/>
</tt:Key>
- <tt:Data>
  <tt:SimpleItem Name="Direction" Value="Unknown"/>
  <tt:SimpleItem Name="HasCrossed" Value="false"/>
  <tt:SimpleItem Name="Position" Value="(-0.276773,-0.238261)"/>
  <tt:SimpleItem Name="Speed" Value="0.949510"/>
</tt:Data>

```

Below the XML, a list of events is shown with their meta types and tns1 URIs:

- meta type: Event
tns1: VideoAnalytics/tnsx: ObjectMotion:
- meta type: Event
tns1: RuleEngine/LineDetector/tnsx: Objecttns1: RuleEngine/LineDetector/tnsx: Obj
- meta type: Event
tns1: RuleEngine/LineDetector/tnsx: Objecttns1: RuleEngine/LineDetector/tnsx: Obj
- meta type: Event
tns1: VideoAnalytics/tnsx: ObjectMotion:
- meta type: Event
tns1: VideoAnalytics/tnsx: MotionAlarm:

For Metadata configuration see the picture below.

For detailed rules of filter management consult ONVIF specification <http://www.onvif.org/specs/core/ONVIF-Core-Specification-v220.pdf>, chapters 9.5.5 and 9.7.3.

Metadata

Metadata configuration

Include analytics

Filters:

Include events

Content	boolean(//tt:SimpleItem[@Name="VideoSourceConfig
Topic	ObjectMotion

Filter expression settings:

Expression type: Topic Concrete

Expression: ObjectMotion

More details:

Prefix list

tns1	http://www.onvif.org/ver10/topics
tnsx	http://www.synesis.ru/onvif/topics
tt	http://www.onvif.org/ver10/schema

TopicSet

```

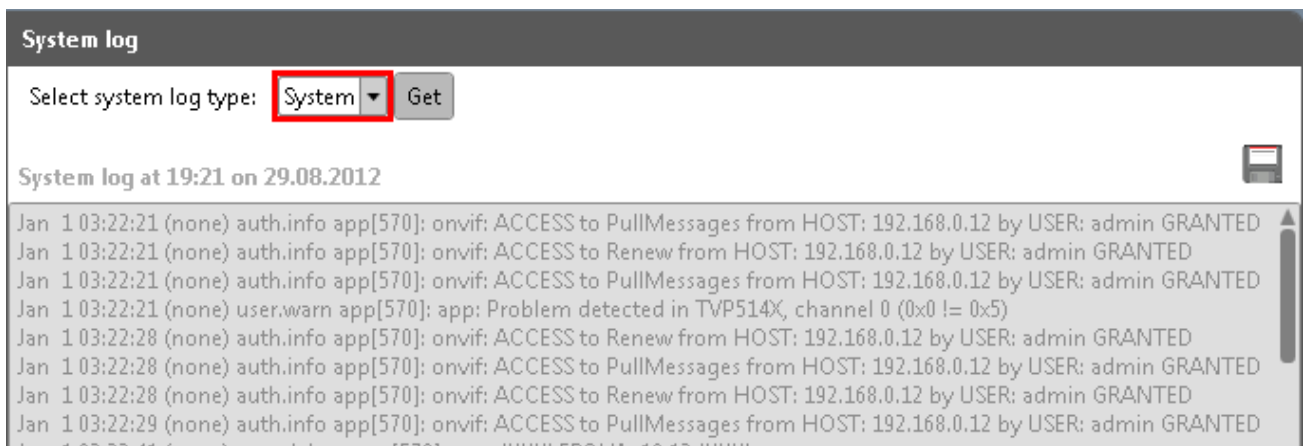
- <root>
- <tns1:VideoSource>
  - <tnsx:SignalLoss wstop:topic="true">
    - <tt:MessageDescription
      IsProperty="true">
      - <tt:Source>
        <tt:SimpleItemDescription
          Type="tt:ReferenceToken"
          Name="VideoSourceToken"/>
        </tt:Source>
      - <tt:Data>
        <tt:SimpleItemDescription
          Type="xs:boolean"
          
```

10. Maintenance and troubleshooting

This document provides only the easiest ways of troubleshooting. If you are not sure you will manage yourself, consult our support service (support@synesis.ru phone.+7 (495) 660-77-47)

Information on what may have caused the trouble in the application is contained in *System log*.

1. In order to get the information about the operations on the device, go to *System log* tab.
2. Select *System* as log type and click *Get*.

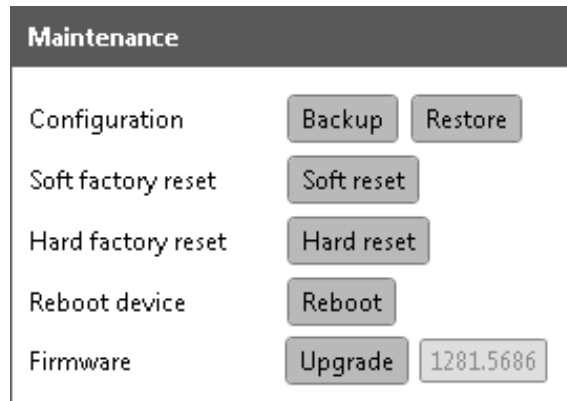


3. To save the information into a separate file (.txt) and click  icon.

10.1 Configuration Backup

Configuration backup allows restoring the correct settings in case they have been damaged, reset or lost after the device break down. It is possible to back up all the settings, except video stream processing parameters that are stored in the form of profiles.



1. To save the current settings, go to *Maintenance* tab.

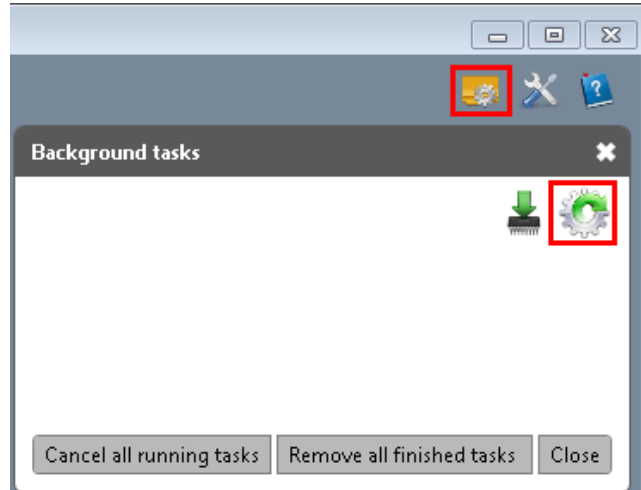


2. Click *Backup* in *Configuration* line. You will be offered to save the settings into a separate file with *.backup* extension.

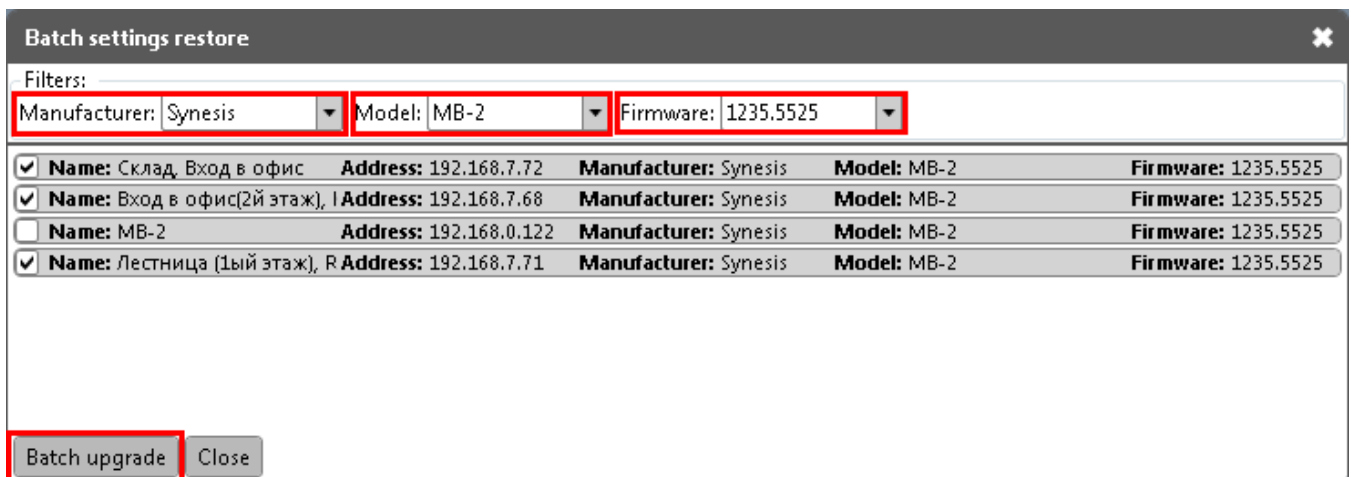
When necessary, you can import the backup file with the help of *Restore* button.

10.2 Configuration Backup in Packet Mode

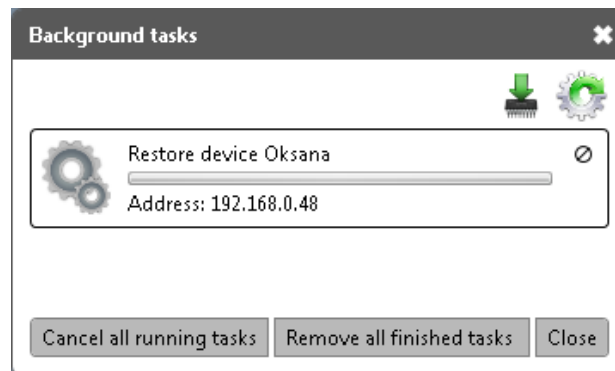
1. In order to restore configuration on several devices simultaneously, click  button in the right top corner and select *Batch settings restore* ( button in *Background tasks* window).



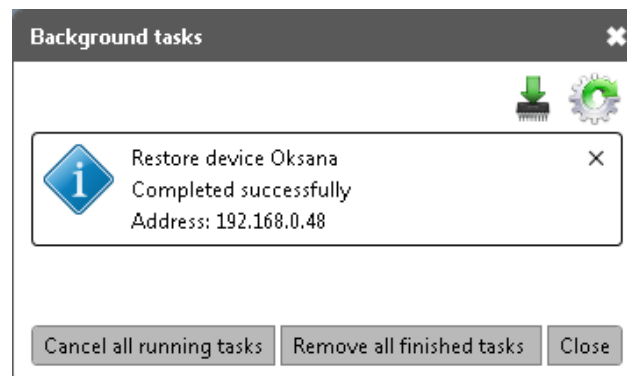
2. In filters select the device manufacturer, model and firmware version.



3. Check only the devices requiring settings restore and click *Batch Upgrade*.
4. In the next window select the backup file.
5. Settings restore will start in the background mode.



6. After the restore is completed, the following message will appear.



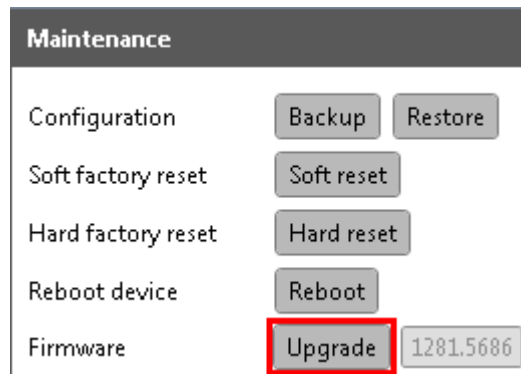
7. In order to clear the list, click Remove all finished tasks.

10.3 Firmware Upgrade (for devices by Synesis)

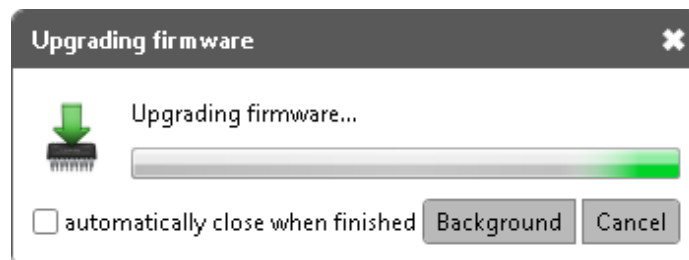
10.3.1 Firmware Upgrade for a Single Device

Firmware version is regularly upgraded and is available to download from Synesis website (<http://synesis.ru/ru/surveillance/downloads>).

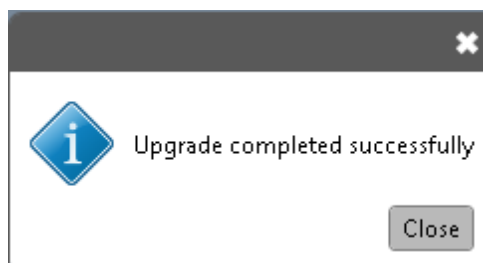
1. Download a file from Synesis web-site (with .bin extension), corresponding to your device.
2. Click *Upgrade* at *Maintenance* tab.



The following message is displayed:



3. You can switch the process to the background or check *automatically close when finished* option.
4. After the process has been finished, the following message is displayed.

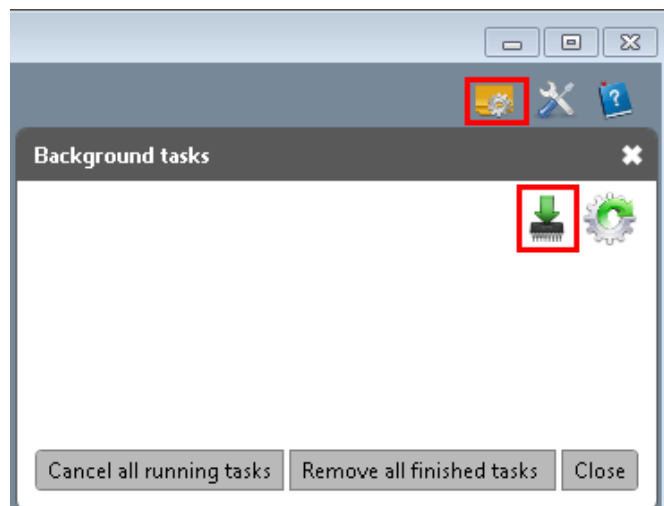



Firmware update does not affect video analytics settings and other functions, so recurrent device configuration is not required.

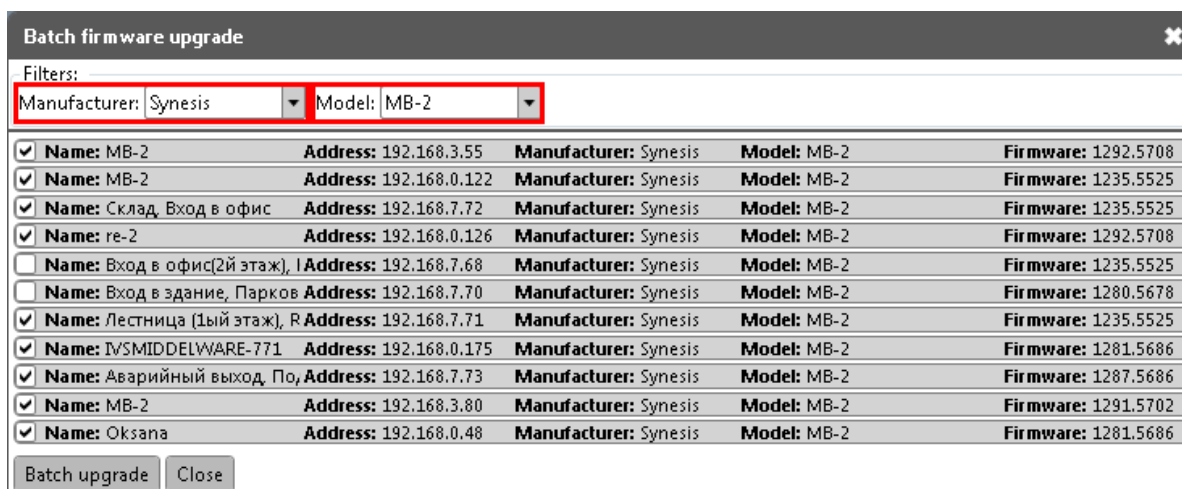
10.3.2 Firmware Upgrade in Batch Mode

ONVIF Device Manager allows upgrading the firmware in batch mode for all the devices connected.

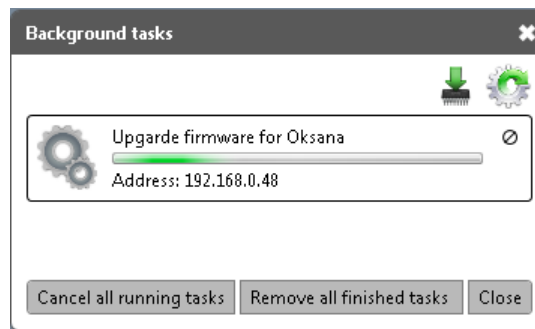
1. Click  icon in the top right corner to open *Background tasks* window.



2. In Background tasks click .
3. In filters select manufacturer and the model of devices to upgrade.

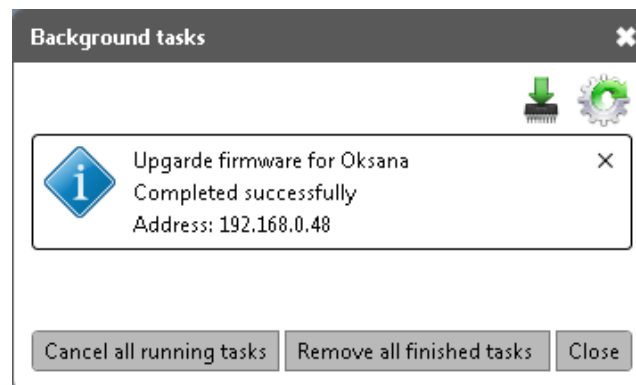


4. Leave checked only those devices in the list that require upgrade.
5. Click *Batch upgrade*. The upgrade will start in batch mode.



6. In order to cancel firmware upgrade, click *Cancel all running tasks*.

After the upgrade is complete, the following message will appear.

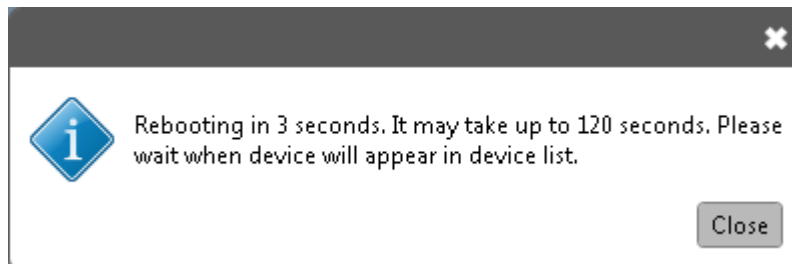


7. To clear the list, click *Remove all finished tasks*.

10.4 Device Reboot

Device reboot can help repair insignificant faults of video analytics or other functions, caused by hardware failures. When you need to solve a problem with your device individually, it is recommended to reboot it first.

Click *Reboot* in *Maintenance* tab. The following message is displayed.

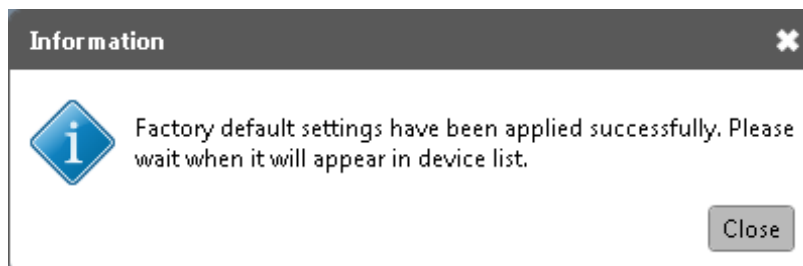


After the reboot the device appears in the list on the left.

10.5 Soft Factory Reset

During soft reset all except the network settings are discarded. Soft reset is applied in cases when the network is configured correctly, but the rest of the settings should be discarded.

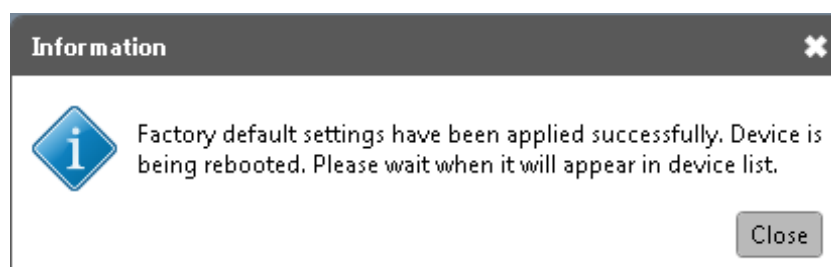
Click *Soft Reset* at *Maintenance* tab. After reset the following message is displayed.

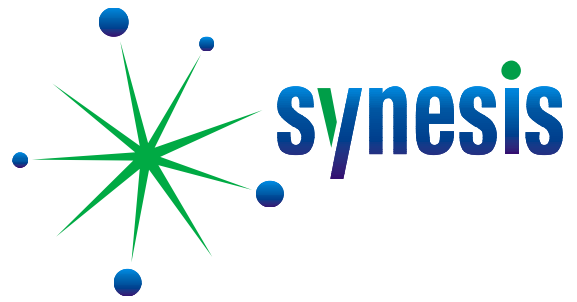


10.6 Hard Factory Reset

During hard factory reset all the settings are discarded. If your network settings do not coincide with the default application settings, you will have to configure the network again.

Click *Hard Reset* in maintenance tab. After the reset the following message is displayed.





LLC "Synesis"
Russian Federation, 107078, Moscow,
Sadovaya-Chernogriazskaya str., 3-B
korp. 1, off. 54
+7 (495) 660-77-47

LLC "Synesis"
Republic of Belarus, 220043
Minsk, pr-t Nezavisimosti, 95
pom. 12, off. 316
+375 (17) 281-77-85

ONVIF Device Manager user forum
<http://sourceforge.net/projects/onvifdm/forums>

Customer service center:
<http://mbx.synesis.ru/>

The information in the document can be changed without notification.