MIRASYS

Mirasys VMS Admin Guide

Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

MIRASYS

1 CONTENTS

2 Overview of This Guide 9
3 Technical Support 9
4 What is the Mirasys VMS software? 9
4.1 What does a System Contain? 9
4.2 VMS Servers 10
4.3 Main Server 10
4.4 Client Programs 11
4.5 Network Requirements 11
5 OS Compatibility 11
6 Configuring the System 12
7 Log In 13
7.1 Logging in 13
7.1.1 User credentials 13
7.1.2 How to log in 13
7.2 Locking System Manager 14
7.3 How to access Server address selection 14
8 Management User Interface 16
8.1 Menu bar 16
8.2 Maintenance 17
8.3 Help 17
8.4 Exporting system camera information to the CSV 17
9 System 19
9.1 System settings 21
9.1.1 General System Settings 22
9.1.2 Configuring viewing station settings 23
9.1.3 E-Mail Settings 25
9.1.4 Command Settings 27
9.1.5 Change VMS Server Addresses 27
9.1.6 System Addresses 29
9.1.7 Axis one-click dispatcher settings 31

9.1.8 Update VMS Servers 37
9.1.9 Incident Reporting Settings 40
9.1.10 Storage Locker Settings 49
9.1.11 List Management settings 53
9.1.12 Object Data Store Settings 70
9.2 Backup 71
9.2.1 Export logs 71
9.2.2 Back up settings 78
9.2.3 Restore settings 79
9.3 Monitoring 83
9.3.1 Audit trail log 83
9.3.2 SM Server Diagnostics 85
9.3.3 Server Diagnostics 87
9.4 Licenses 90
9.4.1 Getting the license key 91
9.4.2 License details 92
9.4.3 License Management 94
9.5 Watchdog 94
9.5.1 Watchdog settings 95
9.5.2 Watchdog log 96
9.5.3 Watchdog event list 96
9.6 Add-ins 101
9.6.1 Mirasys Camera Drivers 101
9.6.2 Installing External Driver Packages 124
9.6.3 Driver Installation and Usage 126
9.6.4 Installing Metadata Drivers 176
9.6.5 Installing Client Drivers 176
9.6.6 Install client plugin 176
10 The VMS Servers 179
10.1 General 180
10.1.1 Multicast address 181

10.1.2 VMS server failover settings 182
10.1.3 Use as a failover VMS server 183
10.1.4 VMS Server failover is enabled for this VMS server 183
10.1.5 Delay failover to prevent data loss 183
10.1.6 Use automatic failback 183
10.1.7 Use automatic material copying 183
10.2 Port Forwarding 184
10.2.1 Automatic Router Configuration 184
10.2.2 Single Server Behind Router 185
10.2.3 More Than One Server Behind Router 185
10.2.4 More Than One Server On Multiple Sites 186
10.3 Hardware 187
10.3.1 Video 189
10.3.2 Audio Hardware 204
10.3.3 Device Settings 205
10.3.4 Adding cameras by using CSV file 206
10.4 Adding and Removing VMS Servers 210
10.4.1 To add a server to the system(recording server): 210
10.4.2 To remove a server from the system: 211
10.4.3 Connection status: 211
10.4.4 NOTE: 211
10.5 Search in VMS Server settings 212
10.5.1 Search in the VMS Server settings tab 212
10.5.2 Narrow down the search from the VMS Server settings tab 212
10.5.3 Search in individual settings 213
10.6 Cameras 215
10.6.1 Camera Settings contain settings for: 216
10.6.2 Camera settings 217
10.6.3 Advanced 227
10.6.4 RTSP Server Streaming 228
10.6.5 Motion Detection 230

10.6.6 VCA features 237
10.6.7 Privacy 239
10.6.8 License Plate Recognition (LPR) settings 244
10.6.9 Face Recognition (FR) Settings 248
10.6.10 Object Recognition (OR) Settings 252
10.7 VCA settings 255
10.8 Audio 255
10.8.1 Adding, Editing and Removing Audio Devices 255
10.8.2 Audio Settings 257
10.8.3 General Settings tab 257
10.8.4 Audio Detection 260
10.8.5 Scheduler (Audio) 261
10.9 Digital I/O 262
10.9.1 Digital I/O Settings 262
10.9.2 LoopBack I/O 265
10.9.3 Logical I/O 265
10.9.4 Countdown I/O 270
10.9.5 Scheduled IO 271
10.9.6 Properties 274
10.9.7 UniversalOutputDriver 275
10.10 Alarms 277
10.10.1 Alarms settings 277
10.10.2 Custom Alarm Triggers 293
10.11 Storage 299
10.11.1 Adding Storage Space 299
10.11.2 Video, audio and text data storage settings 301
10.11.3 Automatic Deletion of Video, Audio and Text Data 302
10.11.4 Archiving 303
10.11.5 Use OS cache 305
10.11.6 Activity data cache 306
10.12 Text Channel Settings 306

10.12.1 To add text data channels: 307
10.12.2 To edit text channels: 307
10.12.3 To remove all text channels that use the same driver: 308
11 Profiles 308
11.1 Creating a customer-specific profile 311
11.1.1 Adding a profile 311
11.2 Duplicate an existing Profile 311
11.3 Automatic profile updates 312
11.3.1 Enable automatic profile updates 312
11.3.2 Automatic profile updates enabled 313
11.3.3 Automatic profile updates disabled 313
11.4 Devices profile settings 314
11.4.1 Add devices to a profile 314
11.4.2 Selected Device Properties 314
11.4.3 Sort selected device nodes 316
11.4.4 PTZ camera profile settings 317
11.4.5 PTZ control 317
11.4.6 Text channel Device Window Options 318
11.4.7 Adding Device Groups to the list of the selected device 318
11.4.8 Sort Alphabetically 320
11.4.9 Client Plugins 321
11.5 Alarms profile settings 323
11.5.1 Editing Profile Specific Alarm Settings 323
11.5.2 Adding alarms to a profile 324
11.5.3 Editing profile-specific alarm user rights 324
11.5.4 Deleting an alarm from a profile 324
11.6 Maps profile settings 325
11.6.1 Adding Maps to Profiles 326
11.6.2 To remove a site map: 327
11.6.3 To remove an icon from the map: 327
12 Users and User groups 327

12.1 Logging Users Off ... 328
12.2 To log a user off: ... 328
12.3 Monitoring Users ... 328
12.4 User group ... 329
12.4.1 User Roles ... 329
12.4.2 Two-factor authentication ... 354
12.4.3 Protection ... 357
12.4.4 Creating a customer-specific User Group ... 358
12.4.5 Domain Based User Groups (Active Directory) ... 360
12.4.6 Active hours - User group access schedule ... 362
12.5 Creating a customer-specific user ... 366
12.5.1 Identify users through a user name separate from the user login ID ... 367
12.5.2 Adding a public username in the System Manager ... 367
12.5.3 Displaying a public user name to the user in Spotter ... 368
12.5.4 Public user name in Spotter web client ... 369
12.6 User account settings ... 369
12.6.1 User account settings contain the following options: ... 369
12.6.2 Supported languages ... 370
12.7 Disabling or Activating a User Account ... 370
13 ThruCast streaming ... 371
13.1 Stream from the server to the client ... 371
13.2 Stream from the camera directly to the client ... 372
13.3 Supported Cameras ... 372
13.4 Network Optimization ... 373
13.5 Multistreaming and ThruCast for Network Optimization and Storage ... 374
13.5.1 Impact of ThruCast on Image Delay ... 375
13.5.2 Features Not Supported in ThruCast Streaming ... 375
13.5.3 Licenses ... 375
13.5.4 Multiple Viewers ... 375
13.5.5 Installing Client Drivers ... 375
13.5.6 Configuring multi-streaming ... 375

13.5.7 ThruCast Default Setting 376
13.6 Using ThruCast 376
14 Failover Servers 378
14.1 Failover Functionality 378
14.1.1 Failover migration will be triggered in the following conditions: 378
14.2 Failover summary since V9.5.0 379
14.3 Description 379
14.4 Recorder settings cache 379
14.5 Failover process 379
14.6 Manual failover triggering 380
14.7 Minimum requirements 381
14.7.1 IP camera drivers 381
14.8 VMS Server roles 381
14.8.1 VMS Server role FAILOVER 381
14.8.2 VMS Server role BROKEN 381
14.9 Starting point 381
14.9.1 Enabling VMS failover server to the recording server 382
14.9.2 Adding FAILOVER server 383
15 Failback 386
15.1 Failback process 387
15.1.1 Manual failback triggering 387
15.1.2 Automatic failback 387
15.2 Material copying from failover period 388
15.3 Failover log 389
15.3.1 Start Failback for the selected server 390
15.3.2 Start material copying to the selected server 392
15.4 Material copy time after failback – Test results 393
15.4.1 Test setup 393
15.4.2 Test results 394

Mirasys VMS Admin Guide

System Administration

2 Overview of This Guide

This guide is intended for those who set up a Mirasys system.
It shows how to add servers to the system and change their settings, add user accounts and user profiles, and monitor the system.

Please see AI guides for Mirasys LPR, FR, LM, Easy LPR, and VCA guide.

3 Technical Support

For technical support and warranty issues, please contact the system supplier.

4 What is the Mirasys VMS software?

Mirasys software is a distributed digital video management system (VMS or DVMS) for video and audio surveillance applications.
The software can monitor real-time and recorded video, audio and text data and control PTZ cameras, I/O devices, and IP cameras.
The software supports systems consisting of analogue or digital surveillance cameras, supporting the creation of analogue, digital or hybrid (consisting of both analogue and digital) surveillance systems.
A centralized surveillance system domain can consist of up to 150 local or remote VMS Servers.
Mirasys software is sold separately and part of Mirasys video management systems consisting of both the software and the VMS Server hardware.
Please contact your Mirasys supplier for information on Mirasys software or hardware.

4.1 What does a System Contain?

The Mirasys system consists of these components:

- 1-150 VMS Servers
    - **Main Server** (dedicated server – recommended -, one of the video recording VMS Servers, or the only server in a single-server, non-networked environment)
    - **VMS Server** ("recording servers" if the system consists of multiple servers)
- Client applications:
    - Mirasys System Manager

- Mirasys Spotter
- Mirasys Spotter Web
- Spotter Player
- System Monitor
- VAU (VMS Application Updater)
- Spotter Viewer

4.2 VMS Servers

The VMS servers record video and audio from multiple cameras and audio channels and write the data to a storage device. A server is a computer with storage, the Windows operating system, and the installed Mirasys VMS software with required drivers.

You can access a VMS Server locally or over a network using the System Manager and Spotter programs and monitor server functionality through the Spotter Diagnostics plugin.

Several devices can be connected to a VMS Server:

- PTZ (dome) cameras and keyboards
- External devices, such as sensors, to the digital inputs
- External devices, such as doors, lights, and gates, connected to digital outputs
- Special integrated devices like radar, IoT device or 3rd party system
- Storage or backup unit (NAS, SAN, or RAID, for example)

4.3 Main Server

In a networked system, one of the servers must be set as the Main Server.

A Main Server is the central server of a surveillance system. All other VMS Servers connect to it, and all client applications communicate through the Main Server.

If the system contains only one server, then that server is the Main Server. If there is more than one server, the Main Server can be set freely.

In a more extensive system we recommended that the Main Server is a server dedicated for this purpose alone

> Main Servers **must** have *SQL Server Express 2014* or other *Microsoft SQL Server 2014* installed.

The Main Server functionality is the following:

- It verifies the identity of all programs and users who try to log on to the system (authentication).

- It stores all system configuration data.
- It stores all user data.
- It monitors the system.
- It synchronizes the clocks on all servers.
- It generates reports.
- It stores watchdog events.
- It stores alarms.
- It stores audit trails.

4.4 Client Programs

System administrators use the **System Manager** program for these tasks:

- Configuring the servers.
- Adding user accounts and user profiles.
- Monitoring the system.

System operators use the **Spotter** application for:

- Monitor real-time and recorded video and audio
- Control digital I/O switches and PTZ cameras
- Export video and audio clips to local media
- Receive and handle alarm notifications
- Create video matrixes via the optional, separately sold Agile Video Matrix (AVM) software
- Use other plugins like Grafana reporting or list management

4.5 Network Requirements

The network requirements apply to systems where users access the servers over a network.

5 OS Compatibility

Mirasys VMS V9 supports the following operating systems:

- Windows 10

- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Make sure that the “Desktop Experience” and “Media Foundation” features are activated for Windows server operating systems.

6 CONFIGURING THE SYSTEM

After connecting the cameras and other devices to the servers, configure the system settings and add user accounts and user profiles.

To configure the system, perform these steps:

1. Add servers to the system and configure their settings.
2. Add the correct licenses for the servers.
3. Add IP cameras and other IP devices.
4. Add user profiles.
5. Add user accounts.

Install the client programs on each computer used to access the system over a network.
A separate “Spotter only” installer is provided.

After configuring the system, **back up system settings and all VMS Server settings** on the **System** tab.This way, you can restore the settings, for example, if a hard disk fails.

7 LOG IN

This section describes how to log in and log off from System Manager.
Only system administrators or users with monitoring rights will be allowed to log in to System Manager.

7.1 LOGGING IN

7.1.1 User credentials

Default username and password

Username: Admin
Password: 0308
Please ensure that the default username and password are not in use after installing the system. They should not be used even in closed networks.

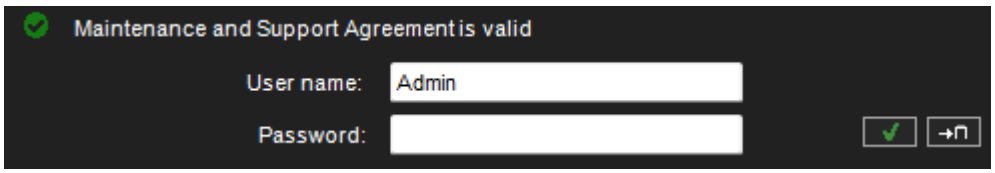
7.1.2 How to log in

To login to System Manager do one of the following:

- Double-click the shortcut icon **System Manager** on the desktop.
- Click **Start**, point to **Programs,** and then to **DVMS**. Click **System Manager**.

In systems that have only one Main Server address configured, the System Manager login screen is shown. In systems with multiple main servers and addresses configured, or if the user presses the **Delete** key in the initial startup phase, the site selection screen is shown.

1. On the login screen, type your username in the **Username** box and your password in the **Password** field.



The username and password are case-sensitive.

1. Click **OK**. A progress bar is shown on the screen while the program loads.

7.1.2.1 Log off or change user

After the program starts, the user interface is shown. To **log off** or to **change the user** click on the menu bar **File** and then **Log off. To quit** the program**:**

- On the menu bar, click **File** and then **Exit**.

- Close the application window.

The user can only have one System Manager application running at any one time.
It is not possible to have the System Manager simultaneously connected to multiple servers.
To connect to another Main Server, exit from the current Main Server and choose another Main Server from the site selection screen.

7.2 Locking System Manager

You can manually lock the program to protect it, for example, when you go away from your desk.

To lock the program, do one of the following:

- On the menu bar, click **File** and then **Lock Program**.
- On the status bar, click **Lock program**.

To unlock the program:

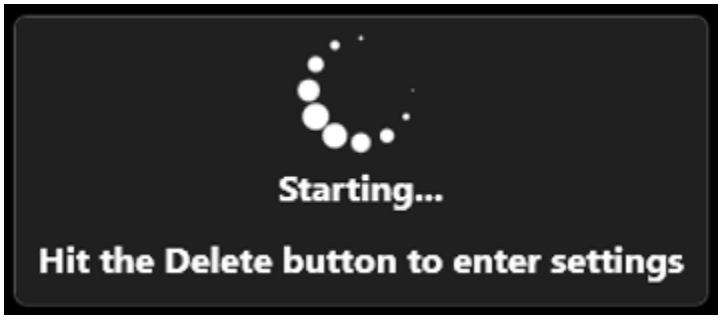
- After locking the program, the login screen is shown.
    - Type the user name in the **User name** box and the password in the **Password** box.
- Alternatively, the user can also leave System Manager directly from the lock dialog by clicking the **Exit** button.

The password is case sensitive.

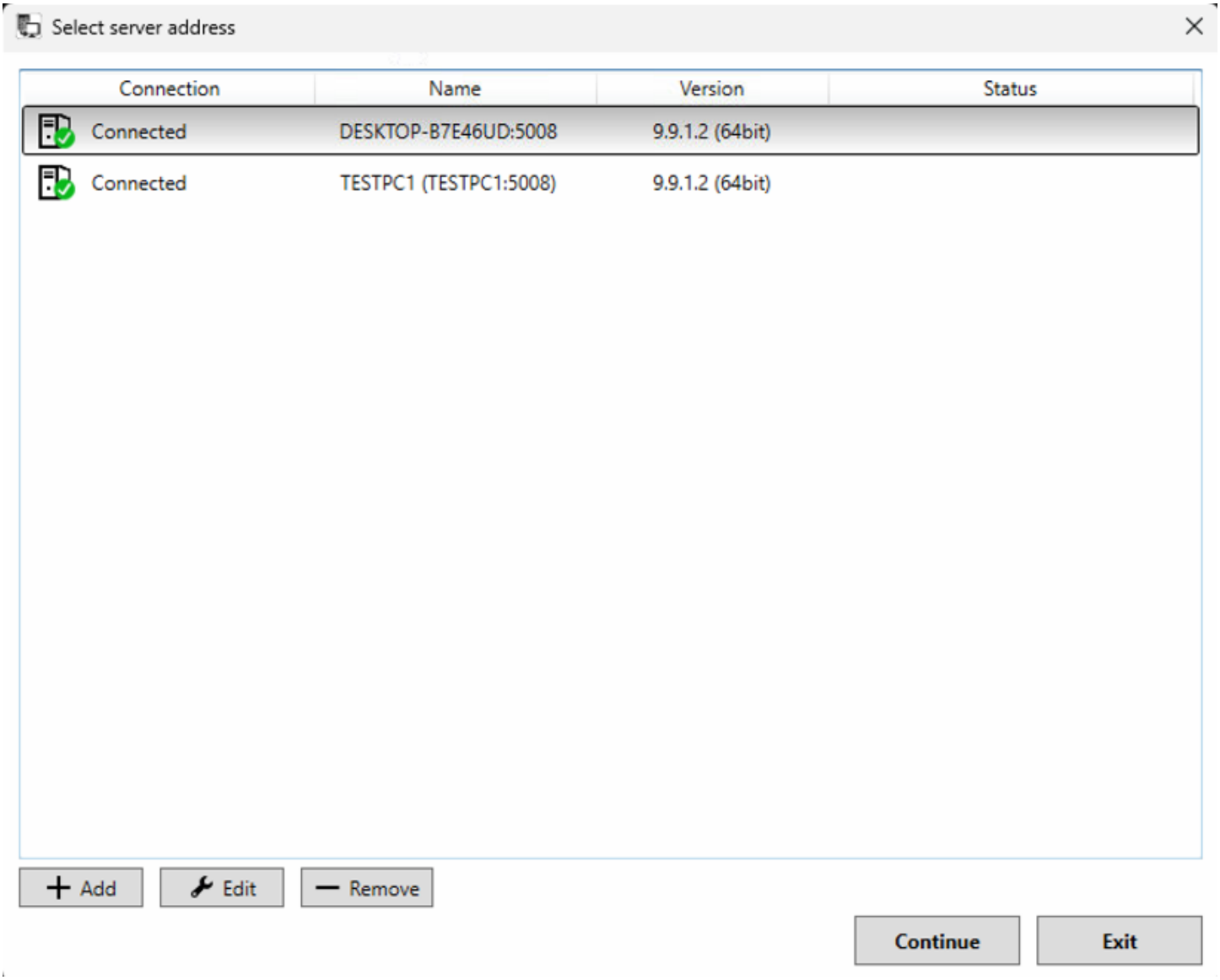
7.3 How to access Server address selection

In this guide, we will go over how you can edit the server address in the client software. Server address selection allows users to add new server addresses, edit current ones, or remove them.

1. Right-click the System Manager or Spotter shortcut and select **Run as administrator**.
2. Click **Yes** to run this application as administrator rights.
3. After this you get a new window, press the **Delete** key on the keyboard to open the Server address selection window.



4. In this window, you can add new server addresses, edit current ones, or remove them.



1. When all needed changes are done, select the desired server address and click **Continue** to make the connection to this server.

8 MANAGEMENT USER INTERFACE

The System Manager User Interface contains these elements:

8.1 MENU BAR

- File

- Log Off
- Lock Program
- Import
- Export

8.2 MAINTENANCE

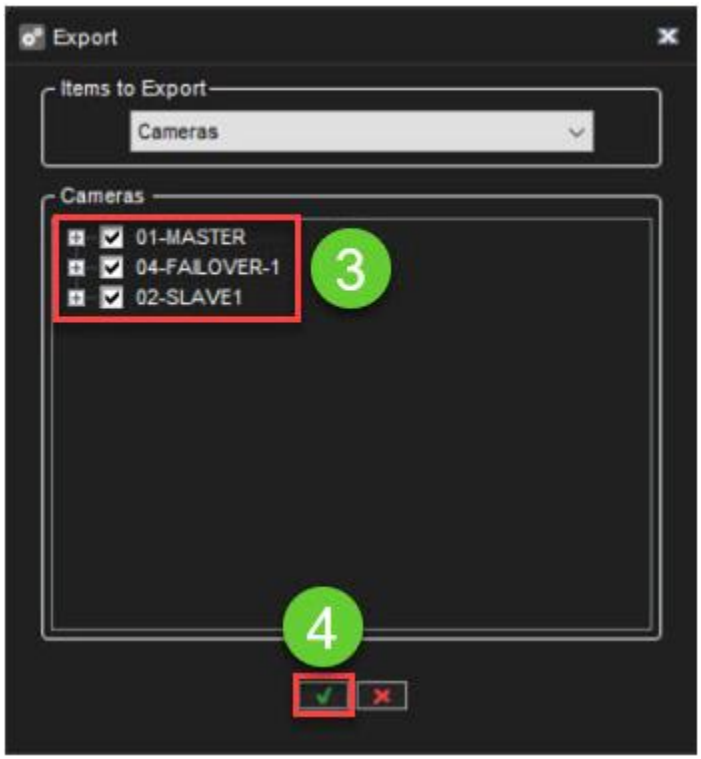
Set maintenance state on to control the failover transition state off.

8.3 HELP

About to see information about the program version, **Online help** to access online user documentation, and **Help Topics** to use the PDF guide.

8.4 EXPORTING SYSTEM CAMERA INFORMATION TO THE CSV

1. Click **File**
2. Click **Export**
3. Select the servers
4. Click **OK**



5. Select the location
6. Enter the name of the export
7. Click **OK**



9 SYSTEM



You can edit and backup system settings on the System tab, monitor the system and examine diagnostic information about the course.
You can also change license keys for servers on this tab, such as adding more camera channels and installing a new IP camera, metadata, and client plugin drivers.
Also, you can configure the software watchdog.

The tab contains these tools:

- System settings

- General system settings
- E-mail settings
- Command settings
- Change VMS server addresses
- System addresses
- Update VMS Servers
- Backup
- Export logs
- Backup settings
- Restore settings
- Monitoring
- SM Server diagnostics
- Local recorder diagnostics
- Licenses
- Watchdog
- Watchdog settings
- Watchdog logs
- Add-ins
- Install driver
- Install metadata driver
- Install client driver
- Install client plugin

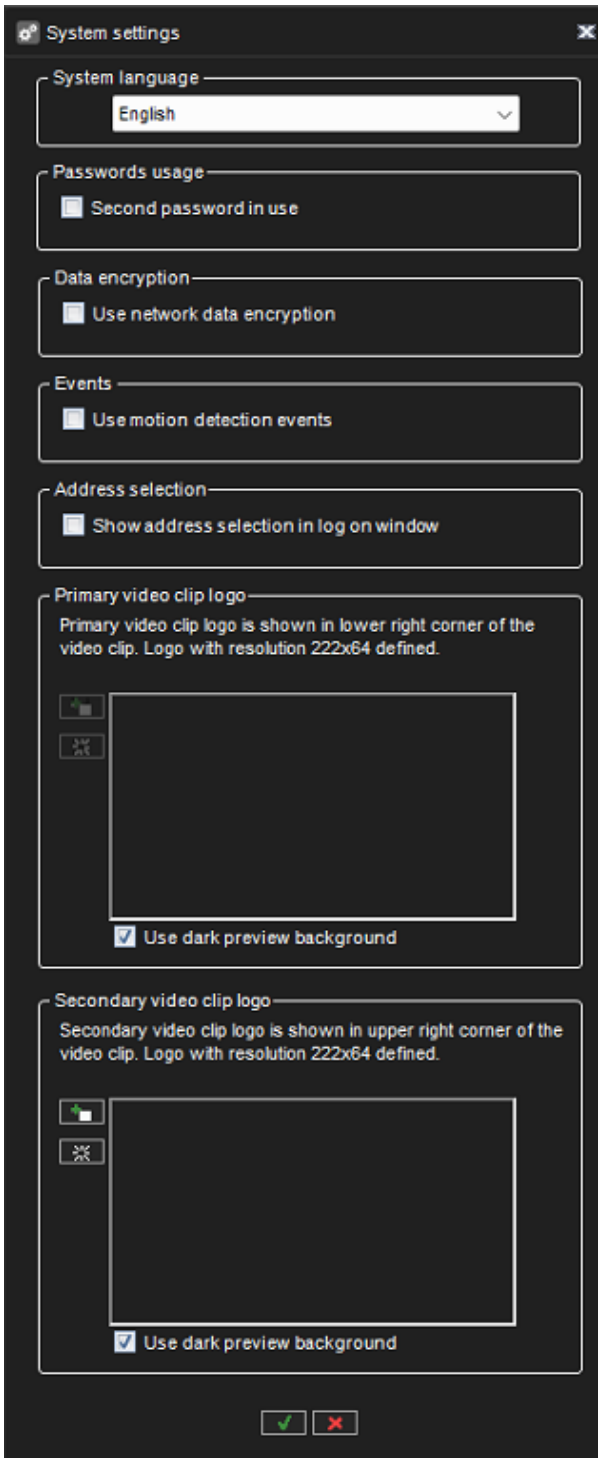
To open a tool, do one of the following:

- Click the tool and then click Edit
- Double-click the tool.
- Drag the tool from the **System** tab to the workspace

9.1 SYSTEM SETTINGS



9.1.1 General System Settings



9.1.1.1 In this section, you can control the following:

- System language
- The password usage

It is possible to configure the system to require two separate passwords for all users.
This is done by activating the "Second password in use" option in the general system settings.
When this mode is selected, all users are required to give two passwords.

The default second password is empty. This feature allows limiting so that no single person can review videos alone.

If one password is known to one person and the other password is known to another person, both persons must be present when reviewing videos.

- Data encryption
- Events (the setting for sending motion information to clients and over integrations)
- Address selection
- Primary video clip logo(Logos that are attached to exported video clips)
- Secondary video clip logo(Logos that are attached to exported video clips)

9.1.2 Configuring viewing station settings

9.1.2.1 Configuring settings for viewing stations:

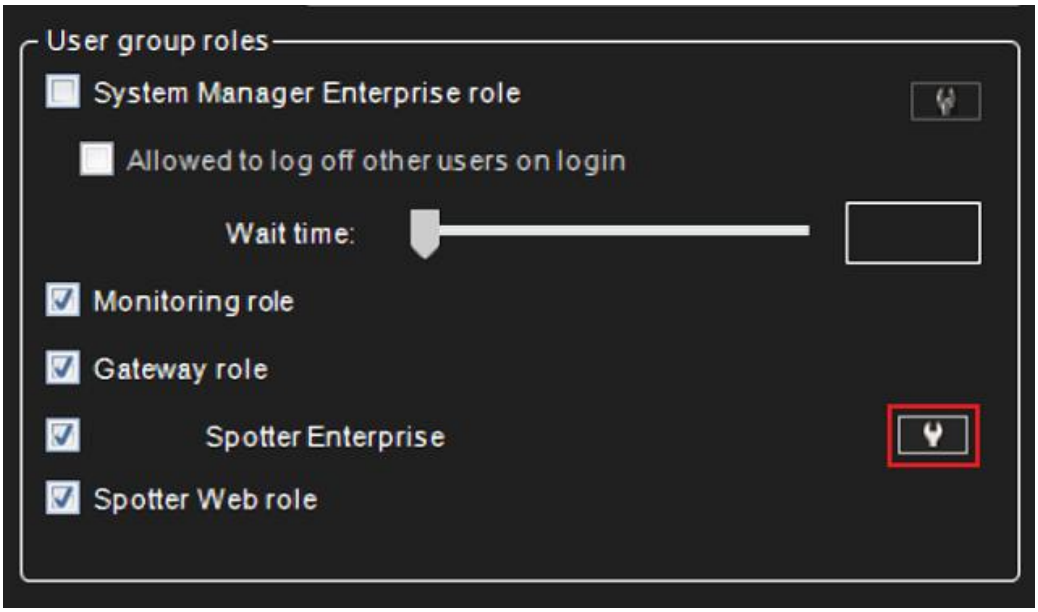
1. Go to the **System** tab in System Manager
2. Double-click on **Viewing station settings**
3. Click **Add new Spotter view station**
4. Set the name, address, and port for the station
5. Save changes

Viewing stations can be created, edited, or deleted in Viewing station settings.

9.1.2.2 Enabling sharing with viewing stations in user role settings:

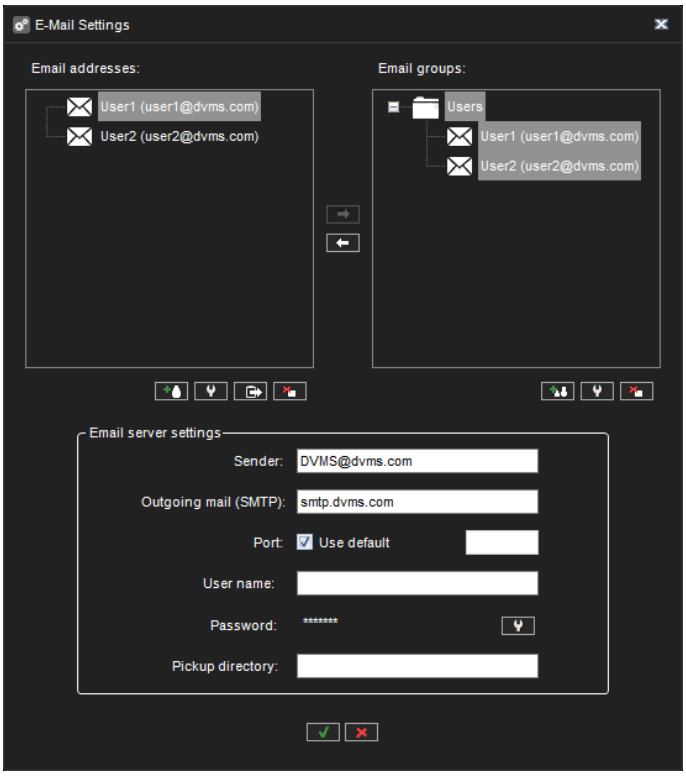
1. Go to the **Users and user groups tab** in System Manager
2. Double-click on a user group

3. Click **Edit Mirasys Spotter Enterprise role properties** in the User group roles section



1. Go to the **Viewing Stations** tab
2. Tick the checkbox for Enable sharing with viewing stations, and select the viewing stations the operator is allowed to share with from the list
3. Save changes

9.1.3 E-Mail Settings



You can specify e-mail addresses and groups which can be defined to receive reports about events specified in the Software Watchdog.

9.1.3.1 To set the e-mail notification settings:

1. On the **System** tab, open **E-mail settings**.
2. Type the sender's e-mail address into the **Sender** field. Note that some e-mail applications are configured to accept messages only from valid e-mail addresses.
3. Type the name of the outgoing mail server into the **Outgoing mail (SMTP)** field. The specified server will be used for sending all e-mail notifications.
4. Type the login information and port for the SMTP server into the appropriate fields.
5. Set the events for which notifications will be sent as instructed in the Software Watchdog.

Note: Emails are not sent to all system email recipients.

The administrator can control which Watchdog events and alarms to which email recipients or groups the email is sent.

9.1.3.2 To add new e-mail addresses to the system:

1. On the **System** tab, open **E-mail settings**.

2. Click **Add new e-mail address** to add a new address.



3. Type the recipient's name and e-mail address into the **Name** and **Address** fields.
4. Click **OK**.

9.1.3.2.1 To add a new e-mail group to the system:

1. On the **System** tab, open **E-mail settings**.
2. Click **Add new e-mail address** to add a new address.



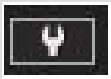
3. Type the group name
4. Click **OK**.

9.1.3.3 To add one or more recipients to a group:

1. Highlight the desired group on the group list
2. Highlight the desired recipient(s) in the recipient list
3. Click on the arrow to add the selected recipients to the selected group

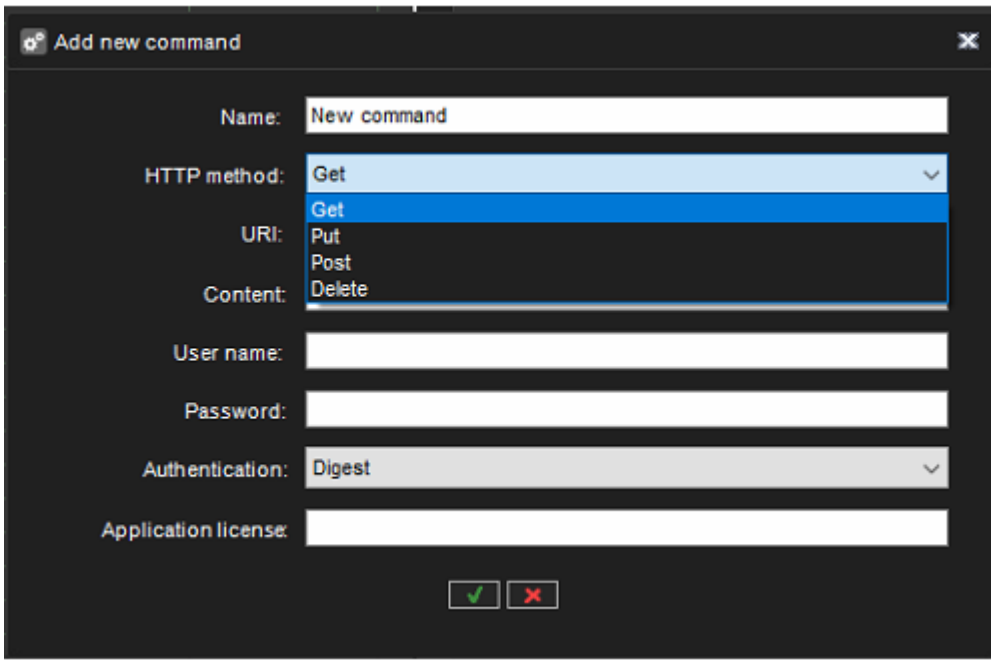


9.1.3.4 Other available actions:

	Editing email names, addresses, and group names and removing persons from groups is possible with the edit buttons.
	Persons can be removed from groups with the arrow.
	Persons and groups can be removed with the button.
	Test email can be sent with a button to a selected email address using the settings defined in the email settings dialogue.

9.1.4 Command Settings

Command settings are used for HTTP command sending



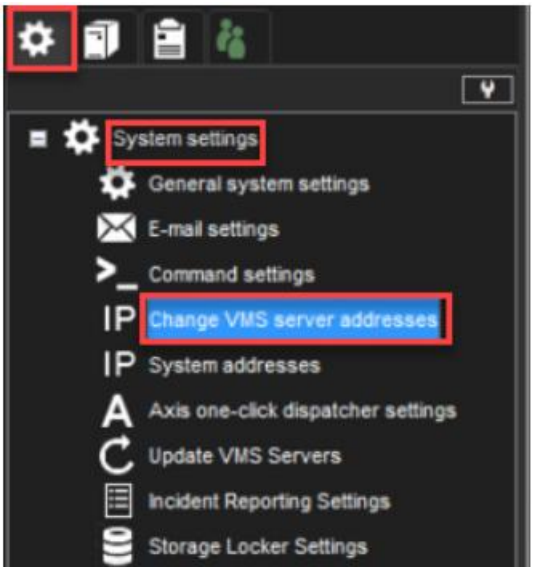
9.1.5 Change VMS Server Addresses

If the server will function as the Main Server of a system, and if it will be accessed over a network, you have to set the server's IP address through the System Manager application. IP address and DNS names can be modified in the **Change VMS Server addresses** tool.

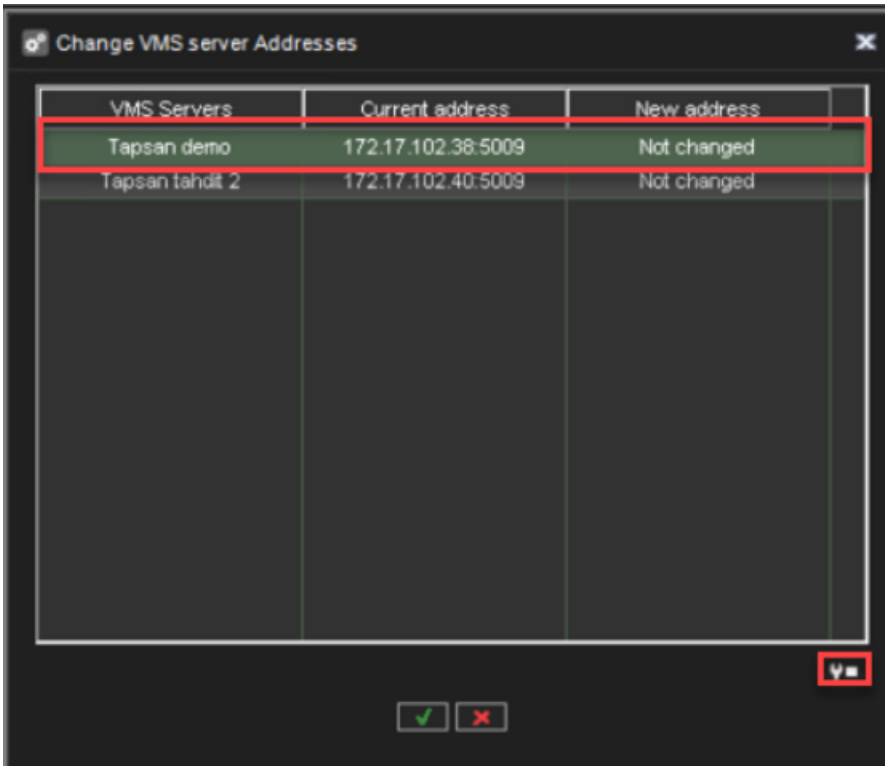
> You only need to set the local IP address for the Main Server of a system if the server can be accessed over a network. If the server is accessed locally, there is no need to set the address.

9.1.5.1 Changing a server's IP address or DNS name:

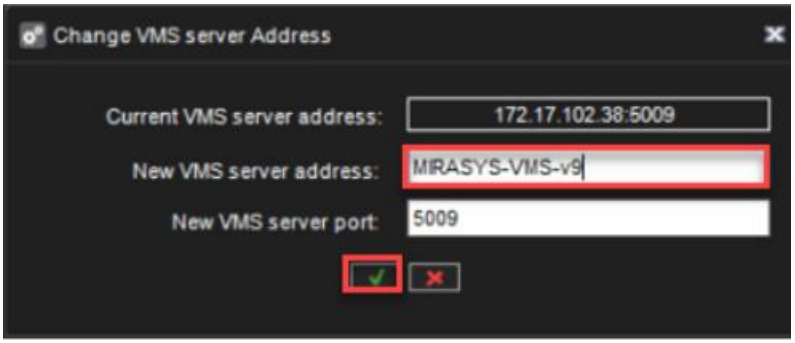
1. On the **System** tab, open **Change VMS server addresses**.



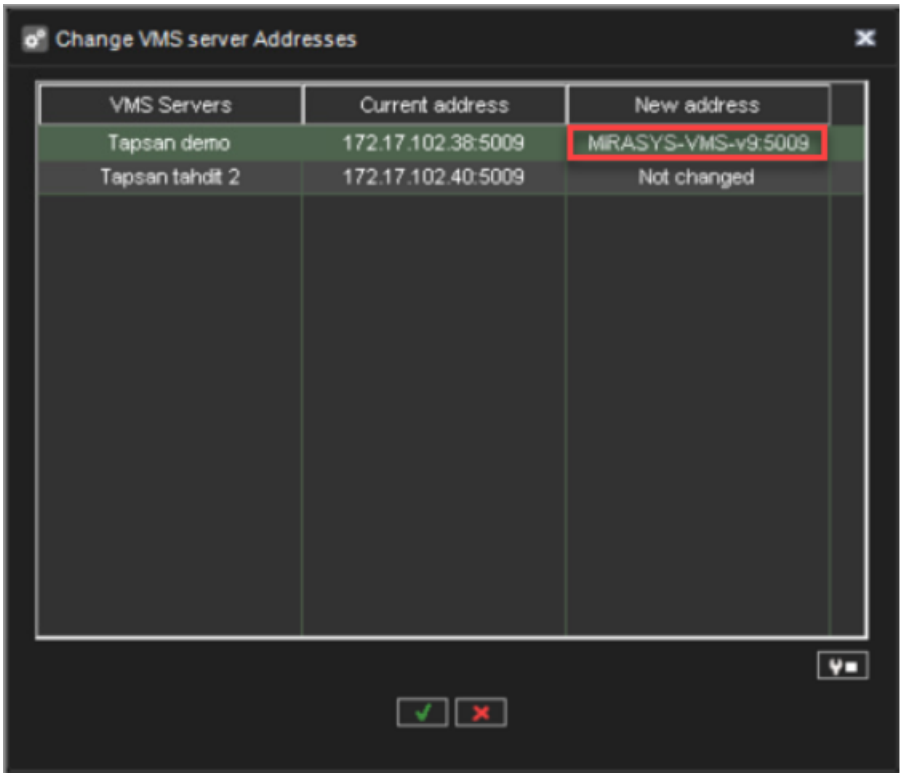
1. Click the server and click **Change VMS Server address**.



1. Type the new IP address or DNS name of the server into the **New VMS server address** field.
2. Click **OK**.



The changed address can be seen in the “New address” field.



9.1.6 System Addresses

A Main Server is the central server of a surveillance system.

All other VMS Servers connect to it, and all client applications communicate through the Main Server. During the login phase, the client applications can select the Main Server they will connect to.



You can define multiple Main Server addresses that the client applications can connect to. The addresses can be provided as IP addresses (e.g. *http://195.168.0.1*) or DNS names (e.g. http://www.example.com).

Note: *Users can connect to any of the defined Main Server addresses provided they have a compatible username and password for the Main Server.*

9.1.6.1 To add a Main Server address:

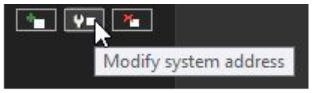
1. On the **System** tab, open **System addresses**
2. Click **Add new system address**.



3. Type the new system address (either IP address or DNS name) to the **Add** field.
4. Click **OK**.

9.1.6.2 To edit a Main Server address:

1. On the **System** tab, open **System addresses**.
2. Click on the Main Server address with the changed IP address.



3. Click Modify system address .
4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

9.1.6.3 To remove a Main Server address:

1. On the **System** tab, open **System addresses**.
2. Click on the Main Server address you want to remove.
3. Click **Remove system address**.



9.1.7 Axis one-click dispatcher settings

9.1.7.1 Installation steps

Install the O3C-server as described in the guide "AXIS O3C Server Reference. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

9.1.7.1.1 Important things:

1. Install the O3C-server as described in the guide "AXIS O3C Server Reference. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

Important things:

- setup provider certificate authority:

Directory in which the CA should be set up [default: ca]: (by default ca)

Passphrase for the CA key (DO NOT FORGET THIS!) [default: N/A]: pAs_sw!ord (some password)

Valid time, in days [default: 7300]: 100 (any number)

9.1.7.1.1.1 Issue a server certificate:

Path to the CA directory [default: ca]: (as above)

Passphrase for the CA key [default: N/A]: pAs_sw!ord (as above)

Subject Alternative Names (separated by comma) [default: N/A]: 172.17.102.56 (very important!!! Should be equal IP address of O3C server)

Valid time, in days [default: 398]: 100 (as above)

Result:

Concatenated server certificate and key saved to: ca/issued/stserver_EA363E5578E696E7.pem

Register O3C server as service in Windows SCM: there is needed the Power Shell tool for Windows! And for install call:

.\setup_service.ps1 add -c C:\o3c-server\o3c-server.conf

9.1.7.1.2 Configure o3c-server.conf

listen_client = 172.17.102.56:80

IP and port where the server will wait for the client (the camera) connections

stserverid = test_o3c_server

Any string

cert_file = C:\o3c-server\stserver_EA363E5578E696E7.pem

issued server certificate created after command: "pkitool issue-server-cert"

provider_ca = C:\o3c-server\stserver_ca.crt

CA certificate from ca directory created after the command: "pkitool setup-provider-ca"

provider_name =

can be left blank

credentials = root:root

for device access requests

9.1.7.1.3 O3C-server service

By default, the service is called Axis O3C Server in Services or O3C-server in command prompt.

1. Start the O3C-server service
2. Enable One-click technology on the camera as described in the 4.1 part of the guide.
3. Disable firewalls or add O3C-server to the exceptions
4. Register the camera as described in guide 4.2 part.
    a. http://172.17.102.56/admin/dispatch.cgi?action=register&user=adp_mirasys_100&pass=GQ41lSRbbEb4w3sorkN8&mac=B8A44F17AAFA&oak=8A22D6434817&server=172.17.102.56:80
    b. where:user=adp_mirasys_100, pass=GQ41lSRbbEb4w3sorkN8 - Mirasys credentials (Provider name and password) from Axismac=B8A44F17AAFA, oak=8A22D6434817 - MAC address and OAK key from the camera

c. To find the MAC address using the following string in the browser: http://172.17.100.84/axis-cgi/admin/param.cgi?action=list&group=Network

d. server=172.17.102.56:80 - as "listen_client" in o3c-server.conf

5. Check that the camera was connected to the O3C-server: call in the browser th string: http://172.17.102.56:80/admin/status.cgi 172.17.102.56 - IP address of O3C-server

6. And check that there is a comment about the connected client as follows: "id=4.b8a44f17aafa srcaddr=172.17.100.84:34148 accepted=1 v=2 rx=0 tx=0 connected=2022-01-10T12:45:40.875571Z

Total number of clients: 1"

PS: the camera tries to connect to the server every 20 seconds

1. Check that we can get options from the camera: for that, it needed to configure the proxy settings for browser -

2. Open system Internet Options

3. Select Connections tab -> Select LAN settings button -> to enable "Use a proxy server for LAN (...)" and input the proxy IP address and port. (in the current case there is a local IP address and port 80)

4. After that we can get the camera capabilities in the browser:

   a. http://b8a44f17aafa/axis-cgi/param.cgi?action=list&group=root.RemoteService where b8a44f17aafa - MAC address of the camera

9.1.7.1.3.1 Filter for wireshark for Axis P1375:

((ip.src == 172.17.100.84) && (ip.dst == 172.17.102.56)) || ((ip.src == 172.17.102.56) && (ip.dst == 172.17.100.84))

9.1.7.2 Add Axis One-Click Camera

1. Open **System tab**

2. Go to **System Settings** and open **Axis one-click dispatcher settings**

3. Enter all necessary details and click **OK**



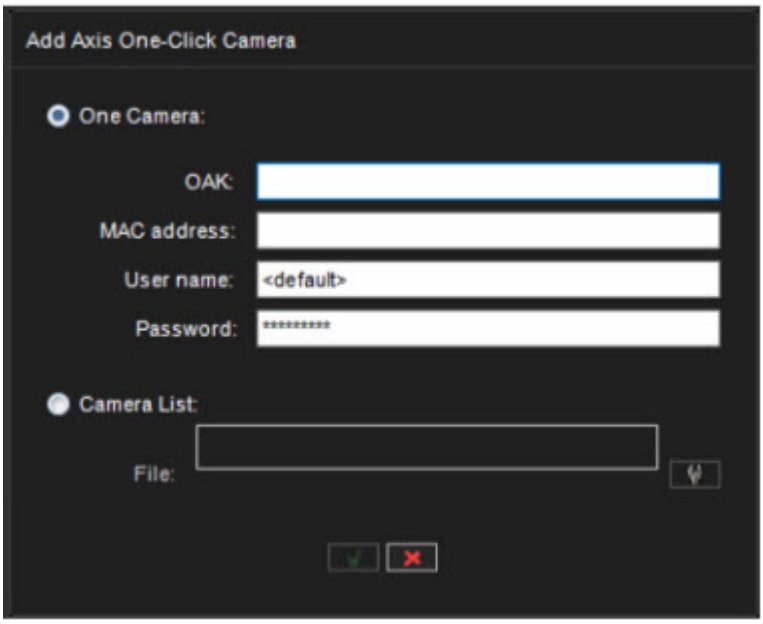
4. Open the **VMS Servers tab**

5. Click **Hardware**

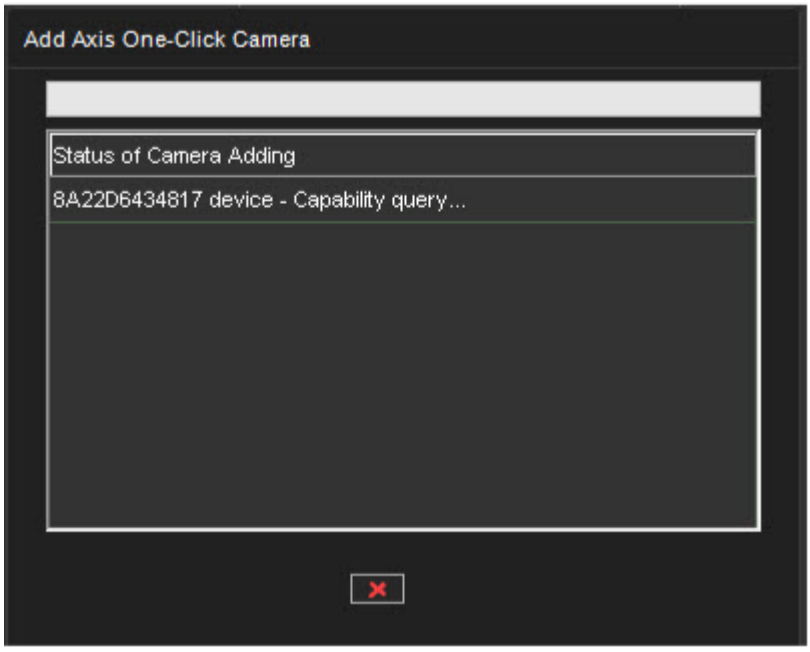
6. Click **Add Axis One-Click Camera** icon



7. Enter Axis One-Click Camera details and click **OK**



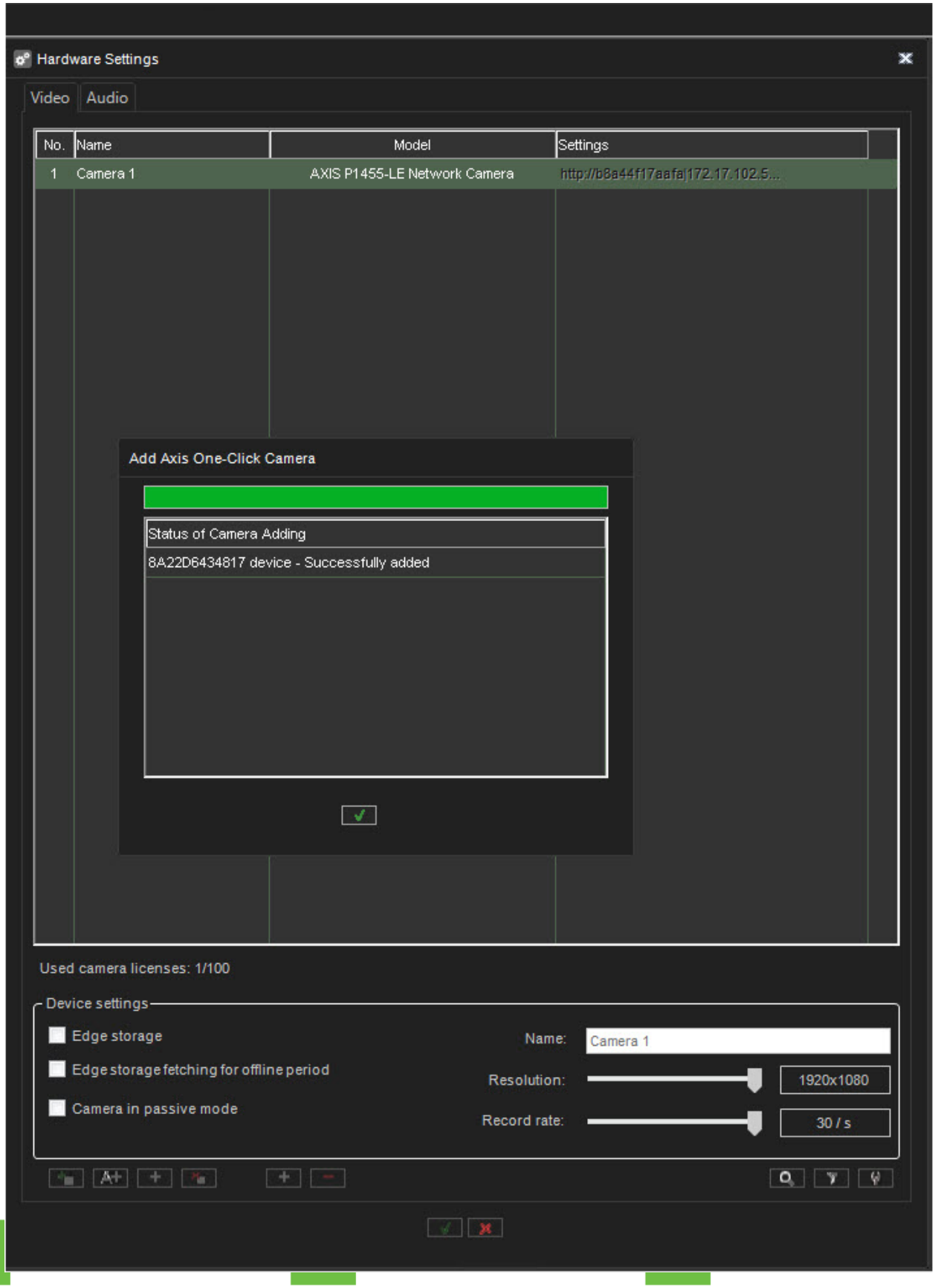
After clicking the OK, the camera query starts



When the camera query is finished, the device will be added to the hardware list

8. Click **OK** to finalize

MIRASYS

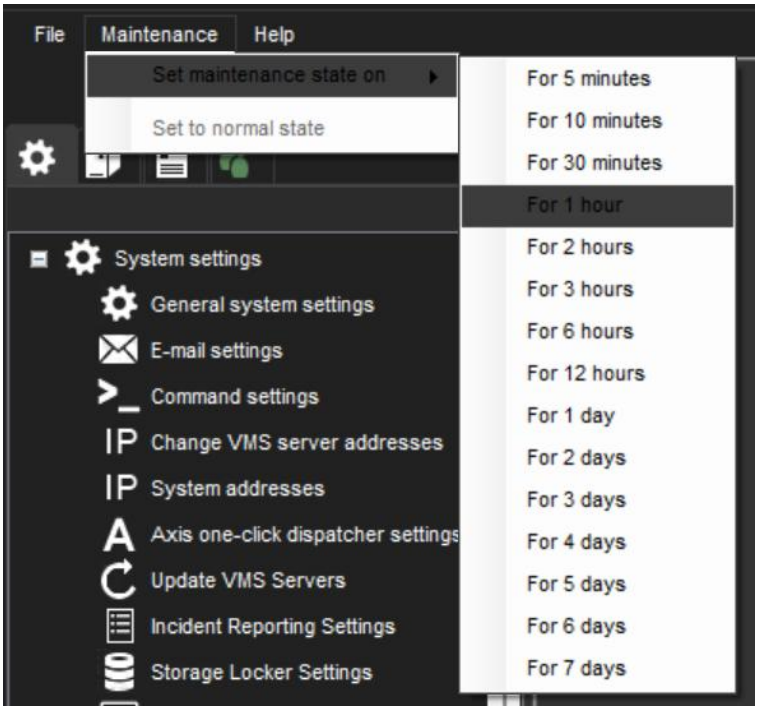

Hardware Settings
Video
Audio
No.
Name
Model
Settings
1
Camera 1
AXIS P1455-LE Network Camera
http://b8a44f17aafa|172.17.102.5...
Add Axis One-Click Camera
Status of Camera Adding
8A22D6434817 device - Successfully added
Used camera licenses: 1/100
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Camera 1
Resolution:
1920x1080
Record rate:
30 / s

9.1.8 Update VMS Servers

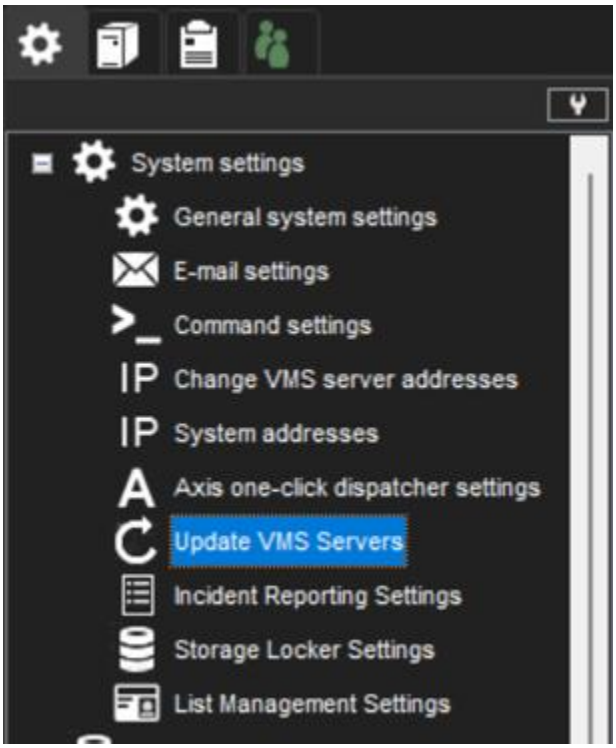
It is possible to update all connected VMS Servers remotely via the **Update VMS Servers** –option
The Main server must be upgraded from the Windows **Control Panel\Programs\Programs and Features\Uninstall or change a program.**

> Please remember to set the **Maintenance state on** before upgrading.

1. Click **Maintenance**
2. Select **Set maintenance state on**
3. Select the duration of the maintenance mode



9.1.8.1 Updating VMS servers

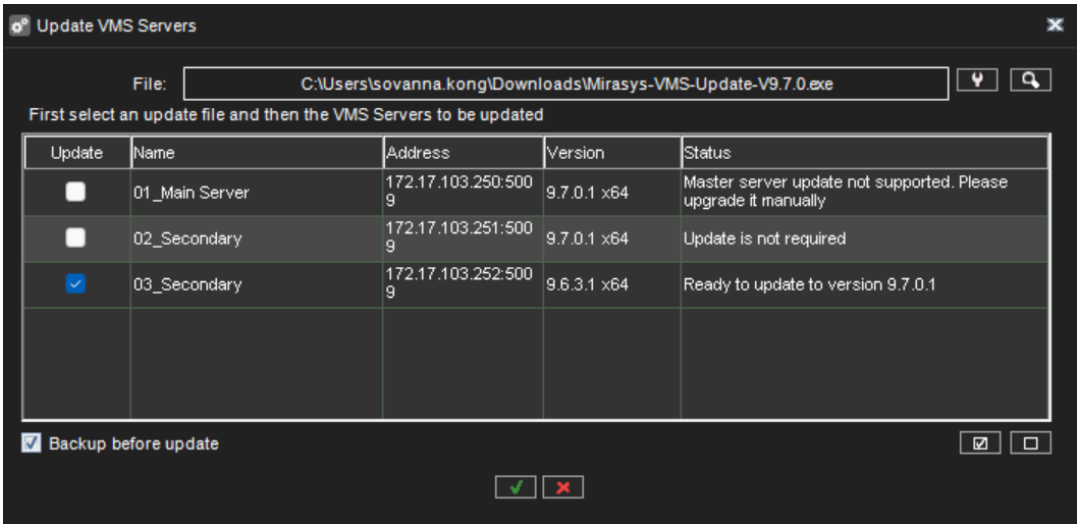


To update servers, first, select the installation file with the button:



The list is updated to show which servers can be updated with the selected installation file.

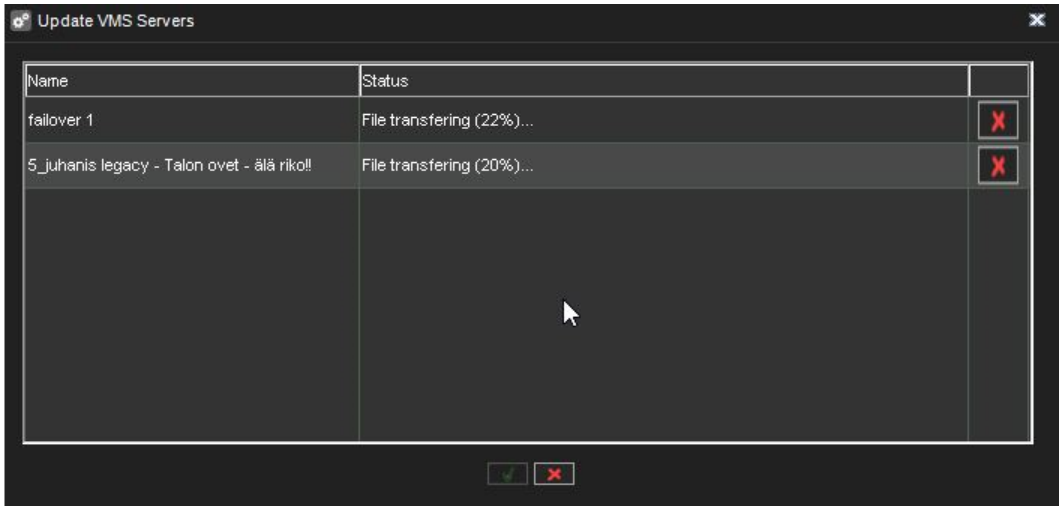
Note: *When performing a major version upgrade, for example, from VMS 6. x to 7. x, it is usually necessary to first upgrade the server licenses, and only after this upgrade the VMS software.The Update VMS Servers dialogue will inform the user if a license upgrade is needed before the software update.*Next, choose which servers you want to update and if you want to perform a backup before updating.



By selecting this button



you will start the update, and an update progress dialogue is shown:



This dialogue can be closed at any time without affecting the server updates.

Notes:

- The progress dialogue might display no status information for the installation file transfer and update progress if the network connection is slow or intermittent.

- This is no cause for alarm; in most cases, the update will be successful, but it might take a long time (20 – 30 minutes).
- It is recommended to prepare for the possibility to have remote access to any such servers.

- If a local server were selected to be updated, the system manager would automatically close after this dialogue is shown.
- In rare cases, some servers require system restart after remote VMS software update if the connection between the Main Server and VMS Server is not returning after the update.
  - It is recommended to monitor the connection to VMS Servers after the update.
- Since Version 7.4.3, Mirasys VMS has had support for 64-bit servers. The upgrade from 32-bit (x86) to 64-bit can be achieved precisely by installing any DVMS version.
  - After the update, the control panel of windows will show DVMS-x64 for 64-bit DVMS.

9.1.9 Incident Reporting Settings

From the Incident Reporting settings, the user predefines the parameters, which will be used while viewing or exporting the Incident or Daily log reports.

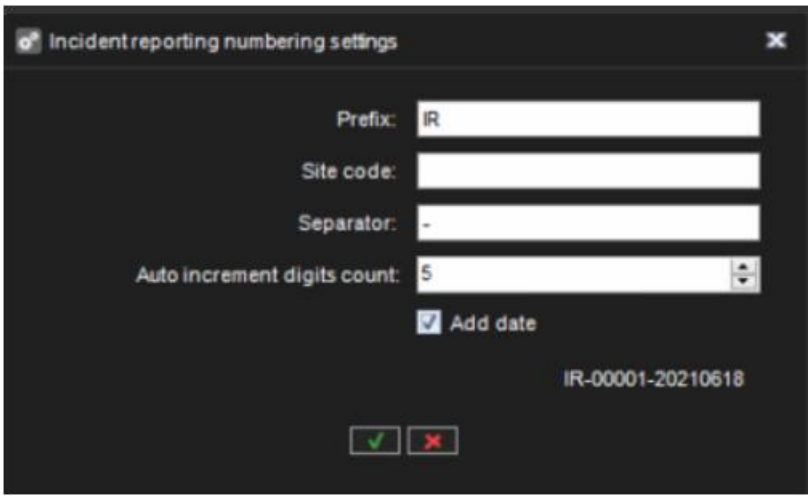
9.1.9.1 Company information

- Company name
- Company address
- Company logo

9.1.9.2 Reporting numbering

Incident Reporting numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



9.1.9.3 Daily log numbering details:

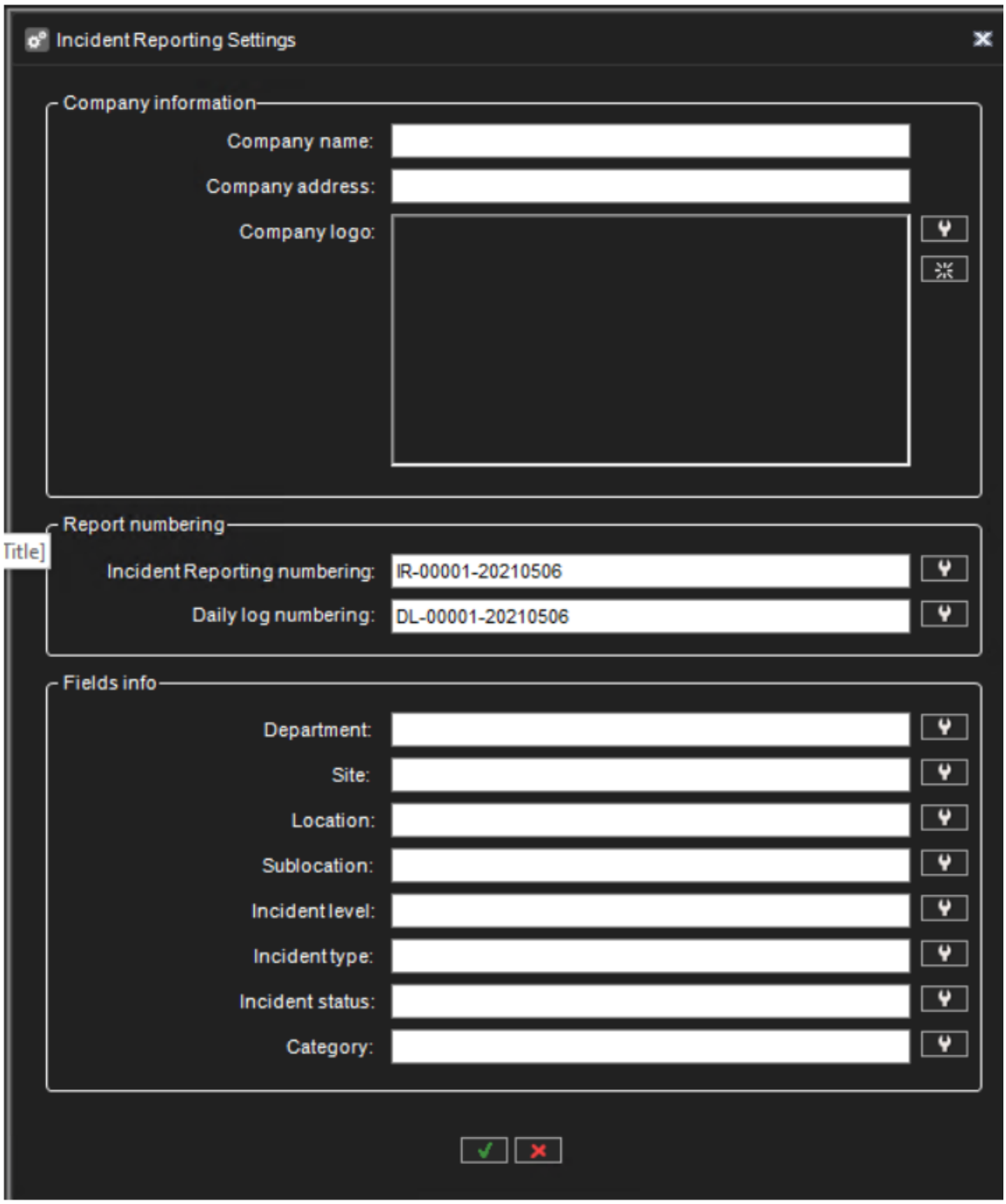
- Prefix
- Site code
- Separator
- Autoincrement digits count



9.1.9.4 Fields info

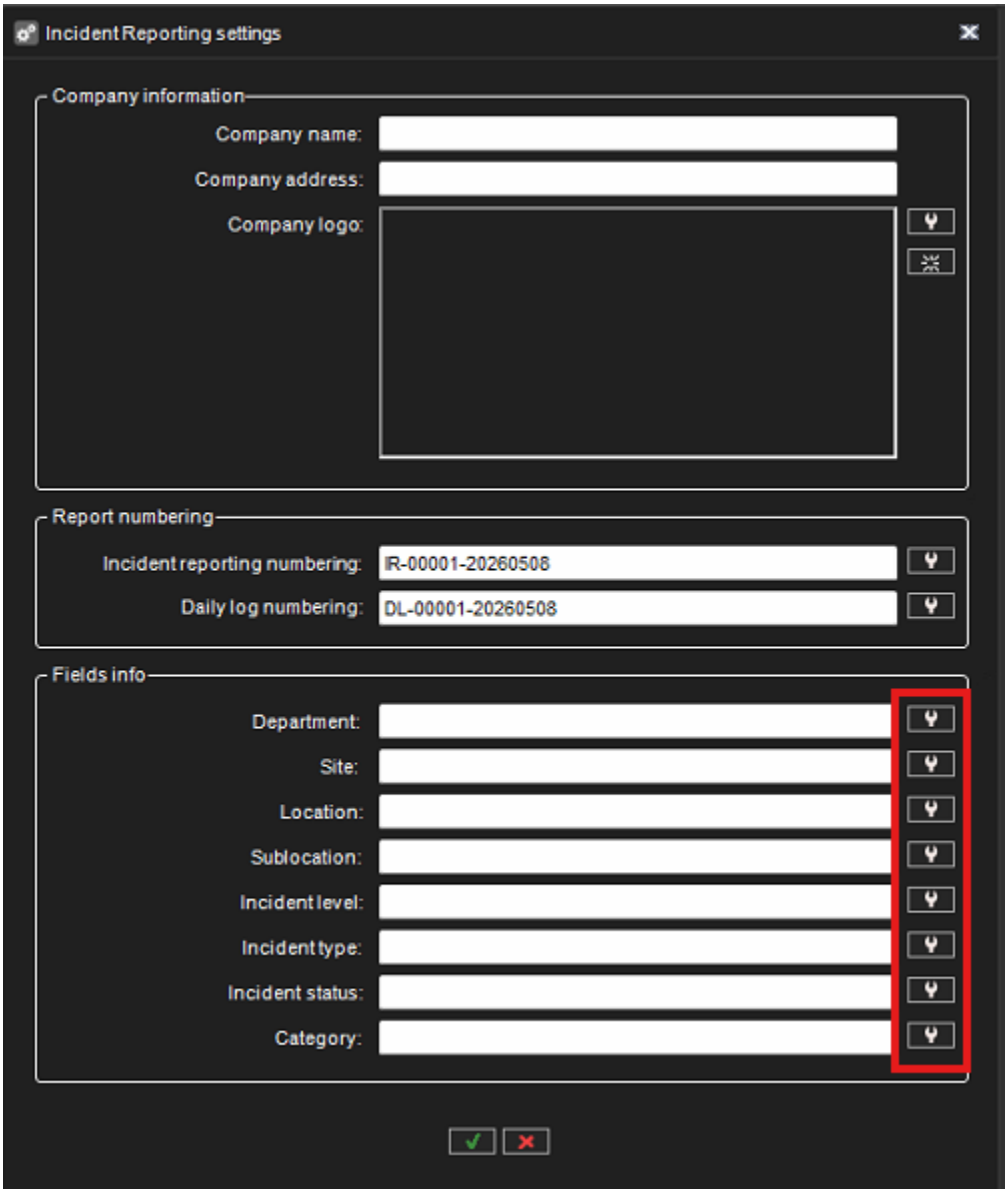
- Department
- Site
- Location

- Sublocation
- Incident level
- Incident type
- Incident status
- Category

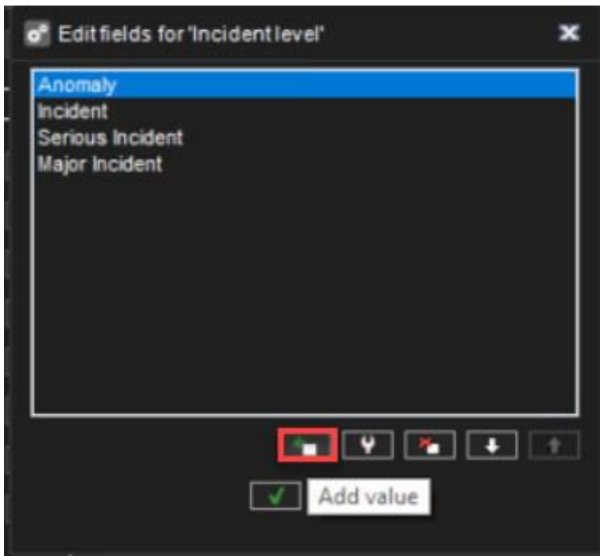


9.1.9.5 Add values

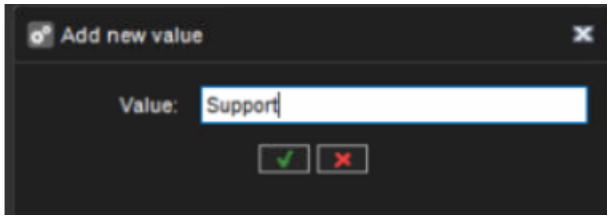
1. Select the correct field and click **Update values**



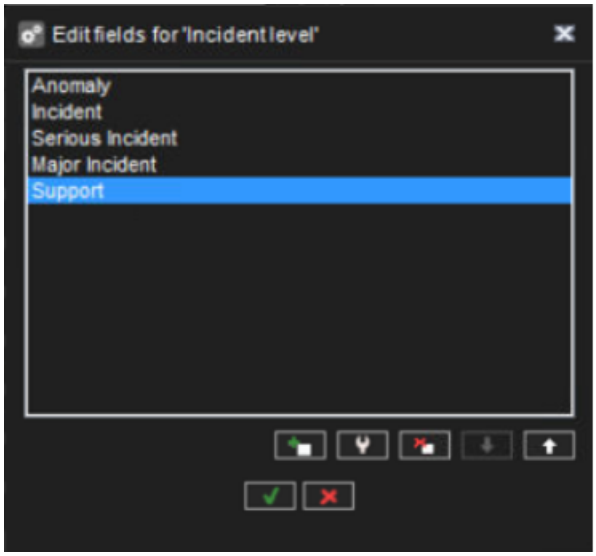
2. Click **Add value**



3. Enter the name of the value
4. Click **OK**

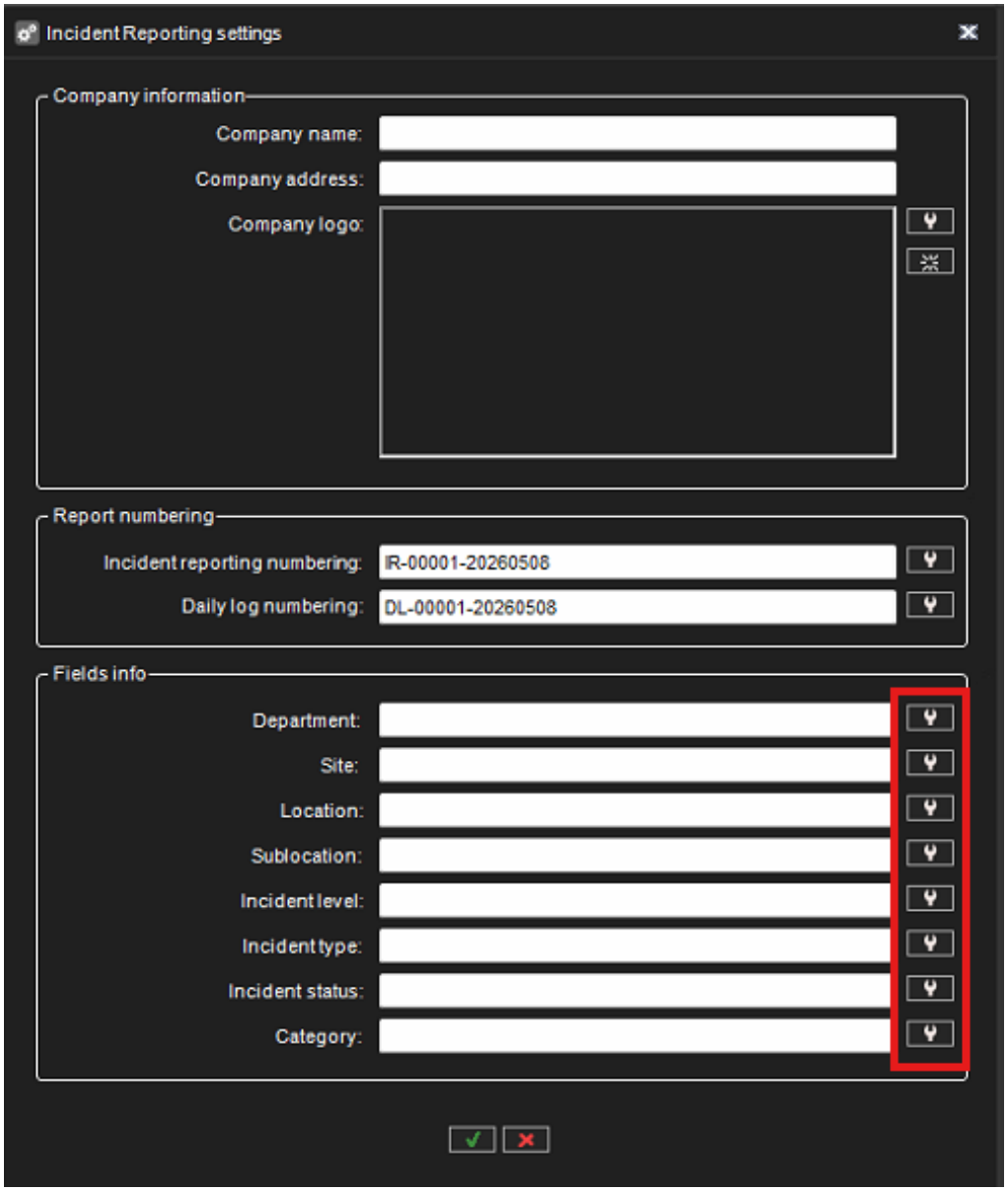


5. New added value can be seen in the list

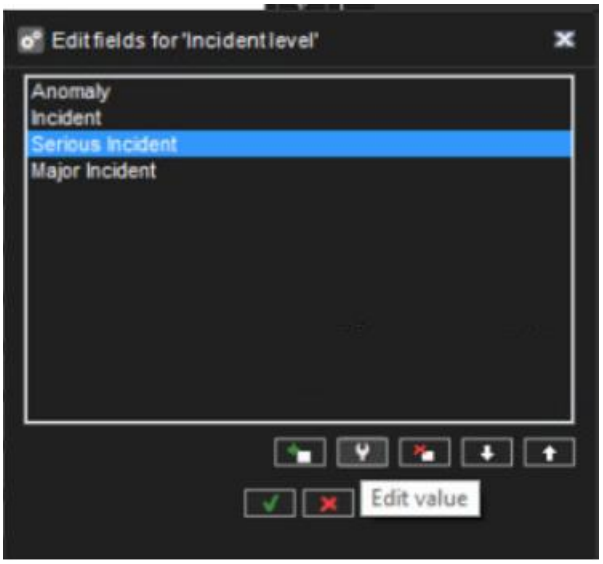


9.1.9.6 Edit values

1. Click icon **Update values**



2. Select a value from the list and click **Edit value**

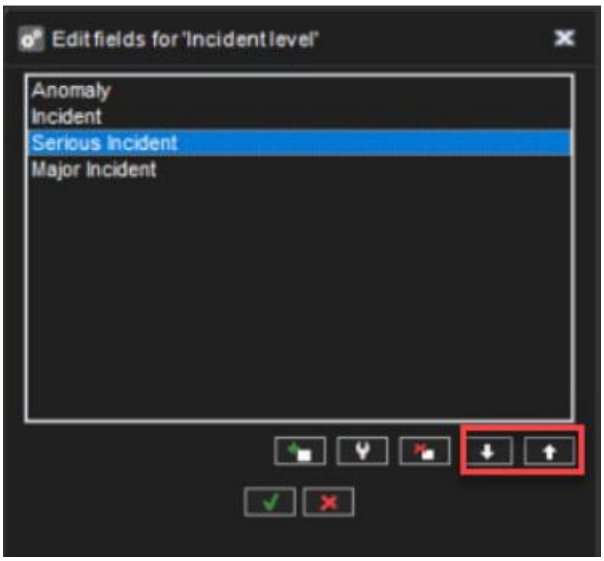


3. Enter a new value name and click **OK**



9.1.9.7 Changing the order of the values

1. Select the value and click arrows to set the proper order of the values.
2. Click **OK** to confirm changes



9.1.10 Storage Locker Settings

Storage Locker Settings contains the following values:

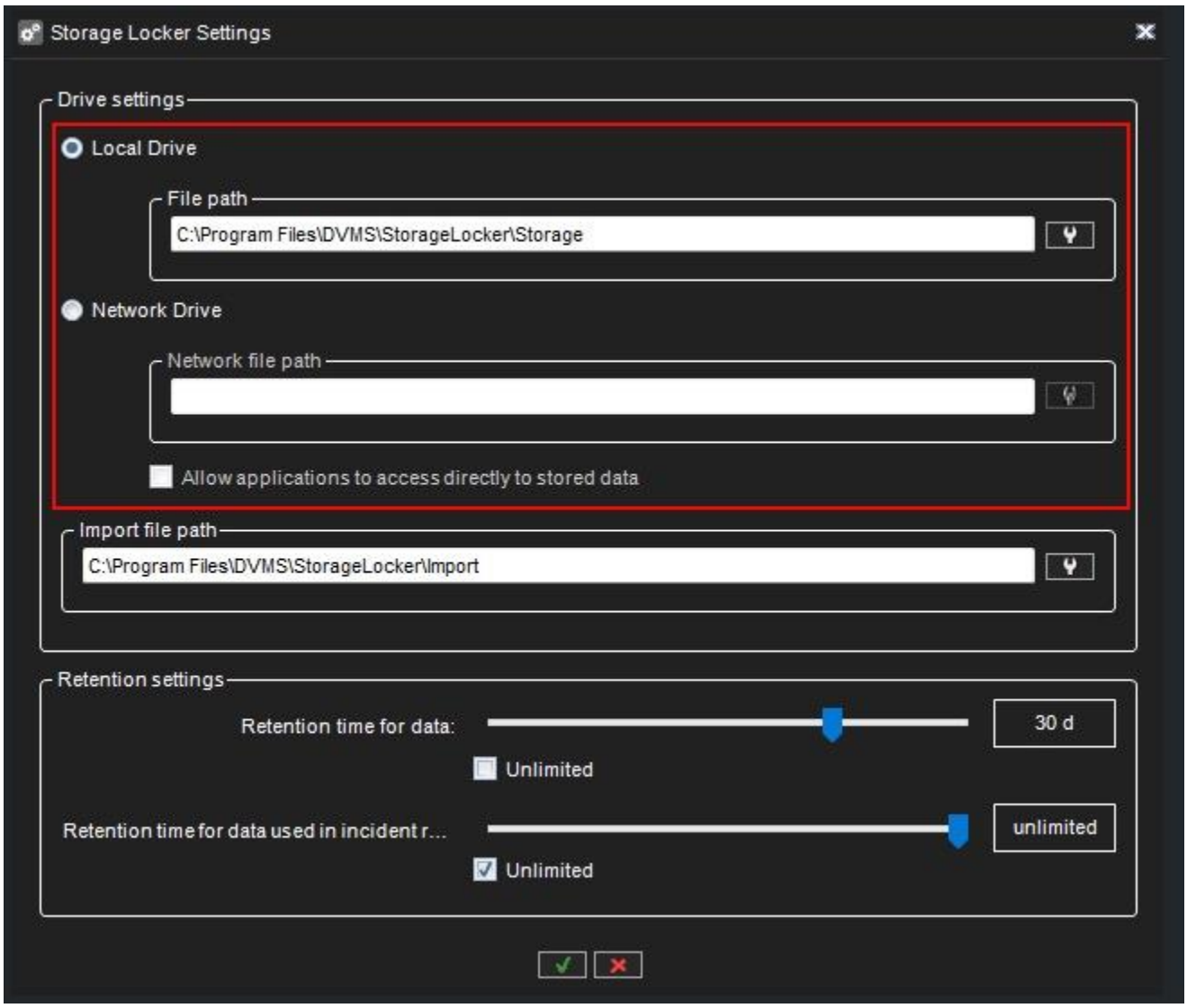
9.1.10.1 File path:

Defines the location of the Storage Locker file storage that can be either local or network disk. As the default location, Storage Locker file storage is located in the main server's local disk.

9.1.10.1.1 Changing the file path

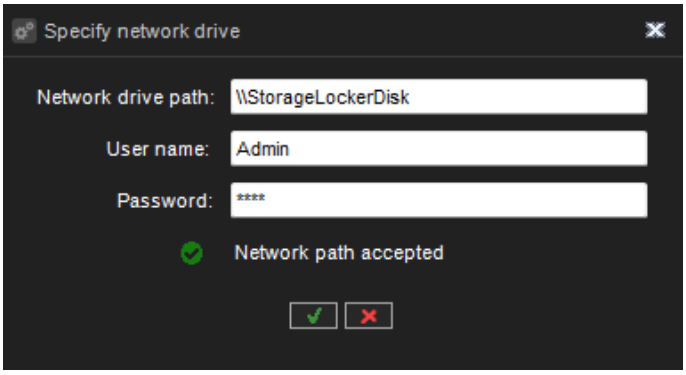
Please note that old storage locker data is not copied to the new location

1. Select if a local drive or network drive is used.



2. If the local drive is selected, click **Set file path for data storage.** Select a new location and click **OK.**

3. If a network drive is selected, click **Set network file path for data storage.** Specify network path, username, and password and click **OK.**

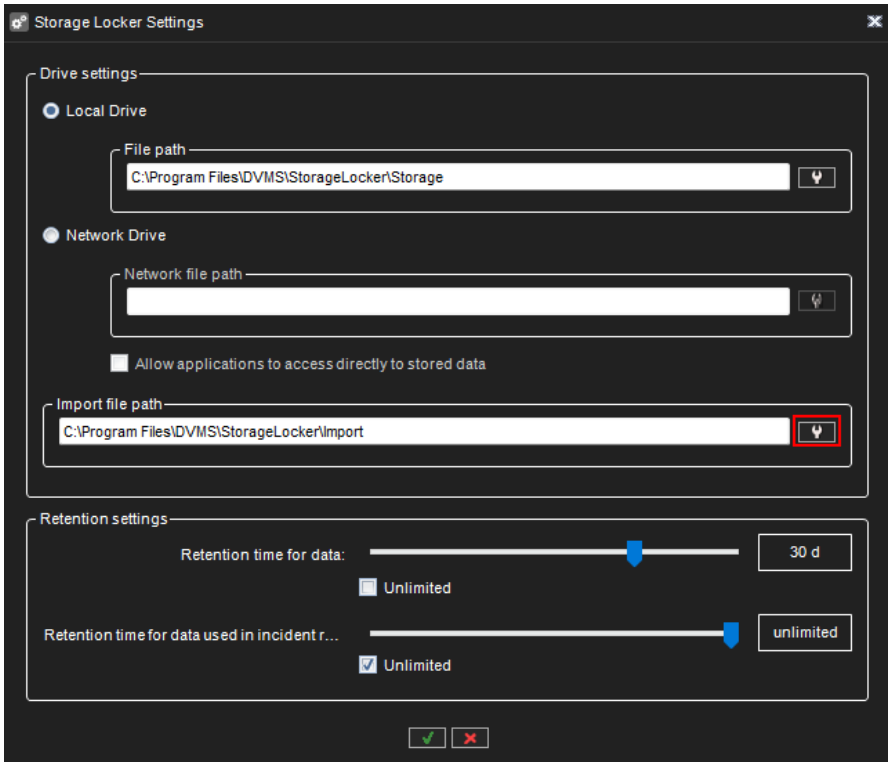


When a network drive is used for Storage Locker data storage, it is possible to allow Spotter applications directly to access saved data from the network disk by checking the option **Allow applications to access directly to stored data**.

9.1.10.2 Import file path:

If someone has exports that are needed to be added to the Storage locker, those exports should be placed in a folder that is defined in Storage locker settings as "Import file path". How to use:

- Each import data need to be in its own folder, files that will be placed into the import folder directly will be ignored
- Each import folder can have several subfolders
- Images and clips can be placed in one folder, Storage locker will import them one by one
- SEF archives should be in their own folder and not mixed with other data (like images, clips, etc.)
- Import data should be copied all at once if something should be added - it should be copied with its own folder, files added to existing folders are not supported (those files will not be processed)

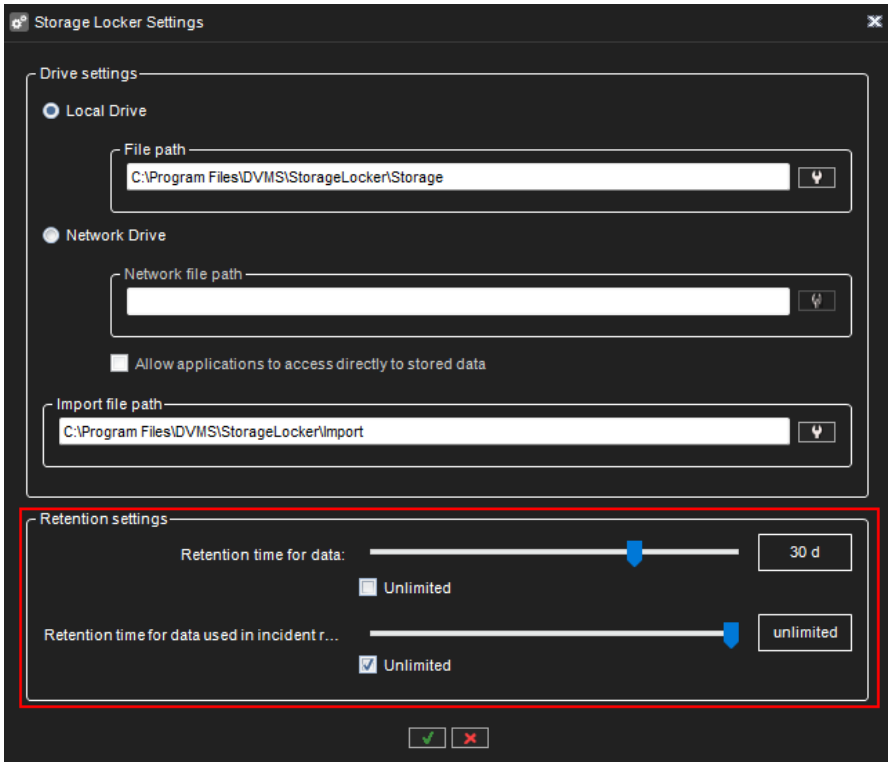


9.1.10.3 The retention time for data

The retention time for data sets defines how long Storage Locker retains data, which are not used in any Incident Report

9.1.10.4 The retention time for data used in the incident reports

The retention time for data used in incident reports defines how long Storage Locker retains data, which are used in any Incident Report



9.1.11 List Management settings

List management makes it possible to define identities and lists so that the allowed or not allowed identities can be defined.

The settings define and manage identity and list management settings. Settings allow you to:

- Add, edit, and delete identities containing license plates and face images
- Add, edit, and delete lists and manage list content
- Import and export lists and identities
- Configure LPR and FR event database retention limits
- Enable and define integration and its settings

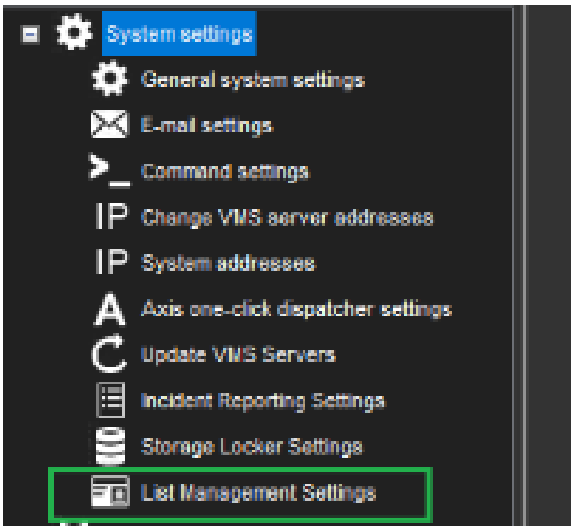
The System Manager application provides several dialogs to access and modify the list management service data and settings. The dialogs can be found in the “System settings“ section.

> Integration requires LPR and FR integration licenses.

9.1.11.1 List Management Settings

How to open the **List Management Settings** dialog:

1. Go to the **System** tab
2. Under **System settings**, double-click the **List Management Settings** tree node, as shown in the picture below:



1. When you double-click **List Management Settings,** the dialog loads the settings from the list management service and displays them if successful. If loading fails, an error message is displayed to the user, and the dialog is closed.

9.1.11.2 List Management Settings dialog

In the dialog, you can find the following tabs:

- **Identities** - list of identities and their settings
- **Lists** - identity lists and their settings
- **Import/Export** - import/export functionality to restore/save list management data to CSV text format
- **Database Settings** - parameters related to the list management service database
- **Integration Settings** - integration enabling and integration settings

All changes you make in these dialog tabs can be saved by clicking the **OK** button.

If you do not need to keep the changes, you can close the dialog with the **Close** or the **Cancel** button.

Below you can find a detailed description of each tab.

9.1.11.2.1 Identities tab

In the **Identities** tab, you can perform operations with identities:

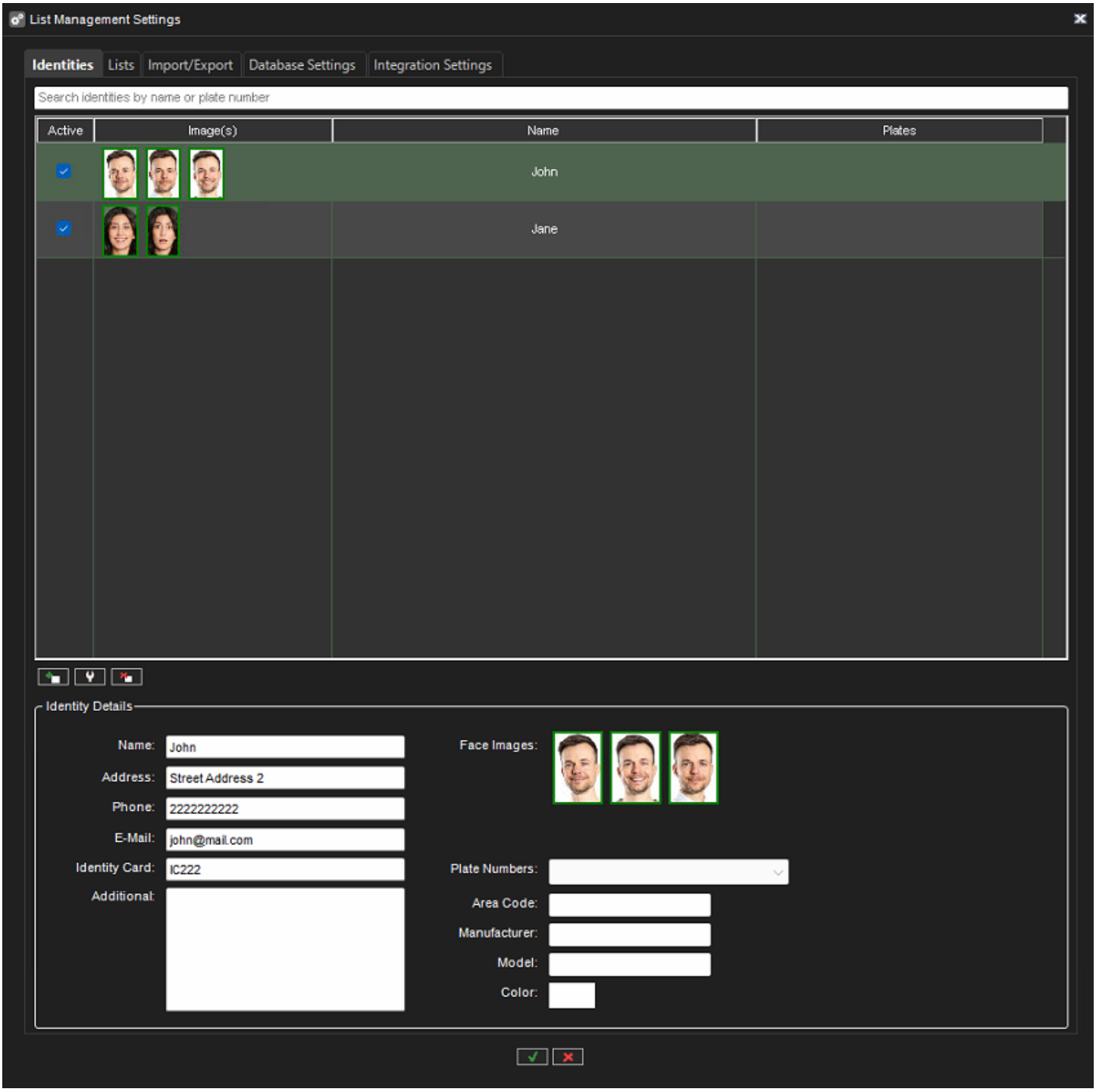


Figure 1 Identities tab

Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

Identity selection is done using the left mouse button. If you must select multiple identities (multiple rows in the list), you can use the left mouse button + Ctrl/Shift keys. With multiple selections, you can set selected identities to the "active" or "not active" state by clicking the checkboxes in the “Active“ column.

Above the list of identities, you can find the **Search** field: when you type here, the list of identities is automatically filtered if the text is found in identity names or plates.

You can add and remove selected identities with the **Add** and **Remove** buttons below the identity list.

You can see detailed information about an identity in the **Identity Details** area, but all these fields are read-only. To modify the selected identity, you can click the **Modify** button or double-click it with the mouse button.

When you add or modify an identity, the following dialog is shown:

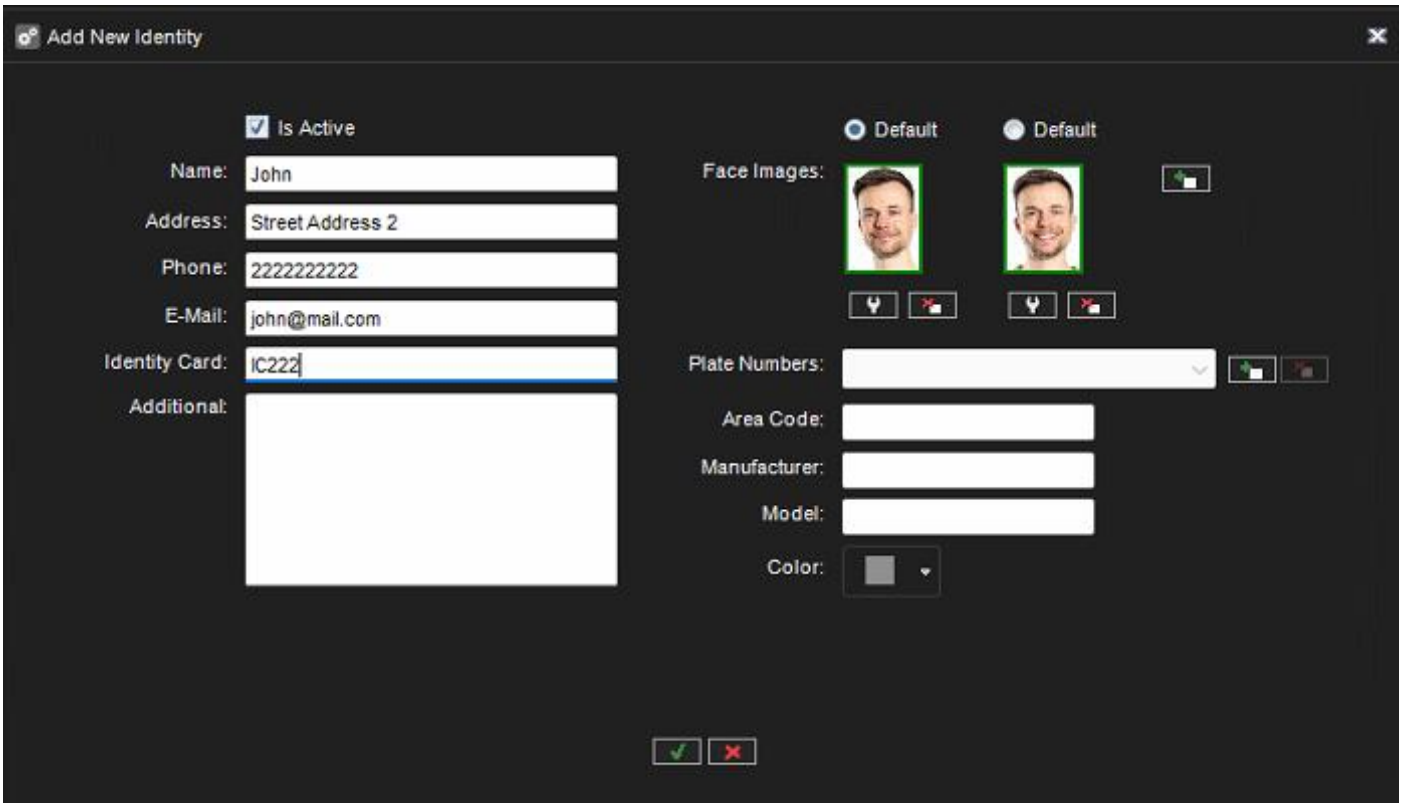


Figure 2 Add/Modify Identity dialog

You can change any field of data or add/remove identity face images or vehicles (license plates).

To add a face image, click the **Add a new face image** button, and the following dialog will open:

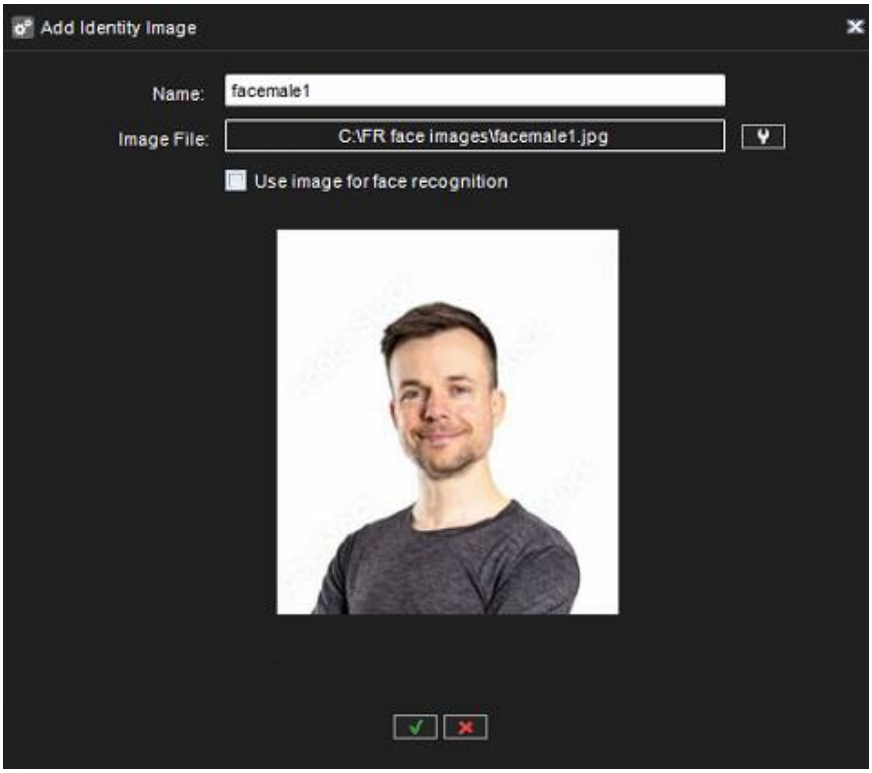


Figure 3 Add Identity Image dialog

You can write a face image name and select a face image file here. After file selection, the image will be loaded, and the feature vector data of the image will be calculated. An image can be selected to be used in FR by selecting the "Use image for face recognition" checkbox. To remove a face image, click the **Remove selected face image** button below the image in the Add/Modify Identity dialog.

The maximum number of face images for an identity is 3. All face images selected to be used with face recognition will be used when doing identity face matching, so using multiple face images for an identity may increase the face detection confidence.

To calculate the face feature vector, at least one face recognition service must be started and registered in the VMS.

9.1.11.2.1.1 Face image quality requirements

Images used for face recognition require a minimum resolution of 168x256 pixels to prevent false matches. The minimum size of the face in the image is 112 pixels. If an image is detected as too large, it will be resized automatically.

The quality value of an image is indicated by one of three colors in an outline around the image. Red (low) means that the image is not accepted due to quality requirements not being met. Yellow (medium) indicates that while the image can be used, it is recommended to update to an image with higher quality. Green (high) means that the image meets the quality requirements and therefore can be used. The face quality value is displayed for all selected images in the identity settings, and the user will receive a warning message if at least one of the used identity face images must be updated. Identities in the identity list can be sorted based on image quality (lowest to highest or vice versa) by clicking the image column.

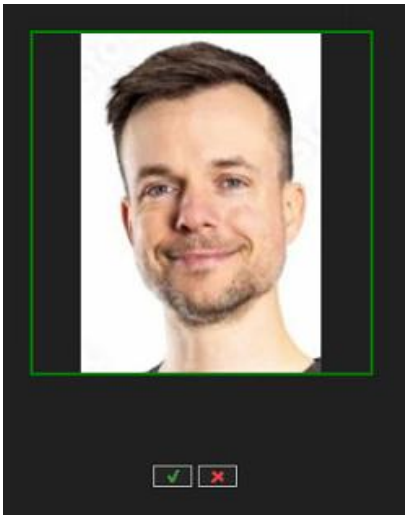


Figure 4 Face image with good quality

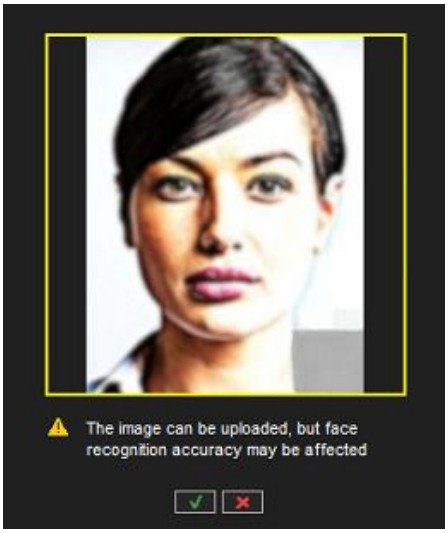


Figure 5 Face image with medium quality

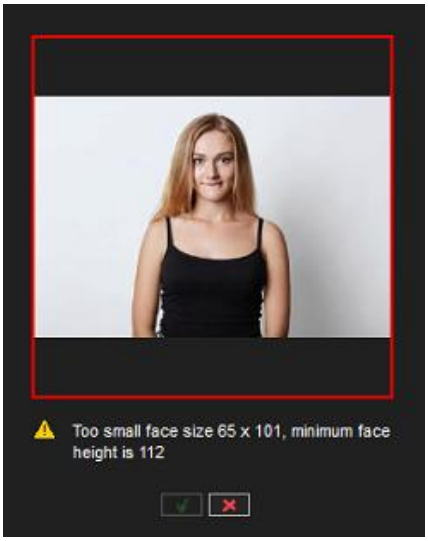


Figure 6 Face image with low quality

9.1.11.2.1.2 Selecting images for FR and LPR

The system administrator can select which identity images are used for FR and LPR. High-quality images are recommended, as they help face detection to function more accurately. When only License Plate Recognition is in use, the administrator can select any identity image to be used. An image can be selected for FR by checking "Use image for face recognition" in the identity image upload dialog, or by modifying an existing identity and clicking **Edit selected identity image**, which opens the identity image dialog where the same checkbox can be ticked.

9.1.11.2.1.3 Set face image as default

One of the face images for an identity will be used as the default image. An identity image can be set as the default image by clicking the radio button for **Default** above the image in the Add/Modify Identity dialog:

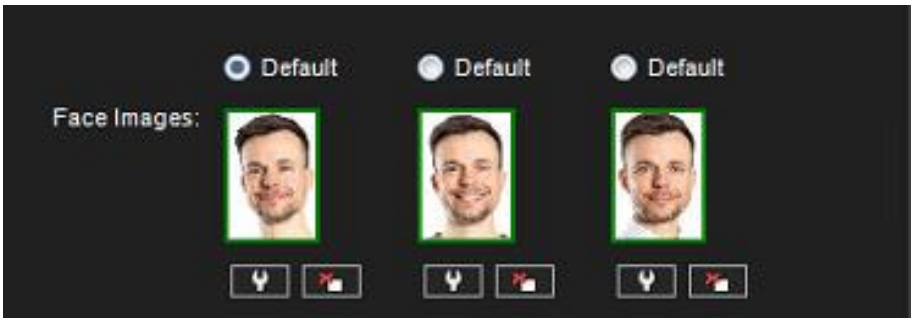


Figure 7 Setting a face image as the default

9.1.11.2.1.4 Add or remove vehicles

You can add or remove vehicles. To add a vehicle, click the **Add a new vehicle** button, and the following dialog will open:

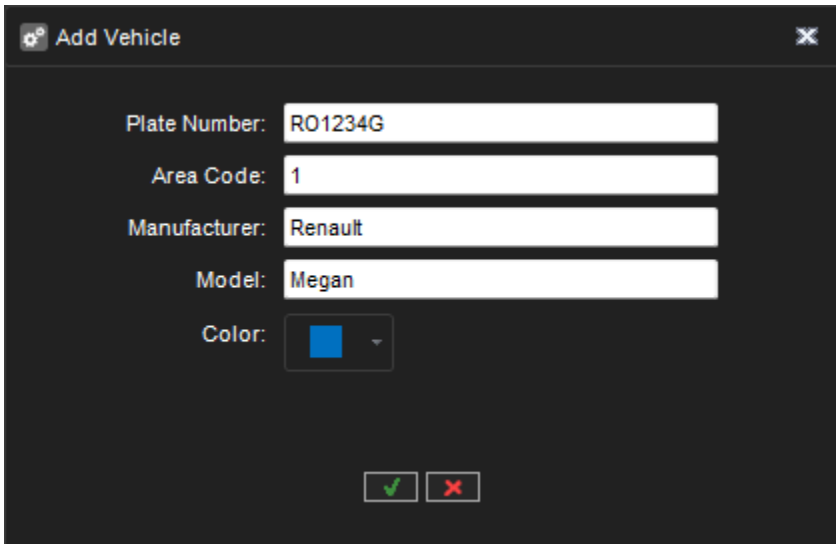


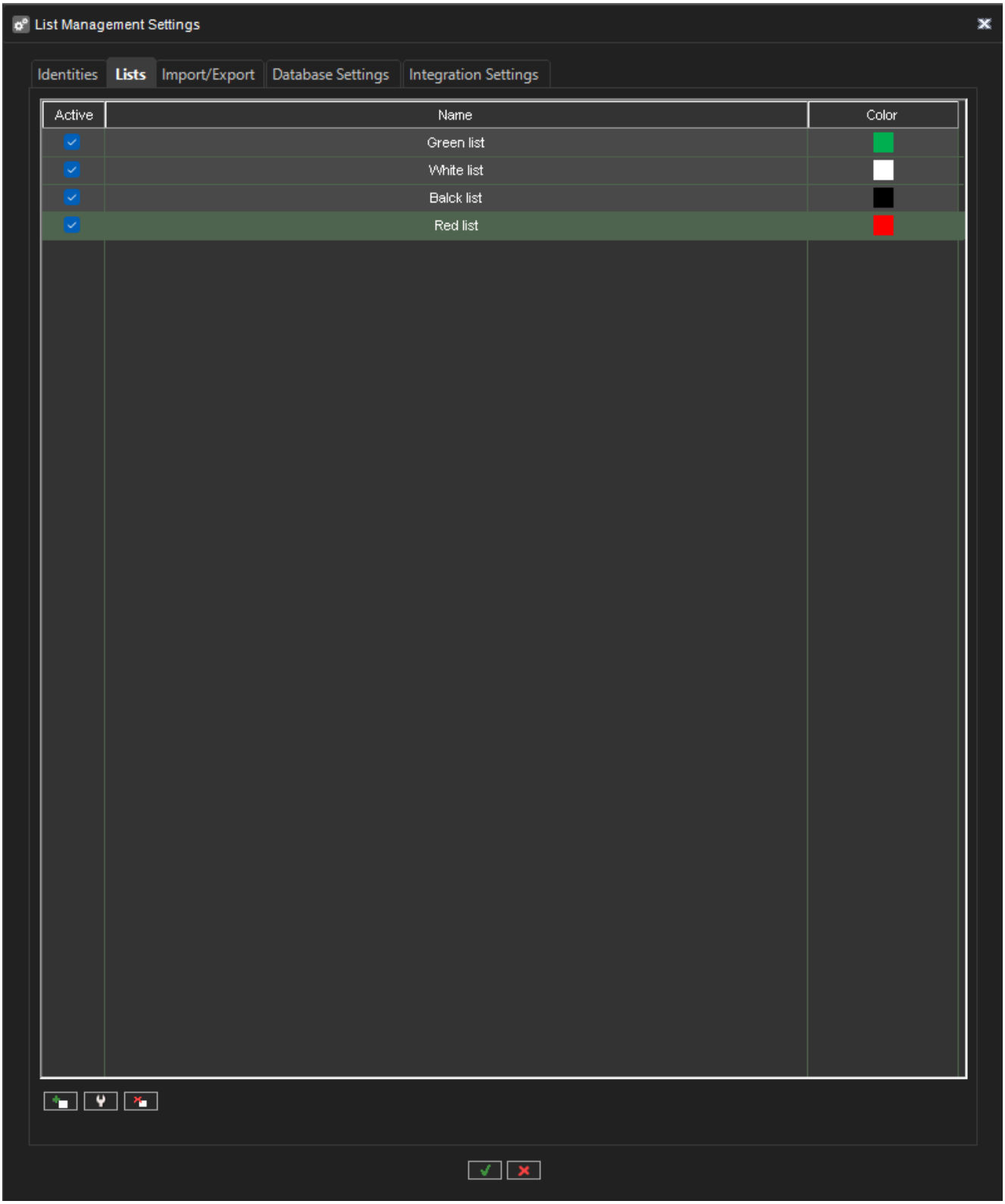
Figure 8 Add Vehicle dialog

In the **Add Vehicle** dialog, you can type the license plate number, area code, manufacturer, model, and vehicle color. To remove a vehicle, you need to select it in the combo box and click the **Remove selected vehicle** button.

9.1.11.2.2 Lists tab

In the **Lists** tab you can perform operations with identity lists:

MIRASYS



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

Figure 9 Lists tab

List selection is done using the left mouse button. If you need to select multiple lists (multiple rows), then you can use the left mouse button + Ctrl/Shift keys. With multiple selections, you can set selected lists to the **active** or **not active** state by clicking the checkboxes in the **Active** column.

You can add and remove selected lists with the **Add** and **Remove** buttons below the lists.

To modify the selected identity list, you can click the **Modify** button or double-click it with the mouse button.

When you add or modify the identity list, the following dialog is shown:

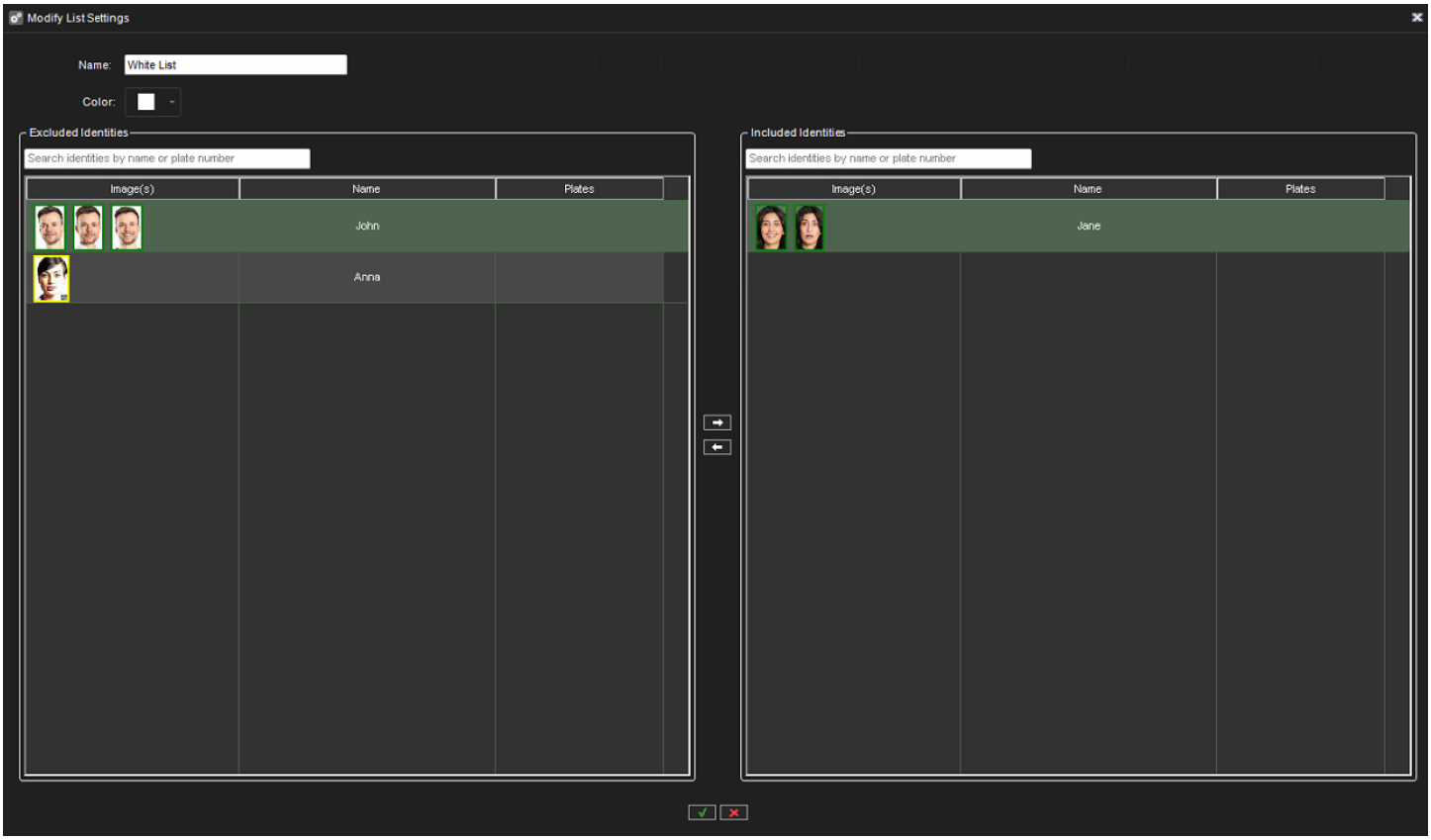


Figure 10 Add/Modify List Settings dialog

You can move identities to the list or remove them from the list, define the name of the list, and color.

9.1.11.2.3 Import/Export tab

In the **Import/Export** tab you can import list management data from a CSV file or export list management data to a CSV file:

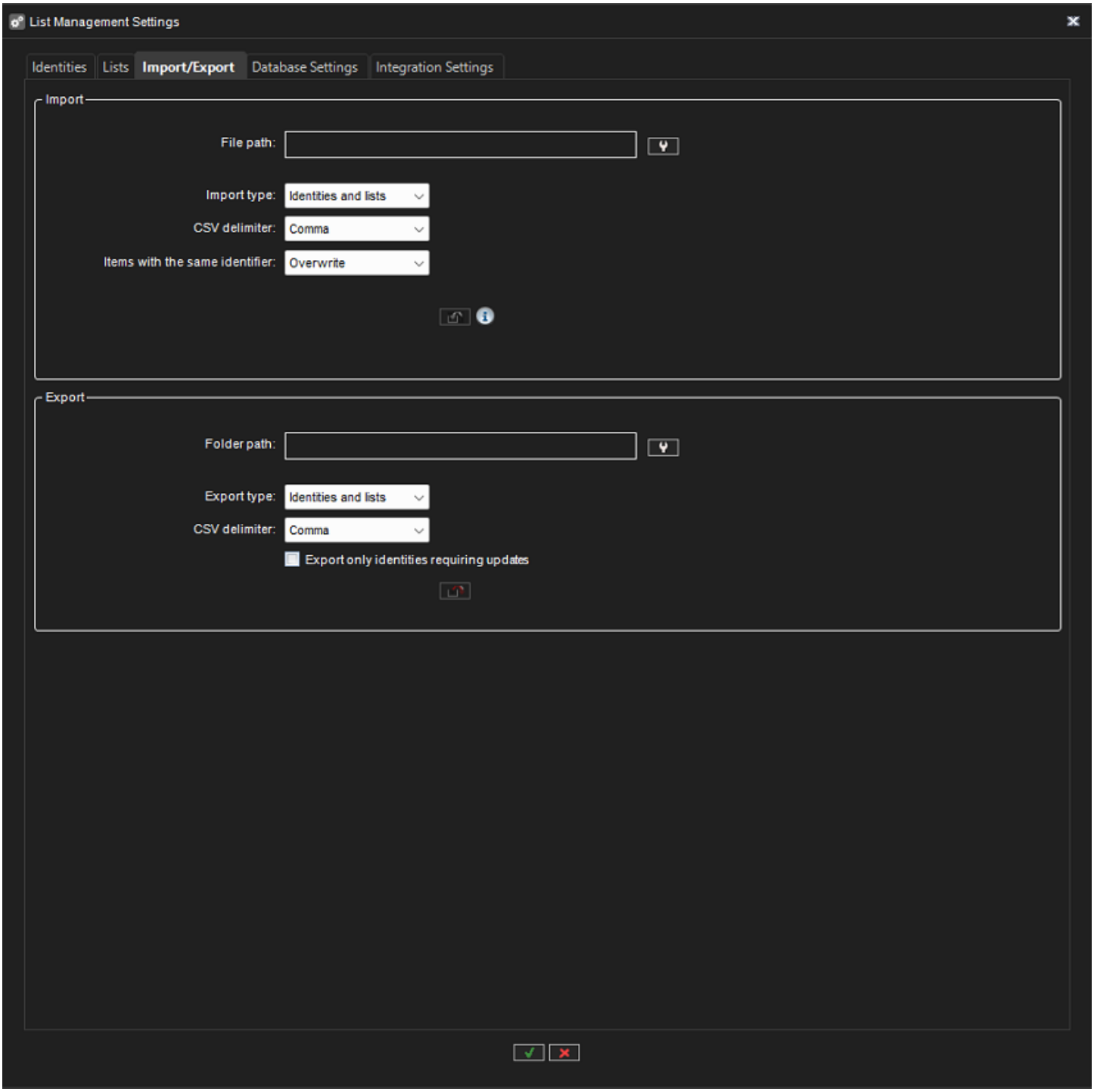


Figure 11 Import/Export tab

9.1.11.2.3.1 Import parameters

The following parameters must be set for the import process:

- **File path** - path to the CSV file which contains list management data
- **Import type** - "Identities only" or "Identities and lists"
- **CSV delimiter** - "Comma" or "Semicolon"
- **Items with the same identifier** - "Skip", "Overwrite", or "Create new" identifier for them

When the correct parameters are selected, the **Import data from file** button is active, and the user can start the import process. During the process, the user will see the progress and result of the import.

9.1.11.2.3.2 Export parameters

The following parameters must be set for the export process:

- **Folder path** - path to the folder where list management data will be exported and where the CSV file will be created
- **Export type** - "Identities only" or "Identities and lists"
- **CSV delimiter** - "Comma" or "Semicolon"
- **Export only identities requiring updates** - can be turned on or off

When the correct parameters are selected, the **Export data to file** button is active, and users can start the export process. During the process, users will see the progress and result of the export.

When the system is upgraded to a new version, old face images with compatibility issues that are used with FR must be re-added for all identities in the List Management settings. The user will receive a warning about this in the LMS installer (the warning is only shown if the upgrade contains face feature vectors from an older version). Identity images can be updated one by one or in bulk using the CSV file import and export. If the CSV import contains low-quality face images, the user will receive a warning. Identity export can be used for exporting only the identities with low-quality images, making it easy to update a large number of outdated images.

9.1.11.2.4 Database Settings tab

In the **Database Settings** tab, you can set up database settings for the list management service:

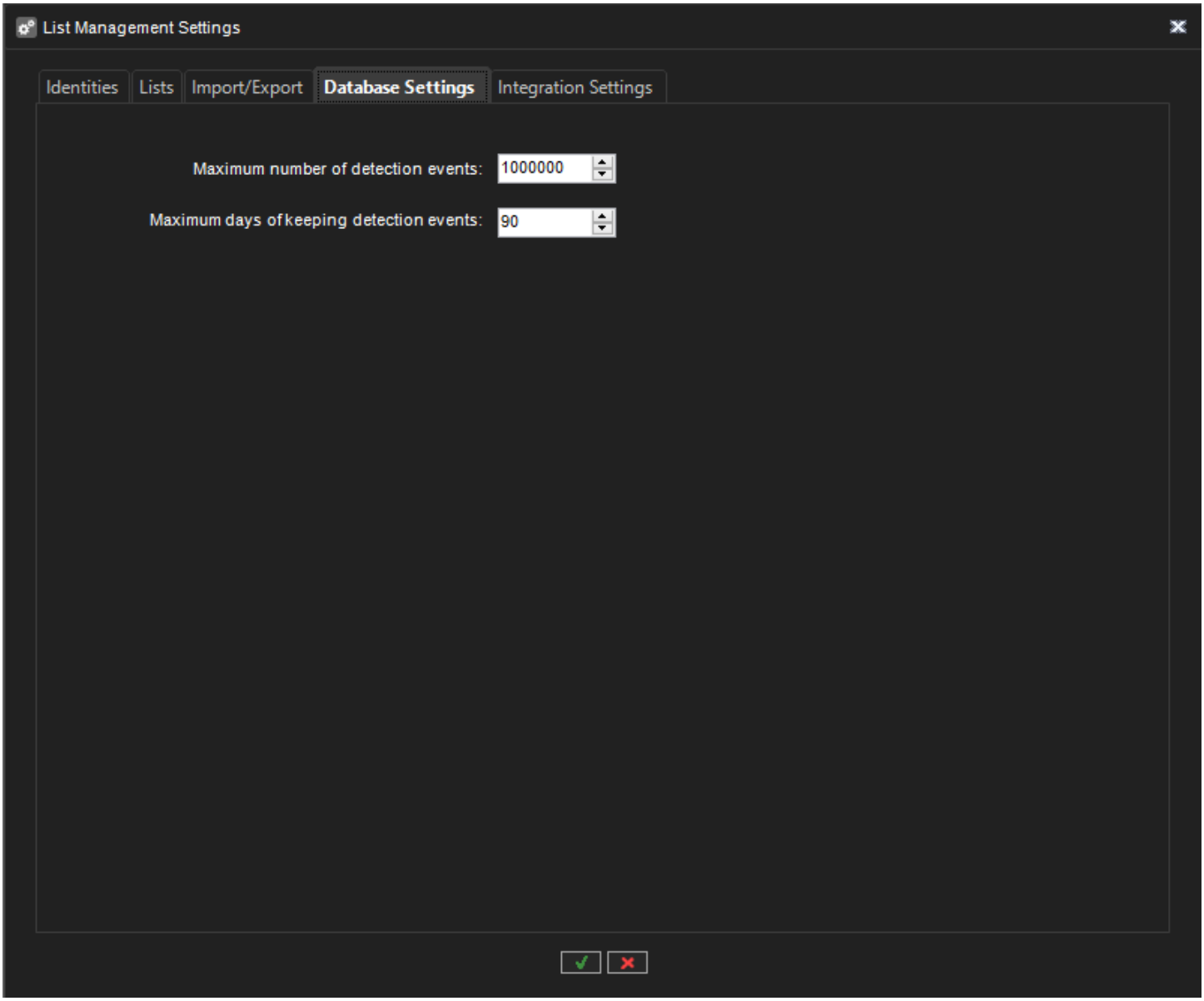


Figure 12 Database settings tab

Changes to the settings don't affect disk usage or the size of the database until a cleaning of the database is completed.

WARNING: Using high limits may lead to unintended mass data deletion and increased system load. It is recommended to start with smaller limits and verify the results before executing larger operations.

9.1.11.2.5 Integration Settings tab

In the **Integration Settings** tab, you can set up integration settings for the list management service:

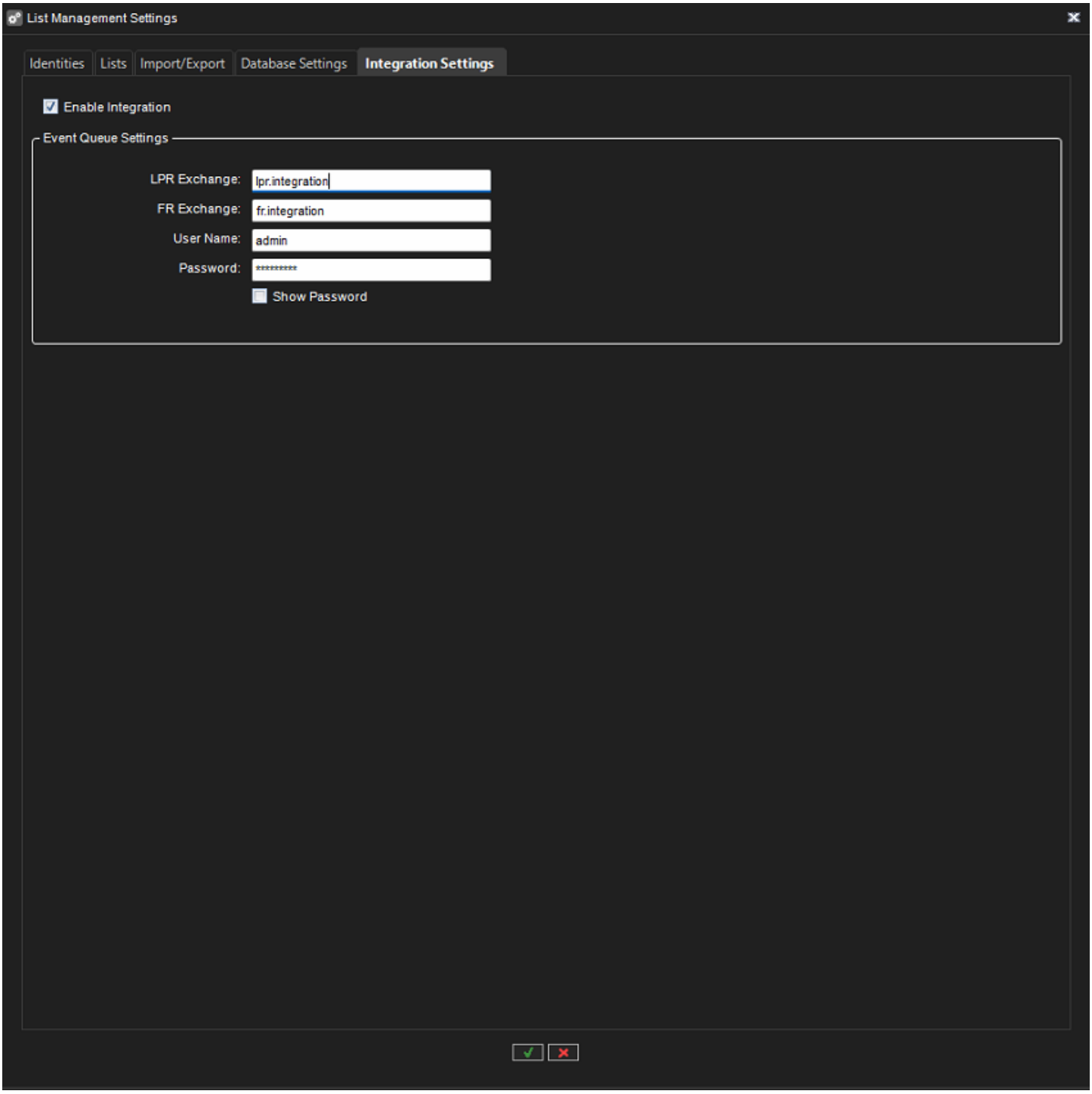


Figure 13 Integration Settings tab

Here you can define settings for the event queue and enable/disable integration settings. The tab is not visible if the license does not enable list management integration.

9.1.11.3 List management data update notification

If list management data has been changed in another application, the System Manager will receive an event with updated information and display the following message:

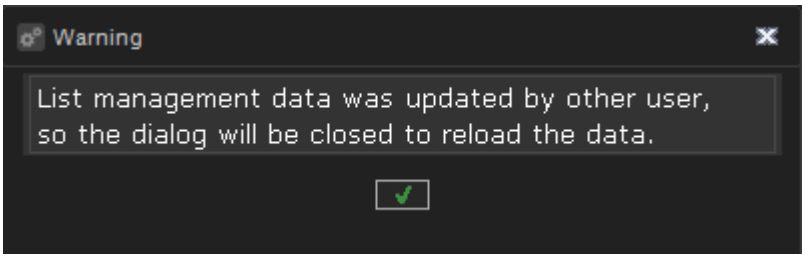
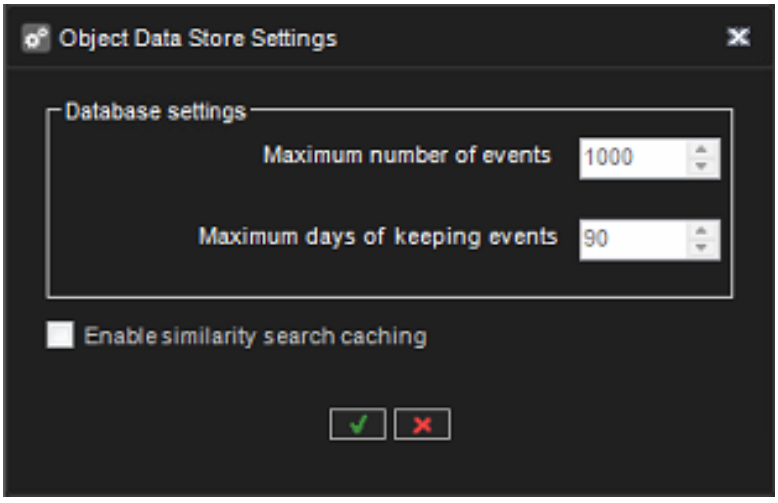


Figure 14 Data update warning

When you click the **OK** button of the message dialog, all settings dialogs will be closed to reload data from the list management service. All changes that were not saved will be lost.

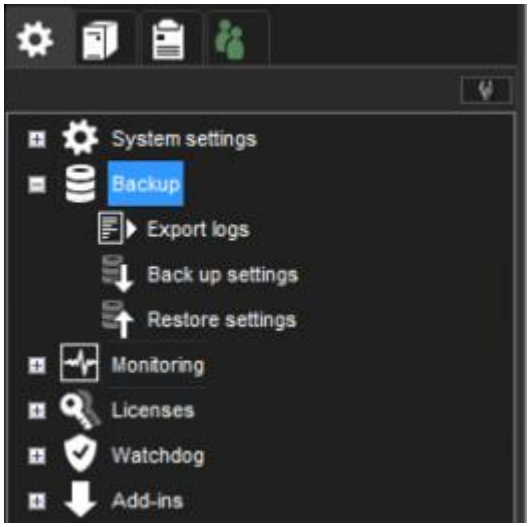
9.1.12 Object Data Store Settings

To select the maximum number of events to store in the database, and for how long to retain those events, go to **System Settings** > **Object Data Store Settings** in System Manager. Here, you can also enable similarity search caching.



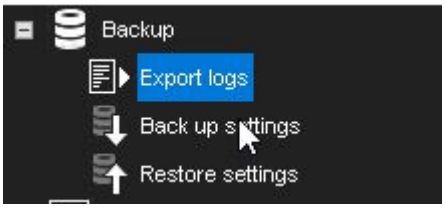
WARNING: Using high limits may lead to unintended mass data deletion and increased system load. It is recommended to start with smaller limits and verify the results before executing larger operations.

9.2 BACKUP



9.2.1 Export logs

Export log files and send them to the system supplier should there be a problem with the system.



Log files are saved to a compressed (zipped) file that can be placed to a removable or non-removable device.

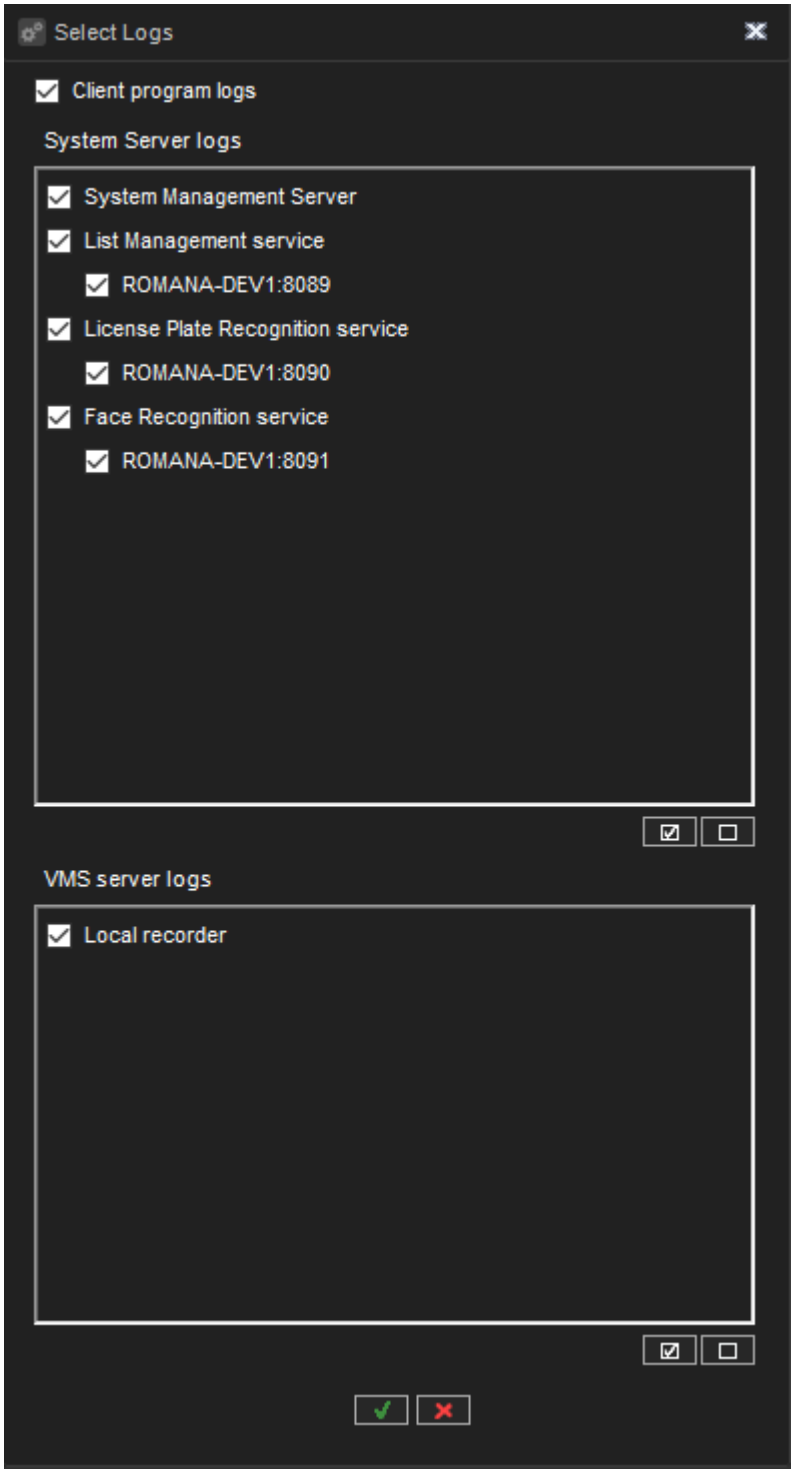
9.2.1.1 Export log files via System Manager

1. Open the System Manager application for export logs and choose the **Export logs** subitem in the **Backup** tree item on the **System** tab.
2. Select logs that can be exported in the

Select Logs window.

If there are problems with a server select logs on the **System Server logs** panel. In addition, select client program logs.

> The client logs are from the machine where you are accessing the system manager application.

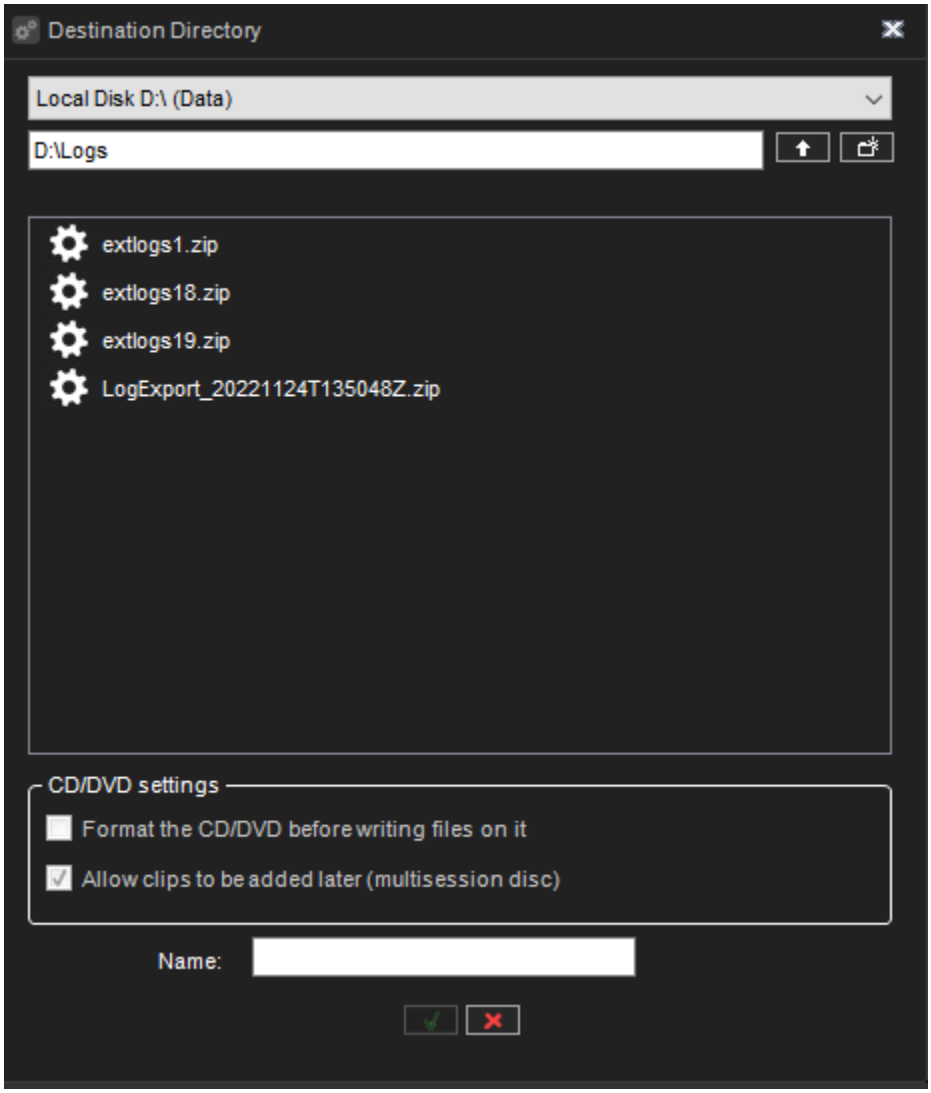


Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

For fast selection, you can use the **Select All** and **Clear Selections** buttons placed under the **System Server logs** and **VMS server logs** panels. Select or clear all selections for specific service groups (e.g. **License Plate Recognition service**) that contain specific services by clicking on the services group checkbox.

3. Click **OK**.

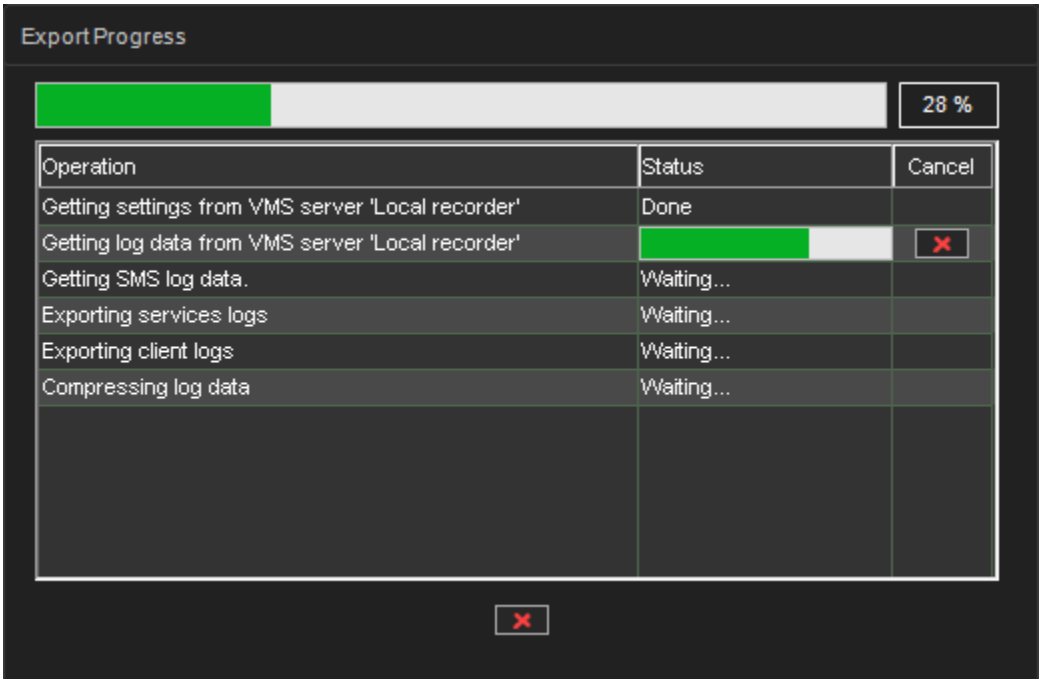
4. Select the storage device and the folder where you want to save the log files in the **Destination Directory** window.



To create a new folder, click the **New folder** button.

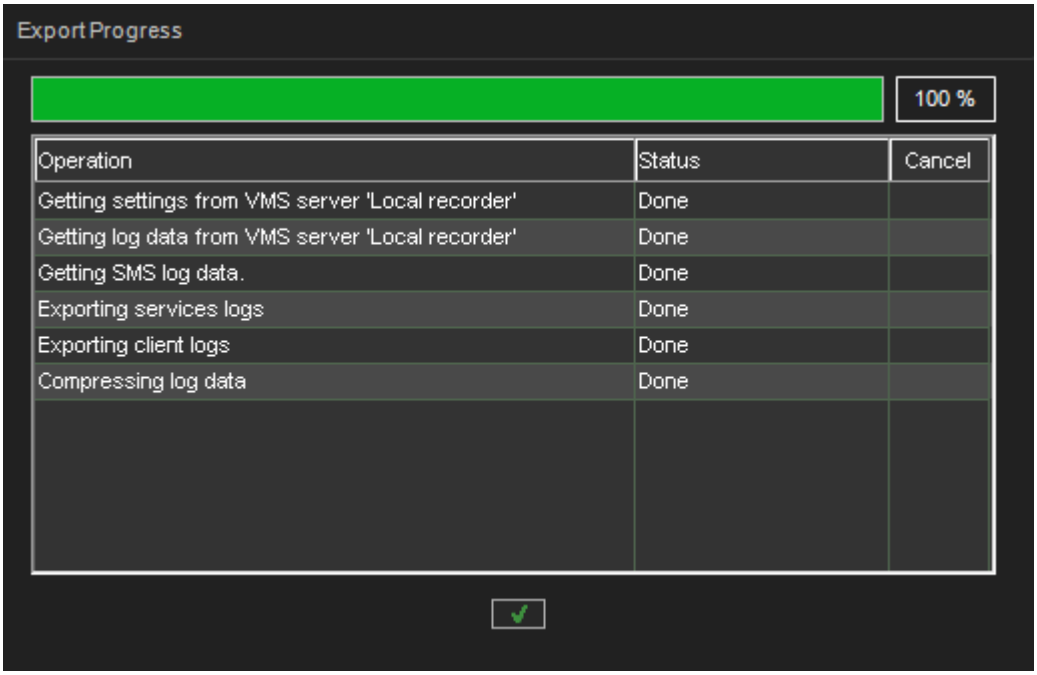
Type a name for the ZIP file in the **Name** fields and click **OK**

You can see the progress of exporting in the **Export Progress** window. Operations are executed in order from top to bottom.



It is seems like the operation is stuck it can be cancelled.
Cancel all export by clicking on the **Cancel** button at the bottom of the window.

5. Click **OK** to close the window once the export is completed.



6. The system exports the files to a ZIP file. Send the ZIP file to the system supplier. Services log files are stored in inner ZIP archives in the main ZIP file.

The typical content of logs ZIP archive is the following:



- FRService_ROMANA-DEV1_8091_Log.zip
- LMService_ROMANA-DEV1_8089_Log.zip
- LPRService_ROMANA-DEV1_8090_Log.zip
- SpotterAuditLog_9.6.0.68.txt
- SpotterAuditLog_9.6.0.70.txt
- SpotterLog_9.6.0.68.txt
- SpotterLog_9.6.0.70.txt
- SpotterLog_9.6.0.70.txt.1
- SpotterLog_9.6.0.70.txt.2
- SpotterLog_9.6.0.70.txt.3
- SpotterLog_9.6.0.70.txt.4
- SpotterLog_9.6.0.70.txt.5
- SystemManagerAuditLog.txt
- SystemManagerLog.txt
- SystemManagerLog.txt.1
- SystemManagerLog.txt.2
- SystemManagerLog.txt.3
- SystemManagerLog.txt.4
- SystemManagerLog.txt.5
- SystemManagerLog.txt.6
- SystemManagerLog.txt.7
- SystemManagerLog.txt.8
- SystemManagerLog.txt.9
- SystemManagerLog.txt.10
- SystemMonitorAuditLog.txt
- VAULog.txt
- SM_ExportServiceLog.txt
- SM_IRServerLog.txt
- SM_SLServerLog.txt
- SM_SMLog.txt.9
- SM_SMLog.txt.2
- SM_SMLog.txt.3
- SM_SMLog.txt.4
- SM_SMLog.txt.5
- SM_SMLog.txt.6
- SM_SMLog.txt.7
- SM_SMLog.txt.8
- SM_SMLog.txt
- SM_SMLog.txt.1
- SM_SMLog.txt.10
- Local recorder_ExportServiceLog.txt
- Local recorder_IRServerLog.txt
- Local recorder_ROMANA-DEV1Application.evtx
- Local recorder_ROMANA-DEV1System.evtx
- Local recorder_SLServerLog.txt
- Local recorder_CLIDVRLog.txt
- Local recorder_DVRLog.txt
- Local recorder_DVRLog.txt.1
- Local recorder_DVRLog.txt.2
- Local recorder_PerformanceLog.txt
- Local recorder_PerformanceLog.txt.1
- Local recorder_PerformanceLog.txt.2
- Local recorder_StartupLog.txt
- Local recorder_StartupLog.txt.1
- Local recorder_WDLog.txt
- Local recorder_Alarms.txt
- Local recorder_Cameras.txt
- Local recorder_CameraSets.xml
- Local recorder_DriverInfo.txt
- Local recorder_Drivers.xml
- Local recorder_PluginDrivers.xml
- Local recorder_Settings.xml

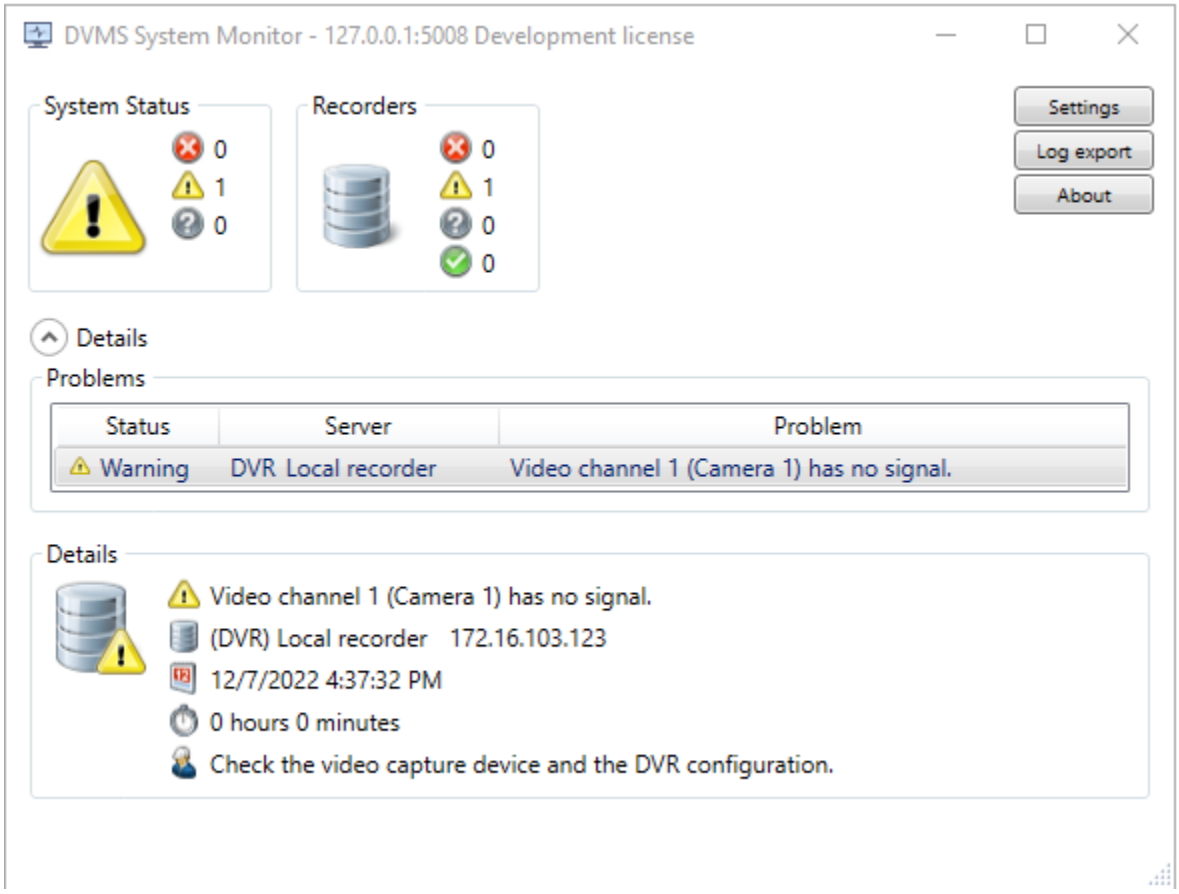
Some service sub-archives can be missed if there are no connections to services.

9.2.1.2 Export log files via System Monitor

It is possible to collect system logs via the System Monitor application.

1. Open System Monitor and click the

Log export button:



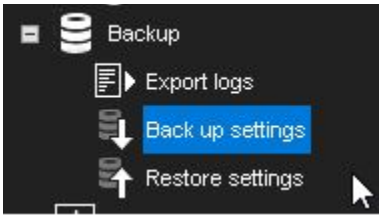
2. Choose the archive name and path for saving in the **Save as** dialog to save the export archive.

3. Click **Ok** to start collecting logs.

The System Monitor can collect **SM server** logs (also ones include **Incident Reporting** log, **Storage Locker** log, and **Export services** log), **DVRs** logs, clients' logs (**Spotter**, **System Manager**, etc.), and logs of all **List management**, **Face Recognition,** and **License Plate Recognition** services observed in the current system.

The typical content of logs ZIP archive is the same as for ZIP archive from System Manager. Some service sub-archives can be missed if there are no connections to services.

9.2.2 Back up settings

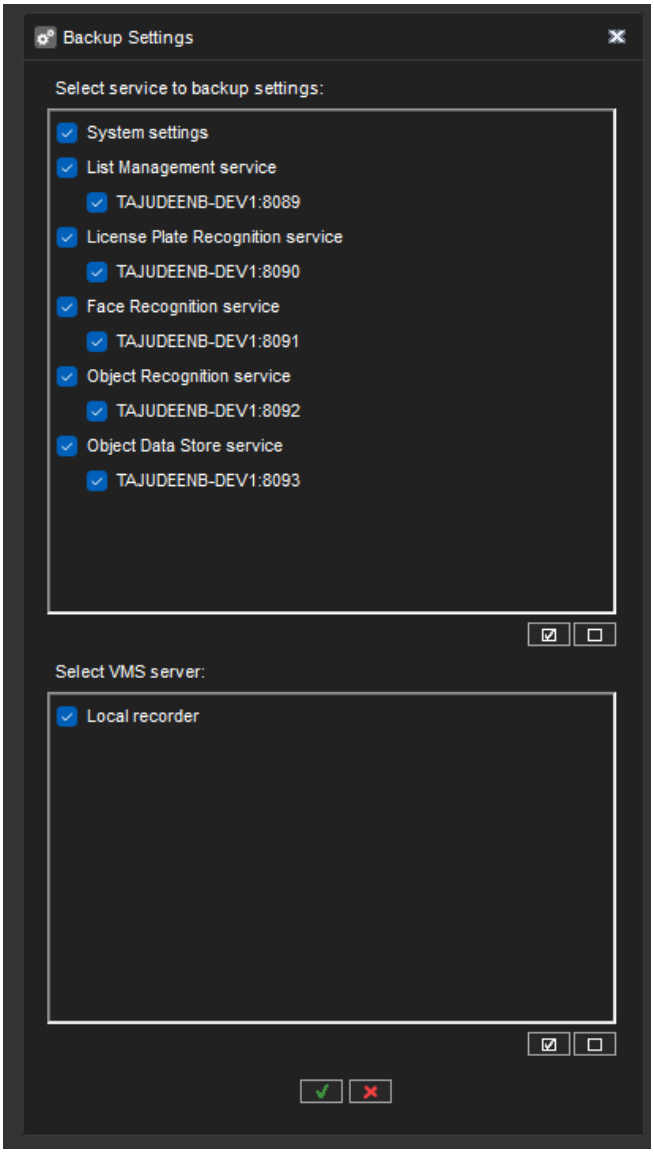


Backup system settings to be able to restore them if the hard disk that contains the settings fails:

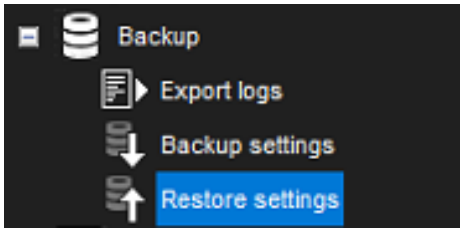
- You can back up system settings and server settings.
- System settings contain data about the servers, profiles, and user accounts.
- VMS Server settings contain data about the devices connected to the servers and their parameters.
- You can save the backup copy to a hard disk, network drive, CD/DVD, floppy disk, or another removable or non-removable device.
- Backup files have the file extension ".vbk".

9.2.2.1 How to backup settings

1. On the **System** tab, open **Backup settings**. The **Backup settings** dialogue box is shown.
2. Select the system and server-specific settings that you want to back up and click **OK**.
3. Select the storage device and the folder where you want to save the backup file. To create a new folder, click the **New folder** button.
4. Type a name for the file and a description and click **OK**. The description is optional. The system creates the backup file.



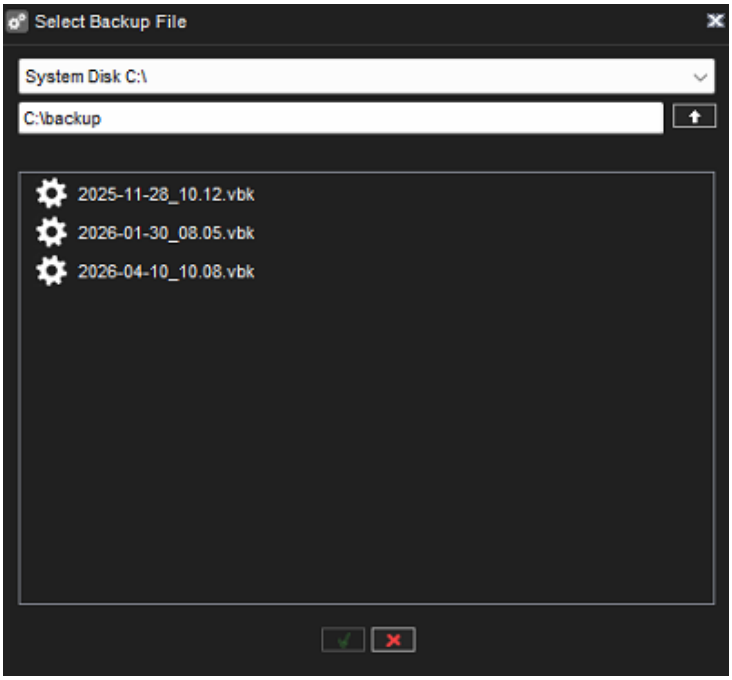
9.2.3 Restore settings



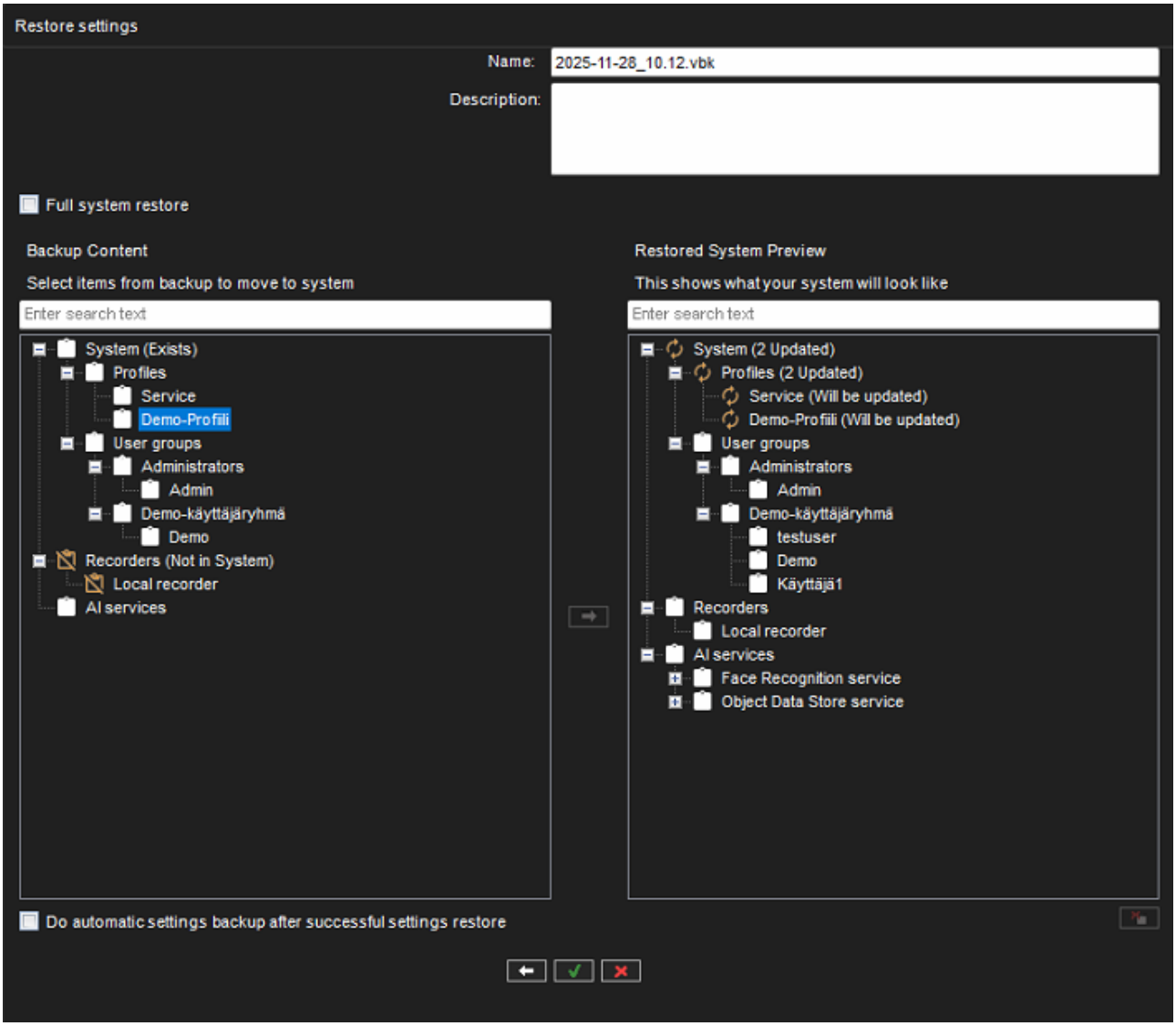
If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs.

9.2.3.1 Restoring the settings

1. On the **System** tab, open **Restore settings**. The "Select Backup File" dialogue box is shown.



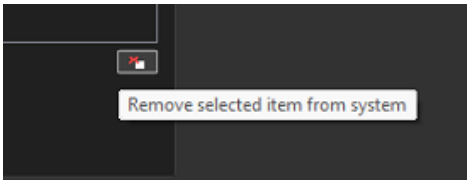
1. Find and select the backup file (.vbk) and click **OK**. The system decompresses the file and then shows the **Restore settings** dialogue box. The dialogue box shows the settings and their description.



2. Select the settings you want to restore and click **Select to restore**. The dialog box shows what is included in the backup.

A full system restore can be done by enabling the checkbox **Full system restore**. All changes made by the user can be cancelled by clicking **Reverse all changes**, and an individual setting can be removed from the restore by selecting it from the “Restored System Preview” panel and clicking **Remove selected item from system**.





Selecting **Do automatic settings backup after successful settings restore** is recommended, especially when restoring the system after a failover has happened.

After making the selections, click **OK**. The settings are restored, and a summary of the process is shown.

1. Click **OK** to accept the new settings or **Reverse all changes** to return to the "Restore settings" dialogue.

9.2.3.2 Content status and icons

The status of the backup content is indicated with an icon and a status text next to the main folder name in the "Restore settings" dialog. The icons have the following meanings:

- 

  The item already exists in the current setup, item is not updated

- 

  The item partially exists in the current setup

- 

  The item does not exist in the current setup

- 

  The item is updated in the current setup

- 

  The item is added to the current setup

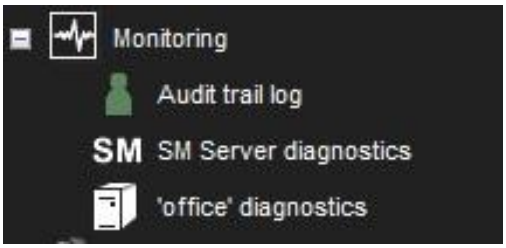
- 

  The item is deleted from the current setup

9.3 MONITORING

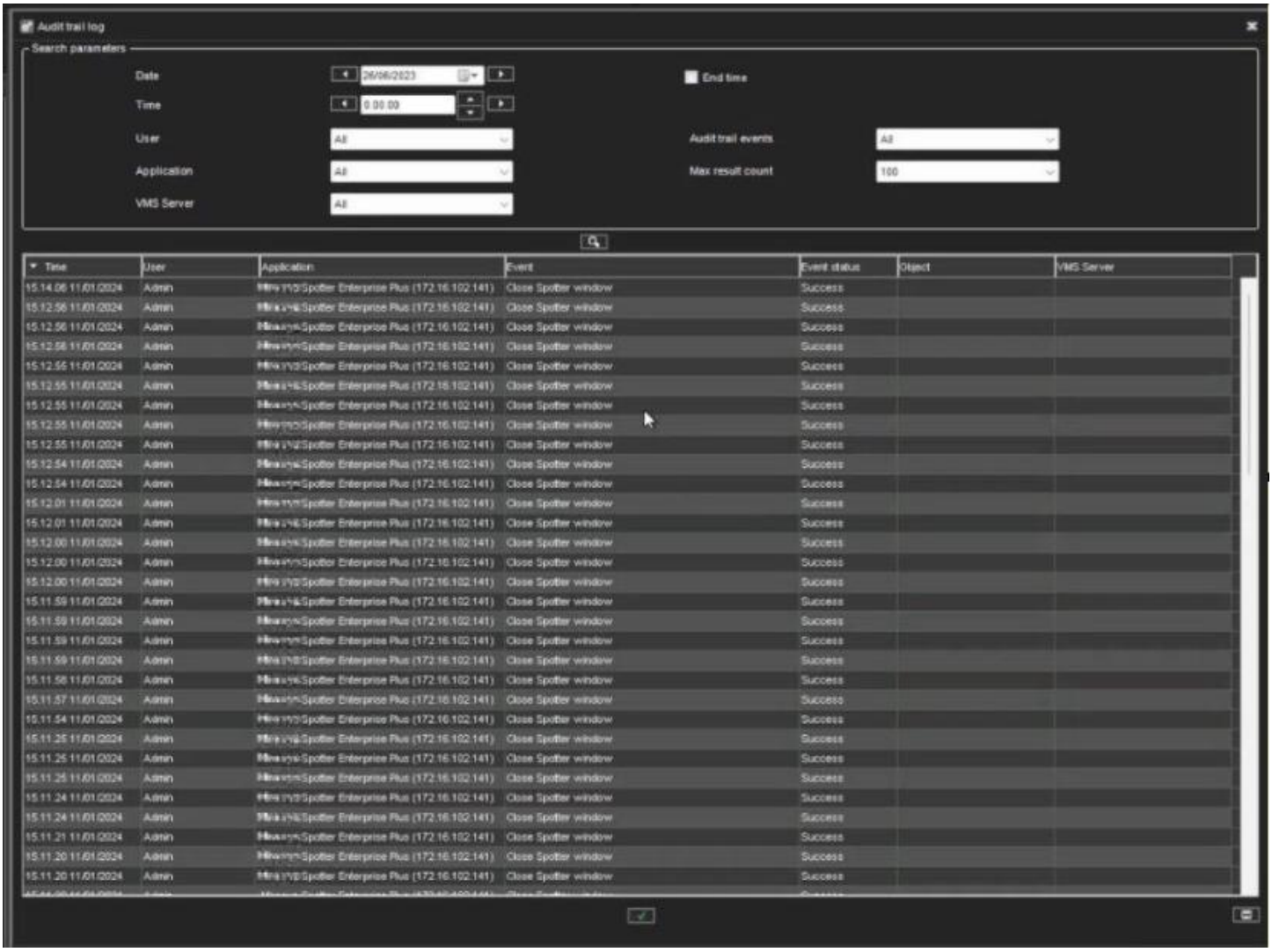
9.3.1 Audit trail log

The Audit trail log can be used to search VMS system user activity information. It can be accessed in System Manager at the System tab tree under Monitoring.



9.3.1.1 Audit trail log

In the audit trail log dialog admin can search for audit trail events using several search parameters. Results are listed in the result list ordered by time. Found audit trail events can be sorted by other audit trail event information by clicking the list headers.



9.3.1.2 Search parameters

Following search parameters can be used for audit trail event searching.

- **Date** - Select the date for the search to start. Buttons on the left and right decrease or increase the day of the date.
- **Time** - Select the time of the date for the search to start. Buttons on the left and right decrease or increase the hour of the time. Buttons up and down increase or decreases minutes of the time by ten.
- **User** - User whose audit trail events will be searched. All = search without filtering users.
- **Application** - Application to search. All = search without filtering applications.
- **Max result count** - Maximum number for how many audit trail events will be searched starting from start time.

- **VMS Server** - The VMS Server drop-down shows all possible values for VMS Servers that can be selected.
- **End time check box** - If checked, it enables search end date and time selection similar way as for start time. If not checked, end time is not used as a search filter (= search until now)
- **Audit trail events** - Operation to search: none, one, many, or all operations can select. If none or all is selected, then search without filtering operations. The following buttons can be used with operations:
    - Enlarge operation list view
    - Select all
    - Unselect all

9.3.1.3 Results list

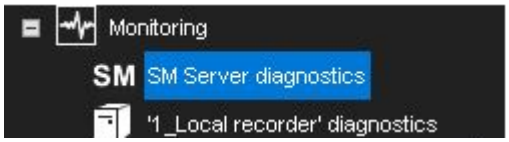
Found audit trail events are listed in the search result list. The list contains information about each audit trail event.

- **Time** - Time of the user action.
- **User** - Username who did the user action.
- **Application** - Application where the user action was taken.
- **Event** - Name of the user action. When the even is related to camera audit, and the operator needs to add a comment before accessing playback material, the event contains the comment.
- **Event status** - If the operation was successful or not.
- **Object** - The object depends on the operation itself. For example, if you open a camera, the name of that camera is shown.
- **VMS Server** - Displays on which VMS server the operation occurred.

9.3.1.4 Audit log export

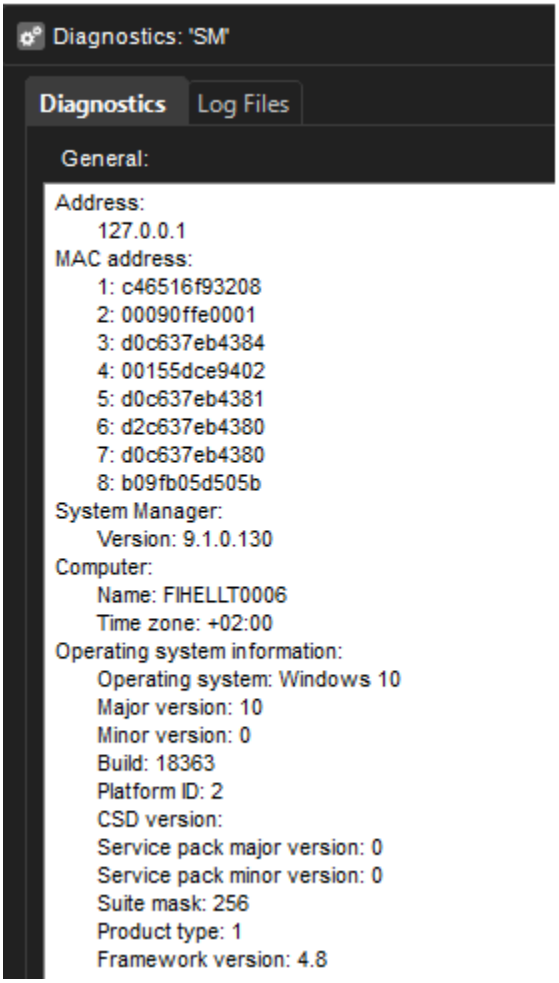
Listed audit trail events can be exported to a PDF file as an audit trail report by clicking the button under the audit trail events results list. The location and the name of the exported file and the comment for the report can be given on the save report dialog. The audit trail log report title is created of the export time and the user who exported the report. The report contains all the audit log entries with the same information that is listed in the audit trail event result list.

9.3.2 SM Server Diagnostics



SM Server Diagnostics shows information about the System Management Server that runs on the Main Server.

9.3.2.1 General



In SMServer Diagnostics, you can examine this information:

- SM Server version
- Computer name and time zone
- Operating system information
- Major version
- Minor version
- Build
- Platform ID
- CSD version

- Service pack major version
- Service pack minor version
- Suite mask
- Product type
- Framework version

9.3.2.2 Log Files

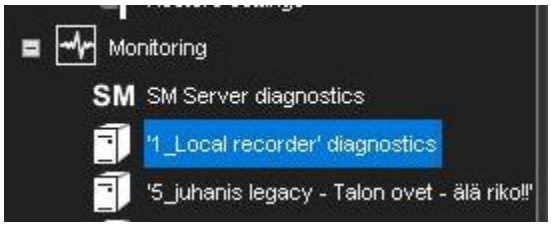
If there are problems with the system, you can access the system log files on the **Log Files** tab.

To examine a log file:

- Select the file from the drop-down list.

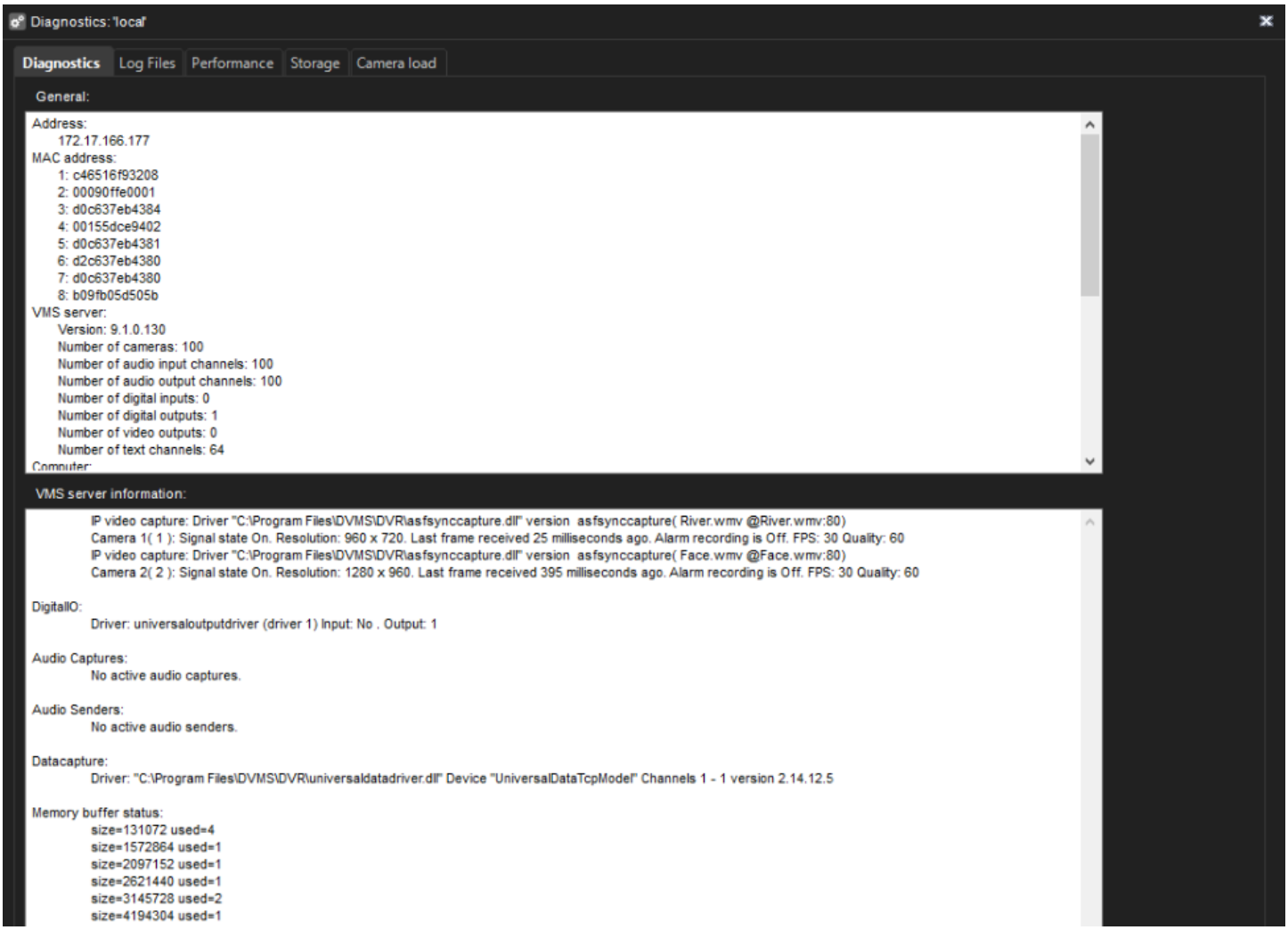
The contents are shown in the **Contents of the selected log file.**

9.3.3 Server Diagnostics



VMS Server diagnostics shows information about the server and the CPU and network usage.

9.3.3.1 Diagnostics



The **Diagnostics** tab shows this information:

- Information about the server:
- Software version
- Model
- Number of cameras, audio channels, digital inputs, digital outputs, and video outputs
- The name of the computer and the time zone
- Operating system information
- Processor information

- Installed drivers, for example, capture drivers, video output drivers, digital output drivers, and PTZ drivers.

9.3.3.2 Log Files

The **Log files** tab shows a list of log files.

To see the contents of a log file:

- Select the file from the drop-down list. The contents are shown in the **Contents of the selected log file**.

9.3.3.3 Performance

On the **Performance** tab, you can monitor these:

- CPU usage.
- Usage of physical memory.
- Usage of virtual memory.
- Network traffic.
- Used disk space.

9.3.3.4 Storage

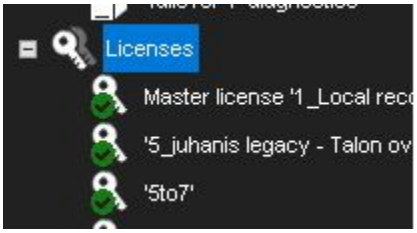
On the **Storage** tab, you can monitor disk and file properties. For example, you can examine free disk space or monitor saved data by the camera and audio channel.

GeneralTotal recording capacity. Shows the total storage capacity that is reserved for the recordings.

Used space. The quantity of space that the recordings have used.
Free space. Free space is available for recordings.
% used. The percentage of the disk's capacity that is used.
Average saving speed. Calculated by dividing the quantity of data saved since the server was last started by the uptime.
VMS Server uptime. Shows the time that the server has been operating since it was last started.
The counter shows the difference between the current time and the start time in days, hours and minutes.
DisksTotal recording capacity. Shows the storage capacity that is reserved for the recordings on the selected disk.
Used space. Used recording space on the selected disk.
Free space. Free space is available for recordings on the selected disk.
% used. The percentage of space used of the total capacity reserved for the recordings.
Total recording cache. Shows the total capacity of the cache that is used for the temporary storage of data before it is permanently written on a disk.
Because of the cache, video and audio can be recorded immediately when the server is started. The cache is also used for pre-event recording.
The system automatically calculates how much cache space it must have and allocates space accordingly.
Used recording cache. Temporary space that is currently in use.
Free recording cache. Temporary space that is currently free.
CamerasOldest time. The date and time of the oldest image in the store.

Newest time. The date and time of the newest image in the store.
Total no. of images. The total number of images in the store.
Average image size. The average image size.
Used space. This value shows how much space the images and metadata files from this camera use.
% used. This value shows what percentage of space this camera has used of the total capacity reserved for the recordings.
Audio channels Oldest time. The date and time of the oldest audio sample in store.
Newest time. The date and time of the newest sample in store.
A total number of samples. The total number of audio samples in store.
Average sample size. The average audio sample size.
Used space. This value shows how much space the audio samples and metadata files from the audio channel use.
% used. This value shows what percentage of space the audio channel has used of the total capacity reserved for the recordings.
Text channels Oldest time. The date and time of the oldest text data sample in store.
Newest time. The date and time of the newest sample in store.
A total number of samples. The total number of text data samples in store.
Average sample size. The average text data sample size.
Used space. This value shows how much space the text data samples and metadata files from the text channel use.
% used. This value shows what percentage of space the text channel has used of the total capacity reserved for the recordings.

9.4 LICENSES



By default, without a VMS license, the server supports only one IP camera. The server needs a valid license for full functionality.
Depending on the installation, you may need to upgrade the license information when adding new functionality or cameras to the system.

To get a license key, please contact your supplier and follow the license upgrade procedure as detailed by the supplier.

If you have any problems in upgrading the license, please contact *orders@mirasys.com*.

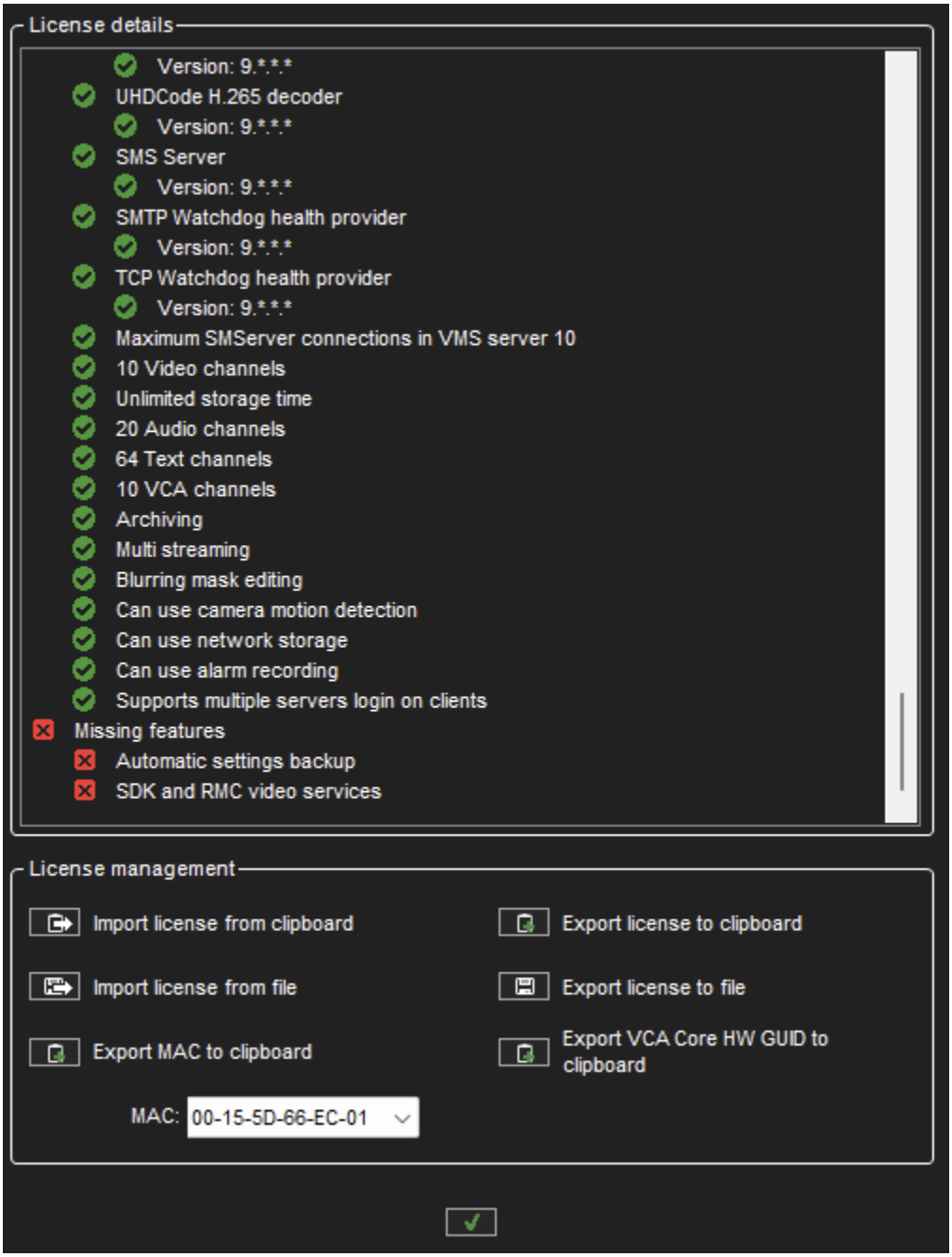
You can also add more camera channels and features such as VCA capabilities to a server by getting a new license key.

For the license key, you need the MAC address of the server.

9.4.1 Getting the license key

1. Start System Manager. The License Information dialogue box is automatically shown when no license key has been specified.
2. On the **System** tab, under **Licenses**, double-click the server that you want to update.
3. In the License Information dialogue box, copy the MAC address and send it to Mirasys. In return, you will receive the license key as a text file.
4. Click **Import license from the file**.
5. Click **OK**. The system is updated immediately.

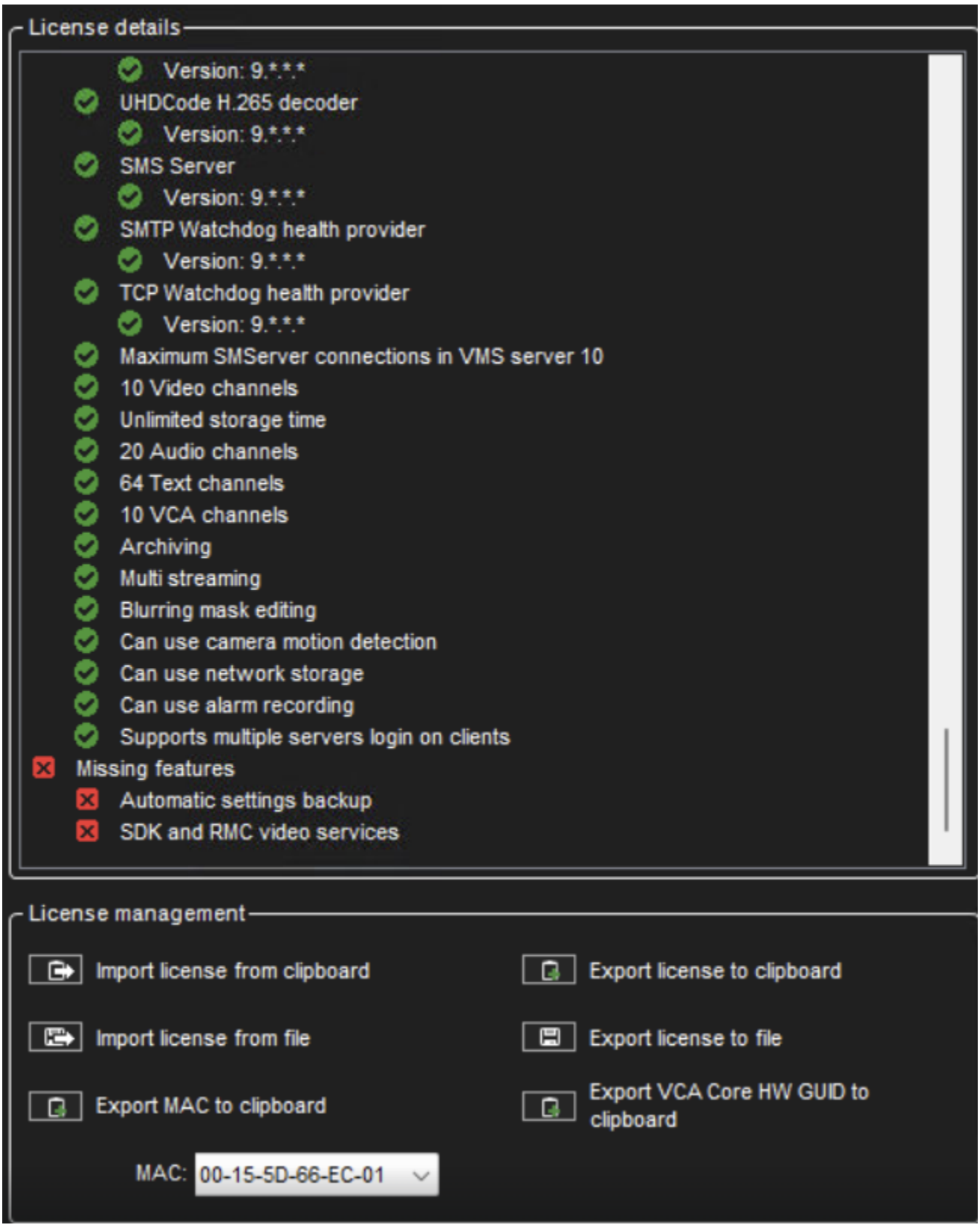
The default unregistered state that allows the use of one IP camera has been time-limited.
The unregistered state can be active for up to 60 days, after which a valid license key is required. Unless a valid license key is added to the system within 60 days after the installation, the system will cease to operate.



9.4.2 License details

License details show all supported features of the license.

MIRASYS



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

9.4.3 License Management

9.4.3.1 To import a license key:

1. Click **Import license from the file**.
2. Browse to the license file location
3. Click **OK**. The new license is updated immediately.

9.4.3.2 To export a license key:

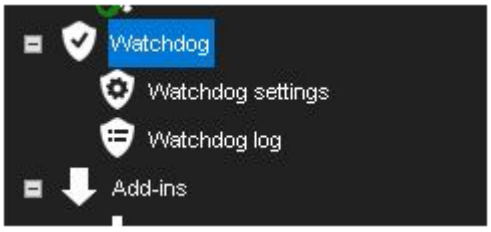
1. Click **Export license key to file** to create a text file for the license or **Export license key to the clipboard** to copy the key to the clipboard.
2. If exporting the license to a file, set the destination folder and the name of the file.
3. Click **OK**.

9.4.3.3 To export VCA Core HW GUID

1. Click **Export VCA Core HW GUID to clipboard**
2. Select **Export also license serial number**
3. **Click Ok**



9.5 WATCHDOG



The system has a software watchdog (system monitoring service) that monitors the system and performs specific actions if problems occur.

In the Watchdog tool, you can select the events for which the notification list is notified through e-mail and access watchdog logs, which contain the events that have occurred and the actions that have taken place.

9.5.1 Watchdog settings

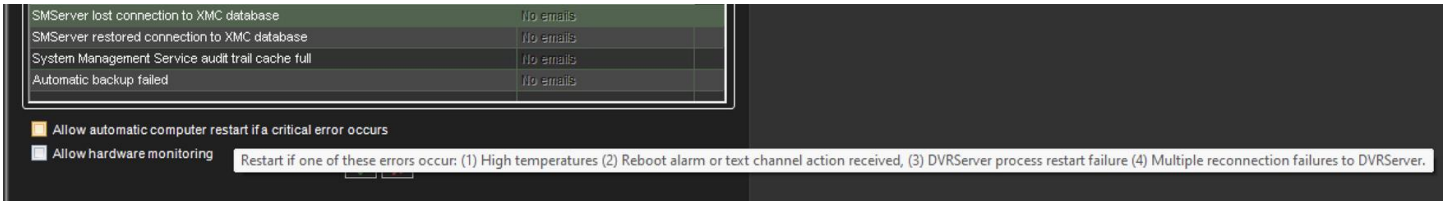
In watchdog settings, you can select what events trigger a report to be sent to e-mail addresses specified in E-Mail Settings
You can select different events for each server.
Alternatively, you can select the same events for all servers by selecting **All VMS Servers** from the drop-down list.
In addition to e-mail notifications, notifications can be performed through digital outputs.
All event types are written to the watchdog logs, regardless of the e-mail settings.

9.5.1.1 To add or remove events on the notification list:

1. On the **System** tab, select **Watchdog settings**.
2. Mark the **Send mail** checkbox for each event type for which a notification e-mail should be sent.
3. Click **OK**.

9.5.1.2 Automatic restart

Tick the box **Allow automatic computer restart if a critical error occurs** to allow your computer to restart automatically in case of high hardware temperatures, if there is a reboot action received (alarm or text channel), in case of a recorder process restart failure or multiple reconnection failures to the recorder. The computer will not be restarted more than once a day.



You can also allow hardware monitoring if needed.

9.5.1.3 Digital output notifications

In addition to e-mail notifications, notifications can be performed through digital outputs.
Notifications through digital output are created as server-specific; you need to select a specific server from the **VMS Server** drop-down list.

To set a digital output notification:

1. On the **System** tab, select **Watchdog settings**.
2. Select a server from the **VMS Server** drop-down list. As digital output signals are server-specific, you cannot select **All VMS Servers**.
3. Click on an event.
4. Select the digital output channel you want to use from the **In Use** drop-down menu.

5. If you want to send a pulse signal to the output channel, mark the **Pulse** checkbox and select the pulse length with the slider.
6. Click **OK**.

9.5.2 Watchdog log

By default, the system shows the watchdog logs from all servers.
However, you can select one or several servers from the list on the left.
You can sort the logs by clicking the column headings.
To update the list without closing the window, click the **Refresh** button.

9.5.2.1 Additional Watchdog Delivery Methods

The Watchdog functionality includes the following protocols:

- TCP
- Customizable e-mail form

Each protocol has its driver:

C:\Program Files\DVMS\DVR\WDEventProviders\

- WDEventProviderSMTP.xml
- WDEventProviderTCP.xml

At this moment, these files need to be edited manually. Each XML file contains the documentation regarding the configuration options.
The new configuration options include filtered and conditional warnings (i.e. "send warning X only once in every 60 minutes" or "send warning X only if condition Y is not met in two minutes"), and customizable warning message format.
After the files have been edited, Watchdog needs to be restarted for the changes to take effect.

***Note**: This feature is recommended only for advanced users. XML files are highly vulnerable to spelling errors and mistyped strings and keys.*
Even a tiny error can cause fatal errors. Mirasys takes no responsibility for XML errors caused by editing the files.

9.5.3 Watchdog event list

Id	Event	Description
0	SmServerDown	WDServer detected that SMServer process stopped
1	SmServerUp	WDServer detected that SMServer process started
2	DvrServerDown	WDServer detected that DVRService process stopped
3	DvrServerUp	WDServer detected that DVRServer process started

MIRASYS

Id	Event	Description
4	NetworkDown	WDServer detected that network is down
5	NetworkUp	WDServer detected that network is up
6	DvrStatusOK	WDServer got ok status from recorder
7	DvrRefreshing	WDServer got settings refreshing status from recorder
8	DvrVideoCaptureLoadFailure	WDServer got video capture driver load error status from recorder
9	DvrAudioCaptureLoadFailure	WDServer got audio capture driver load error status from recorder
10	DvrDataCaptureLoadFailure	WDServer got text data driver load error status from recorder
11	DvrNoFileSystem	WDServer got no file system status from recorder
12	DvrDiskFailure	WDServer got disk failure status from recorder
13	VideoChannelOK	WDServer got video channel ok status from recorder
14	VideoChannelNoSignal	WDServer got video channel no signal status from recorder
15	VideoChannelNotStarted	WDServer got video channel not started status from recorder
16	VideoChannelNoCapture	WDServer got video channel no capture status from recorder
17	AudioChannelOK	WDServer got audio channel ok status from recorder
18	AudioChannelNoSignal	WDServer got audio channel not started status from recorder
19	AudioChannelNotStarted	WDServer got audio channel no capture status from recorder
20	AudioChannelNoCapture	WDServer got audio channel not started status from recorder
21	DataChannelOK	WDServer got text data channel ok status from recorder

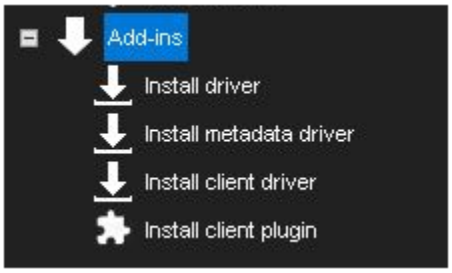
Id	Event	Description
22	DataChannelNoSignal	WDServer got text data channel not started status from recorder
23	DataChannelNotStarted	WDServer got text data channel no capture status from recorder
24	DataChannelNoCapture	WDServer got text data channel not started status from recorder
25	WDConnectionDown	Connection between WDServer and SMServer is down
26	WDConnectionUp	Connection between WDServer and SMServer is up
27	DvrSecurityFailure	WDServer got security failure status from recorder
28	DvrOtherInitFailure	WDServer got other initialization status from recorder
29	DvrArchiveFailed	WDServer got archive failed status from recorder
30	DvrMapNetworkDriveFailed	WDServer got map network drive failed status from recorder
31	DvrInsufficientDiskSpace	WDServer got insufficient disk space status from recorder
32	DvrNASDiskConnectionLostFailure	WDServer got NAS disk connection lost status from recorder
33	DvrNASDiskInitializationFailure	WDServer got NAS disk initialization failed status from recorder
34	SMServerDBConnectionLost	SMServer has detected that database connection lost
35	SMServerDBConnectionRestored	SMServer has detected that database connection is restored
36	SMServerAuditTrailCacheFull	SMServer has detected that audit trail cache is full
37	DvrTemperatureLpcOk	NOT IN USE
38	DvrTemperatureLpcWarning	NOT IN USE
39	DvrTemperatureLpcFailure	NOT IN USE

Id	Event	Description
40	DvrTemperatureCpuOk	NOT IN USE
41	DvrTemperatureCpuWarning	NOT IN USE
42	DvrTemperatureCpuFailure	NOT IN USE
43	DvrTemperatureHddOk	WDServer has detected that HDD temperature is ok
44	DvrTemperatureHddWarning	WDServer has detected that HDD temperature is in warning level
45	DvrTemperatureHddFailure	WDServer has detected that HDD temperature is in failed level
46	DvrTemperatureDisplayAdapterOk	NOT IN USE
47	DvrTemperatureDisplayAdapterWarning	NOT IN USE
48	DvrTemperatureDisplayAdapterFailure	NOT IN USE
49	DvrTemperaturePsuOk	NOT IN USE
50	DvrTemperaturePsuWarning	NOT IN USE
51	DvrTemperaturePsuFailure	NOT IN USE
52	DvrTemperatureAcpiOk	NOT IN USE
53	DvrTemperatureAcpiWarning	NOT IN USE
54	DvrTemperatureAcpiFailure	NOT IN USE
55	DvrTemperatureRamOk	NOT IN USE
56	DvrTemperatureRamWarning	NOT IN USE
57	DvrTemperatureRamFailure	NOT IN USE
58	DvrMetadataDatabaseConnectionError	WDServer got metadata database connection error status from recorder
59	GatewayUp	WDServer has detected that Gateway service is started
60	GatewayDown	WDServer has detected that Gateway service is stopped

Id	Event	Description
61	DvrFatalRuntimeError	WDServer got fatal runtime error status from recorder
62	SMSServerUp	WDServer has detected that SMSServer service is started
63	SMSServerDown	WDServer has detected that SMSServer service is stopped
64	LicenseIsAboutToExpire	SMServer has detected that license is about to expire
65	LicenseHasExpired	SMServer has detected that license is expired
66	AutomaticBackupFailed	Automatic backup generation has failed in SMServer
67	DvrBrokenAtMaintenance	Recorder failure has been detected on maintenance mode and failover is ignored
68	DvrBrokenAndChangedWithFailoverDvr	Recorder failover has occurred
69	DvrBrokenWithoutPossibilityToChangeWithFailoverDvr	Recorder failure has been detected but there is no free failover servers
70	RPMServerUp	NOT IN USE
71	RPMServerDown	NOT IN USE
72	PublicWebApiServerUp	NOT IN USE
73	PublicWebApiServerDown	NOT IN USE
74	ExportServerUp	WDServer has detected that Export service has started
75	ExportServerDown	WDServer has detected that Export service has shutdown
76	StorageLockerServerUp	WDServer has detected that Storage Locker service has started
77	StorageLockerServerDown	WDServer has detected that Storage Locker service has shutdown
78	IncidentReportingServerUp	WDServer has detected that Incident Reporting service has started

Id	Event	Description
79	IncidentReportingServerDown	WDServer has detected that Incident Reporting service has shutdown
80	DvrFailbackDone	Recorder failback operation has been performed successfully on SMServer
81	DvrFailbackFailed	Recorder failback operation has failed on SMServer
82	DvrFailbackOnMaintenance	Recorder failback operation has been ignored because recorder is in maintenance mode

9.6 ADD-INS



9.6.1 Mirasys Camera Drivers

A list of Mirasys Camera Drivers.

9.6.1.1 OnvifIPCapture

Purpose

To capture MJPEG, MPEG-4, H.264, and H.265 compressed video data from ONVIF-compliant IP cameras and video-servers, and to support the PTZ functionality of these devices.

Supported cameras:

- All ONVIF-compliant IP devices.
  Supported ONVIF Profiles: S, G, T, M

Note:

- The Edge Storage functionality (Profile G) is integrated for single-channel devices only.

Supported features

- Auto-search
- H.264 video compression

- H.265 video compression
- MPEG-4 video compression
- MJPEG video compression
- Digital I/O
- PTZ
- Parallel auto-search
- Multiple streaming
- Audio (2-way)
- Device motion detection
- Multicast streaming
- CCRiA (Can Change Resolution in Alarm)
- CCFiA (Can Change Framerate in Alarm)
- Edge Storage (video)
- Dynamic UI (since DVMS 8.1.2)
- HTTPS encrypted streaming (RTSP over HTTPS tunneling)
- Focus/Iris adjustment
- Privacy Zones

Supported files

- OnvifIPCapture.dll
- OnvifIPCapture.xml
- Readme_OnvifIPCapture.txt

Latest version

1.9.25.0

Release date

19.10.2026

9.6.1.2 NewAxisIPCapture

Purpose

To capture MJPEG, MPEG4, and H.264 compressed video data from Axis IP devices (cameras and video-servers) and to support PTZ functionality.

Supported features

- Auto-search
- H.264 video compression
- H.265 video compression
- MPEG-4 video compression
- MJPEG video compression
- Digital I/O
- PTZ
- CCRiA (Can Change Resolution in Alarm)
- CCFiA (Can Change Framerate in Alarm)
- Privacy zones
- Device motion detection (firmware version before 5.50)
- Audio (2-way)
- Multiple streaming
- Parallel auto-search
- Edge Storage (video only)
- Multicast streaming
- Dynamic UI (since DVMS 8.1.2)
- AXIS License Plate Verifier
- Vaxtor LPR

Supported files

- NewAxisIPCapture.dll
- NewAxisIPCapture.xml
- Readme_NewAxisIPCapture.txt

Latest version

2.9.15.0

Release date

23.10.2026

9.6.1.3 NewBoschIPCapture

Purpose

To capture H.265, H.264, MPEG-4, and MJPEG compressed video data from Bosch IP cameras and video-servers, and to support PTZ functionality of Bosch IP devices.

Supported features

- Auto-search
- H.265 video compression
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Multiple streaming
- Two-way audio (G.711Ulaw, AAC)
- Privacy zones
- Device motion detection
- Digital I/O
- PTZ
- Parallel auto-search
- Edge storage
- Multicast streaming
- CCRiA (Can Change Resolution in Alarm)
- CCFiA (Can Change Framerate in Alarm)
- HTTPS support (except sending audio to camera)

Supported files

- NewBoschIPCapture.dll

- rcpp4.dll or rcpp4x64.dll (v4.61.0.25)
- NewBoschIPCapture.xml
- Readme_NewBoschIPCapture.txt

Latest version

1.8.1.0

Release date

23.09.2026

9.6.1.4 BOSCH_AutoDomeBPDrvG3

Purpose

Old PTZ driver

9.6.1.5 PelcoIPCapture

Purpose

To capture H.264, MPEG-4, and MJPEG compressed video data from Pelco IP cameras and to support the PTZ functionality of Pelco IP cameras.

Supported features

- Auto-search
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Digital I/O
- PTZ
- Parallel auto-search

Supported files

- PelcoIPCapture.dll
- PelcoIPCapture.xml
- Readme_PelcoIPCapture.txt

Latest version

1.8.3.5

Release date

20.02.2019

9.6.1.6 VivotekIPCapture

Purpose

To capture MJPEG, MPEG-4, and H.264 compressed video data from Vivotek IP devices (cameras and video servers) and to support PTZ and IO functionality of Vivotek IP devices.

Supported features

- Auto-search
- H.264 video compression
- H.265 video compression
- MPEG-4 video compression
- MJPEG video compression
- Digital I/O
- PTZ
- Parallel auto-search
- Multiple streaming
- Can Change Resolution in Alarm (CCRiA)
- Can Change Framerate in Alarm (CCFiA)
- Dynamic UI (since DVMS 8.1.2)
- Audio (2-way)

Supported files

- VivotekIPCapture.dll
- VivotekIPCapture.xml
- Readme_VivotekIPCapture.txt

Latest version

2.0.1.2

Release date

21.10.2024

9.6.1.7 EHIIPCapture

Purpose

To capture H.265, H.264, MPEG-4, and MJPEG compressed video data from Hikvision, Ernitec, and Interlogix IP cameras, DVRs/NVRs, and encoders, to support PTZ functionality and other features described below.

Supported cameras:

- Hikvision IP cameras
- Hikvision DVRs/NVRs
- Hikvision encoders
- Interlogix IP cameras
- Ernitec IP cameras

Supported features

- Auto-search
- Parallel auto-search
- MJPEG video compression
- MPEG-4 video compression
- H.264 video compression
- H.265 video compression
- Digital I/O
- PTZ - Continuous PTZ movement is used by default for all cameras
- Device motion detection
- Multiple streaming
- Audio (two-way)
- Edge storage (ISAPI devices only)
- Can Change Resolution in Alarm (CCRiA)
- Can Change Framerate in Alarm (CCFiA)
- Multicast streaming

- ANPR with a list management interface and separate parameters to include/exclude license plate and detection images

Supported files

- EHIIPCapture.dll
- EHIIPCapture.xml
- HikvisionDVRConnector.xml
- HikvisionEncoderConnector.xml
- Readme_EHIIPCapture.txt

Latest version

2.1.22.0

Release date

06.02.2026

9.6.1.8 EIPCapture

Purpose

To capture MJPEG, H.264, and MPEG-4 compressed video data from e-Vision (El.MO), Dynacolor, and Planet IP cameras, and to support the PTZ functionality of PTZ cameras of specified manufacturers.

Supported cameras:

- El.MO NH-series cameras (e-Vision TPMX10x)
- Dynacolor HD IP cameras (e-Vision TDMX10x)
- Dynacolor HD WDR IP cameras (e-Vision TPMX20x)
- Dynacolor V-series cameras (e-Vision TPMX30x/TDMX30x)
- Dynacolor IP PTZ cameras (e-Vision ElDome)
- Planet ICA-HM131/HM131R/HM126/HM126R IP cameras
- Planet ICA-H652 IP PTZ cameras
- Dynacolor Full HD Quad-Stream cameras

Supported features

- Auto-search
- MJPEG video compression

- MPEG-4 video compression
- H.264 video compression
- Digital I/O
- PTZ
- Parallel auto-search
- Multiple streaming

Supported files

- EIPCapture.dll
- EIPCapture.dat
- EIPCapture.xml
- Readme_EIPCapture.txt

Latest version

2.3.2.5

Release date

02.11.2016

9.6.1.9 GatewayIPCapture

Purpose

To capture MJPEG and Native compressed video data from Gateway servers and to support PTZ and I/O functionality.

Supported cameras:

- All Gateway servers with Promesa 3.0 or higher

Supported features

- Auto-search
- MJPEG video compression
- Native video compression
- Digital I/O
- PTZ

- Parallel auto-search

Supported files

- GatewayIPCapture.dll
- GatewayIPCapture.xml
- Readme_GatewayIPCapture.txt

Latest version

1.0.4.0

Release date

11.08.2016

9.6.1.10 HTTPIPCapture

Purpose

To capture MJPEG compressed video data from HTTP IP devices.

Supported features

- Auto-search
- Parallel auto-search
- MJPEG video compression

Supported files

- HTTPIPCapture.dll
- Readme_HTTPIPCapture.txt

Latest version

1.0.1.0

Release date

07.02.2020

9.6.1.11 IPCameraCapture

Purpose

To capture JPEG/MPEG-4/H.264 compressed video and audio data from UDP, Amano, GANZ, Ernitec, Sprinx IPE/NVC, and IPN/IPX series of IP video servers and cameras, and support the PTZ functionality of these devices.

Supported features

- Auto-search
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Digital I/O
- PTZ
- Can Change Framerate in Alarm (CCFiA)
- Parallel auto-search
- Two-way Audio
- Multiple streaming
- Multicast streaming
- Time synchronization
- Edge Storage

Supported files

- IPCameraCapture.dll
- IPCameraCapture.xml
- Readme_IPCameraCapture.txt

Latest version

1.7.3.0

Release date

20.02.2019

9.6.1.12 LGEIPCapture

Purpose

To capture H.264 and MJPEG compressed video data from LG Electronics IP devices.

Supported features

- Auto-search
- Parallel auto-search

- MJPEG video compression
- H.264 video compression
- Digital I/O
- PTZ

Supported files

- LGEIPCapture.dll
- Readme_LGEIPCapture.txt

Latest version

1.0.6.3

Release date

20.02.2019

9.6.1.13 NewActiIPCapture

Purpose

To capture MPEG4/MJPEG/H.264 compressed video data from Acti, Messoa NIC910/930/950HPRO, and Vido AU-GxxIP IP cameras.

Supported features

- Auto-search
- Parallel auto-search
- Device motion detection
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Multiple streaming
- Multicast streaming
- Privacy mask
- Two-way audio
- Digital I/O

- PTZ
- Edge storage (starting from firmware 6.07.23 and higher)

Supported files

- AADP.dll
- ADADP.dll
- AFADP.dll
- FFMCodec.dll
- FisheyeSDK.dll
- KMpeg4.dll
- PTZParser.dll
- NewActiIPcapture.dll
- NewActiIPCapture.xml
- Readme_NewActiIPCapture.txt

Latest version

2.4.2.0

Release date

29.08.2018

9.6.1.14 NewArecontIPCapture

Purpose

To capture MJPEG/H.264 compressed video data from Arecont IP cameras.

Supported features

- Auto search
- MJPEG video compression
- H.264 video compression
- Digital I/O
- Multiple streaming
- Parallel auto-search

- Can Change Resolution in Alarm (CCRiA)
- Can Change Framerate in Alarm (CCFiA)
- Two-way Audio

Supported files

- NewArecontIPcapture.dll
- NewArecontIPCapture.xml - example of a custom parameters file
- Readme_NewArecontIPCapture.txt

Latest version

2.2.3.0

Release date

15.08.2019

9.6.1.15 NewIQEyeIPCapture

Purpose

To capture MJPEG/H.264 compressed video data and G.711 compressed audio data from IQEye IP cameras.

Supported features

- Auto search
- MJPEG video compression
- H.264 video compression
- Digital I/O
- CCFIA (enabled through IQEye.xml configuration file)
- Audio (G.711 only)

Supported files

- NewIQEyeIPcapture.dll
- IQEye.xml
- Readme_NewIQEyeIPCapture.txt

Latest version

1.4.6.0

Release date

21.02.2014

9.6.1.16 NewMobotixIPCapture

Purpose

To capture MJPEG compressed video data from Mobotix cameras and to support PTZ functionality

Supported features

- Auto-search
- MJPEG video compression
- MxPEG video compression
- Digital I/O
- PTZ
- Parallel auto-search
- Audio

Supported files

- NewMobotixIPCapture.dll
- NewMobotixIPCapture.xml
- Readme_NewMobotixIPCapture.txt

Latest version

1.4.2.0

Release date

27.01.2022

9.6.1.17 NewPanasonicIPCapture

Purpose

To capture JPEG/MPEG4/H.264/H.265 compressed video data from Panasonic IP cameras and to support PTZ functionality.

Note that the old Panasonic Driver is PanasonicIPCapture.

Supported features

- Auto search

- Parallel auto-search
- JPEG video compression
- MPEG4 video compression
- H.264 video compression
- I/O
- PTZ

WV series only:

- Device motion detection
- Multiple streaming
- Multicast streaming
- Privacy mask
- Two-way audio
- CCFIA
- CCRIA
- Edge storage
- H.265 video compression
- Vaxtor ANPR

Supported files

- NewPanasonicIPcapture.dll
- NewPanasonicIPCapture.xml
- Readme_PanasonicIPCapture.txt

Latest version

1.6.3.0

Release date

13.03.2025

9.6.1.18 NewSiquraIPCapture

Purpose

To capture MJPEG, MPEG-4, and H.264 compressed video data from Siqura C/S-5x/6x IP codecs and MD/HD-2x/6x PTZ cameras, and to support PTZ functionality of specified Siqura devices.

Supported features

- Auto-search
- MJPEG video compression
- MPEG-4 video compression
- H.264 video compression
- I/O
- PTZ

Supported files

- NewSiquraIPCapture.dll
- Readme_NewSiquraIPCapture.txt

Latest version

1.9.5.2

Release date

10.02.2015

9.6.1.19 NewSonyIPCapture

Purpose

To capture MJPEG, MPEG-4, and H.264 compressed video data from SONY IP devices and to support additional functionality of SONY IP devices.

Supported cameras:

- All SONY IP cameras (except SNC-RZ30 and SNC-HM662 cameras) and G5 video servers.

Supported features

- Auto-search
- MJPEG video compression
- MPEG-4 video compression
- H.264 video compression
- Digital I/O

- PTZ
- Device motion detection
- Privacy Zones
- Can Change Resolution in Alarm (CCRiA) (G2-G4 cameras only)
- Can Change Framerate in Alarm (CCFiA) (G2-G4 cameras only)
- Parallel auto-search
- Multiple streaming (for G5-G7 cameras)
- Audio (2-way) (for G5-G7 cameras)
- Time synchronization (for G5-G7 cameras)
- Edge Storage (for G5-G7 cameras)
- Dynamic UI (since DVMS 8.1.2)

Supported files

- NewSonyIPCapture.dll
- NewSonyIPCapture.xml
- Readme_NewSonyIPCapture.txt

Latest version

2.6.4.0

Release date

22.08.2019

9.6.1.20 PSIAIPCapture

Purpose

To capture H.264 compressed video data from PSIA IP cameras.
The PSIA version 1.1 is supported.

Supported Cameras:

- PSIA-compatible IP cameras

Supported features

- Auto-search

- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Digital I/O
- Parallel auto-search
- Dynamic UI (since DVMS 8.1.2)

Supported files

- PSIAIPCapture.dll
- Readme_PSIAIPCapture.txt

Latest version

1.2.6.0

Release date

03.07.2024

9.6.1.21 RTSPIPCapture

Purpose

To capture H.265/H.264/MPEG-4/MJPEG compressed video data from RTSP IP devices.

Supported features

- Auto-search
- Parallel auto-search
- H.265 video compression
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Multicast streaming (RTP only)
- Audio input

Supported files

- RTSPIPCapture.dll

- RTSPIPCapture.xml
- Readme_RTSPIPCapture.txt

Latest version

1.6.5.0

Release date

11.03.2026

9.6.1.22 SIPIPCapture

Purpose

Driver for specific Zenitel devices working over SIP protocol: To capture H.264 compressed video data from SIP Proxy.

Supported features

- Auto-search
- H.264 video compression
- Two-way audio

Supported files

- SIPIPcapture.dll
- Readme_SIPIPCapture.txt

Latest version

1.0.0.0

Release date

17.11.2016

9.6.1.23 StanleyIPCapture

Purpose

To capture H.264 and MJPEG compressed video data from Stanley IP cameras, to support PTZ functionality and other features described below.

Supported features

- Auto-search
- Parallel auto-search

- MJPEG video compression
- H.264 video compression
- Digital I/O
- PTZ
- Multiple streaming
- Device motion detection
- Privacy zones

Supported files

- StanleyIPCapture.dll
- StanleyIPCapture.xml
- Readme_StanleyIPCapture.txt

Latest version

1.2.1.6

Release date

24.09.2021

9.6.1.24 WisenetIPCapture

Purpose

To capture H.265/HEVC, H.264, and MJPEG compressed video data from Wisenet IP devices and to provide additional functionality (Digital I/O, PTZ, Privacy Masking, etc.) for these devices. SUNAPI specification version 2.x is supported.

Supported features

- Auto-search
- Parallel auto-search
- H.265/HEVC video compression
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Device motion detection

- Multiple streaming
- Audio (2-way)
- Multicast streaming
- Privacy Masking
- Digital I/O
- PTZ
- Edge Storage (since DVMS 8.0.0)
- Dynamic UI (since DVMS 8.1.2)
- CCRiA (Can Change Resolution in Alarm)
- CCFiA (Can Change Framerate in Alarm)
- Time synchronization
- Video loss detection
- Vaxtor ALPR
- WisenetRoadAI

Supported files

- WisenetIPCapture.dll
- WisenetIPCapture.xml
- Timezones.xml
- Readme_WisenetIPCapture.txt

Latest version

1.3.4.0

Release date

23.09.2026

9.6.1.25 DahuaIPCapture

Purpose

To capture H.265, H.264, MPEG-4, and JPEG compressed video data from Dahua IP devices and to provide additional functionality (Digital I/O, PTZ, Privacy Masking, etc.) for these devices.

MIRASYS

Supported features

- Auto-search
- Parallel auto-search
- H.265/HEVC video compression
- H.264 video compression
- MPEG-4 video compression
- MJPEG video compression
- Device motion detection
- Multiple streaming
- Audio (2-way)
- Multicast streaming
- Privacy Masking
- Digital I/O
- PTZ
- CCFiA (Can Change Framerate in Alarm)
- Edge Storage
- AES-256 encrypted unicast video streaming (Dahua SDK)

Supported files

- DahuaIPCapture.dll
- DahuaIPCapture.xml
- Readme_DahuaIPCapture.txt
- avnetsdk.dll
- d3dx9_24.dll
- dhconfigsdk.dll
- dhnetsdk.dll
- dhplay.dll

- fisheye.dll
- HWDec.dll
- Infra.dll
- Json.dll
- libcurl.dll
- libeay32.dll
- NetFramework.dll
- ssleay32.dll
- Stream.dll
- StreamConvertor.dll
- StreamSvr.dll

Latest version

1.3.8.0

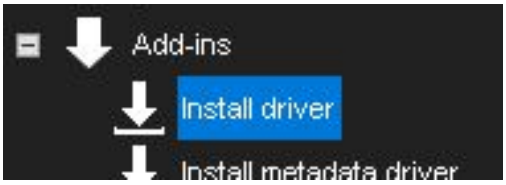
Release date

30.11.2023

9.6.2 Installing External Driver Packages

To use IP cameras, digital I/O devices or text data in the VMS system, the driver for each device must be installed on the server. The software includes all drivers and plugins that have been included in the previous versions of the software.

9.6.2.1 Install a new Driver



New Drivers and Plugins can be installed manually.

9.6.2.1.1 Driver installation packages

To install a new driver, you need a device-specific driver installation package. The package is a compressed (zipped) folder containing the driver files.

When installing a driver installation package, the system compares the files in the installation package to the existing files on the servers. It installs the files only if they do not exist on the servers or if the files in the installation package are newer than those on the servers.

You can also force the system to install any driver version if necessary.

If you want to update an already existing camera driver:

1. Remove the camera from the system before updating the driver.
2. After removing the camera, install the driver file.
3. Then reinstall the camera.
4. After installing a new driver, you need to configure the devices that use the driver.

9.6.2.1.2 How to install a Driver package

1. On the **System** tab, under **Add-ins**, open **Install driver**.
2. Select the drive where the driver package is located, find and select the driver package (.zip file). The **Install Driver** dialogue box is shown.



3. Select the servers on which you want to install the driver.

4. If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**

5. Click **Install**. The **Status** column shows the text **Installed** if the driver is successfully installed. If the driver is not installed, the column shows an error message.

6. Click **Close** to exit the dialogue box.

If you need to update drivers for hardware other than IP cameras, please contact the system supplier.

A 32-bit system requires a 32-bit driver package, and a 64-bit system required a 64-bit driver package.

9.6.3 Driver Installation and Usage

9.6.3.1 ArchiveCapture installation and usage

The path for the archive is set to the address field (auto search window).

The Driver configuration is done through ArchiveCapture.xml:

- Loop functionality
- Original (captured) frames time
- Frame rate (configurable or default)
- Time limits for capture from the saved archive
- Enable/disable video channels

The "channels" and "limit" sections can be disabled at all (attribute enabled="0")

Without `ArchiveCapture.xml` default values will be used.

XML file settings are applied only during the archive search process.

PAUSE, CONTINUE and NEXT_FRAME are implemented over `CIPVideoCapture::SetExtendedProperty`(const char* const `aProperty`, void* aValue, unsigned long `aChannelId`) where:
`aProperty` - command, can be "PAUSE", "CONTINUE" and "NEXT_FRAME"
`aValue` - for future needs, should be NULL
`aChannelId` - channel id

9.6.3.2 CanonIPCapture installation and usage

In all compression modes driver uses RTSP/RTP/UDP/IP protocols for receiving video stream and input states.

HTTP protocol is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default ports are 80,
- **RTSP**: port 554,
- **UDP**: two sequential ports per video stream and two sequential ports per metadata stream (input states) are needed in a port range 3556 to 4556.

For example: if there are 2 IP cameras in a DVMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

CanonIPCapture.xml file is used to configure driver behavior:

- Unicast
- Multicast:Primary
- Multicast:Listener

Parameters for PTZ speed limitation:

- PanSpeed (1 - 100%, limit speed for required percentage value)
- TiltSpeed (1 - 100%, limit speed for required percentage value)
- ZoomSpeed (1 - 100%, limit speed for required percentage value)
- PTZQueueSize (PTZ queue size, can be optimized for slow cameras)

9.6.3.2.1 Limitations

- Old Canon cameras with firmware 1.0.3 or earlier can reboot on each resolution change. This can take 1-5 minutes to complete.
- VB-S cameras have 2 H.264 streams, which can be used for recording and live in VMS. Other series only has the 1 H.264 channel.
- VB-S cameras have a limitation of a maximum framerate of 15 for selected resolutions. If one of those combinations is set, fps will be changed even if DVMS settings are different:
    - 1920x1080 - All sizes
    - All sizes - 1920x1080
    - 1280x960 - 1280x960
    - 1280x720 - 1280x720
- VB-M, VB-H, VB-S series camera Moving Object detection differs from conventional motion detection. The detection creates a static "Background image" and compares any scene change within the detection area with this image.
  The camera sends an "Event ON" status notification when the object enters the detection area and sends an "Event OFF" status when an object comes out from the detection area and the scene is changed back to the original "Background image.""
  If the "Event ON" status continues over 5-minute periods, the camera regards this as a new background, sends the "Event OFF" status, and resumes Alarm detection standby mode.
- **Unicast mode**: The driver will change the camera settings according to the DVMS settings and receive audio and video data from the camera using a Unicast connection.

- **Multicast:Primary**: The driver will change the camera settings according to the DVMS settings and receive audio and video data from the camera using a multicast connection.
- **Multicast:Listener**: the driver will not change camera settings; just receive audio and video data from the camera using the multicast connection.
- If the camera is to be used in several DVMS instances, one DVMS should be set to Multicast:Primary, and others should be Multicast:Listener.
- Several Multicast:Primary configurations or Multicast:Primary and Unicast configurations are not allowed; in other cases, the camera should be overloaded with continuous concurrent settings changes.
- CCFIA and CCRIA are disabled for the VB-M series because cameras from this series require a reboot after settings change.

9.6.3.3 DahuaIPCapture installation and usage

The driver uses RTSP/RTP/UDP/IP protocols for video receiving in all compression modes.

The HTTP protocol is used for parameter setting/retrieving. If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: port 554,
- **UDP**: two sequential ports per video stream are needed in a port range of 3556 to 4556.

For example, if there are 4 Dahua IP cameras in a DVMS, ports 3556, 3557, 3558, 3559, 3560, 3561, 3562, and 3563 will be used. If a port is not free, it will be skipped.

9.6.3.3.1 Limitations

- **Multiple streaming** features may have limitations dependent on the device used (for example, the resolution on the Extra stream cannot be greater than that on the video Mainstream). Please refer to the device manual to learn these limitations.
- The **CCRiA** (Can Change Resolution in Alarm) feature is not supported. It takes longer to apply a new resolution than the signal lost timeout.
- **Cameras with two dependent sensors**, for example DH-SDT4E425-8P-GB-APV1, are not fully supported. Our VMS does not support different resolutions for different channels of the same device. All channels will have the same resolution list, but only supported resolutions can be applied.
  The same is valid for changing the resolution in alarm functionality.
- If Dahua/Stanley devices do not change the resolution or framerate correctly, please update it to a new firmware. Driver will print the following message in the DVRLog.txt:
  - "Can't configure video channels for device <ip>:80, result code: 12002 (Request timeout).” " Device may not accept new video settings without correct Bitrate parameter. The camera sends an

incorrect bitrate range, and the driver will calculate an unacceptable Bitrate by Quality and try to apply it in both CBR and VBR modes. It is possible to override the Bitrate range using the following option in the DahuaIPCapture.xml `<BitrateMap enabled="yes"` Driver has an internal bitrate map for most resolutions up to 1920x1080 for the H.264 codec only. It is possible to add more bitrates for higher resolutions and JPEG codec, as shown in the examples in the driver's XML.

- Dahua device may be added with a lower maximal frame rate than some resolutions support. Please update the firmware. If it is unavailable, please remove the Dahua device from DVMS, set the required video settings using the Web Interface, and add it again.
- If the Dahua device returns many "400" or "500" HTTP errors in response, please update it to a new firmware. In case the firmware update is not available, then there are several parameters in the DahuaIPCapture.xml:
    - `<UseEventManager>false</UseEventManager>` To disable the "EventManeger" poll requests
    - `<InputCheckTimeout>1000</InputCheckTimeout>` To adjust the interval between digital inputs requests, only if disabled the <UseEventManager>false</UseEventManager> option
    - `<Control digitalInputs="false" motionDetection="false" />` To disable digital inputs and motion detection on camera hardware
- Audio functionality limitations:
    - The driver uses audio functionality "as is" without adjusting audio parameters (like output gain). Please configure these parameters via the Web Interface.
    - The driver supports G.711 and G.726 audio encodings. The AAC encoding is not supported.
    - For some firmware versions, Two-Way audio may not work after network disconnections. Please remove the device from DVMS, reboot it, and add it again. To disable this feature for a particular device, set the following option: `<TwoWayAudio>NO</TwoWayAudio>`
- Multicast capture limitations:
    - Multicast capture can be enabled via an XML configuration file using the RTPMode option. This option is read on stream startup, so a refresh of device settings will be enough to activate the changed RTPMode option.
    - The user should guarantee that only one recorder changes the settings of IP devices. Other recorders that use this camera should not change settings.
      Please disable camera settings changes using the following option
      `<ChangeSettings>false</ChangeSettings>`
      In this mode, driver will not change the following camera settings:
      = Quality
      = Resolution
      = Framerate

- `<ChangeSettings>true</ChangeSettings>`
  The driver will change the camera settings according to the DVMS settings and receive audio and video data from the camera using a multicast connection. Please configure this mode only for the primary recorder.
- For the secondary recorder, the following options will be configured the same as for the primary recorder:
  = Multiple streaming option
  = Video Codec for all streams
- Encrypted streaming features known issues and limitations:
  - Dahua IP Capture driver supports receiving encrypted video streams from the IP devices. Processing of encrypted stream is based on 3-rd party Dahua libraries (NetSDK and PlaySDK from Dahua)
  - Stream encryption should be enabled via Web UI before using it in the Mirasys VMS. To enable it, go to device settings, then select the "System" group, then the "Security" or "Safety" subgroup (the name may differ for different devices). Select the ìSystem Serviceî tab in the settings dialog, then enable the "Audio and Video Transmission Encryption" checkbox.
  - If the IP device supports stream encryption, the system will add the "AES-256 Encrypted" transport and select it as the default transport. If you do not need to use stream encryption ñ just select any other transport based on your requirements.
  - The AES-256 algorithm is used for stream encryption according to Dahua's GDPR specification document. The key-frame encryption is used. In other words:
    = The stream encryption may be used for H.265, H.264 and MPEG-4 encodings;
    = The MJPEG stream cannot be encrypted and received via SDK libraries as is.
  - MPEG-4 encryption is supported. However, no device was available to test it in Mirasys. So, the implementation was made based on SDK documentation, but it was not tested.
  - The audio encryption is available via NetSDK but has not been implemented in the Driver.
  - The encryption is not supported for multicast streaming.
- For quick start video capture in Multicast mode, it is possible to configure addresses and ports on the device and in the driver XML file and disable video settings adjustments by the following option <ChangeSettings>false</ChangeSettings>.
- Zoom may not work correctly for the Stanley IPC-STAN-6100IRV camera. It is a camera firmware issue.
- The driver doesn't support Unicode in PTZ preset (preposition) names.
- Please do not try to search the camera with <All drivers> option and the <default> credential or wrong password - **it may lock user account**. Please add the device using a single 'DahuaIPCapture' driver instead.
- This driver does not support Windows XP.

- Cameras with two dependent sensors, like DH-SDT4E425-8P-GB-APV1, are not fully supported because DVMS doesn't support different resolutions for different channels of the same device. So, all channels will have the same resolution list, but only supported resolutions can be applied. The same is valid for changing the resolution in alarm functionality.

9.6.3.4 EHIIPCapture installation and usage

The driver uses RTSP/RTP/HTTP/HTTPS/UDP/IP protocols for video receiving in all compression modes. Also, HTTP/HTTPS protocols are used for parameter setting/retrieving and for Remote stream video. If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP/HTTPS ports must be opened:

- **HTTP**: default port is 80,
- **HTTPS**: default port is 443,
- **RTSP**: port 554,
- **UDP**: two sequential ports per video stream are needed in a port range of 3556 to 4556.

For example, if there are 4 cameras in DVMS, ports 3556, 3557, 3558, 3559, 3560, 3561, 3562, and 3563 will be used. If a port isn't free, it will be skipped.

The EHIIPCapture.xml file can be used to select a 360-degree view (channel) - please specify channel numbers that should be used in the following section in XML:

```
<Channel360>1</Channel360>
<Channel360>2</Channel360>
```

After setting channel numbers for a 360-degree camera, the camera must be removed and added again to detect the correct capabilities for the channels.

Multicast streaming also requires two sequential ports per audio or video stream, but the port numbers depend on device settings or XML configuration.

For example, the device may be configured to send all streams to a single port only. If the 40000 port is specified for this setting, ports 40000-40001 should be opened.

9.6.3.4.1 Limitations

- Only one audio multicast stream is supported. One multicast IP address is used for the audio channel and for the video channel but the multicast audio port for the same stream should be greater than the video port by at least 2, multicast video port for another stream (Live, for example) should be greater than the video port of previous stream (Recording, for example) at least 6.
- The audio channel uses the same multicast IP address as the video stream receiver. If different multicast addresses are defined, this may cause a conflict in the multicast configuration applied by the video channel (from the Dynamic UI configuration) and the audio channel (loaded from the XML file).
- You must enable IGMP Snooping on the network switch for multicast communication.

- For HTTP/HTTPS transport, the following logic is implemented: The RTPoverHTTP dynamic field is added if the communication over HTTP is used or if the communication over HTTPS is used. The device supports the RTPoverHTTPS feature.
- Regarding the TLS certificate, when an RTSP connection over HTTPS (TLS) is made, the camera shares its public certificate during the Handshake procedure. Therefore, clients need not store or have the cameraís public certificate.
- Multiple streaming mode is supported correctly only from DVMS 6.1
- The compression format for Recording and Live streaming should be the same in multiple streaming mode
- Cameras reboot after changing the compression format, so it requires about 30 seconds to restore video after changing the compression format.
- The remote stream has the same resolution as the Recording stream for devices with two streams per channel ("Main" and "Sub"), so the resolution setting is not used for such a stream, which is an HTTP JPEG capture.
- For devices with 3 streams per channel, this limitation does not exist.
- Some versions of Hikvision firmware return a list of resolutions the camera does not support. These resolutions can be applied in DVMS, but camera images will have artifacts.
- Hikvision cameras support only 6 RTSP sessions at the same time. This is a limitation of the Hikvision firmware.
- Motion detection should be configured manually on the device before use in the DVMS. MD functionality may not work correctly with old firmware versions. Please use the latest firmware version to use all driver features.
- Receiving input states should be enabled in the XML configuration file and configured in the device web interface (e.g., enable sending input states with "Notify Surveillance Center").
- The third stream of Hikvsion devices is used as a Live stream and 2nd as a Remote.
- Video loss detection should be configured manually on the device before using it in the DVMS. It can also be disabled/enabled in the configuration file.

9.6.3.5 EIPCapture installation and usage

The driver uses RTSP/RTP/UDP/IP protocols for video receiving in all compression modes.

The HTTP protocol is used for parameter setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: port 554,

- **UDP**: two sequential ports per video stream are needed in a port range of 3556 to 4556.

For example: if there are 4 El.MO or Dynacolor IP cameras in a DVMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

9.6.3.5.1 Limitations

- The WinInet library is used to send/receive HTTP data between DVMS and the e-Vision/Dynacolor camera. The 8.0 version of this library has a limitation: only 2 HTTP connections may be opened at the same time (please refer to the following article: http://support.microsoft.com/kb/183110).> This issue becomes actual after Internet Explorer is updated to 8.0 or higher.
- If the camera's Web interface is opened on the same PC where this driver is used, a few HTTP requests may not be sent because of this limitation. In this case, the camera may not be found by Auto-Search, or some functionality may not work at all.
- The "Video OCX protocol" option should be set to "RTP over UDP" (or "RTP over RTSP(TCP)" in some cases) for correct receiving of the RTP/RTSP video stream. This option cannot be set via CGI request, so please set it manually via the Web interface (Streaming tab) before using the camera.
- The El.MO and Dynacolor cameras (except Dynacolor HD WDR IP cameras) have specific resolution settings. The camera may support different resolutions for different codecs. For example, cameras of the NH-series support the following resolutions (maximal framerate is described in brackets):
    - MJPEG video codec - 1280x960(12.5 fps), 640x480(25 fps);
    - MPEG4 video codec - 640x480(25 fps), 320x240(12.5 fps), 352x288(12.5 fps), 176x144(12.5 fps).
- When you try to set an unsupported resolution, the most suitable resolution will be applied. Please refer to the camera settings (Streaming -> Video Format page, "Video Resolution" section) for detailed information about the camera's supported resolutions.
- The El.MO and Dynacolor cameras support only one or two frame rates (for example, 25 or 12.5 for PAL cameras of the NH-series). Other frame rates may be applied using the "Frame Skip" setting. Usually, the camera supports skipping at 5, 10, and 15 frames internally. If the camera supports 25 fps for a specified resolution, the camera will send a stream with 5, 2.5, and 1.67 fps for appropriate frame skip settings. So, the real framerate may be greater than that applied in VMS when you try to set an unsupported framerate. The most suitable value will be used.
- The video stream for cameras of the NH series has an unsteady frame rate for VGA resolution with the highest frame rate and quality settings (for both MPEG-4 and MJPEG codecs). The real frame rate changes between 18 and 30 values, but the average frame rate value is lower by 1-2 fps than required. This is a camera issue.
- Dynacolor and El.MO cameras apply each request for stream settings, changing approximately 20 seconds. This is a camera feature.
- The IP PTZ cameras have the following issues:

- The camera always returns a 503 HTTP error code for each IO command—this is a firmware problem. The IO module is temporarily disabled for cameras in the IP PTZ series.
- The camera inverts the "focus" command: it performs the "focus near" action for the "focus far" command and vice versa. This is a firmware problem.
- The camera does not restore the connection after unplugging the network cable. After the connection is restored, the camera should be rebooted manually.

- The HD WDR IP cameras have the following issues:
  - The camera sends MPEG-4 frames at a greater frame rate than required. For example, the camera can send up to 16 frames per second for maximal resolution (1280x960) instead of 12.5
  - The camera does not support Frame Skipping for maximal resolution (1280x960) for the H.264 codec. This is a camera feature. As a result, only one framerate (maximal, 25 or 30 fps) will be available for maximal resolution for the H.264 codec.
- The V-series cameras have a problem with the H.264 codec. After applying 100% quality for the H. 264 codec, the camera sends an incorrect video stream (the VLC player doesn't play it, and VMS shows a lot of frame-skipping messages). This issue occurs occasionally.
- The 5 Megapixel 360∞ Fisheye cameras support only fish-eye views. At the moment, they do not support selecting another viewing area.
- Multiple streaming limitations:
  - Starting from DVMS 6.1.1, multiple streaming features are supported for Full-HD Quad Stream cameras. Other cameras will be used as single-stream devices.
  - Recording and Live streams support H.264 encoding only. Remote stream supports both MJPEG and H.264 encodings.
  - Resolutions on different streams depend on each other. The following rule applies for resolution: the resolution of a Live stream cannot be greater than the resolution of a Recording stream. The same rule applies to Remote and Live streams. Please refer to the device manual or Web Interface to learn about these resolution limitations.

9.6.3.6 GatewayIPCapture installation and usage

The driver uses TCP/IP protocols for video receiving and parameter setting/retrieving in all compression modes. The default Gateway TCP port is 9000. If there is a firewall between VMS and the servers, this port must be opened.

A separate profile (not service) should be used for the Gateway driver. This can be configured in the GatewayIPCapture.xml file (Profile name). Otherwise, the count of used cameras can be incorrect.

9.6.3.7 HTTPIPCapture installation and usage

The driver uses the HTTP protocol to receive video streams from IP devices.

The driver expects the HTTP URI to be added to the device and placed in the "IP Address" field.

The required port may be specified separately in the "Port" field or in the HTTP URI. The HTTP URI port has a higher priority; if it is set, the DVMS port field will be ignored.

The stream URI requirements: The HTTP URI should be specified in full format, e.g., http://192.168.1.70:8080/video

Stream URI may be checked over third-party players, like VLC.

9.6.3.7.1 Limitations

- If the camera requires Basic HTTP authorization, the correct user name and password should be set; otherwise, there will be no video.

9.6.3.8 IPCameraCapture installation and usage

The driver uses RTSP/RTP/UDP/IP protocols for video and audio receiving in all compression modes.

HTTP/HTTPS protocol is used for parameter setting/retrieving and for PTZ functionality.

If there is a firewall between DVMS and the UDP IP devices, the following RTSP/UDP/HTTP/HTTPS ports must be opened:

- **HTTP**: default port is 80,
- **HTTPS**: default port is 443 (if enabled on the camera)
- **RTSP**: port 554,
- **UDP**: two sequential ports per audio/video stream are needed in a port range of 3556 to 4556.

9.6.3.8.1 Limitations

- UDP cameras sometimes do not process the PTZ stop command. To avoid this issue, the driver sends four stops.
- There are no iris settings for UDP/Amano/GANZ cameras. Firmware for UDP/Amano/GANZ cameras allows for changes in video standards, but cameras support only one of them (in general).
- 2Mpx cameras have a problem with MJPEG 100% quality - it stops streaming. 2Mpx cameras have different resolutions for MPEG4 codec (no 2Mpx).
- The IPE1100 M cameras have a maximum resolution setting (SETUP > Video & Audio > Video-In > Video Resolution parameter). This setting determines the list of available resolutions—e.g., the minimum resolution for 2Mpx will be VGA, and smaller resolutions will not be available.
- Enabling multiple streaming or multicast streaming features may decrease device performance. Therefore, both video streams will be sent at lower frame rates than currently applied.

- Devices of the IPE series send all streams with unstable frame rates if at least one of these streams is configured for MJPEG encoding. The frame rate becomes stable when the MJPEG stream is stopped. This is a feature of IPE series devices.
- Devices of IPN/IPX may apply video settings for a long period (70-90 seconds) if the multiple streaming feature is enabled. Please wait for the video stream to start before changing the video settings again.
- The IPN/IPX series devices have the following note in the Web Interface: "If a vertical resolution of 1080P is selected, other video streams cannot support a horizontal resolution higher than 1088." The camera behavior may be unexpected if the user tries to apply 1080p resolution for both video streams.
- Multicast capture limitations:
    - Multicast capture can be enabled via an XML configuration file using the StreamingMode option. Refreshing device settings will be enough to activate the changed StreamingMode option.
    - The driver instance can be configured as a primary or listener. The primary instance can change IP device settings and use additional functionality. Listener instances can receive video and audio streams by multicast and use digital I/O functionality.
    - The user should guarantee that only one recorder will change the settings of UDP IP devices. Other recorders that use this device should be in listener mode.
    - The multicast stream uses the same settings until it is restarted, even if stream settings are changed. Changing stream status (starting or stopping) requires 6-10 seconds. So, applying stream settings will take 30-60 seconds.
    - Please note that the driver uses only the default adapter for multicast streaming. So, multicast may not work correctly if your PC has more than one network card. Please contact Customer Support if you encounter a problem with multicast configuration.

Time synchronization functionality limitations:

- The changing of time zone will not affect the system time until reboot. So, to apply the correct time, the driver may reboot the camera after the time zone setting change.
- The Daylight Saving Time option (DST) is always enabled for cameras of the IPN/IPX series. This is a limitation of the camera's firmware.

Edge Storage functionality limitations:

- The Edge storage functionality is supported for IPX/IPN series cameras only, starting from firmware version 1.8.0.4
- The recording on the SD card should be configured manually on the camera's web interface before using this functionality in the VMS.

- The IPN/IPX cameras allow recording on SD card only an H.264 stream. Changing the encoding of the profile used for recording will turn off the storage of video material on SD card.
- The IPN/IPX cameras allow searching recorded materials by events only. This is a limitation of the camera's SDK. Because of this limitation, video recorded using Continuous Recording settings cannot be handled.
- The maximal event duration is 65 seconds (5 seconds pre-recording and 60 seconds post-recording). There is no possibility to configure recording of longer time intervals.

9.6.3.9 LGEIPCapture installation and usage

The driver uses RTSP/RTP/UDP/IP protocols to receive video streams and input states in all compression modes. HTTP protocol is used for parameter setting/retrieving.

If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default ports are 80 and 81,
- **RTSP**: port 554,
- **UDP**: Two sequential ports per video stream and two sequential ports per metadata stream (input states) are needed in a port range of 3556 to 4556.

For example, if there are 2 LG Electronics IP cameras in a DVMS, ports 3556, 3557, 3558, 3559, 3560, 3561, 3562, and 3563 will be used. If a port is not free, it will be skipped.

9.6.3.9.1 Limitations

A few LG Electronics devices do not allow the device model to be received. For these cameras, the model name will be displayed as "LG Electronics IP camera".

The LDW2010F-N camera sends a QCIF stream with 160x112 resolution instead of 176x112 resolution. This is a camera feature.

LG Electronics devices' digital outputs have one specific feature: they have a duration option and cannot be closed for a long time. The device automatically opens the output when the duration period has expired.

The SOAP API doesn't support commands for switching focus and iris modes between auto and manual values. So, if the user wants to use iris/focus adjustment in DVMS, he should change this value via the Web interface to manual.

9.6.3.10 NewActiIPCapture installation and usage

In all compression modes, the driver uses RTSP/RTP/UDP/IP protocols for video receiving. The HTTP protocol is used for parameter setting/retrieval.

If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,

- **RTSP**: port 7070,
- **UDP**: two sequential ports per video stream are needed in a port range of 3556 to 5556.

NewActiIPCapture.xml file is used to configure:

1. Driver behavior:
    - Unicast
    - Multicast:Primary
    - Multicast:Listener
2. The camera's stream mode and mounting type (for fisheye cameras) accept de-warping on the camera.

Possible values for stream modes: SINGLE, DUAL, EPTZ, MD_PRESET, FISHEYE_VIEW

Possible values for mounting types: WALL, CEILING

The first PTZ channel ID for ACTi video servers:
General and IP device-specific configuration is available
E.g:

```
<Device address="192.168.1.75" port="80">
<FirstPTZChannelID>2</FirstPTZChannelID>
</Device>
```

For device 192.168.1.75:80, the first PTZ channel ID will be 2, the next one (for a multichannel device) will be 3, etc.

9.6.3.10.1 Limitations

- ACTi TCM-5311 can stop sending the correct stream when abruptly changing the backlight.
- ACTi MPEG4 cameras need a delay between setting parameters and starting stream (about 3 sec).
- ACTi CAM-6510 doesn't work correctly on 1 fps, so this value is not available for this camera. Acti CAM-6510 camera does not support quality changing, so quality for all values are the same.
- ACTi cameras have different frame rates for different compression formats. Settings are converted automatically to the nearest correct value.
- ACTi E96, B54, B55, and B56 cameras do not support de-warping on camera, so XML configuration has no effect on those models.
- ACD video servers work only with one PTZ camera connected to each channel, with a camera ID = 1. For example, ACD2100 works only with one camera, and ACD2200—with four cameras. ACD multichannel devices have different RS485 ports for PTZ camera connections, and all camera IDs must be equal to 1.
- The real frame rate for ACTi cameras can be different from the settings. It depends on the camera settings (lens compensation and shutter speed) and the level of illuminance.

- Video cameras do not support I/O functionality. They work in PAL, but the factory default is NTSC. After applying the factory default, the camera does not work.
- SED2100 works with ACTi libraries. SED2100 needs to save reboot after every changing of parameters (it takes 30-60sec)
- Preset names are stored in XML file (no camera's preset management)
- For KCM, the K2 fish eye camera can be used in two video stream modes: SINGLE and EPTZ. Stream mode is detected during camera subscribing to DVMS, then driver will keep this mode. To change stream mode, the camera should be removed from DVMS, stream mode should be changed over the camera's web interface, and then the camera can be subscribed. The driver will set it automatically for all other KCM and TCM series in SINGLE video stream mode.
- ACTi driver uses constant bitrate settings that are scaled from the corresponding VMS quality value:
    - CAM values: 256K, 384K, 500K, 750K, 1M, 1.5M, 2M, 2.5M, 3M
    - ACM values: 28K, 56K, 128K, 256K, 384K, 500K, 750K, 1M, 1.2M, 1.5M, 2M, 2.5M, 3M, UNLIMITED
    - TCM/KCM values: 28K, 56K, 128K, 256K, 384K, 500K, 750K, 1M, 1.2M, 1.5M, 2M, 2.5M, 3M, 3.5M, 4M, 4.5M, 5M, 5.5M, 6M, UNLIMITED
- So, VMS quality 50% will be scaled to a 1Mbit/sec bitrate value. The correct DVMS quality should be set to fit the required network bandwidth.
- ACTi video servers have no internal PTZ protocol; they re-send PTZ commands to the camera's COM port in transparent mode. Currently, only the PelcoD protocol is implemented. If an analog camera connected to an ACTi video server cannot work with PelcoD, the driver cannot be used to control the camera.
- Not all stream modes are supported by ACTi fish-eye models. E.g., ACTi I51 supports only DUAL (Panorama), FISH_EYE, and EPTZ stream modes. Other settings will have no effect and will be used in stream mode, which is set on the camera.
- Stream mode and mounting type should be set before the camera is added to DVMS. To change those values, the user should remove the camera from DVMS, make changes in the configuration file, and add the camera to DVMS again.
- Multiple streaming for the fish-eye camera is supported only for those stream modes:
    - DUAL - 2 streams
    - MD_PRESET - 2 streams in WALL mounting type, 3 in CEILING
- Digital PTZ is working for the fisheye camera only in EPTZ stream mode.
- If resolution or stream mode was changed, presets for fisheye camera becomes invalid, need to remove them from DVMS and re-assign again.

- MPEG4 is off for DUAL stream mode because it is available only for 1st stream
- 6VGA and 4VGA stream modes are not supported.
- The Stream mode settings in the NewActiIPCapture.xml file are only for the fish-eye cameras. Other camera's stream mode settings will be received from the camera when it is added to DVMS. If camera has DUAL stream mode setting - multiple streaming will be active, if SINGLE - not.
- In DUAL stream mode, the frame rate in stream 1 has to be higher or equal to it in stream 2. Otherwise, the frame rate in stream one is limited to the stream two frame rate. For example, the frame rate settings in stream one and stream 2 are 30 and 25. The actual frame rate in stream 1 is 25
- KCM/TCM cameras cannot enable privacy masks on the second stream. So, privacy masks are enabled only for single-stream modes (the camera should have a single-stream mode before adding it to DVMS). KCM/TCM cameras have a general issue related to privacy masks and resolutions higher or equal to 1920x1080—the privacy mask can be set only on the left part of the screen (ACTi limitation).
- ACTi ACM cameras have an issue with privacy mask settings. The privacy mask position is correct only for maximum resolution; for smaller resolutions, the privacy mask position can be different from the settings.
- The ACTi ACM series can return Motion Detection capability, but there is no configurable MD on the camera's web page. For those models, "Recorder and camera hardware" MD cannot be used.
- Multicast is not enabled for ACTi CAM models. All those models work with Unicast only. Those cameras cannot be used in several DVMS instances!
- **Unicast mode**: The driver will change the camera settings according to the DVMS settings and receive audio and video data from the camera using a unicast connection.
- **Multicast:Primary**: The driver will change the camera settings according to the DVMS settings and receive audio and video data from the camera using a multicast connection.
- **Multicast:Listener**: driver will not change camera settings, just receive audio and video data from camera using multicast connection.
- If the camera is to be used in several DVMS instances, one DVMS should be set to Multicast:Primary, and others should be Multicast:Listener.
- Several Multicast:Primary configurations or Multicast:Primary and Unicast configurations are not allowed; in other cases, the camera should be overloaded with continuous concurrent settings changes.
- Edge storage is supported only for DEBI series starting from firmware 6.07.23 and higher.
- The camera is synchronized to UTC (GMT +00) to avoid local time issues.
- RTP over RTSP mode will not work for the following camera series. These cameras do not support this mode or have not been fully tested:
    - VIDO AMU-xxx

- ACTI KCM-xxx
- ACTI ACM-xxx

9.6.3.11 NewArecontIPCapture installation and usage

The H.264 compression mode driver uses RTSP/RTP/UDP/IP protocols for video reception at common frame rates. The HTTP protocol is used for parameter setting/retrieval, MJPEG/H.264 stream receiving in case of camera slow frame rates, and MJPEG continuous receiving.

If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: default port is 554,
- **UDP**: two sequential ports per video stream are needed in a port range of 3554 to 4556.

The driver may be configured using an XML configuration file to set the following parameters:

- Indoor lighting compensation value

Channel specific parameters:

- MaxFrameRate - max frame rate for full resolution
- MaxFrameRateHalf - max frame rate for half resolution
- RTP over RTSP transport protocol
- RTP block size (if required by the specific router)
- BitrateMode (CBR, VBR, or Auto - the last one tells the driver to skip quality change on camera)
- BitrateMin (minimum bitrate for CBR)
- BirateMax (maximum bitrate for CBR)
- KeyFrameIntervalMs (Intra frame interval in ms, 0 - all intras)
- IndoorLightFrequency - light frequency

9.6.3.11.1 Limitations

The maximum frame rate value is calculated using the Arecont "secret" formula. The real frame rate can be lower than specified—it depends on network conditions.

Some picture resolutions can differ from settings, e.g., 1600x1200 will be 1600x1184. This happens because the Arecont camera resolution must be divisible by 32 for full and 64 for half mode.

The Arecont max resolution is set on the camera. VMS uses it and half of it. To change the maximum resolution, you need to change it on camera and then add a camera to the VMS.

Arecont cameras have only two full picture resolutions—the max sensor resolution and half of it. The other resolutions are cropped from the max and are not used in the driver.

AV8185 and AV8180 have no IO (information in their documentation is incorrect).

AV3135 has two sensors—day and night. Both work at specific resolutions. VMS shows resolutions for day mode; real frame resolution can differ from settings.

Arecont cameras can dynamically change picture resolution. Actual frame resolution can differ from settings.

DVMS supports only 30 fps max, so all Arecont cameras will have this limitation (even if they support more than 30 fps).

Arecont 4ch cameras can have issues when H.264 + MJPEG is used. It is better to use one compression format for all channels.

9.6.3.12 NewAxisIPCapture installation and usage

The driver uses RTSP/HTTP/HTTPS/RTP/UDP/IP protocols to receive audio and video multicast streams and H.264/MPEG-4 compressed unicast streams. The HTTP protocol is also used for parameter setting/retrieving and audio stream and JPEG video stream receiving in unicast mode.

If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP/HTTPS ports must be opened:

- **HTTP**: The default port is 80,
- **HTTPS**: The default port is 443,
- **RTSP**: The default port is 554,
- **UDP**: Two sequential ports per video stream are needed in the port range 3556 to 4556. If Multicast mode is enabled, two additional sequential ports per audio/video stream should be opened according to the device configuration.

For example, if there are 4 IP cameras in a DVMS, ports 3556, 3557, 3558, 3559, 3560, 3561, 3562, and 3563 will be used. If a port is not free, it will be skipped. The 1024-1025 and 1028-1029 ports should also be opened in addition to the 3556-4556 range if the device is used in Multicast mode and it is configured to use 1024 port for the audio stream and 1028 port for a video stream.

The driver may be configured using an XML configuration file to enable the following functionality if the Axis IP device supports this functionality:

- Multicast audio/video capture
- Axis Views

If you use Axis LPR and have several network adapters, you need to set the correct IP address (addresses) in the configuration file.

9.6.3.12.1 Limitations

For HTTPS (TLS) support, you need to generate and install the CA certificate on the PC certificate store and generate a certificate for each camera using a guide from Axis ("HowTo. AXIS Device Manager. HTTPS certificate management").

The AXIS driver doesn't support the "PTZ Control Queue" option. If this option is enabled, the AXIS device will be detected as non-PTZ.

Privacy zones may be shifted by a few pixels from the rectangle applied in DVMS. The shift depends on image rotation and mirror settings (shifted to the right for a normal image). This is a camera firmware feature.

If the "Aspect ratio correction" option is enabled on the Axis device, the real image resolution may differ from that in VMS. For example, the real resolution will be 768x576 for the 704x576 setting or 192x144 for the 176x144 setting. Please disable this option if your system does not require aspect ratio correction.

If the network connection is lost, Axis cameras of the P33 Series send a few seconds of video and then don't send anything for 5-10 seconds after the connection is recovered. This behavior is caused by the camera's DHCP implementation. Please use a static IP address to avoid this behavior.

The IP device should be configured manually in the following way in case you want to use the Edge storage feature:

1. It is not possible to receive Coordinated Universal Time (UTC) from the camera, so the time zone should be set to "GMT+0:00." The daylight saving time option should also be switched off.
2. Camera events should be configured for video recording according to user preferences. The event duration should be at least 3 seconds.
3. It is recommended that automatic SD cleaning be used to have the required space for video recordings.

The video recordings on the camera's storage may contain gaps of up to 10-15 seconds. This is a camera feature, so please do not use maximal settings for video recording to avoid such gaps.

Axis multi-view cameras (e.g., M3007) can be configured to receive video from a specific stream using the XML configuration file. Different views have different capabilities, so the camera should be re-subscribed to VMS to take changed StreamConfiguration options into use.

Privacy zones functionality can be used if the recording channel uses the "Overview" fish-eye view.

Other views don't support privacy masking functionality because these views are parts of the "Overview" view.

9.6.3.12.2 Multicast capture limitations

- Axis IP devices support multicast capture with Stream Profiles feature support (devices with firmware versions 5.0 or higher) and can be configured via XML file. Older devices will always use unicast streaming.
- The Stream Profiles support may be checked via the Web interface: the section "Video & Audio >> Stream Profiles" should be available. The user may use any existing profile for multicast streaming configuration or allow the system to create a new one. Please see the "MulticastProfiles" section in the XML configuration file for more details.

- Please do not use the same stream profile for different streams - it may cause conflicts during the video settings application.
- Multicast capture can be enabled via XML configuration file using the StreamingMode option. This option is read on stream startup, so a refresh of device settings will be enough to take the changed StreamingMode option into use. Please note that DVMS has optimization for channel restarting since version 7.4.1, so in this case, it will be required to change one of the video options for each camera to restart the stream.
- The driver instance can be configured to be used as a Primary or Listener. The primary instance is able to change IP device settings and use additional functionality. Listener instances are able to receive video streams and audio streams by multicast and allow the use of digital I/O functionality.
- The Listener recorder will not change any configuration on the camera side. For example, if no configured profile is available on camera, it will not be created, and the driver will not be able to receive the video. The camera should be added to the Primary recorder before using it in the Listener configuration.
- The additional streams (Live and Remote) are active in case they are opened in clients only. So, to use updated Multiple Streaming settings, you must start (or keep open) these streams for the Primary recorder after the stream settings have been changed in DVMS. Otherwise, the camera cannot use the latest stream settings.
- Motion Detection and Change option in alarm features (CFiA/CRiA) cannot be used in multicast mode because of timeout issues specified above.
- Users should guarantee that only one recorder will change the settings of Axis IP devices. Other recorders which use this camera should be in listener mode.
- The Axis cameras may not support more than one multicast stream in case if camera is configured to use specific port for multicasting (non-zero "Video port" setting in "System Options >> Network >> RTP" group). The camera will return RTSP 461 "Unsupported transport" error for stream start attempt if one multicast stream is already started. Please configure automatic port selection (set "Video port" setting to 0) to avoid this behavior.
- It is recommended to specify IP address of the network adapter through which camera is connected to receive multicast streaming correctly in case if more than one network adapter is available.

Each Unicode character is stored as symbol code (%u0227, for example) and required 6 bytes for it. So, length of Unicode preposition name may be limited by 11 symbols instead of 64.

Axis P1428-E camera supports only 2 4K (3840x2160) streams at the same time. Please avoid using of 4K resolution for all streams in multiple streaming feature and minimize amount of rules which use 4K resolution for recording to SD card.

The driver allows to switch control mode between "Active" and "Passive" since version 2.5.5.0. In "Passive" mode the driver will not change any video-related parameters, so in this mode the following functionality will not work:

- Privacy zones configuring

- Change options in alarm (i.e. CFiA/CRiA features)

If the camera accepts video parameters via RTSP or HTTP stream URI, the driver will start stream without them. In other words, the stream settings applied via Web-interface will be used.

Applying of privacy masks may take long time (creation of every zone may take up to one second), so it may slow down stream startup. To speed up video subscribing the driver applies privacy masks after video stream startup.

The driver versions before 2.5.7.0 has an issue with privacy masks creation for multiple-sensor devices. The driver always used template for first channel, so privacy zones might displayed incorrectly (for example, displayed on wrong channel).

Please remove privacy zones manually via Web-interface or just reset device to factory defaults in case if you'll meet such behavior. After this driver will create privacy masks using correct templates on next video channel start.

The Axis Zipstream technology (<http://www.axis.com/global/en/technologies/zipstream)> may be used with the driver. The driver has no option for configuring of this feature, so it should be enabled manually via Web-interface.

Please note that:

- The changes of video settings (including Axis Zipstream options) made via Web-interface will affect to the video streams started after the changes. So, it will be required to restart video stream to take the updated settings into use.
- The VMS software required to receive one intra-frame per second to perform post-processing of video stream (VCA, motion detection, etc.). Using of "Dynamic GOP" option may cause a problems with post-processing, so using of this option is not recommended.

The Windows XP is not supported since driver version 2.5.0.0

The new Axis cameras (firmware 5.50 and newer) uses new API for Motion Detection that currently does not supported by the driver. The VMD feature will be disabled for these cameras until new API support will be added to the driver.

Native Axis Licence plate recognition application uses HTTP POST requests to send ANPR data. So, the driver starts the HTTP server to receive those HTTP POST messages. If the PC has more than one network adapter, you need to set correct IP address of the network adapter that is used to communicate with camera to driver's XML file, `AxisANPR/NetworkInterface` parameter. In other cases, the camera will not send ANPR data to the PC. If Failover is used, it is required to set both addresses - main server and failover.

Axis changed date.cgi API to time.cgi API to set / get time from / to camera. But this new time.cgi API works slowly, so the driver receive time from camera with some delay. Also, `time.cgi` still does not have miliseconds, so this time sync is not precise. The Driver tries to calculate time difference between camera and PC with Recorder, but this calcultion is not presice enough. This calculation can be switched off in config file in case if time is synced outside of VMS.

Axis 360 cameras can do the de-warping internally and there is a possibility to use de-warped views as:

- streams (recording, live or remote), that can be configured in the ViewAreaConfiguration section
- channels, that can be configured in the EnableViewModes section

9.6.3.13 NewBoschIPCapture installation and usage

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP or HTTPS ports must be opened:

- HTTP: default port is 80,
- HTTPS: default port is 443,
- RTSP: default port is 554,
- UDP: two sequential ports in a port range from 3556 to 4556 are required per video/audio stream.

For example, if there are 4 IP cameras in a DVMS, ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

For MPEG-4 video stream-receiving driver uses the Bosch RCP+ SDK library. It opens random UDP ports for video data receiving. The driver may be configured using an XML configuration file to set the following parameters for the Bosch IP devices:

- PTZ protocol (PelcoD, OSRD, BiCom)
- Fish-eye video channel (only one can be used)
- Jpeg stream (Recording, Live or Remote, default Remote)
- Edge storage functionality support
- Time sync (enabled / disabled)
- Control mode (active/passive)
- Transport
- Key frame interval
- Video loss check (enabled / disabled)

9.6.3.13.1 Limitations

All Bosch devices should have a user and password set. In other cases, drivers will not recognize the camera (the password shouldn't be empty)

The System Manager will be able to update the driver to 1.3.0.0 from older versions with subscribed Bosch cameras starting from VMS 7.0 version. For older VMS versions, cameras should be removed from DVMS and added again after the driver updates.

If the camera was added without audio channels, to enable them, the camera should also be removed and added to DVMS again.

The driver does not remove or change the old BoschIPCapture driver, but it uses rcpp.dll like the old one.

So, to install the driver, there should be no connected Bosch cameras. Otherwise, the driver installation will fail.

For NTSC cameras connected to the Video-Jet servers series for the MPEG-4 codec, the maximum resolution is 352x240 (CIF). The D1 resolution does not work, so the CIF resolution will be shown instead of D1.

A combination of NTSC and PAL cameras connected to one Video Jet server is prohibited.

The actual framerate for the MJPEG video channel may be lower than the values specified in the settings.

The quality setting in the VMS uses the bitrate value on the camera or video server. So, real picture quality may be the same for different values (if the frame can pass through specified bitrates).

Bosch PTZ cameras use OSRD protocol for controlling the camera. This protocol does not allow a change of iris/focus speed. So, irising and focusing can be performed with a predefined speed value. The speed values can be set via Web-interface. These settings for VG4 AutoDome camera may be found here: Settings > Advanced Mode > Camera > Lens > Setting Group 1

OSRD protocol does not allow you to delete prepositions. Also VG4 camera doesn't allow rewrite existing preposition without confirmation. The camera will show "Overwrite current scene?" question as OSD menu with [Yes] and [No] buttons.

Focus/Iris changing is used for selection confirmation. The driver sends Iris command after preposition saving to avoid a user from manual confirmation of preposition rewriting. This algorithm has an issue: if the preposition slot is empty (not stored yet), you will see Iris changing text.

Bosch video servers pass PTZ commands to cameras, connected through serial port. There is no way to configure the camera's identifier via standard server options. So, connected cameras should be correctly configured (camera's hardware settings) for enabling PTZ control:

- PTZ protocol should be Pelco-D
- PTZ camera identifier should be the same as the video channel's number. For example, for a camera connected to the second video input, the camera ID should be set to 2.

Other serial port settings should be equal to the server's (baud rate, parity bit, stop bit, etc.).

Bosch video servers have no internal PTZ functionality. It only passes commands to their serial ports with connected cameras. So, the driver cannot detect the capability connected to the serial port camera and whether it is PTZ.

All server video channels will be shown as PTZ because of this feature.

NBC255 and NVC255 have VGA and QVGA resolutions. DVMS will show D1 and CIF instead. (Cannot detect those models from device properties)

Multiple streaming is done according to the encoders' capabilities.

Each video channel has two encoders with the number of supported resolutions, so not all resolutions are available for Recording and Live streams.

Some resolutions are supported only by special combinations on the first and second encoders, so the Live stream resolution can differ from the settings if it cannot be set with the current Recording resolution.

The remote stream is MJPEG; it has all available resolutions.

9.6.3.13.1.1 Streaming limitation

- To change H.264 resolution and framerate for secondary stream is it required to disable the "Copy Stream 1" mode in the Web Interface (Settings -> Advanced mode -> Camera -> Encoder Streams -> Stream 2 -> Property will NOT be in the "Copy Stream 1" state for the "Stream 2");
- It is not possible to apply several resolutions (each video channel has two encoders with different sets of supported resolutions);
- Remote stream is MJPEG that has all available resolutions.
- MJPEG in multiple streaming mode does not work for old series with firmware 4.x
- Motion detection for PTZ cameras should be configured on camera's Web page after each camera movement (Bosch limitation).
- Privacy zones for PTZ cameras are not supported.
- Cameras that have COM port will be shown as PTZ in DVMS. They can be connected to PTZ platform and PTZ will work.
- Driver synchronizes PC's time with camera using UTC (GMT+00:00) time for Edge-Storage functionality. Edge-Storage will not work correctly if time will be changed to another one.
- Edge-Storage functionality works only for network loss situations between camera and VMS.

If VMS was restarted or driver was closed - VMS will not receive recorded video from camera.

Also, recording should be configured on camera to use Edge-Storage functionality in VMS.

9.6.3.13.1.2 Multicast capture limitations

- The driver instance can be configured to be used as Active or Passive. Active instance is able to change IP device settings and use additional functionality. Passive instances are able to receive video streams and audio stream by multicast and allows to use digital I/O functionality.
- The Passive will not change following camera settings:
    - Codec
    - Quality

- Resolution
- Framerate

The camera should be added to Active recorder before using in Passive configuration.

User should guarantee that only one recorder will change settings of the camera. Other recorders which use this camera should be in Passive mode.

It is required to specify IP address of the network adapter through which camera is connected to receive multicast streaming correctly in case if more than one network adapter is available. The network adapter marked in Windows as default will be used if no option configured. For audio channel network adapter (in case of several network adapter used in PC) should be set in XML file, dynamic UI is applied only for video channel.

Time Synchronization is disabled for the Passive and Edge Storage may not work properly.

Use should guarantee time synchronization for PC with Active mode recorder and PC with Passive mode recorder.

Old Bosch series with firmware 4.x have the following limitation:

HTTPS mode does not work

MJPEG in multicast mode does not work (only JPEG requests over HTTP)

Privacy zones for firmware 6.22 are not supported.

Old Bosch series (like Gen4) do "auto bounding" sometimes. During this process stream from camera is not fluent.

In Passive mode old cameras with MPEG4 support should be set to correct compression format or "No signal" will be shown.

Edge storage recording should be set to 1st edge storage stream on camera's Web-interface.

The Bosch IP devices may return no information about audio intervals recorded on device's storage via RCP+ requests (by num = 90 + channel ID). As result Audio Edge functionality will not work correctly. The issue was reported to Bosch technicians (at 20/Nov/2019), but there is no solution yet.

Not all Bosch cameras can detect Motion, so it should be cheked on camera's web page if it supports Motion Detection or not

9.6.3.13.1.3 To use camera in secured mode

1. Install certificate on camera and PC with Recorder
2. Set RTP over HTTP streaming mode in camera settings in System Manager;
3. Set correct camera credentials (for sending audio to camera, if it is not needed - any credentials can be used, authentication will be done using certificate); audio to camera is not secured, so it needs correct credentials to work.

Bosch camera with H.264 and H.265 support should be set to required codec before adding to DVMS, because some cameras have different list of supported resolutions / framerates for each codec.

Camera supported resolutions depends from currently set codec (H.264 / H.265). So, camera will be added with currently selected codec, DVMS will not change it during camera add.

Video loss check is used only for encoders with analog cameras to detect that camera is working or not. It should not be used for other Bosch devices.

If audio codec was changed, need to format SD card, because driver will try to receive audio using current settings. If AAC is set to camera but recording was done for G711, edge audio data will not be received correctly.

If multiple streaming is used, all channels should have the same codec (H.264 or H.265), Bosch cameras can not stream both at the same time.

Bosch devices are not processing RTSP PAUSE command correctly (continue to send stream after that).

So, we use RTSP TEARDOWN to stop stream if no motion (when camera based MD is in use).

9.6.3.14 NewIQEyeIPCapture installation and usage

The driver uses RTSP/RTP/UDP/IP protocols for receiving H.264 compressed video and audio streams. HTTP protocol is used for parameters setting/retrieving and MJPEG stream continuous receiving.

If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: default port is 554,
- **UDP**: two sequential ports per audio/video stream are needed in a port range 3554 to 4556.

9.6.3.14.1 Limitations

IQEye cameras have one resolution and several cropped resolutions. Cropped resolutions do not used in driver. Driver use only down sample process to change picture size (size / 2, size / 4 and size / 8). Down sampling is enabled for cameras which support it (cameras IQ73xx, IQ04xx, IQD4xx, IQ54xx do not support it).

IQ712 camera has limitation for maximum fps for MJPEG - 15 fps.

IQEye cameras (except IQ73xx) have only one resolution for H264 ñ 640x480. Others can be used only for MJPEG.

H.264 codec supports only 5,10,15,30 frame rate values for all cameras. Other values used only for MJPEG, they will be scaled to listed above if H.264 codec will be active.

For IQA25S camera for MJPEG codec 2560x1920 and 1280x960 resolutions support maximum fps value 7, for 640x480 and 320x240 resolutions - only 10 fps max.

For IQA25S camera for JPEG codec resolution max /2 should work on 10 fps, but it works as is - max fps is 7, if specified higher - it set 5 or 4 fps, this is firmware issue.

The driver supports only G.711 audio stream receiving. AAC codec is not supported at the moment.

9.6.3.15 NewMobotixIPCapture installation and usage

In all compression modes the driver uses HTTP protocol for video receiving and for parameters setting/retieving.

If there is a firewall between DVMS and the cameras, the following ports must be opened: HTTP: default port is 80.

9.6.3.15.1 Limitations

Real FPS is limited with resolution settings (camera feature): greater resolutions have lower real fps values. For example, for 800x600 resolution maximal FPS is 9 for MJPEG codec.

The audio data may be received as part of MxPEG frame according to HTTP API documentation. So, audio stream is not available for MJPEG stream.

Stream mode changed from "fast" to manual - this setting can be changed in the web-interface.

9.6.3.16 NewPanasonicIPCapture installation and usage

In all compression modes, the driver uses RTSP/RTP/UDP protocols for video receiving, HTTP/HTTPS for parameters setting/retieving and for PTZ functionality.

In H.264/MPEG4 compression mode driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP protocol is used for parameters setting/retrieving and MJPEG stream continuous receiving.

If there is a firewall between DVMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: default port is 554,
- **UDP**: two sequential ports per video stream is needed in a port range 3556 to 4556.

NewPanasonicIPCapture.xml file is used to configure:

- Driver behaviour:
    - Unicast
    - Multicast:Primary
    - Multicast:Listener
- Transmission priority:
    - Bitrate
    - Framerate
    - Best effort
    - Advanced VBR
    - VBR

Minimum bitrate (for Best effort mode only)

9.6.3.17 NewSamsungIPCapture installation and usage

In all compression modes, the driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP/HTTPS protocols is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following ports must be opened:

- **HTTP**: default port is 80,
- **HTTPS**: default port is 443,
- **RTSP**: port 554,
- **UDP**: two sequential ports per video stream is needed in a port range 3556 to 4556.

For example: if there are 4 Samsung IP cameras in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

NewSamsungIPCapture.xml file is used for:

1. Configuration of driver behaviour:
    - Unicast
    - Multicast:Primary
    - Multicast:Listener
2. Video channels settings:
    - Video channel protocol (RTP over UDP, RTP over RTSP)
    - Bitrate mode (CBR/VBR)

9.6.3.17.1 Limitations

The capabilities of Samsung cameras cannot be retrieved for earlier firmware versions. All camera capabilities (excluding camera model name) for these cameras are hard-coded into the driver. So, all cameras should be updated to the latest firmware version.

Samsung cameras do not support configuring of inputs using CGI commands. Input configured as "disabled" by default. Please set input configuration to "NO" (i.e. "Normal Open") in the web-interface before adding the camera to the VMS.

Samsung camera frame rates may differ from settings (+/- 3 fps)

Driver stores preset names in XML file (Unicode names are supported)

The Samsung PTZ devices do not support speed parameter for "move to preset" command. So, move-to-preset speed will always be the same.

Samsung cameras apply each privacy zone configuration by separate request (add/remove). For modifying of zone position we should remove previous configuration and add new position by different requests. Each add/remove request is processed by the camera during 0.6 - 0.8 second. So, updating of positions of 10 privacy zones may takes up 16 seconds.

Time-zones for discontinued cameras may be set incorrectly during time synchronization.

The IP device should be configured by user manually in the following way in case is user want to use Edge storage feature:

1. There is no possibility to know is any file is writing at the moment. So please do not set Post-Alarm duration option to long timeouts - it may case skipping of this interval by the driver.
2. It is recommended to switch off "Record 1 fps forcibly" option. However, this option may be disabled for some settings of recorded profile (please refer to camera's manual for details). You can use separate video profile for recording video for HD and Full-HD cameras in this case.
3. It is recommended to use automatic SD cleaning to have a required space for video recordings.

Samsung cameras of 7000 series have an issue with recording of video data by event. The camera doesn't record anything however events configured for recording were signaled. The camera starts writing of video after rebooting or sometimes after resetting camera's settings to factory default. This is camera issue.

Old Samsung camera models like SNP-570 and SND-460 which uses STW SDK (STW cameras in next notes) with firmware version prior than 1.3.5 do not support retrieving camera properties. These cameras will be detected as "Samsung IP Camera" and will work in PAL video mode only.

Samsung STW cameras don't support "switch output off" command. Outputs will be switched off automatically by camera according to output settings in Web-interface.

Samsung STW cameras send MPEG-4 stream with 12.5 FPS for 10 and 15 FPS settings.

Samsung STW cameras decrease video quality value for MPEG-4 codec automatically during moving. This is camera feature (according to information from Samsung Techwin Support).

Frame rate has fluctuations in MPEG-4 compression mode for Samsung STW cameras. This caused by receiving RTP packets with incorrect sequence number. This is camera problem.

A video stream from Samsung STW cameras has FPS fluctuation if exposure settings for camera are invalid. To correct the settings, use the "Camera Setup" button on Live View page in Web-interface.

Samsung STW cameras take disabled state (returns HTTP responses with status code 500 for all requests) after the connection was lost for a short time and then recovered. The problem is reproduced with 30% probability for MJPEG codec only.

FPS settings are applied incorrectly for MJPEG video stream. This camera problem is actual for Samsung STW cameras with firmware version 1.3.5 or previous. So, real FPS for MJPEG video stream may be lower than required.

MJPEG stream stops after a long working time (for example, during overnight tests). This is because camera returns HTTP responses with status code 500 for all requests. In this case camera should be rebooted manually. This issue is actual for Samsung STW cameras.

SNP-1000A camera sends MJPEG stream with 8-9 FPS for 10 FPS and D1 resolution settings. This is firmware problem.

SNP-1000A camera stops processing HTTP requests after losing and restoring network connection (for example, after "No signal" during 2 minutes). This is because camera returns HTTP responses with status code 403 for all requests. In this case camera should be rebooted manually.

SNP-1000A and SNC-550 cameras do not support MPEG-4 RTP services. Only MJPEG video stream is available for these cameras.

SNP-1000A camera pans between 0 degree and 350 degrees. Degree values between 351 and 359 are not available - this is camera feature.

SNP-1000A camera does not support continuous move commands. The driver implements emulation of continuous moving mechanism. This mechanism reduces to following issues:

- Camera moving will be discrete.
- MJPEG stream sometimes stops for a few second during camera moving with highest speed. Probably, camera firmware isn't able to process video stream and a lot of moving commands at the same time.
- Incorrect camera moving in bottom position when try moving down. The camera inverts vertical scale and moves up if command "move down" is received and camera passes through bottom position. But next" move down" command will not be inverted and camera will move to bottom position again.

Preposition storing does not work for SNP-1000A camera with current firmware version. Firmware update is required.

The cameras of 7002 series have limitation for number of active profiles. The number of active video streams will be limited by 2 if each of them will use 1024x768 or greater resolution. So, multiple streaming feature may not work correctly for these cameras.

The driver supports G.711 audio encoding only. So G.711 encoding should be selected manually via Web-interface if camera supports more than one audio encodings.

VMS doesn't support privacy zones for PTZ cameras. So, the privacy zone support will be detected if camera doesn't support pan/tilt movement.

Samsung devices with WR3.0 software platform version have an issue in SSL implementation which doesn't allow to use POST commands. As result privacy zones functionality cannot be used when HTTPS support is activated. Samsung promised to fix it in the next firmware release.

Samsung devices with WR3.0 software platform version send video stream with low frame-rate (for example, 2-3 instead of applied 20) in case if audio stream was subscribed before video stream. This behavior is caused by RTSP

module implementation on camera side. Please save camera settings again without any change to return the camera to normal streaming mode.

In case of using constant bitrate (CBR) settings for Samsung devices with profile support the VMS quality is converted to bitrate settings as a percentage using the following limits:

- 2Mbps - 15Mbps for resolution width 1600px and greater;
- 1024Kbps - 10Mbps for resolution width between 1024px and 1600px;
- 512Kbps - 5Mbps for resolution width between 640px and 1024px;
- 64Kbps - 2Mbps for resolution width lower than 640px.

Correct VMS quality should be set to fit required network bandwidth. Other cameras use standard quality settings, not bitrate.

Bitrate can be limited to 6Mbps in case if video profile configured in Record mode to internal flash card (Edge Storage). The driver will not change GOP size value for video profiles configured in Record mode. To avoid this limitation please configure separate profile for internal recording material using camera's Web Interaface (in the "Video profile" section).

To use VBR with audio and multiple streaming camera should have firmaware 2.x or higher. With old firmware video for multiple streaming will not work.

Multicast is not enabled for Samsung models with old SDK (non-profile cameras). All those models work with Unicast only. Those cameras cannot be used in several VMS instances!

Unicast mode: The driver will change camera settings according to VMS settings and receive audio and video data from the camera using the unicast connection.

Multicast:Primary: The driver will change camera settings according to VMS settings and receive audio and video data from the camera using the multicast connection.

Multicast:Listener: The driver will not change the following camera settings:

- Quality
- Resolution
- Framerate

For Multicast:Listener the following options will be configured in the same way as Multicast:Primary:

- Multiple streaming option
- Video Codec for all streams

If the camera should be used in several VMS instances, one VMS should be set to Multicast:Primary, and others should be Multicast:Listener.

Several Multicast:Primary configurations or Multicast:Primary and Unicast configurations are not allowed, in other case camera should be overloaded with continious concurrent settings change.

Multicast address and port should be set for each profile on camera's Web interface, or multicast will not work. When multiple streaming is on, driver creates MLIVE profile - multicast address and port should be set to it too.

Area zoom and Centering functionality is available for Samsung cameras with SUN API 2.0 support.

Iris change is slow due to camera limitation). One click - one change.

When the camera is moved (or zoomed) auto iris and auto focus are applied.

To support Audio in Edge Feature VMS version 7.4.3.71 or higer is requred.

The new camera series (like QNO/QNV/QND-7010R samples) have limitations for using of 2 megapixel and greater resolutions for H.264 streams:

- Over 2MP resolutions (2592x1520 / 2560x1440 / 2304x1296) The maximal frame-rate will be divided between amount of active streams:
    - 20 fps / 2 streams = 10 fps per stream;
    - 20 fps / 3 streams = 6 fps per stream.
- One over 2MP stream + 2MP streams:
    - 15 fps per stream for dual streaming configurations (example: 2592x1520 @ 20fps + 1920x1080 @ 20fps)
    - 10 fps per stream for triple streaming configurations (example: 2592x1520 @ 20 fps + 1920x1080 @ 20 fps + 1920x1080 @ 20 fps)
- 2MP (1920x1080) streams only:
    - No limitation for 2 streams (20 fps per stream)
    - 15 fps per stream for 3 streams

Changing option by alarm (CCFiA/CCRiA) functionality is available for devices which allows to change options faster than 2 seconds. The devices released before year 2015 do not support this feature.

The Windows XP is not supported since driver version 2.2.18.1

9.6.3.18 NewSiquraIPCapture installation and usage

In all compression modes the driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP protocol is used for parameters setting/retrieving and for PTZ functionality.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,

- **RTSP**: default port is port 554,
- **UDP**: two sequential ports per video stream is needed in a port range 3556 to 4556.

For example: if there are 4 Siqura codecs in a DVMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

9.6.3.18.1 Limitations

H.264 decoder may sometimes fail to decode the received picture frame generating an error in the DVR log file.

Sometimes an analog dome-camera does not process PTZ commands. For example, dome camera sometimes does not stop after controlling has ceased, or does not move after abrupt direction change. Moreover, another HTTP command with the same parameters will be ignored, until a HTTP command with different parameter is received. Probably, it is a feature of Siqura video-server.

MJPEG video from Siqura MD2x/HD2x cameras stops for a moment during live. It seems like one frame skips. The same behavior occurs in Web-interface. This is camera problem.

Siqura MD2x cameras with old hardware base do not support Output functionality. The driver cannot detect hardware information, so output will be shown in DVMS in any case.

Siqura devices do not support continuous Iris changing - this is firmware feature.

All preset commands described in MD2x/MD6x/HD2x/HD6x protocol (filename "NKF - Protocol Hotkey 20090805") as commands for access to special camera functionality will be disabled in PTZ module. So, supported preset count for Siqura PTZ cameras will be less than 256.

Live MJPEG Encoder on Siqura PTZ cameras work with lower priority than other encoders (MPEG-4 and H.264). So, real framerate values may be less than required for MJPEG HTTP channel, especially in low-light-level conditions.

Driver stores preposition names in XML file. Unicode preset names are supported since driver version 1.9.2.0

9.6.3.19 NewSonyIPCapture installation and usage

The driver uses the following protocols for video receiving:

- HTTP/HTTPS protocol is used for receiving MJPEG video and motion detection stream;
- RTP/UDP/IP protocols are used for receiving MPEG-4, H.264 video stream and audio stream;
- RTSP protocol is used for controlling of RTP stream for G5 (5-th generation) and newer devices;
- HTTP protocol is used for sending audio stream to camera.

HTTP/HTTPS protocol is also used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP/HTTPS ports must be opened:

- **HTTP**: default port is 80,

- **HTTPS**: default port is 443,
- **RTSP**: default port is 554,
- **UDP**: two sequential ports per video stream are needed in a port range 3556 to 4556.

For example: if there are 4 SONY IP cameras are configured for receiving MPEG-4 or H.264 video in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

The driver may be configured using XML configuration file to set the audio parameters for the SONY G5-G7 IP devices.

9.6.3.19.1 Limitations

- The SNC-DM160, SNC-DM110 and SNC-CM120 camera models support a Light Funnel function:
- The driver sets Light Funnel always to "auto" mode. When it gets active in low illumination, it increases the image sensitivity, but with 1280x960 resolution it switches automatically to a lower, 640x480 resolution.
- Activation/deactivation delay for light funnel is about 40 seconds.
- Light funnel does not work when one of the following is set:
    - The image size is one of the following:
        - JPEG - 960x720: MPEG4 - OFF
        - JPEG - 768x576: MPEG4 - OFF
        - JPEG cropping is on
        - SolidPTZ is on
        - Iris open is on.
- Please note that when Light Funnel is off, the max frame rate is 15 fps. For more details, please see the camera's user guide.
- With high picture resolutions, the frame rate may be lower than requested.

9.6.3.19.1.1 Analog Video-Out feature notes

- The driver disables Analog Video-Out feature for SONY G4 IP cameras (4-th generation). Enabling of this feature causes a limitation of supported codecs and resolutions (for example, SCN-CS20 camera will support only 640x480 resolution)
- The driver doesn't change Analog Video-Out setting for G5/G6 SONY IP cameras. Please note that the camera's performance may be affected if this feature is be set to "On"

9.6.3.19.1.2 Motion Detection feature notes

- Please configure motion detection zones manually via the web interface before using the Motion Detection driver functionality.
- SONY cameras may not send the correct motion events stream when the Motion Detection page is opened on the camera's web interface. This means that MD functionality will not work correctly in this case.

9.6.3.19.1.3 Other limitations

- SNC-DM160, SNC-DM110 and SNC-CM120 cameras support 1280x960, 960x720 and 768x576 resolutions and are used only with JPEG compression, but these resolutions are also shown with MPEG-4 in System Manager camera settings. If one of these resolutions is selected with MPEG-4, the actual resolution is always 640x480.
- SNC-CS20, SNC-DS60 and SNC-DS10 cameras support 768x576 resolution only with JPEG compression, but this resolution is shown in System Manager also with MPEG-4.
- All P models of G3 cameras (3-rd generation) have maximum framerate of 8 fps (N models 10 fps) with H.264 compression, but System Manager camera settings shows 25 fps as a maximum. Because some camera models can give up to 12 fps the driver uses that value as the framerate maximum.
- With JPEG compression System Manager shows framerates of the G2 cameras (2-nd generation) as 1 to 25, but the cameras supports only 5, 6, 8, 10, 15, 20 (and 30 in NTSC mode) fps.
- Preset functionality and Privacy zones functionality will not work correctly in VMS 5.9.8. This issue is caused by incompatibility of some program interfaces.
- In some scenarios SONY cameras start to send video for MJPEG codec with greater frame rate than required. For example, after zooming SONY SNC-Z20P camera sends MJPEG video stream with 24-25 fps, even if frame rate setting set to 20 in System manager. This is a feature of the camera's firmware.
- SONY SNC-Z20 camera sends MJPEG video stream with lower framerate than required when maximal resolution and quality settings are set. For example, maximal frame rate for 736x544 resolution and 100% quality setting cannot be greater than 3. This is camera feature.
- SONY SNC-Z20 camera supports Zoom and Focus functionality, but it doesn't support Pan/Tilt functionality at all. However, VMS shows Pan/Tilt control on Device window in any case (even if Pan/Tilt is not supported by camera and this control is disabled by the driver). This is a VMS issue.
- SONY SNC-Z20 camera doesn't support preset functionality. But the "Add Preposition" button is always enabled for it in VMS 5.4.4. This is VMS issue.
- SONY SNC-CH210 supports 2048x1536 resolution only for MJPEG video codec (aspect ratio setting should be set to 16:9 value). For other codec maximal resolution value is 1600x1200.
- A few of G5 cameras (5-th generation) have limitation to privacy rectangle size. The rectangle cannot be greater than 1/16 of camera image:

- 640x480 pixels for SNC-CH220/DH220 cameras (relative to the maximal 1920x1080 resolution)
- 200x140 pixels for SNC-EM520/EM521 cameras (relative to the maximal 800x600 resolution)

- So, real privacy zones may be lower than applied by users because of this camera's feature.
- SONY G5 cameras send HD video stream with speed up to 15 Mbps. Subscribing HD resolution high-quality video for H.264/MPEG-4 codec or HD resolution video for MJPEG codec from more than one camera may cause lags in video stream. For example, real frame-rate will jump within 2..13 interval for 15 fps setting.
- SONY G5/G6 cameras restart own video encoder after video options changing. This operation takes 3-8 seconds, so CCRiA and CCFiA features (change options by alarm) cannot be used with these cameras.
- SONY SNC-VB630 camera starts H.264 stream by motion with 10-20 frames per second instead of applying 50 fps when 1% of quality is selected. Please use 2% quality value to avoid this behavior.
- The SONY G6 cameras uses quality settings (variable bit-rate) to set quality of H.264 stream. Previous camera generations uses Constant bit-rate (CBR) option for MPEG-4 and H.264 encodings.
- Multiple streaming feature is available for SONY G5 and G6 devices and for VMS version 6.1.1 and newer. Older SONY devices do not support this feature.
- The SONY G5/G6 cameras apply video settings during several seconds and may stop streaming during this procedure. So, starting of any stream may cause re-subscribing of other active streams.

9.6.3.19.1.4 SONY G5 cameras have the following limitations for the Multiple streaming feature

- The SNC-RS44/RS46/RS84/RS86 cameras support up to 3 streams. Other G5 devices support only 2 streams (Recording and Live)
- Resolution of second stream cannot be greater than 640x480 except case when it is equal to resolution of first stream.
- Resolution of third stream should be equal to current resolution of first or second stream.
- The G5 cameras may not start video stream in case in MJPEG is selected for Live stream with maximal resolution. This issue is caused by unexpected camera behavior (RTSP PLAY request returns error code 451). Please change encoding or decrease resolution settings in case if you met this issue.
- The driver will select suitable resolution automatically during settings applying in case if current resolution is not supported by the camera. So, stream resolution may differ from settings applied in VMS. Please refer to camera's Web-interface to learn video settings limitations.
- The SONY G5/G6 cameras may have an issues with encoding/decoding of G.726 audio stream (noise, no audio, etc.). Please use G.711 codec in case of problems with G.726 codec.
- Audio output (sending to camera) may not be restored after signal lost for SONY G6 cameras.

Camera may return HTTP error 503 code. To restore audio output funtionality please reboot the camera via Web Interface, "System" – "Initialize" - "Reboot".

9.6.3.19.1.5 The SONY G7 camera limitations

"Output modes":

The SONY G7 can work in the several different "Output modes". The "Output mode" option can be changed in the "System" – "Installation" section of the Web Interface.

Before changing this mode it is recommended to remove camera from the VMS. After changing the output mode it is necessary to re-add the camera to the system.

Multiple streaming feature is available only in the following "Output modes":

- "4K Multi streaming"
- "Intelligent cropping (FullHD)"
- "Intelligent cropping (VGA)"

The camera in the "HDMI" output mode can not be detected and added.

The available list of video resolutions, video codecs and frame rates is limited and depends on selected "Output mode" and "Aspect ratio". Please re-add camera to the VMS after changing this mode.

- The SONY G7 cameras have frame rate values with the floating point. The driver will round the value to nearest integer.
- The H264Quality option is not acceptable for the SONY G7 device series. The driver will convert the “Quality” value into the bit rate value for the H.264 codec.
- For the SONY G7 cameras in the "4K" output modes the H.264 high resolution stream cannot be decoded correctly by VMS video codec if "B picture" option is enabled on camera. The driver disables it by default.
- If the Edge Storage recording is enabled the bit rate will be limited to 8Mbps or less for the H.264 codec.
- SONY H-series devices (like SNC-HM662 camera) use different SDK than other SONY G6 cameras and cannot be added by native SONY driver. Please use Vivotek IP Capture driver instead for this device series.
- SONY SNC-EMX32R/52R devices use different SDK than other SONY G6/G7 cameras and cannot be added by native SONY driver. Please use BOSCH driver (NewBoschIPCapture) instead for this device series.

The Time synchronization feature uses the following rules:

- The time synchronization procedure is initialized by any of the following condition:
- Windows system time change;
- Windows time-zone change;

- Any error occurs on previous time synchronization;
- Previous successful synchronization was performed more than 30 minutes ago.

These conditions are checked every 5 minutes

- The new time will be set to IP device in case if difference between device's and recorder's times is 10 or more seconds
- The SONY HTTP API allows to apply time in GMT format, so the driver will not update time-zone settings on IP device
- Change options in alarm (CRiA/CFA) feature can be used in "Active" control mode only. In case of "Passive" mode the driver will not change any option on the IP camera, so stream will keep going without resolution or frame-rate changing.
- The Windows XP is not supported since driver version 2.6.0.0

9.6.3.20 OnvifIPCapture installation and usage

In all compression modes driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP protocol is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: default port is 554,
- **UDP**: two sequential ports per unicast audio or video stream is needed in a port range 3556 to 4556.

For example, if there are 4 IP cameras in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562, and 3563 will be used. If a port is not free, it will be skipped.

The multicast streaming also requires two sequential ports per audio or video stream, but the ports numbers depends from device settings or XML configuration. For example, the device may be configured to send all streams to the single port only. The ports 40000-40001 should be opened in case if 40000 port is specified for this setting.

9.6.3.20.1 Limitations

- PTZ Area Zoom command is combined by default with PTZ Center command, if supported
- The PTZ Center command is performed with little accuracy, since the accuracy is highly dependent on the camera mechanism, vertical and horizontal angles of view, optical aberrations (e.g. distortion) of the current lens. There is currently no place to enter and store these settings.
- The driver requires media profile for receive presets from the IP device. So, they may be loaded after video stream was subscribed.

- The driver uses timestamps for authentication on the device according to the ONVIF specifications. So, time on ONVIF-compliant device and time on PC whereVMS Recorder installed should be synchronized before using of this device.
- The driver doesn't support Unicode preposition names.
- Multiple streaming feature may have limitation dependent from used device (for example, resolution on encoder1 cannot be greater, that resolution on video encoder2). Please refer to device manual to learn these limitations.
- Multiple channel devices may support different capabilities for different channels. For example, first channel supports H.264 and MPEG-4 stream with 1920x1080 resolution and second stream supports H.264 encoding only but with greater 4096x2160 resolution. The VMS architecture does not allow to pass different capabilities for different channels, so capabilities from all channels will be combined (i.e. MPEG-4 encoding and 4096x2160 resolution will be available for both channels in sample above).

The driver will select suitable option automatically in case if user will try to apply option value that doesn't supported by current video channel.

- In some cases user can face "No signal" problem because of wrong configuration applied on the ONVIF-compliant device ("ter:Action > ter:ConfigurationConflict" message will appear into the log file). In this case user should correct settings in VMS according to device capabilities if Multiple streaming is enabled. If Multiple streaming option is not used, please apply minimal settings on additional streams via Web-interface or disable them at all.
- ONVIF compliant devices may not be able to switch streaming mode from "single stream" to "triple stream" without applying of settings for second stream. In other words, Remote stream may not be setup correctly in case if Live stream was not started after Multiple Streaming feature was enabled.
- The driver applies settings for different streams in series, not at the same time. So, starting of additional streams may take more time that starting of Recording stream only.
- The driver uses PTZ service version 2.0 according to the ONVIF specifications. However, old devices may use previous 1.0 version of PTZ service, so the driver will not detect PTZ capabilities correctly. Please use XML configuration file to specify correct PTZ Service version in this case.
- The driver uses Pull-Point mechanism for receiving states of digital inputs and to monitor motion detection stream. If ONVIF-compliant device supports this mechanism, it should set WSPullPointSupport capability in tds:GetCapabilitiesResponse according to section 9.9 of ONVIF Core specification. The digital inputs and VMD functionality will not be detected if this capability is set to unsupported.

9.6.3.20.1.1 Audio functionality limitations

The driver use audio functionality "as is" without adjustment audio parameters (like output gain). The manufacturer specific parameters like "input/output interval" or "output duration" has no appropriate options in ONVIF specifications. Please configure these parameters via Web-interface manually before camera usage.

9.6.3.20.1.2 Multicast capture limitations

Multicast capture can be enabled via XML configuration file using StreamingMode option. This option is read on stream startup, so refresh of device settings will be enough to take changed StreamingMode option into use.

Please note that VMS has optimization for channel re-starting since version 7.4.1, so in this case it will be required to change one of video option for each camera stream to restart them. The audio settings should also be updated to take the option into use.

The driver instance can be configured to be used as Primary or Listener. The primary instance is able to change IP device settings and use additional functionality. Listener instances are able to receive video streams and audio stream by multicast and allows to use digital I/O and VMD functionality.

The driver selects combination of video sources, video encoders and media profiles during capabilities detection. It is required to select the same encoding on both Primary and Listener instances to allow them to select the same media profile. Otherwise the Listener driver instance will try to subscribe another profile and will receive another multicast stream or will not receive any data at all.

The Listener recorder will not change any configuration on ONVIF-compliant device side. For example, if there is no media profile available on camera - it will not be created and the driver will not be able to receive the video or audio stream. The ONVIF device should be added to Primary recorder before using in Listener configuration.

The additional streams (Live and Remote) are active in case if they are opened in clients only. So, to take updated Multiple Streaming settings into use it is required to start (or keep opened) these streams for Primary recorder after stream settings have been changed in VMS. Otherwise the latest stream settings will not be applied to camera.

User should guarantee that only one recorder will change settings of ONVIF-compliant IP devices. Other recorders which use these devices should be in Listener mode.

It is required to specify IP address of the network adapter through which camera is connected to receive multicast streaming correctly in case if more than one network adapter is available. The network adapter marked in Windows as default will be used if no option is configured.

The driver may write message about invalid multicast configuration (like: `ter:InvalidArgVal > ter:InvalidMulticastSettings`). This message means that something is wrong with multicast configuration and video or audio stream cannot be started.

Please specify Multicast section in XML configuration file to resolve the problem or adjust values if this section already exists.

Several ONVIF-compliant IP devices (Axis, for example) allows to keep video stream while the client changing it's video parameters. As result, such device will keep active stream for Multicast:Listener instance with previous settings and start another stream for Multicast:Primary instance with updated settings.

It is required to enable video options monitoring on listener side by using VideoSettingsMonitoringInterval parameter. More details may be found in comments in the configuration file.

9.6.3.20.1.3 Video Motion Detection functionality limitations

- The device should support 'tns1:VideoSource/MotionAlarm' topic-set to support motion detection functionality. The custom topic sets like 'tns1:VideoAnalytics/tnssamsung:MotionDetection' may also be supported, but they will work for single-channel device only because these topic sets have no video source or channel identifiers as source data in event notifications.
- There is no IP device related motion detection settings in VMS available. So, the motion detection settings (areas, sensitivity, object size and etc.) should be configured on IP device manually before using this functionality in VMS.
- The motion detection may be used with Multicast streaming. The "Recorder and camera hardware" option should be enabled on both Primary and Listener recorders to pause/resume video stream correctly.
- There is no possibility to detect time of video options applying without camera configuration change. The driver adds support of CFiA/CRiA features for all devices, but it cannot guarantee that camera will switch options by alarm fast enough.

Please try CFiA/CRiA feature on test setup before taking them into use with security systems.

9.6.3.20.1.4 Other notes

The driver uses "RTP over RTSP" transport for video/audio streaming by default since driver version 1.5.0.0

The digital inputs returned by the ONVIF-compliant device are sorted by token name to be sure that they will not be reordered by the device on initial state request. As result real input numbers may differ from VMS values (like "1", "2", ..., "10" list will be sorted as "1", "10", "2", ..., "9").

Change options in alarm (CRiA/CFA) feature can be used in "Active" control mode only. In case of "Passive" mode the driver will not change any option on the IP camera, so stream will keep going without resolution or frame-rate changing.

The Windows XP is not supported since driver version 1.5.0.0

9.6.3.21 PelcoIPCapture installation and usage

Driver uses RTSP/RTP/UDP/IP protocols for MPEG-4, H.264 video receiving.
HTTP protocol is used for parameters setting/retrieving, JPEG video receiving and for PTZ functionality.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- HTTP: default port is 80 for Sarix cameras and 49152 for non-Sarix cameras,
- RTSP: port 554,
- UDP: Two sequential ports per video stream is needed in a port range 3556 to 4556.
- TCP: 3549 is default port for GENA DigitalInputs notifications.

Please also see the `PelcoIPCapture.xml`, DigitalIOListener section, port value

For example: if there are 4 Pelco cameras in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

For the Sarix, Endura and the newest series driver from vesrion 1.8.0.0 will use GENA notification architecture. The driver will automatically configure Windows Firewall to allow incoming connections to DigitalIOListener port. See also addFirewallRule option.

The "DigitalIOListener" section, "address" and "port" options can be used to specify external IP address and port in case port forwarding from external network to the same TCP port.

9.6.3.21.1 Limitations

- Quality and resolution configuring for JPEG codec for non-Sarix cameras are not supported. All JPEG images will be received in 4CIF. SystemManager camera settings will be ignored in this case.
- Pelco Sarix cameras allow to access them via SOAP requests without user authentication by default. So, any unauthorized user can subscribe and configure Pelco Sarix camera. To avoid such behavior please set "Public User Access Level" setting to "Disabled" on Users tab in Web-interface.
- Firmware version cannot be retrieved from Pelco IP cameras. This is a feature of Pelco API.
- Pelco cameras apply video stream settings approximately 30 seconds. So, CCRiA and CCFiA features cannot be implemented for Pelco IP cameras.
- Sarix MPEG-4 encoder doesn't support resolutions greater than 704x576. The driver automatically sets resolution to 704x576 if user tries to apply any greater resolution.
- Driver cannot receive number of inputs and/or outputs for IP110 camera from time to time. To fix this problem try to remove camera from the camera list and then add it again.
- Actual framerate for JPEG compression may be less than required framerate,because frames capturing over HTTP has delays.
- IO functionality for SARIX cameras does not work properly at the moment. The states of the inputs cannot be retrieved. The output component does not work properly because input states are unknown.
- List of supported frame-rates may differ for different codecs for Sarix cameras. In case if user tries to apply unsupported frame-rate value, the next greater frame-rate value will be applied (for example, 7.5 value will be applied instead of unsupported 6 value). If user tries to apply greater value than maximal supported value, the maximal value will be applied automatically. Please refer to camera's Web-interface to view list of the supported frame-rate values.

Speed parameter is not supported by Pelco PTZ IP cameras for the following PTZ functions:

- Focusing;
- Zooming;

- Iris changing;
- Moving to preset position.

So, the driver will use these functions as is: camera will process them with constant speed in all cases.

- Spectra HD camera sends H.264 video stream with lower frame-rate than required (for example real 1 fps instead of 4 fps applied) in case if frame-rate value is even. Most of odd values (except 1 and 25) are processed correctly. This is a firmware issue.
- The driver is unable to parse SOAP response from camera if any non-standard symbols (like umlauts or hieroglyphs) are used in configuration names. Using of these symbols may cause incorrect driver behavior, so please avoid using of these symbols when configuring Sarix camera via Web-interface.
- Pelco 1080p cameras may not send H.264 encoded video stream with 1080p resolution for low frame-rates (from 1 to 4). This is known issue of Pelco firmware. Please refer to Pelco Knowledge Base for details: <http://www.pelco.com/sites/global/en/sales-and-support/faq/faq_main.page?AID=12392>

To resolve the problem in VMS software please apply the lowest quality for these settings.

- The GetAlarmStates call used for digital input querying is deprecated and is not recommended for commercial use by Pelco support team. Querying of digital inputs every 2 seconds may cause camera hanging after 2-3 days of working. So, the digital input functionality is disabled by default, but it may be enabled via XML configuration file in case if it will be required.

It may be required to re-add the camera after configuration file change.

Port 3549 should be allowed for incoming connections in the Windows Firewall for the DigitalIO functionality for the Sarix, Endura and higher series. See also PelcoIPCapture.xml, DigitalIOListener section, port value.

Older versions of the cameras have a problem if the Digital Outputs requests are sent very often. If the user configures the frequent changes the Output (more often than one switch per minute) the camera may hang after several days. To avoid this issue please disable Digital Outputs functionality using driver configuration file.

Pelco Optera series Panoramic IP cameras (IMM12018, IMM12027 and IMM12036 models) have specific implementation of stream dewarping which was not integrated with native driver yet.

Please use ONVIF IP Capture driver instead for this device series.

9.6.3.22 PSIAIPCapture installation and usage

In all compression modes driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP protocol is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- HTTP: default port is 80,
- RTSP: port 554,

- UDP: two sequential ports per video stream is needed in a port range 3556 to 4556.

For example: if there are 4 cameras in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

9.6.3.22.1 Limitations

Only primary video channel is supported (if camera has several channels)

9.6.3.23 RTSPIPCapture installation and usage

The driver uses RTSP/RTP/UDP/IP protocols for receiving video stream from IP devices.

The driver expects RTP or RTSP URI for adding of the device. This URI should be placed in "IP Address" field.

The required port may be specified separately in "Port" field or may be included in RTSP/RTP URI. RTSP URI port has higher priority, if it is set, VMS port field will be ignored.

The stream URI requirements:

- The RTSP URI should be specified in full format, e.g.: `rtsp://192.168.1.70:554/?h264x=0`
- For cameras that send several video streams (like ACTi) correct track ID should also be specified: `rtsp://192.168.1.75:7070/track1`
- The RTP streaming devices should also have correct prefix: `rtp://62.97.61.37:15000/`
- The RTP steam URI also accepts multicast addresses: `rtp://239.232.192.255:20000/`

Please note, that stream URI may be checked over third-party player, like VLC or QuickTime

If there is a firewall between VMS and the cameras, the following ports must be opened:

- **RTSP**: default port is 554,
- **UDP**: two sequential ports per video stream are needed in a port range 3556 to 4556 for RTSP mode. The specified in parameters port should be opened for RTP streaming mode.

For example: if there are 2 IP cameras in a VMS, then ports 3556, 3557, 3558, and 3559 will be used for RTSP sessions. If a port is not free, it will be skipped.

The RTSP streaming may also be configured via RTSPIPCapture.xml configuration file. It allows to change the following options:

- RTP video transport. The following types are supported: RTPoverUDP and RTPoverRTSP `<RTPMode>RTPoverRTSP</RTPMode>`
- Keep-alive messages disabling. A few devices may not support keep-alive processing, so it may be disabled by 0 option specifying `<KeepAlive>1</KeepAlive>` These values can be set to each device separately.

The lip sync tracing can be enabled using the following option: `<LogLevel>4</LogLevel>`

9.6.3.23.1 Limitations

- If camera requires RTSP authorization, correct user name and password should be set, in other case it will be no video.
- RTP mode notes:
    - The RTP video streaming IP devices should be able to send SPS and PPS headers in the stream. The driver will not be able to decode H.264 stream correctly without these headers.
- The driver is unable to start RTP streaming by itself - it uses only RTP stream that continuously generated by the device.
- Audio synchronization using RTCP may NOT work in following cases:
    - if the device will send RTCP report after data packet;
    - for the RTP over RTSP mode;

In case if RTCP synchronization is available you may find the following messages in the DVRLog.txt:

"Video frame time was synchronized by RTCP successfully"

9.6.3.23.1.1 MPEG2 TS format notes

- Version 1.2.0.0 of the driver supports only H.264 and AAC codecs for the MPEG2 TS format.
- It is not possible to receive only video or audio stream because they transmitted over single RTP stream.
- Audio channel will be detected for all devices which MPEG2 TS format (MPEG II transport stream).

Please set the following value to "false" to disable audio on selected device:

```
<AudioChannel>
  <Enabled>false</Enabled>
</AudioChannel>
```

The Windows XP is not supported since driver version 1.0.1.5

9.6.3.24 SIPIPCapture installation and usage

Zenitel configuration example:

`<Zenitel PBX number>@<Zenitel Address>:<Zenitel SIP Port>@<SIPProxy_address>`
(e.g. 500@10.90.91.98:5060@10.90.91.99)

9.6.3.25 StanleyIPCapture installation and usage

In all compression modes driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP protocol is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- HTTP: default port is 80,
- RTSP: port 554,
- UDP: two sequential ports per video stream is needed in a port range 3556 to 4556.

For example: if there are 4 cameras in VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port isn't free, it will be skipped.

9.6.3.25.1 Limitations

- Driver detects capabilities for currently enabled profile only. If user changed profile in camera web interface, it is required to update camera capabilities in VMS (re-start auto-search in System Manager or re-add camera).
- In VMS is not possible to set different number of resolutions for different compression formats, so in System manager will be displayed all supported resolutions. If some resolution is not supported by compression format, the nearest valid resolution will be used.
- Different resolutions support different maximum framerate, so driver will use the nearest valid framerate value. For example, if maximum framerate for 1080p resolution is 15 fps and user applies 30 fps in System Manager settings, the driver will set 15 fps to camera.
- H.264 video stream doesn't have quality setting, so to control stream quality constant bitrate mode (CBR) is used. 1% of quality in System Manager means minimum bitrate value and 100% quality means maximum bitrate value.
- For multiple streaming each stream will have only one codec and one resolution. For example, first profile in camera has the following combinations:

-> H.264 :1920 x 1080

-> H.264 :720 x 480

-> JPEG :720 x 480

-> JPEG :352 x 240

So, first stream will have H.264 codec and 1920x1080 resolution, second stream will have H.264 codec and 720x480 resolution, third stream will have JPEG codec and 720x480 resolution. And fourth combination (JPEG codec and 352 x 240 resolution) will be used for first stream again. Multiple streaming can be disabled in driver XML file.

Privacy zones can be bigger then displayed in System Manager, because Stanley cameras use fixed blocks to set mask (20 blocks in horizontal and 12 block in vertical).

9.6.3.26 VivotekIPCapture installation and usage

In all compression modes driver uses RTSP/RTP/UDP/IP protocols for video receiving. HTTP protocol is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP ports must be opened:

- **HTTP**: default port is 80,
- **RTSP**: port 554,
- **UDP**: two sequential ports per video stream is needed in a port range 3556 to 4556.

For example: if there are 4 Vivotek IP cameras in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, it will be skipped.

9.6.3.26.1 Limitations

- Sometimes camera goes to the "HTTP only" mode according to network capabilities detection mechanism (camera internal mechanism). To return camera to the "RTP" mode it should be rebooted.
- Camera skips channel settings while switching from the "quality priority" mode to the "frame rate priority" mode. Video mode can be set in driver XML file.
- Default viewing mask for high resolution doesn't show all picture. It can be configured using Web-interface.
- Maximum frame rate for high resolutions is lower than declared.
- Commands for iris changing are not working for tested SD7323 camera.
- AAC audio decompression is supported from VMS 7.4.4 or higher.
- Sony H-series devices (like SNC-HM662 camera) uses Vivotek OEM SDK unlike other Sony G6 cameras. The Vivotek native driver should be used for these devices instead of Sony native driver.
- The Windows XP is not supported since driver version 1.6.1.0
- CCRiA and CCFiA features available only for devices 8xxx series or higher
- When resolution is changed by alarm, user can see one invalid frame. This is device issue - camera send one invalid frame - and driver cannot skip it, because all headers looks ok.

9.6.3.27 WisenetIPCapture installation and usage

In all compression modes driver uses RTSP/HTTP/HTTPS(TLS)/RTP/UDP/IP protocols for video receiving. Also HTTP/HTTPS protocol is used for parameters setting/retrieving.

If there is a firewall between VMS and the cameras, the following RTSP/UDP/HTTP/HTTPS ports must be opened:

- **HTTP** : default port is 80,
- **HTTPS**: default port is 443,

- **RTSP**: default port is 554,
- **UDP**: two sequential ports (starting from even value) per unicast audio or video stream in a port range 3556 to 4556.

For the communication via HTTPS (TLS) is needed to select RTSP over HTTP transport which siutable as for HTTP and for HTTPS.

For example, if there are 4 IP cameras in a VMS, then ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 and 3563 will be used. If a port is not free, the port pair will be skipped.

The multicast streaming also requires two sequential ports per audio or video stream, but the ports numbers depend from device settings or XML configuration.

For example, the device may be configured to send all streams to the single port only. The ports 40000-40001 should be opened in case if 40000 port is specified for this setting.

9.6.3.27.1 Limitations

- License plate recognition is configured directly in the VaxALPR plugin installed on the camera in accordance with the manual "VaxALPR On-Camera Software. Software Setup and Camera Configuration. Hanwha Manual". There is no possibility to adjust the accuracy of LPR using XML.
- It is recommended to use cameras with Whisenet 5 and Wisenet 7 processors for Vaxtor ALPR plugin (VaxALPR).
- Regarding the TLS certificate, when RTSP connection over HTTPS (TLS) is made, camera shares its public certificate during Handshake procedure, therefore client need not store or have camera's public certificate.
- Do not set a blank username for authorization. If the username is empty then authorization content headers will not be added to the HTTP requests.
- The camera may return non-rotated resolution capabilities in case if "Hallway view" option is set to 90 or 270 degrees (like 800x448 option instead of real 448x800 resolution). The stream is received with correct (rotated) resolution in this case.
- Privacy masks are applied based on maximum resolution size according to SUNAPI specifications. As result they may do not correspond to displayed positions in case if cropped image or image with different aspect ration is used. This is normal behavior. Please use maximal resolution in System Manager/Spotter Admin applications for privacy mask editing.
- Privacy masks may appear and disappear several times for SNB-9000 camera (firmware version 1.02_160215) during applying of configuration by the driver. This is camera-related issue and it was reported to Hanwha Techwin support, however they have no plan to release new firmware version at the moment.
- Privacy masks do no supported for PTZ devices since Mirasys VMS has no possibility to setup mask position using spherical coordinates.

- The several cameras like PNM-9030V supports privacy masking only for overview channel. The rest channels display part of overview channel and have no possibility to setup own masks.

Since VMS has no possibility to setup capabilities for each video channel separately, all camera channels will have the same (maximal) number of available masks. However, masks will work only for overview channel in this case. Privacy mask settings for other channels will be ignored.

The Wisenet PNM-9030V sample supports privacy masking feature for "Overview" channel only.

The picture for other channels has no privacy masking support. So, all objects covered by masks on "Overview" channel's picture, may be easily seen on the other ones.

This is Hanwha's concept and it's mentioned in camera's specifications.

The SNB-9000 camera (firmware version 1.02_160215) is unable to change codec by SUNAPI call.

This is camera-related issue and it was reported to Hanwha Techwin support, however they have no plan to release new firmware version at the moment.

Please change the codec manually via Web-interface in case if you'll meet problem with video settings applying.

The SNB-9000 camera changes resolution by alarm (CCRiA feature) during 8 seconds. This behavior is caused by several delays on camera side during stream re-subscribing and cannot be improved on driver side. The changing of frame-rate in alarm (CCFiA) takes 2 seconds because of the similar camera behavior.

So, please remember about these limitations in case if CCRiA/CCFiA features should be used with this camera in your setup.

The driver does not allow to use PTZ functionality for cameras with "Cropped image" features (like SNB-9000 or SNV-8080 cameras).

The cameras with motorized focus/zoom lenses do not support continuous zooming/focusing like PTZ cameras. The zoom/focus change is used as step-by-step adjustment in Web-interface. As result, zoom/focus change is discrete. The driver also keeps sending of repeatable step commands while zoom/focus key is pressed to emulate continuous movement.

Hanwha box cameras (with 'B' character in model, like XNB-xxxx or QNB-xxxx) supports External PTZ feature which allows to use the camera with PT-platform. Unfortunately there is no way to detect is the camera connected to PT-platform or not via HTTP API calls, so box cameras with External PTZ feature support will be detected as PTZ. This is HTTP API / camera hardware limitation.

The Hanwha's devices has the following limitations for preset positions names:

- Only alphanumeric symbols (A-Z, a-z, 0-9) are allowed;
- Length of preset name is limited by 12 symbols.

As result the driver since version 1.0.2.0 stores preset position in '*.preset' XML files. In case if file contains no preset positions, the driver tries to load actual information about preset positions from the Wisenet IP device.

Using of XML storage also allows to use Unicode symbols in preset position names.

The GOV Length value is set to half of current frame-rate (i.e. 2 key frames per second) automatically for recording profile and cannot be adjusted via Web-interface or via HTTP API commands. Select another profile as "Record" profile if this limitation is not suitable for your configuration.

The multi-sensor Wisenet IP device may have different resolution capabilities for different channels. For example, the PNM-9030V sample supports 6096x2540 and 2688x1120 resolutions for first channel, up to 2592x1944 resolution for next 4 ones and up to 1920x1080 for 6-th and 7-th channels.

Unfortunately, the VMS has no possibility to specify different resolution sets for different channels - this is software architecture limitation. In other words, all resolutions (6096x2540, 2688x1120 and 2592x1944) resolutions will be available for all channels.

In case if selected resolution isn't supported by the channel, the nearest greater or maximal resolution will be applied instead. For our example in case of 2592x1944 selection the 2688x1120 will be applied for 1-st channel and 1920x1080 for the 7-th one.

Audio channel uses the same video profile that is used for Recording video stream receiving.

It may cause the conflict in multicast configuration applied by video channel (from Dynamic UI configuration) and by audio channel (loaded from XML file).

So, audio channel changes multicast configuration only in case if it was not changed by video channel yet. Otherwise existing multicast configuration is used for multicasting of audio stream.

The device video profile is used for audio receiving and sending. Any change in video profile setting which causes RTSP session re-starting may also cause audio stream re-subscribing.

The VMS has no possibility to configure audio settings in System Manager, so these settings should be configured via XML configuration file.

By default only audio encoder (<Encoding> option) is specified: AAC for audio input and G.711 for audio output. The other audio options (including volume/gain) are configured to use values that currently selected in camera's Web-interface.

Wisenet cameras may have frame-rate limitation dependent on amount of profiles which are streaming at the same time:

- New Q-series can support 1920x1080 stream by total 45fps. For example, QND-6082R camera supports up to 30 fps for H.264 stream with maximal 1920x1080 resolution. In case of streaming from single profile the camera gives 30 fps stream. However, in case of streaming from 2 different profiles with the same H.264 1080p @ 30 fps stream settings, the camera will stream each of them with 22fps only.
- New L-series can support 1920x1080 stream by total 30fps.
- The Mirasys VMS has an issue with decoding of G.726 audio stream from several samples like

Wisenet XND-8080R. The issue will be fixed in next driver releases, please use G.711 or AAC encoding in case if you'll meet problem with G.726 audio decoding.

The driver supports only new version of Edge-Storage feature, which is available since VMS version 8.0. The Edge-Storage capability will not be detected for earlier VMS versions.

Wisenet SNF-8010 camera has an issue with searching of recorded data intervals: it detects only intervals intervals whose begin and end is inside or requested period. Other camera samples detects intersections also (i.e. recording start time is before requested period, and end time is inside the period or after it).

The SNF-8010 camera is discontinued already (since 2018 year), so the issue will not be fixed on camera side. Mirasys also has no plans to add separate processing logic for single model to the driver.

The several multi-sensor devices support recording of material by limited amount of channels.

For example, the PNM-9030V sample allows to record video from "Overview" channel only.

In this case the driver will use Edge-Storage feature only for channels which has "Recording" capability in "Recording" attributes group.

The SUNAPI v2.x specifications have the following limitations for HTTP and RTSP requests related to storage functionality processing:

- The milliseconds are not available.
- The time should be specified in local format (no UTC support) in all requests.
- The time intervals returned by the device are also in local time.

These limitations may cause the following issues:

- Since time resolution is one second, the switching between recording and edge materials and vice versa may cause repeatable fragments not longer than one second duration or may have missed data no longer than one second;
- Conversion between local time and UTC time may cause problems with material selection while switching to or from daylight saving time (DST).
- Changing the time zone may cause the selection of the wrong time interval during interval receiving.
- The Wisenet devices support only one RTSP connection for playback at the same time. So, in case of using a multiple-channel device, the lost data will be received from the device's SD card in series: all intervals from all channels will be posted to a single queue, and will be extracted from the queue only if no other intervals are processed at the moment.

The driver can be used with Windows 7 or a newer operating system. Older operating systems are not supported.

For the WisenetRoadAI, the most precise detection mode is "**On lost**" - it produces the most correct results. To have faster detection, "**On reliable**" mode can be used. In this case, the detection will be faster, but it can produce

false detections sometimes. "**On detect**" and "**On update**" modes are not recommended. Metadata format should be set to "**Onvif**" (forced by the driver).

The WisenetRoadAI application can show different results on the **Events** tab, but it will have the same results on the Search tab if "**On lost**" mode is used.

9.6.4 Installing Metadata Drivers

It is possible to update and install new metadata drivers using the **Install metadata drivers** –option in the **System** tab.

9.6.5 Installing Client Drivers

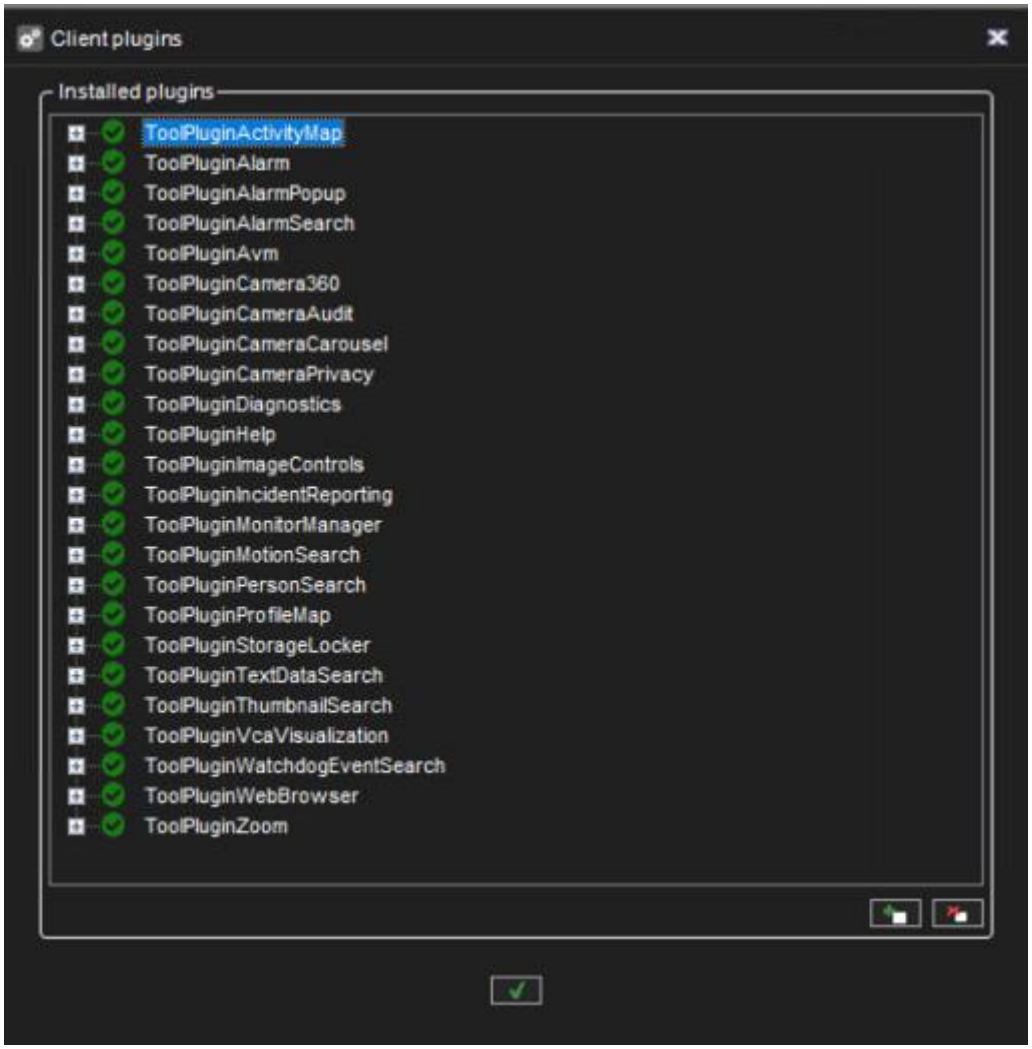
ThruCast (direct streaming from camera to Spotter client) requires a different type of camera driver.

These are called (Managed) ThruCast Client drivers.

The client camera drivers are installed similarly as spotter plugins and metadata drivers, using the **Install client driver** option in the system manager.

9.6.6 Install client plugin

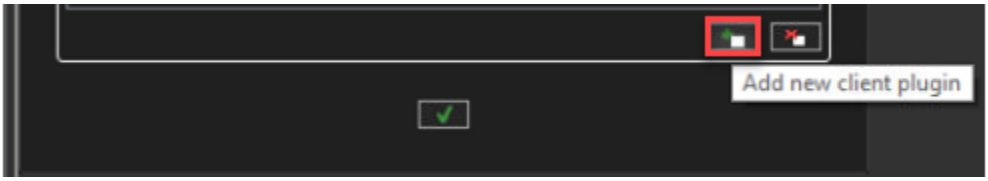
Client plugins for user interfaces such as Spotter can be installed through System Manager.



Plugin installation can be opened from the system tab under Add-ins.

9.6.6.1 To install a client plugin:

1. Open the **Install client plugin**.
2. Click **Add new client plugin**. Browse for the correct file and select it.



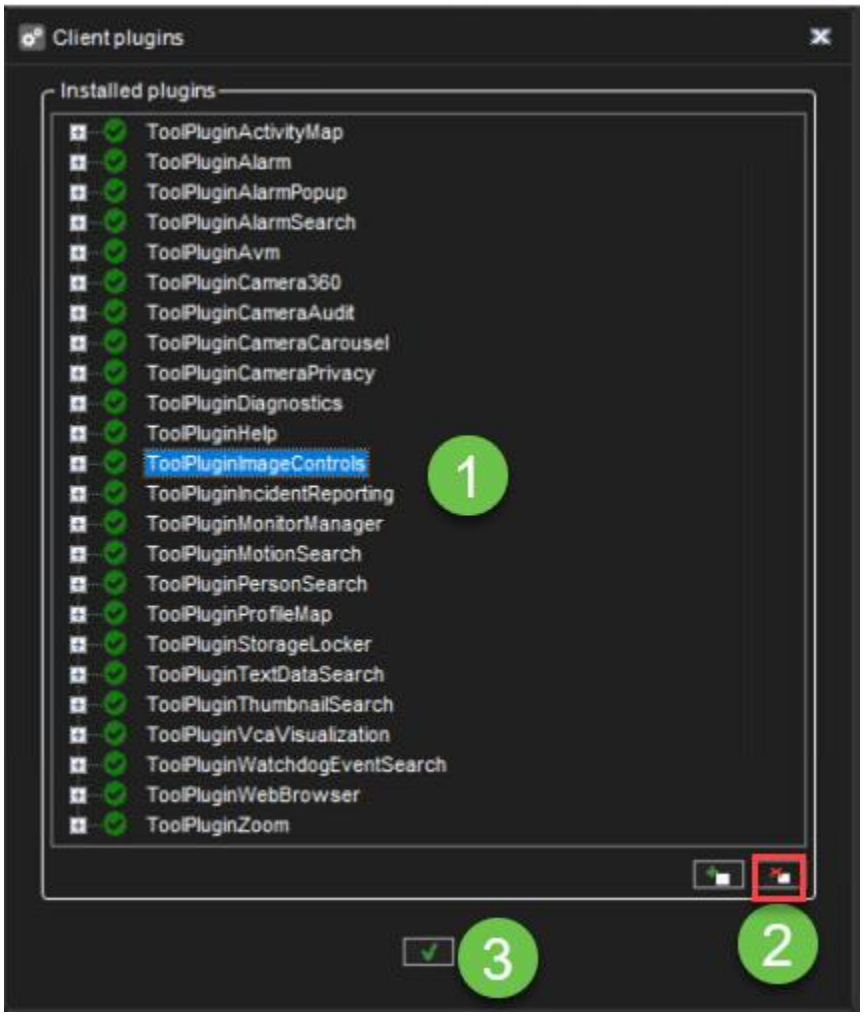
1. Find and select the plugin package (.zip file) and click **OK**. The **Install Plugin** dialogue box is shown.

2. If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**
3. Click **Ok**

9.6.6.2 To remove a client plugin:

Open the **Install client plugin**

1. Select plugin from the list
2. Click **Remove client plugin**
3. Click **Ok**



10 THE VMS SERVERS

On the **VMS Servers** tab, you can configure these settings for each server:

Icon	Name	Description
	General	Change the name and the description of the server. Here you will also find the IP address of the server.
	Port forwarding	Users can see what the automatic port forwarding has configured as ports for this server. The ports can be changed if necessary.
	Hardware	Add IP cameras and select camera and audio drivers.
	Cameras	Change camera parameters, recording schedules and motion detection settings.
	Audio	Change audio detection settings and recording schedules.
	Digital I/O	Set digital I/O settings.
	Alarms	Set up alarm conditions and alarm actions.
	Storage	Add a hard disk to a server and set the storage times for video, audio, and alarm files.
	Text channels	Set the names and descriptions of text data channels here.

To access the settings, do one of the following:

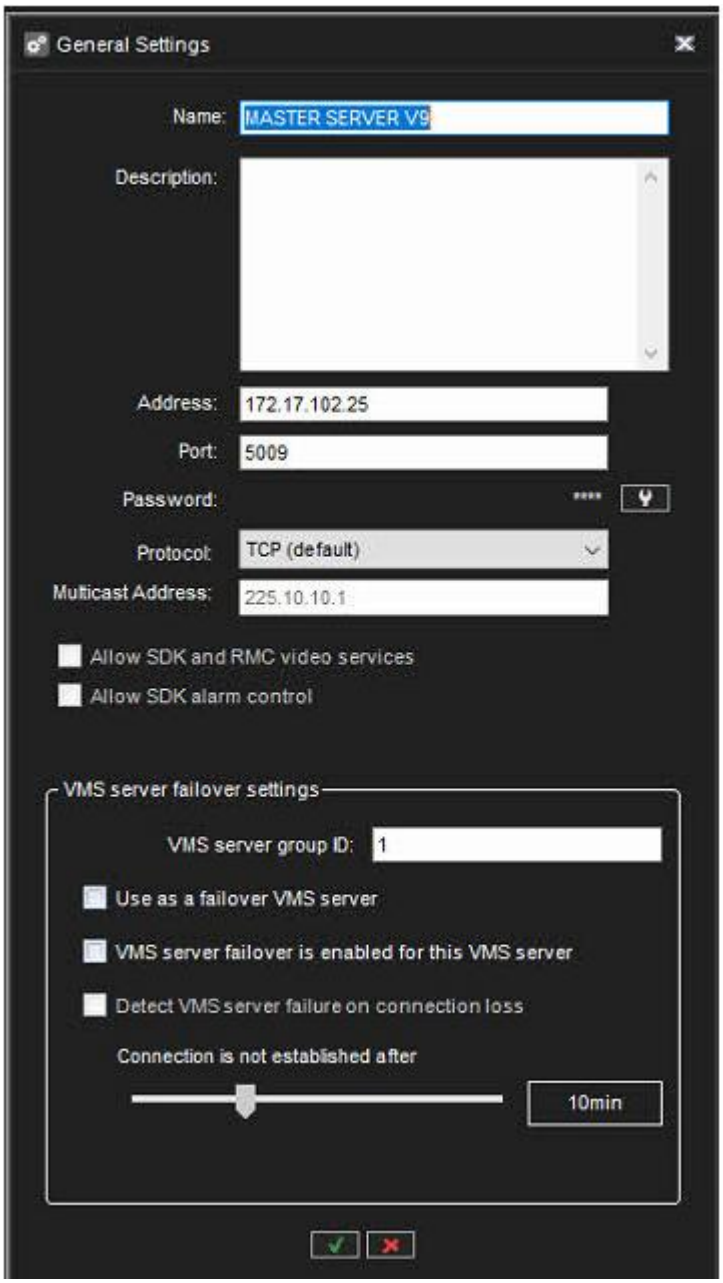
- Select the settings you want to configure (for example, Cameras) and then click Edit in the lower-right corner of the navigation pane.



- Double-click the settings that you want to configure.
- Drag the settings from the **VMS Servers** tab to the workspace.

10.1 General

- VMS server name
- Description
- Password
- Protocol
- Multicast Address
- VMS server failover settings



10.1.1 Multicast address

When a single workstation stream is opened multiple times, the server – and the network – face unnecessary strain as each stream is treated as a separate entity.
Multi-casting enables a single stream to be opened and sent to multiple workstations simultaneously.
When using multi-casting, the stream for each video channel is sent to the LAN only once.
All applications on the LAN can receive the single stream, so network bandwidth usage is lower than when sending a stream for each application separately.

The feature needs to be configured in System Manager and through network settings.
Please refer to your network infrastructure service for information on enabling multi-casting support on the network level.

To configure multi-casting in System Manager:



1. In the server's General settings, change the protocol from **TCP (default)** to **RTP Multicast**.
2. Edit the multicast address.
3. Repeat steps 1-2 for all required servers in the system. Note: Each multicast address needs to be separate.

10.1.2 VMS server failover settings

When adding a new server to the system, it can be defined to be a failover server.
A failover server is a backup server that shall assume any server duties determined to be under failover protection.

Failover servers must have the same file system (same drive letters) as the VMS Servers under failover protection, and they can only be used for IP camera backup purposes.

When in standby mode, failover servers appear under a separate folder in the *VMS Server* list.

When any VMS Server is deemed to be broken or inaccessible, they have moved under the *"Broken VMS Servers"* folder.

Any available failover server shall take the responsibilities of the failed server.
Failover settings can be controlled from the general settings of the selected server.
The failover transition is done if all material disks are broken or the server is inaccessible for longer than a defined period.

10.1.3 Use as a failover VMS server

This setting define that the server is used as a failover VMS server

10.1.4 VMS Server failover is enabled for this VMS server

This setting defines the selected server role that will be transferred to the failover server during the error situation

10.1.5 Delay failover to prevent data loss

During material copy from the failover recorder, the restored recorder checks its recorded data first, then copies only missing material (including video, audio, text data, metadata, and ANPR data).

This functionality can be enabled in the System Manager > VMS Servers General dialog, checkbox *Wait for the recorder to apply settings*).

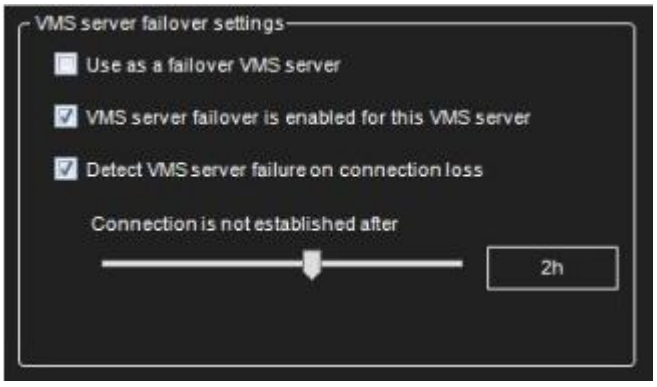
> Delay Failover can be enabled only for recorders V9.7 or newer, as recorders pre-V9.7 do not support selective material copy, and data will overlap.

10.1.6 Use automatic failback

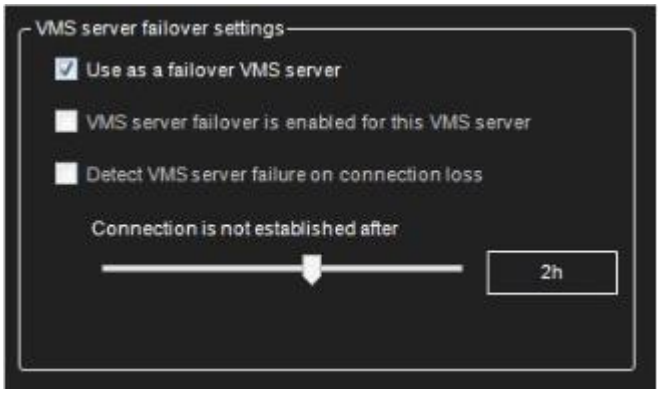
This setting enables the automatic failback feature to this server

10.1.7 Use automatic material copying

This setting enables the automatic material copying feature to this server



For example, under failover protection, if inaccessible for longer than 2 hours, the failover switch would happen.



10.2 PORT FORWARDING

The basic idea with port forwarding is that it can access one or more VMS Servers or Main Servers behind a router that does Network Address Translation (NAT).

Typically, this situation happens when the client is outside the network and needs to access servers inside a company network.When installing a VMS Server, the installer offers the option to turn on the automatic port forwarding. The default state is off
If the port forwarding is not activated when the system is installed, it can be activated from the second tab, "VMS Servers".
Open the view "Port forwarding" and activate the selection "UPnP is in use."

10.2.1 Automatic Router Configuration

When a VMS Server starts up, it tries to discover UPnP devices from the network.
The router needs to support UPnP (Universal Plug and Play), which must be enabled on the device.
The server has continuous UPnP device discovery when running, so if any network changes are done, the server will automatically detect new routers and do port forwarding to them.
Only UPnP devices with external (WAN) addresses are detected.

If the user wants to remove port forwarding automatically, he can do this from the system manager.
After this, the server will remember that the settings were removed and not port forward to this router.
The software does not allow to delete port forwarding mapping if the server is added to the system with an external address.

Deleting the port forward mapping would disconnect the system, and no further configuration would be possible.

If forward port settings are changed, and the connection to the server has not returned after a while, it might be necessary to reboot the router.

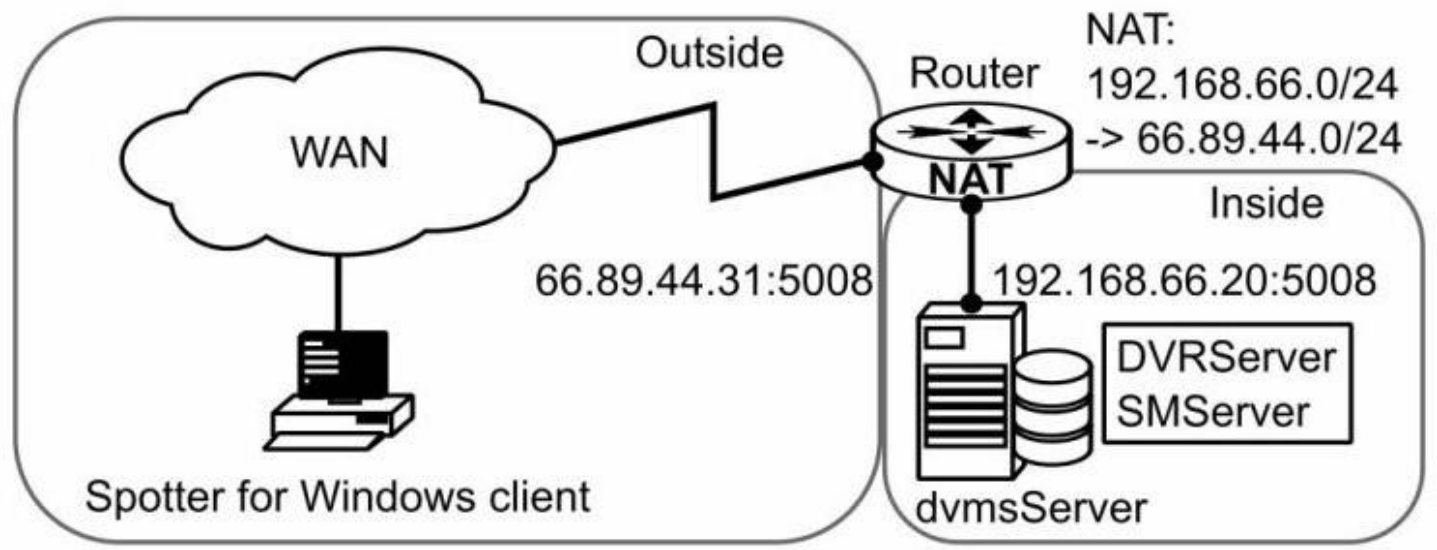
Servers need four ports for the server to server communication. The first server that does port forwarding will claim ports **5008**, **5009**, **5010** and **5011**.

The second server will claim ports **5012-5015**, the third server ports 5016-5019. And so on. (Assuming all the ports are available).

The first port is used for SMServer communication (**5008, 5012, 5016…**)
The second port is used for DVRServer process communication (**5009, 5013, 5017…**)
When connecting to a Main Server, the port is typically 5008. When adding new servers to the Main, the port is typically 5009. If there are more than one server on-site, then the ports are 5009 +4, 5009 + 8 etc.

10.2.2 Single Server Behind Router

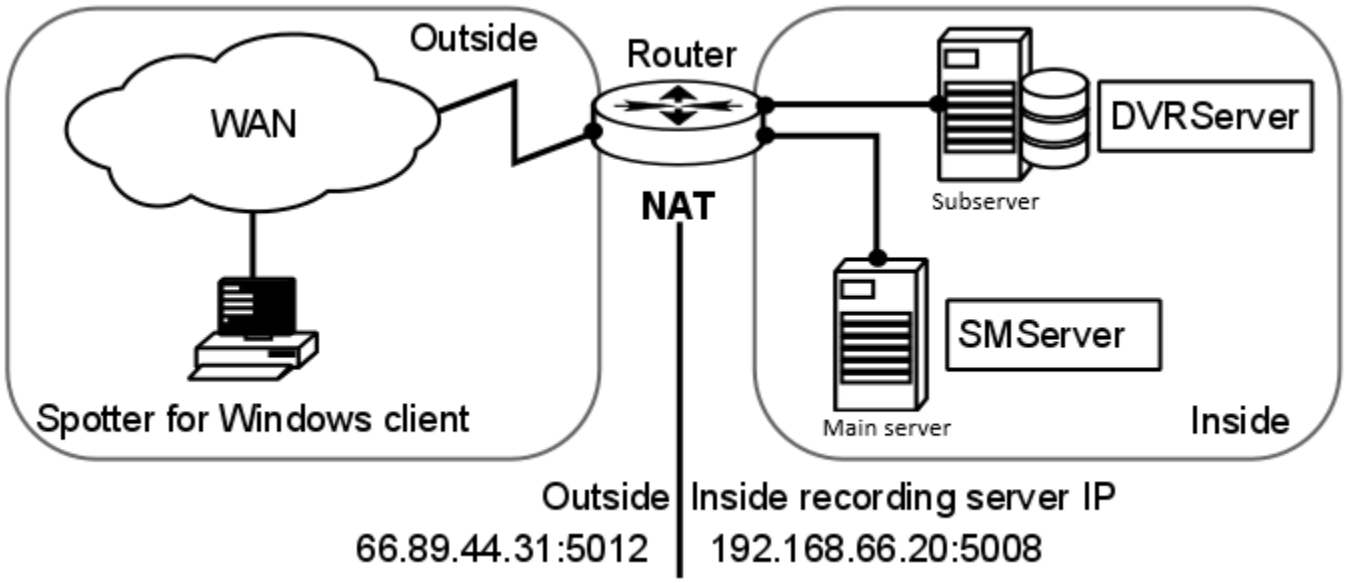
Scenario 1: Using a system with **a single server behind a router/firewall**



If the user is accessing a single server from the WAN, he needs to connect to the VMS Server with the outside IP address that the router has translated.
The user can check the port forwarding what the port in use is, but it is highly likely port 5008.

10.2.3 More Than One Server Behind Router

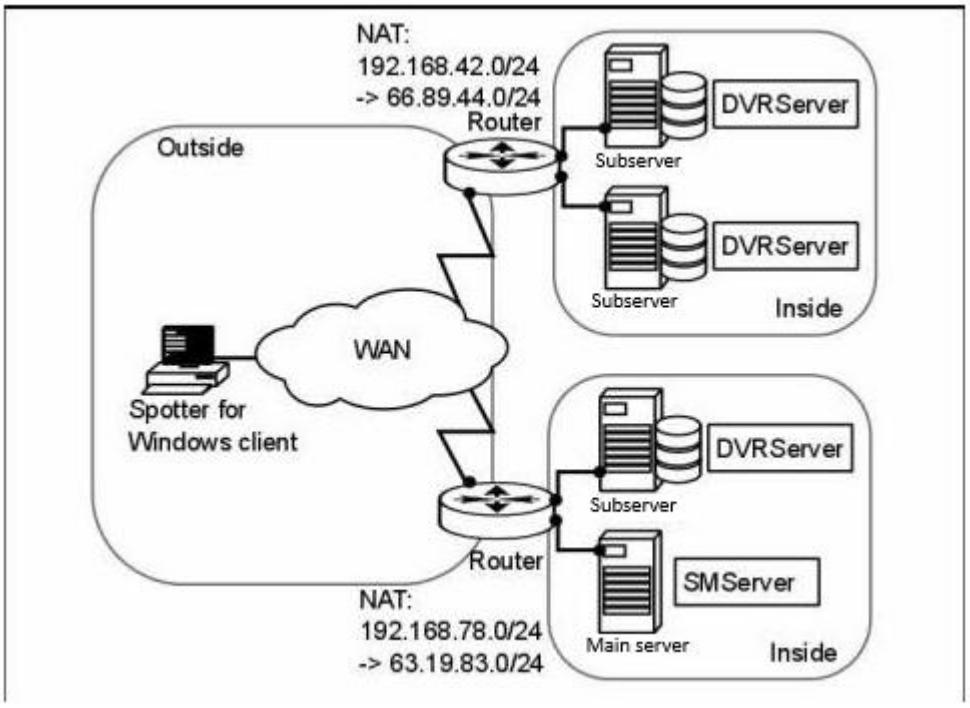
Scenario 2: More than one server behind a single router (WAN address)



If the user configures a more extensive system with multiple servers on a single site, he can add the servers to the System Manager application with the external or internal IP addresses.
When adding a new VMS Server, if the server has done automatic port forwarding, a note shows that he can choose between an internal IP address and an external IP address.
If the server is to be used from the WAN, then the external IP address should be chosen.
The exact ports that the server has done port forwarding to can be found by starting the System Manager on the local server.
When adding a server to a Main Server when not on the local site (cannot use the local IP address), the user must know the external IP address and know the first port that the port forwarding was done to.
If the added server is a single, standalone server, the port is most likely 5009.
If multiple servers are on the same site, they most likely get the ports starting with **5009, 5013, 5017, 5021**…

10.2.4 More Than One Server On Multiple Sites

Scenario 3: More than one server on more than one site



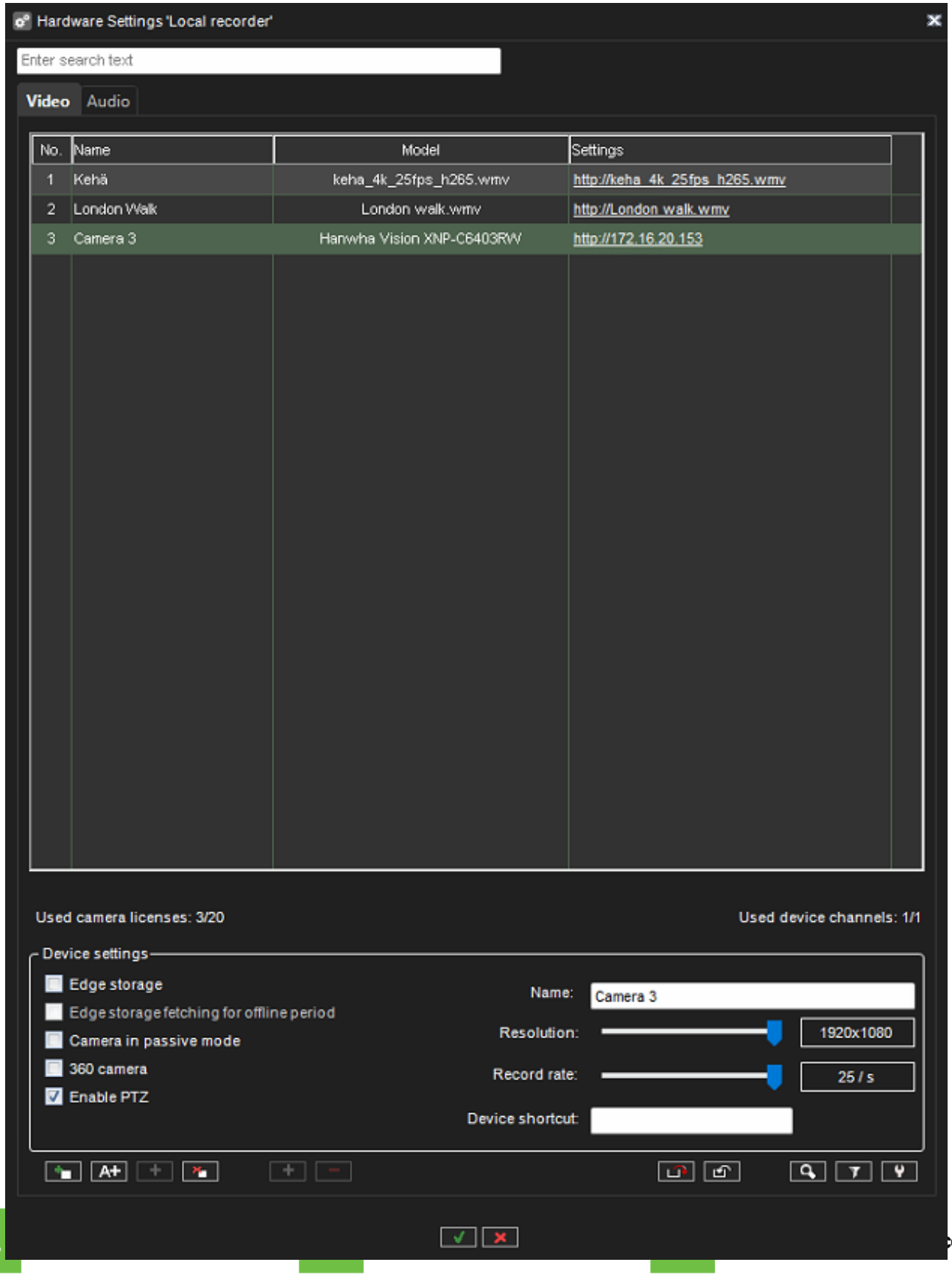
The same principle applies as in Scenario 2, but this time NAT needs to be taken into account when assigning VMS Servers to the Main Server from the other site.

10.3 HARDWARE

Before using the system manager application to search for the camera, please do the following actions:

- Configure the IP address to the camera
- Define the username and password to the IP cameras
- Check that the camera time zone and time is the same as the VMS server

MIRASYS


Hardware Settings 'Local recorder'
Enter search text
Video
Audio
No.
Name
Model
Settings
1
Kehä
keha_4k_25fps_h265.wmv
http://keha_4k_25fps_h265.wmv
2
London Walk
London walk.wmv
http://London walk.wmv
3
Camera 3
Hanwha Vision XNP-C6403RW
http://172.16.20.153
Used camera licenses: 3/20
Used device channels: 1/1
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
360 camera
Enable PTZ
Name:
Camera 3
Resolution:
1920x1080
Record rate:
25 / s
Device shortcut:

Also the information about used/total license count and information about used/total channels for selected multi-channel device were added below the "Devices" list in the "Hardware settings" dialog.

10.3.1 Video

When adding an IP camera, the following search modes are available.

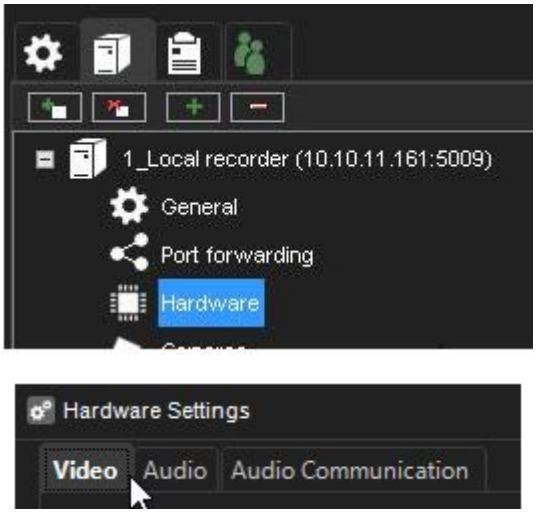
- ***All drivers***: Automatic search with all drivers. The system will attempt to use all available drivers. The mode option combo-box is disabled.
- ***Selected drivers***: Automatic search with specific drivers only. The system will use only the drivers specified via the Selected Drivers dialogue during the automatic search.
    - The additional combo box will show all drivers that are currently selected. A user may use all of them (using the “All” option) or select only one driver.
- ***Currently active drivers***: Search the camera using all drivers who are currently used. If this option is selected, the system will use only drivers currently used for already added cameras.
    - For example, if we have Sony and Axis cameras subscribed, the search will be done by Sony and Axis drivers only.
    - The mode option combo-box will contain a list of used drivers if the user wants to use one of them and an “All” option for using all drivers from this list for searching.
- ***Driver***: Add a camera using a specific driver. The system will use only the specific driver for search.
    - The mode option combo-box will contain a list of all installed driver names to search.
    - If a search with specified drivers fails, the system will prompt whether the user wishes to search using all drivers.
    - The driver currently used for the search also should be excluded.
- ***Camera model***: Add camera by model name. This mode is used for adding a camera by using an older capture driver using pre-defined capabilities from the driver configuration XML file.
    - The mode option combo box will contain a list of available models.

The ***Selected drivers*** -mode will be selected by default for adding the new camera for the first time.

Next time the dialogue is opened, the system will remember the previous model and driver selection to allow the user to add similar cameras faster.
Opening the existing camera using the Modify button will show a dialogue with the Currently active drivers search mode and driver name in mode option combo-box (except cameras added by mod, el of course).
The system will not store last used options for modifying cases because the options will be available for adding cameras only

10.3.1.1 Add device

IP cameras or analogue video servers (encoders) can be managed through the **Video** tab of **Hardware settings**.



To add a new IP camera when the IP address is known:

1. On the **Video** tab, click **Add device**



2. Type the IP address or DNS name of the camera or video server.

Change the port number if needed. Usually, port 80 is used.

3. Type the username and password for the camera.

4. Click **OK**.

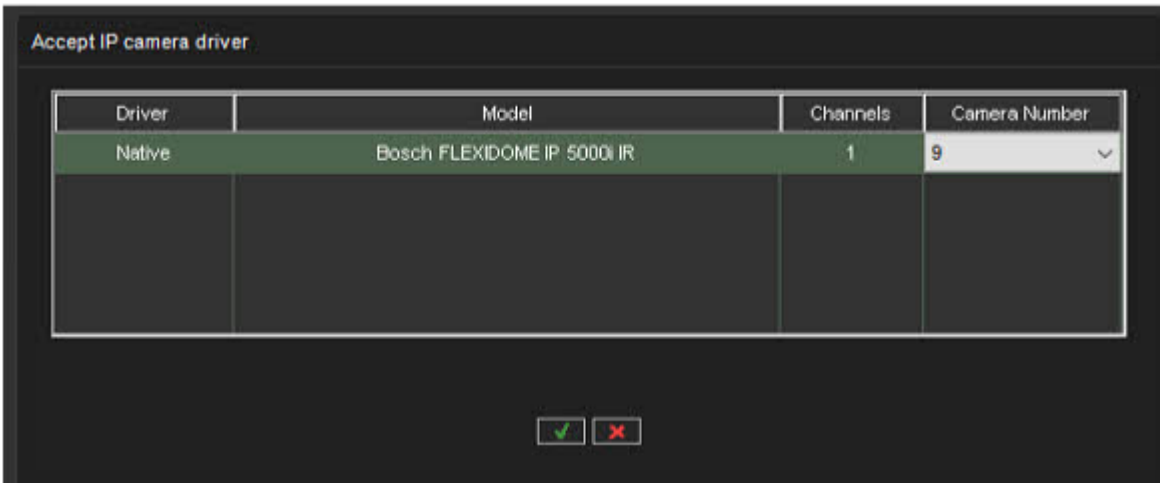


The system will now communicate with the camera and display which drivers can connect to the camera.
The camera may support **ONVIF**. In this case, the **ONVIF** driver may also detect it.

5. Select a driver from the list.

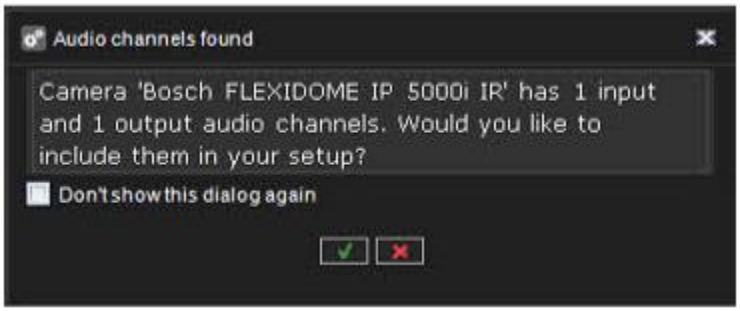
Typically, it is recommended to use the **Native** driver if it exists.
For multichannel devices, the **Channels** option can add the device with less than the maximum number of channels.
The user can also see what will be device camera number

6. Click **OK**



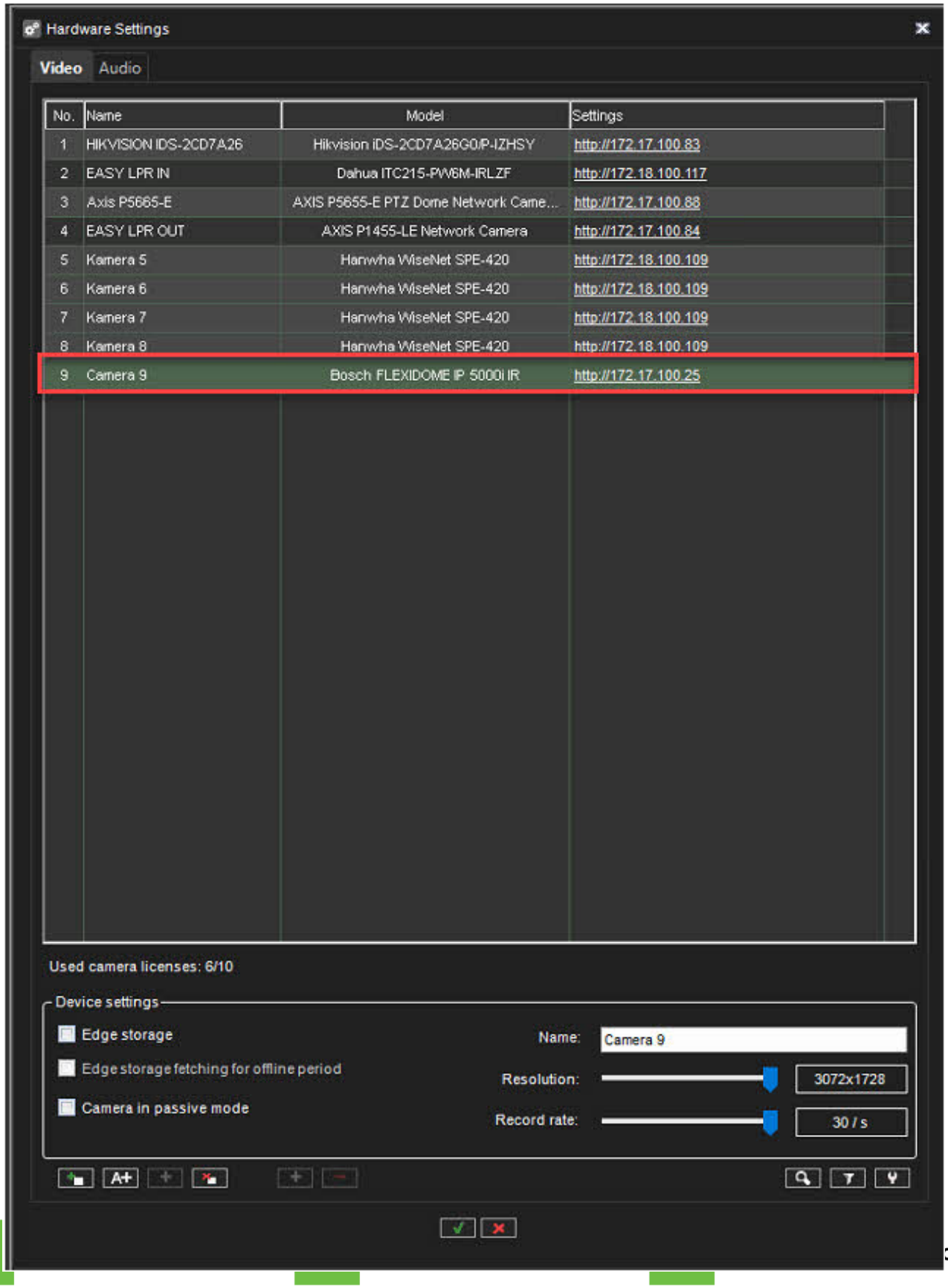
If the camera supports audio channels, you will see dialogue about this.

7. Click **OK** to add also audio channels or **X** add an only video channel



After the camera adding device can be found from the **Hardware settings** list

MIRASYS


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 EASY LPR IN Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 EASY LPR OUT AXIS P1455-LE Network Camera http://172.17.100.84
5 Kamera 5 Hanwha WiseNet SPE-420 http://172.18.100.109
6 Kamera 6 Hanwha WiseNet SPE-420 http://172.18.100.109
7 Kamera 7 Hanwha WiseNet SPE-420 http://172.18.100.109
8 Kamera 8 Hanwha WiseNet SPE-420 http://172.18.100.109
9 Camera 9 Bosch FLEXIDOME IP 5000i IR http://172.17.100.25
Used camera licenses: 6/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Camera 9
Resolution:
3072x1728
Record rate:
30 / s

New device can be inserted to the empty "slot" if its number of channels is the same or less then number of consecutive "not used" camera numbers.

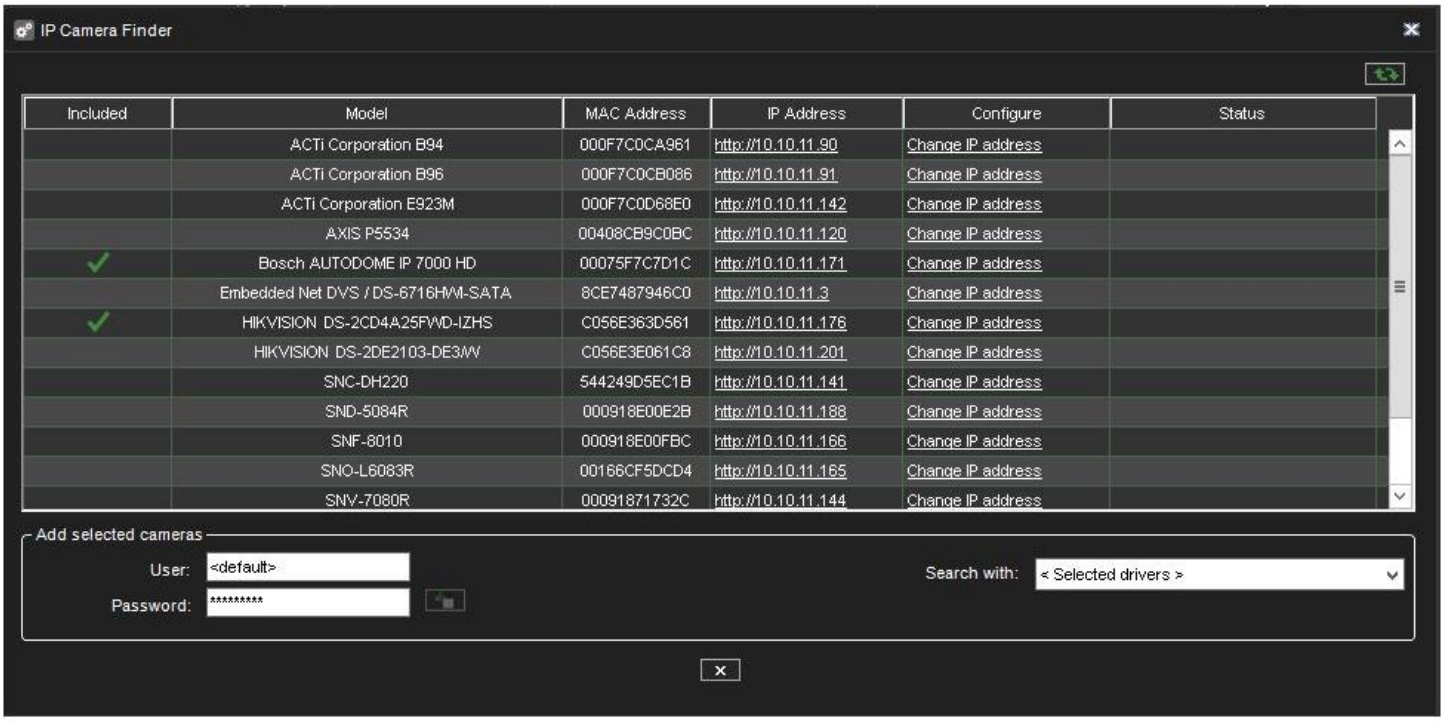
User can select channels that will be added during device acceptance. When he start device search and device is found, he will see the following dialog:

10.3.1.2 IP Camera Finder

1. Click the **IP camera finder**



The system will now scan the local IP network for active IP addresses and then communicate with each found IP address if it is a supported IP camera.
The resulting list is displayed after the search is complete.



Cameras can be selected from the list. Selecting multiple cameras is possible with SHIFT or CTRL keys.

1. Type the username and password for the cameras.
2. Click **Add Selected Cameras**.



3. The system adds the selected cameras to the system with the selected username and password.

4. If the system cannot add some of the selected cameras, an error status message is displayed in the **Status** column; you can repeat steps 4-5 for the cameras with the correct credential information.

5. Click **Close** to exit the **IP camera finder**.

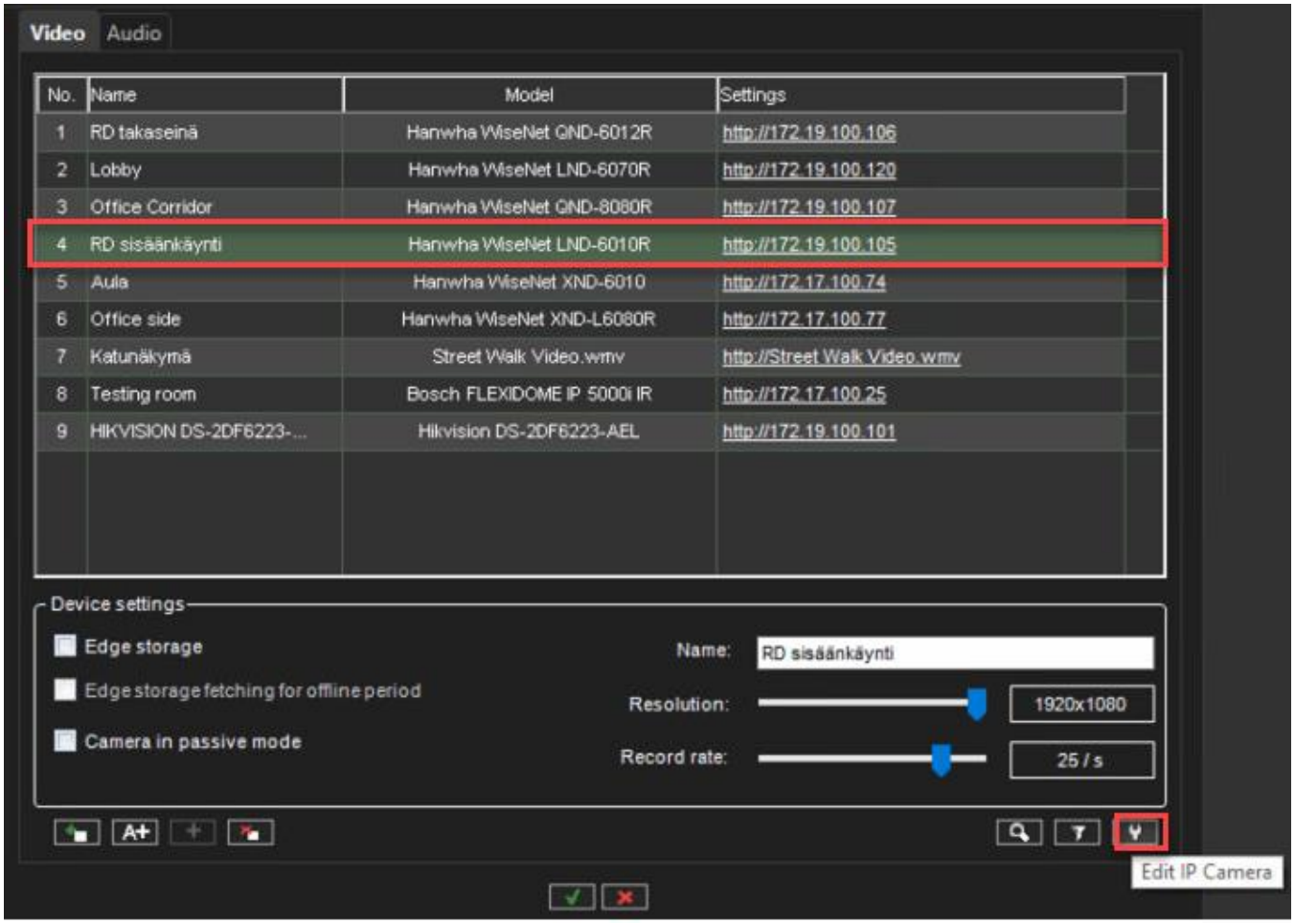
6. Save the Hardware settings by pressing **OK** in the list:



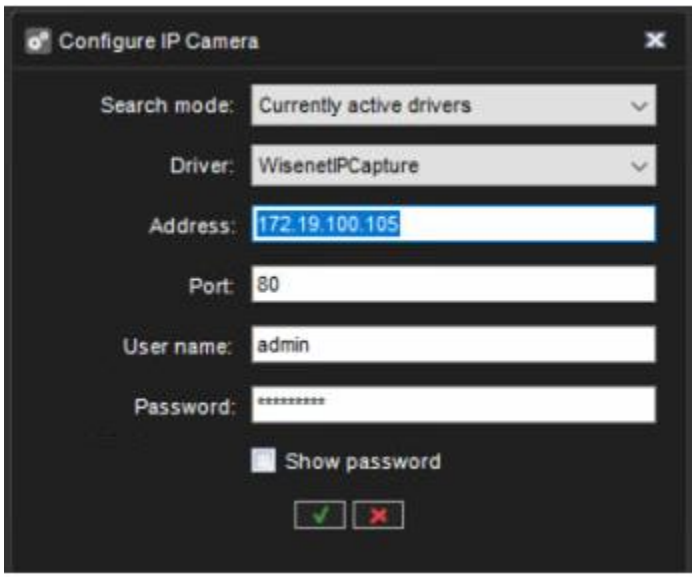
10.3.1.3 Edit IP Camera

Edit IP Camera allows users to change **camera address, port, username or password**

1. Select camera from the list
2. Click **Edit IP Camera**



1. Do needed modifications
2. Click Ok to confirm changes



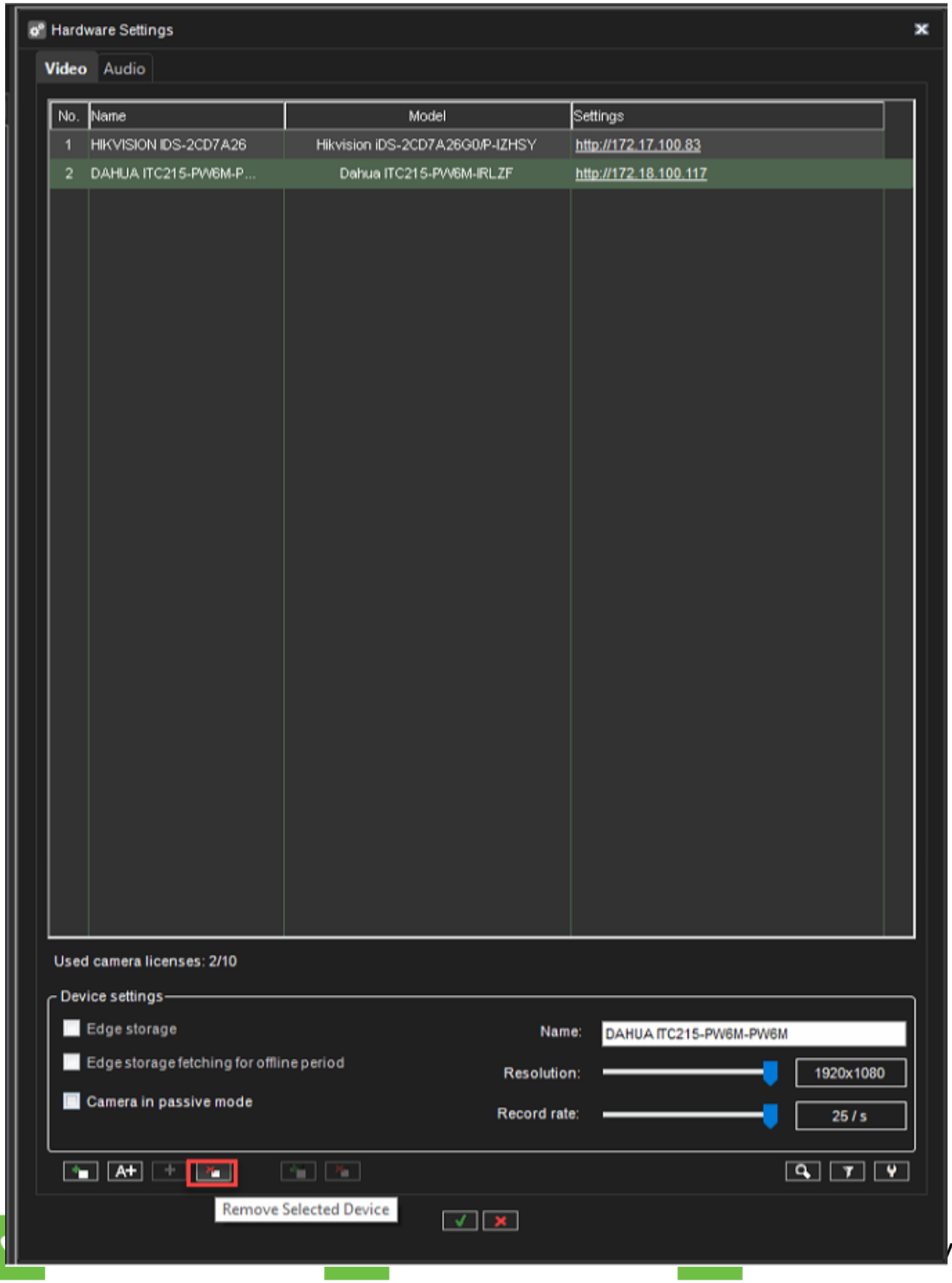
10.3.1.4 Removing IP cameras and encoders

If you open the "**Hardware Settings**" dialogue in System Manager, you will see 2 buttons below the list of cameras:

- The "**Add video channel to the selected device**" button
- The "**Remove video channel from the selected device**" button

10.3.1.4.1 To remove an IP camera:

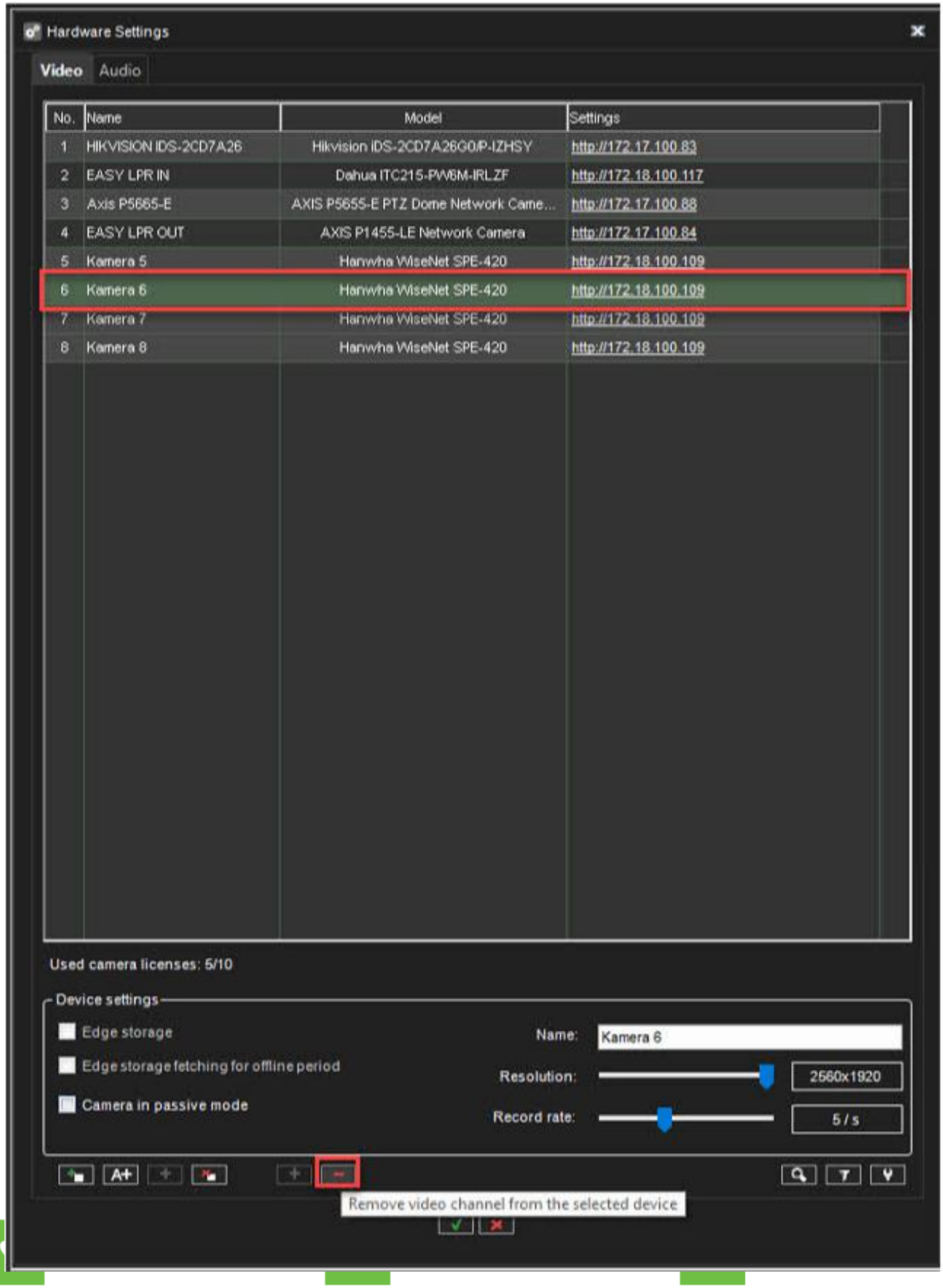
1. Select camera from the list on the **Video** tab
2. Click **Remove Selected Device** in the lower right corner of the tab.
3. When asked to confirm the deletion, click **OK**.


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1
HIKVISION IDS-2CD7A26
Hikvision iDS-2CD7A26G0/P-IZHSY
http://172.17.100.83
2
DAHUA ITC215-PW6M-P...
Dahua ITC215-PW6M-IRLZF
http://172.18.100.117
Used camera licenses: 2/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
DAHUA ITC215-PW6M-PW6M
Resolution:
1920x1080
Record rate:
25 / s
A+
Remove Selected Device

10.3.1.4.2 To remove video channels from the encoder or multi-lens cameras:

1. Select the correct channel from the list
2. Click **Remove video channel from the selected device**
3. Click **OK**

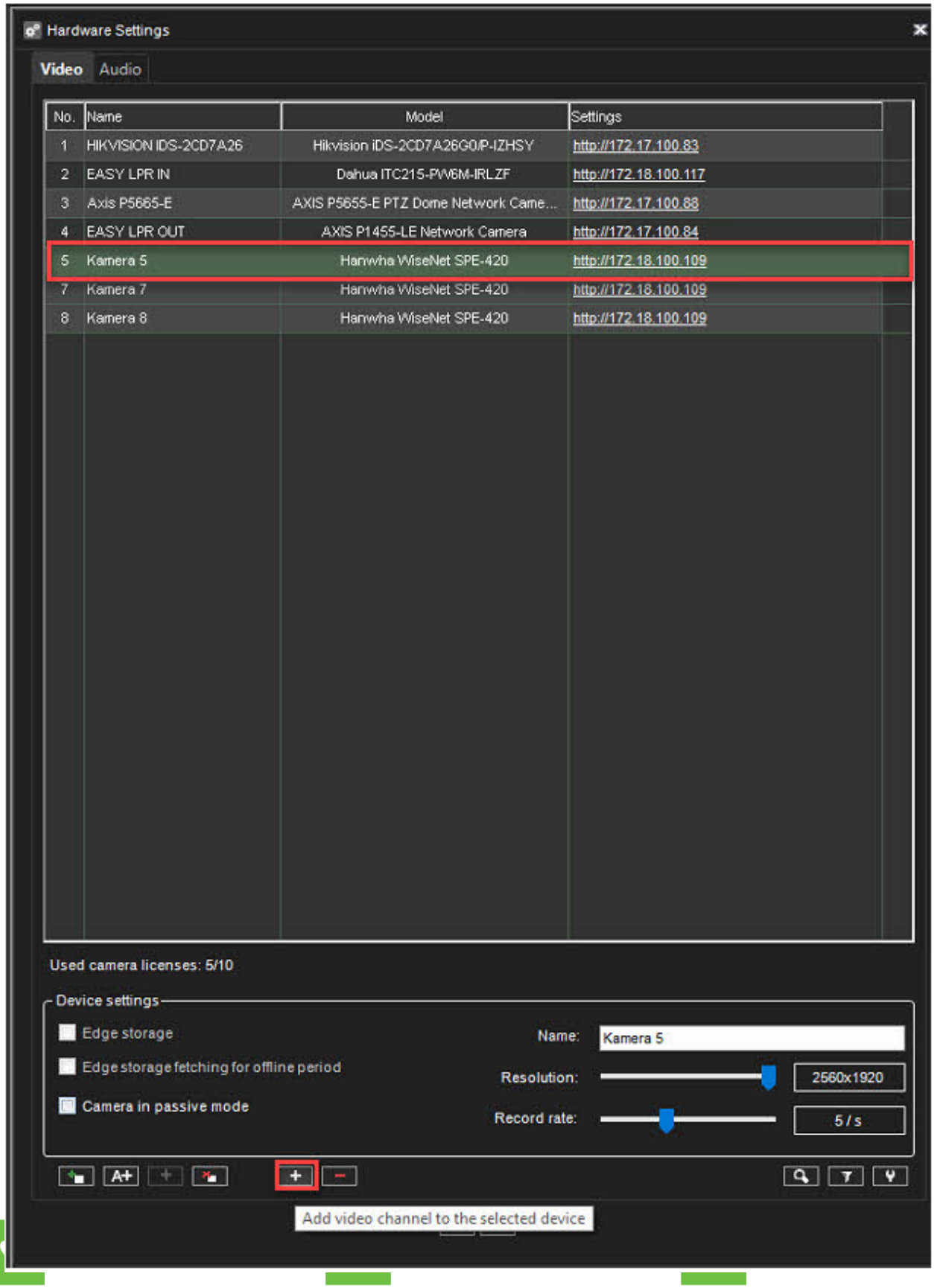
MIRASYS


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 EASY LPR IN Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 EASY LPR OUT AXIS P1455-LE Network Camera http://172.17.100.84
5 Kamera 5 Hanwha WiseNet SPE-420 http://172.18.100.109
6 Kamera 6 Hanwha WiseNet SPE-420 http://172.18.100.109
7 Kamera 7 Hanwha WiseNet SPE-420 http://172.18.100.109
8 Kamera 8 Hanwha WiseNet SPE-420 http://172.18.100.109
Used camera licenses: 5/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Kamera 6
Resolution:
2560x1920
Record rate:
5 / s
Remove video channel from the selected device

10.3.1.4.3 To add video channels to the encoder or multi-lens cameras:

1. Select the correct device from the list
2. Click **Add video channel to the selected device**
3. Click **OK**

MIRASYS


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1
HIKVISION IDS-2CD7A26
Hikvision iDS-2CD7A26G0/P-IZHSY
http://172.17.100.83
2
EASY LPR IN
Dahua ITC215-PW6M-IRLZF
http://172.18.100.117
3
Axis P5665-E
AXIS P5655-E PTZ Dome Network Came...
http://172.17.100.88
4
EASY LPR OUT
AXIS P1455-LE Network Camera
http://172.17.100.84
5
Kamera 5
Hanwha WiseNet SPE-420
http://172.18.100.109
7
Kamera 7
Hanwha WiseNet SPE-420
http://172.18.100.109
8
Kamera 8
Hanwha WiseNet SPE-420
http://172.18.100.109
Used camera licenses: 5/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Kamera 5
Resolution:
2560x1920
Record rate:
5 / s
Add video channel to the selected device

10.3.1.5 Replacing an existing IP camera in the Mirasys VMS

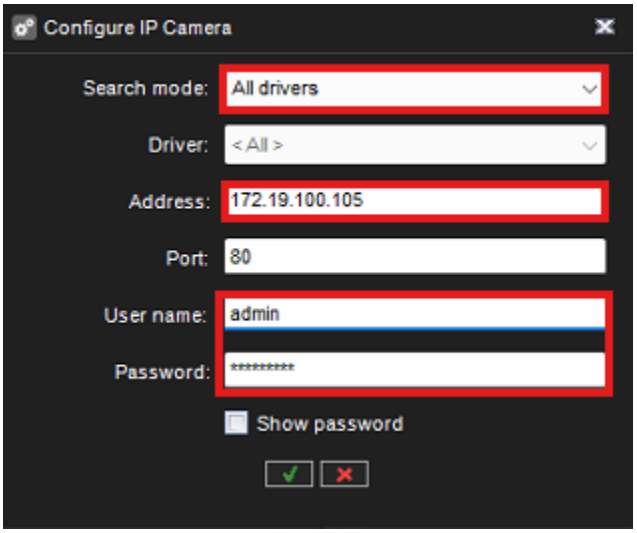
If the new camera uses a different driver than the current one, the old camera must be removed before adding the new camera.

To replace the existing IP camera with a new one, complete the following steps:

- Add an existing IP camera address for the new IP camera
- Set the same username and password for the new IP camera
- Connect the camera to the network
- Select the camera from the **Hardware** list
- Click **Edit IP camera**



1. Select **Search mode: All drivers**
2. Check that the camera has the correct IP address
3. Check that the username and password are correct
4. Click **OK**
5. Select the correct driver from the **Accept IP camera driver** selection
6. Click **OK**



10.3.2 Audio Hardware

If a camera has compatible IP audio input or output channels, you can add them simultaneously when adding the camera through the automated search tools.
After IP audio inputs and outputs for a camera have been added to the system, they can be edited and removed through the **Audio** tab.

10.3.2.1 Information shown:

1. Camera hardware ID
2. Channel type(Input)
3. Channel type(Output(
4. Device model



10.3.3 Device Settings

10.3.3.1 Edge Storage

The Edge storage functionality enables uninterrupted recording during network blackouts. The recorder monitors the cameras' online/offline states and gets data for the period when cameras were detected to be offline. The information is stored in the SQL database. In practice, in a network blackout, the video feed can be stored on an SD memory card on the camera.

Once the network connection has been re-established, video is transmitted from the camera's SD card to the server. Please refer to the camera manufacturer documentation to see what cameras support the feature.

Edge storage must be enabled in the device settings. This feature is configured solely through the camera's configuration utility. Please refer to the camera's documentation for instructions on enabling Edge storage.

10.3.3.2 Edge storage fetching for offline period

When this option is enabled, edge storage fetching is performed in cases where the recorder was not working for a specific time period, and after the recorder starts, it attempts to get data from cameras for the period when the recorder was down.

10.3.3.3 Camera in passive mode

- If multiple servers have the same camera configured, then one should be made **Active,** and the others should be **Passive**.
- This way, only the Active server settings are communicated to the camera.

10.3.3.4 360 Camera

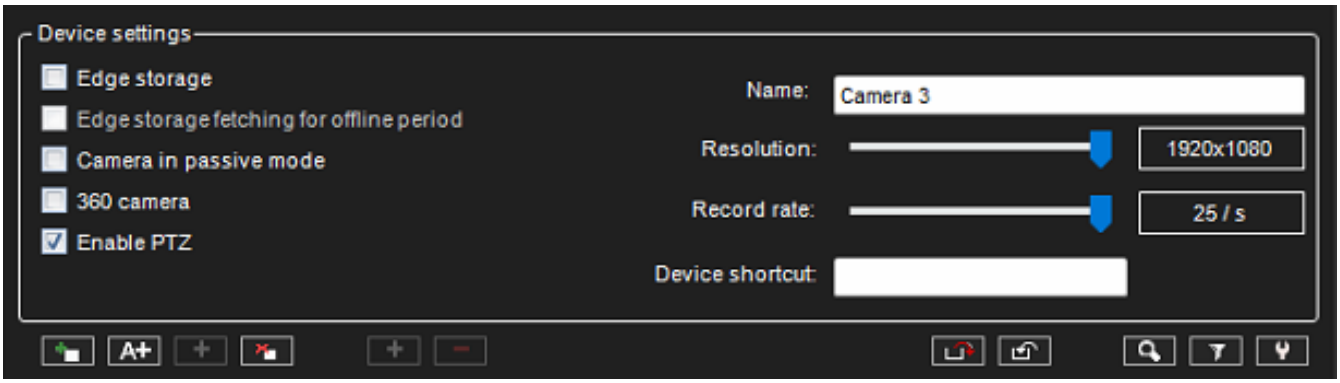
When this setting is enabled, the camera is registered as a 360 camera.

10.3.3.5 Enable PTZ

PTZ capabilities can be turned on or off for the camera with this option. This setting is visible only when the camera is detected to be a PTZ camera.

10.3.3.6 Camera information

Camera name, resolution, record rate, and device shortcut can be set directly from the **Video** tab.



10.3.4 Adding cameras by using CSV file

VSM camera settings can be exported to a CSV file and imported to VMS from a CSV file. This allows administrators to make bulk changes to camera settings and then import changed settings to the VMS system. It is also possible to add new cameras to VMS using this functionality.

10.3.4.1 CSV file import and export

System Manager Hardware settings have the following buttons for exporting camera settings to a file and importing camera settings from a file in CSV format.



10.3.4.1.1 CSV file format

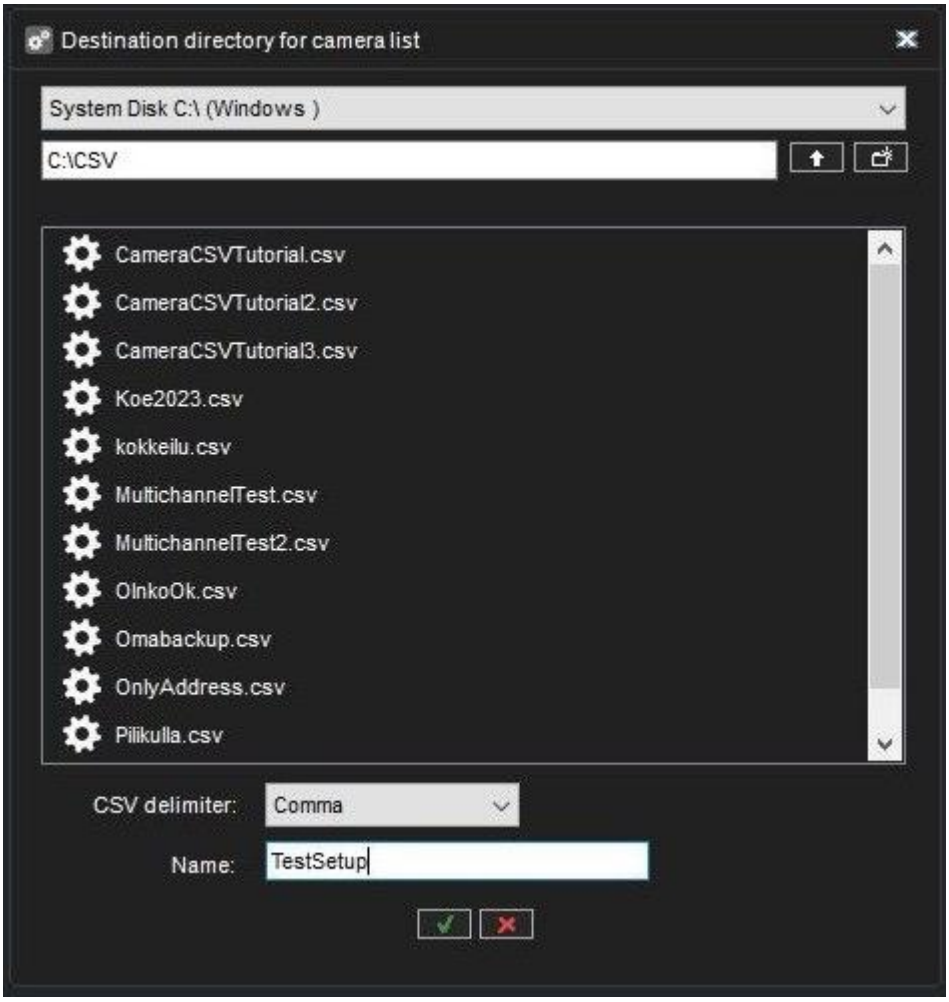
CSV file format for each camera uses the following header names.

- **Name** - Name of the camera channel.
- **Number** - Number of the camera channel on the VMS server.
- **Description** - Camera channel description.
- **AdmDescription** - Camera channel administrative description.
- **Address** - Camera device address.

- **Port** - Camera device port.
- **UserName** - Camera device user name.
- **Password** - Camera device password.
- **Driver** - Driver name / native (search from all available native drivers) / ONVIF (use of ONVIF driver). Logic uses the first driver that includes the given driver name string. For example, axis → NewAxisIPCapture.
- **Channel** - Used channel of the driver if the device supports more than one channel. With one-channel devices, this can be left empty.
- **IsInUse** - Is the camera in use?
- **IsAudioInUse** - Is audio in use if the driver supports it?
- **IsIOInUse** - Is I/O in use. This has meaning only when exporting CSV files. At import, I/O is used automatically if the device supports it.
- **Is360** - Is 360 camera.
- **Framerate** - Recording stream frames / second rounded to close available value. The header for other streams: Framerate1, Framerate2, Framerate3.
- **Resolution** - Recording stream resolution in format width x height (for example 1920x1080) rounded to close available value. For other streams: Resolution1, Resolution2, Resolution3.
- **Codec** - Recording stream used compression codec. Rounded to close available value: JPEG, MPEG, H264, WMC9, PARSE, H265, MXPEG. For other streams: Codec1, Codec2, Codec3.
- **Quality** - Recording stream compression quality rounded to close available value in range 1-100. For other streams: Quality1, Quality2, Quality3.
- **Bitrate** - Recording stream bit rate rounded to close available value. For other streams: Bitrate1, Bitrate2, Bitrate3.

10.3.4.1.2 Export

Users can select the folder where the camera settings CSV file is exported to and give the name of the file. Users can also define the delimiter that is used in the CSV file.



When the export is successful, a blinking green icon is shown. In error, a blinking red icon is shown.

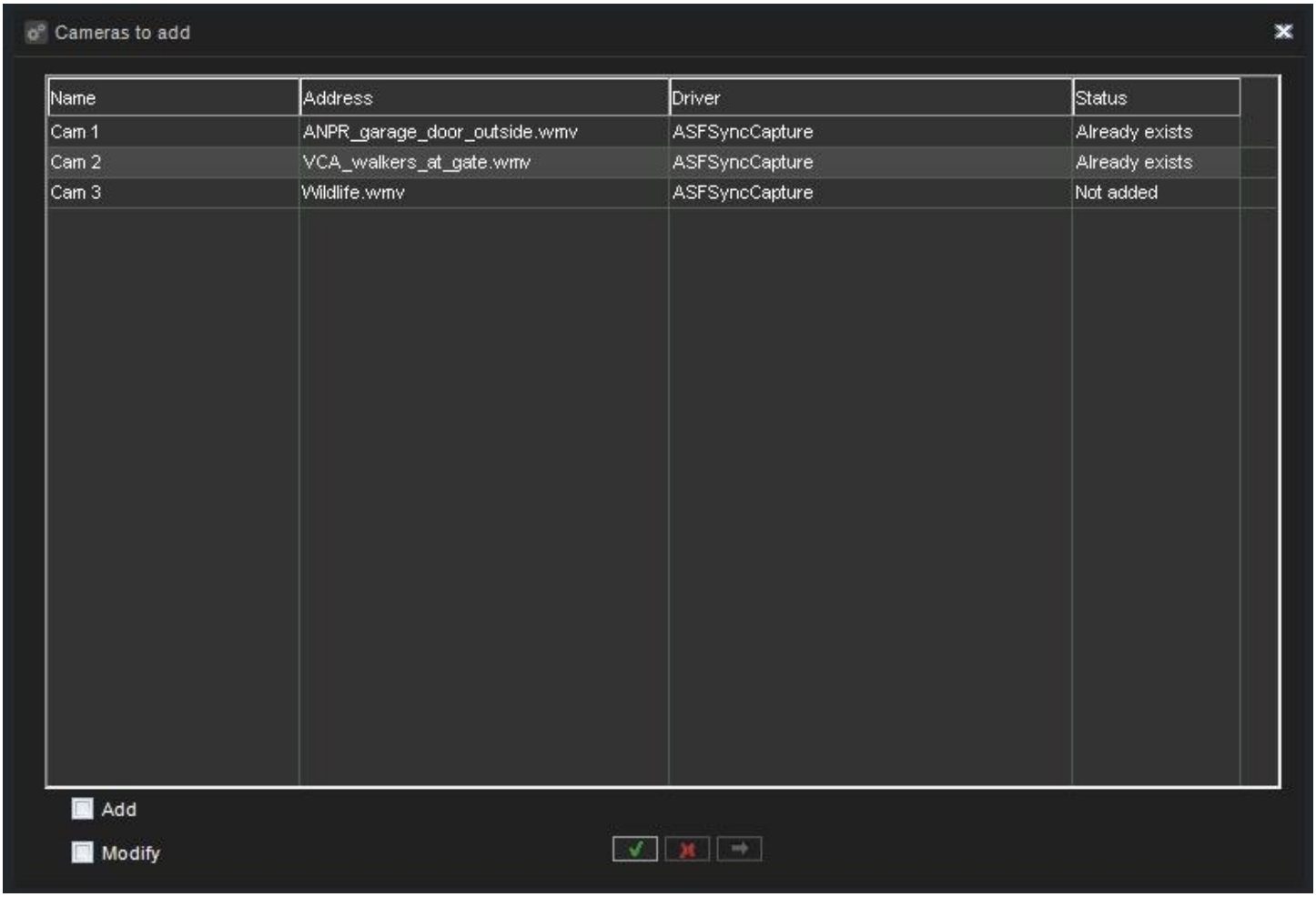
10.3.4.1.2.1 Import

When the user clicks the import button, the select file dialog is shown to select the CSV file to import. When the file is selected, the camera adding view is shown if CSV file parsing and validation are done successfully.

The following validation rules are used when parsing imported CSV files.

- CSV file column delimiter is a comma (,) or semicolon (;).
- The order of the header names (i.e. column order) is free.
- Unused header names (i.e. columns) can be left off.
- Only the Address header name is mandatory. If it is missing, CSV file data is not accepted.
- If some property names and data do not exist, an internal default value is used.

- For validation errors and warnings, a message popup is generated, and more information is printed in the System Manager log.



Cameras imported via CSV can be set to passive mode as part of the import process. System Administrators can specify this setting within the CSV file.

Multiple streaming state (enabled or disabled) can be used when this is supported by the camera, as well as bitrate mode for bitrate.

Audio channels will not be automatically added if it is not added when importing CSV files.

Please note that when importing multi-channel devices with a set channel number in a “Number” column, a channel number for each device has to be manually defined. It is also necessary to assign the recorder’s channel number (from column Number) to the device channel number (Channel column). This can be resolved by not including the Number and Channel columns.

After the CSV file validation and parsing, the status column informs if the camera is already added to the system (Already exists) or if it is the new camera (Not added).

Add and Modify check boxes appear if there are modifications to existing cameras and new camera configurations in the imported CSV file. These options can be used to select if cameras from the CSV file are added and/or modified.

Execute button is enabled when there are cameras to be added or modified. By clicking the execute button, settings from the CSV file are applied (modified and/or added) to the current settings.

After the settings apply, the status for each camera is updated, the Dialog can be closed after the settings apply by clicking the ok button or from the cancel button before the settings apply.

Modified camera settings and/or added cameras are applied to the VMS server once the hardware settings are saved.

10.4 Adding and Removing VMS Servers

You can have (depending on the license) from 1 to unlimited servers in one system.
One server should not belong to more than one Main Server (SMServer).
You can specify a password for each server.
The system will prompt for the password if someone tries to add the server to another system.

10.4.1 To add a server to the system(recording server):

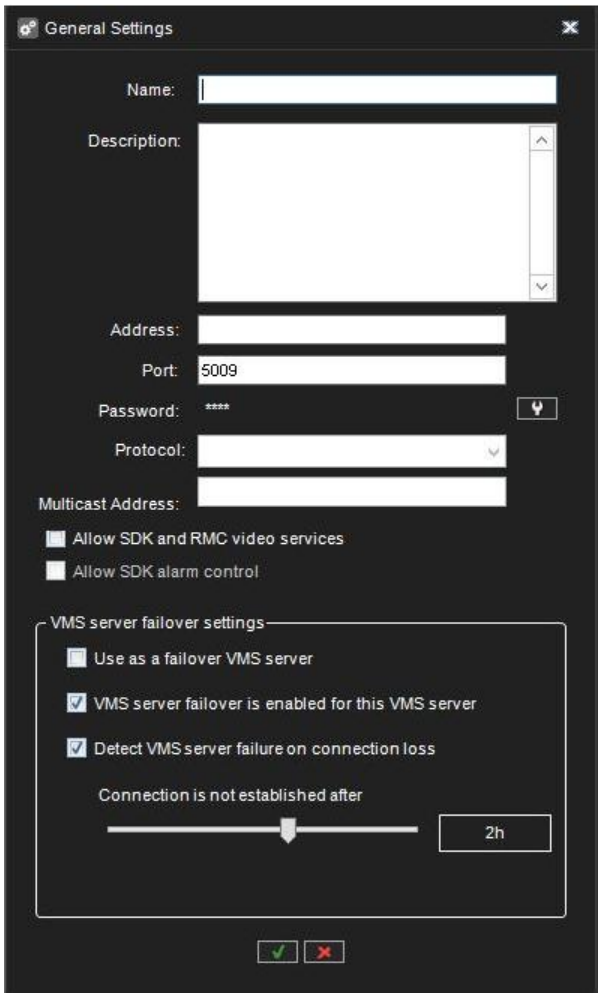
1. Open the **VMS Servers** tab



2. Click Add VMS Server



3. The **General Settings** dialogue box is shown.
4. Type name for the server
5. Enter a description, if needed
6. Type the IP address or DNS name of the server.
7. Enter the password for the server, if needed
8. Click **OK**. The server and the devices connected to it (cameras and audio channels) are added to the list.
    a. Note: *If the server is password-protected, the system prompts for the password.*



10.4.2 To remove a server from the system:

1. Select the server that you want to remove.
2. Click Remove **VMS Server**



3. Click **OK** to confirm.

10.4.3 Connection status:

If the connection to the server is lost, the System Manager application will automatically try to connect to the server.

10.4.4 NOTE:

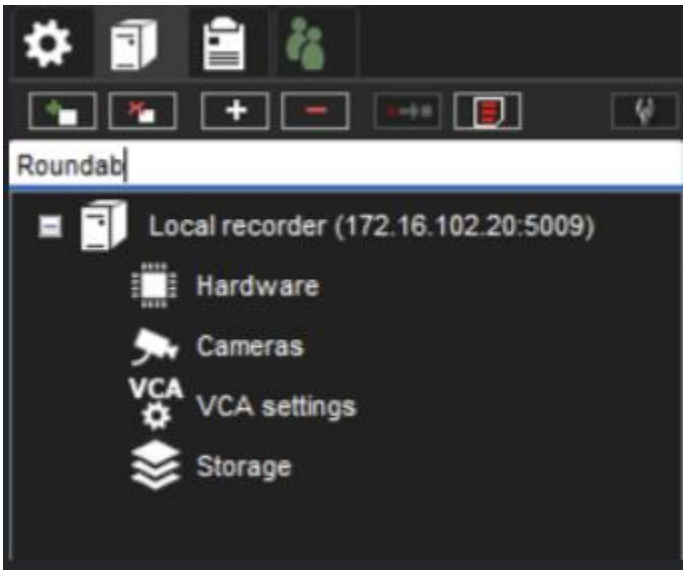
When you have added Mirasys VMS as a subserver, please do the following actions:

1. Change Admin user password using a subserver System Manager
2. Disable SMServer service from the subserver

10.5 Search in VMS Server settings

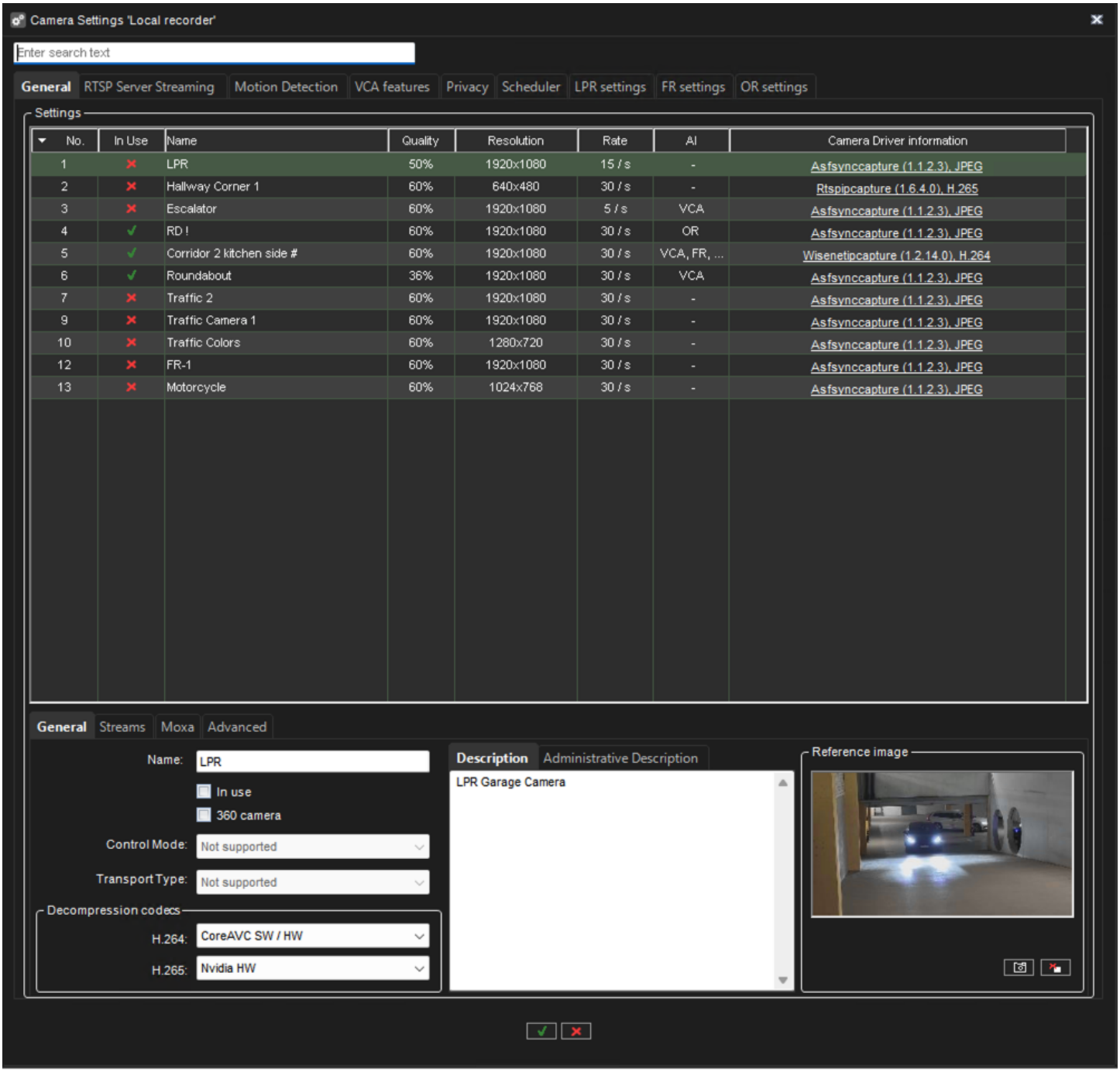
10.5.1 Search in the VMS Server settings tab

In the VMS Server settings tab, you can search for a specific device. For example, if you have several recorders and are looking for a specific camera, like "Roundabout camera", and you need to narrow down in what recorder it is, you can search in the recorder tab and it will then only display the VMS server, and underneath only the settings where you can find the Garage camera.



10.5.2 Narrow down the search from the VMS Server settings tab

If you open, for example, camera settings under the Search in VMS Server settings tab, the Roundabout camera from the example above is already filtered out. The search can be reset in the individual settings tabs.

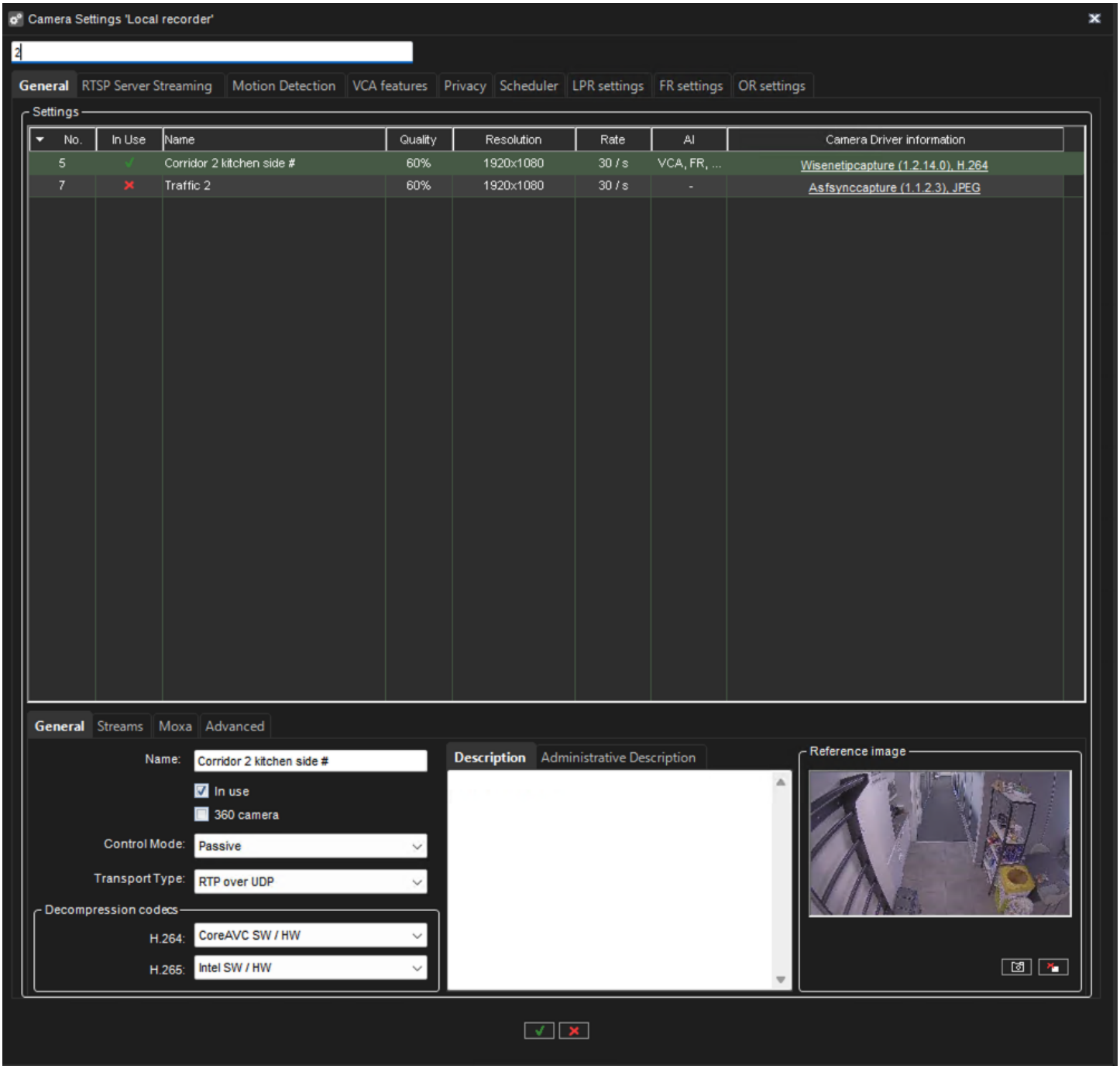


10.5.3 Search in individual settings

Within individual settings, you can search for a device. There is a search bar in the following settings:

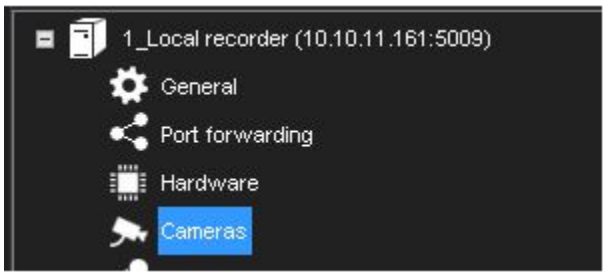
- Camera settings

- Audio settings
- Hardware settings
- Digital I/O settings
- Storage settings
- Alarm settings
- Text channel settings



10.6 CAMERAS

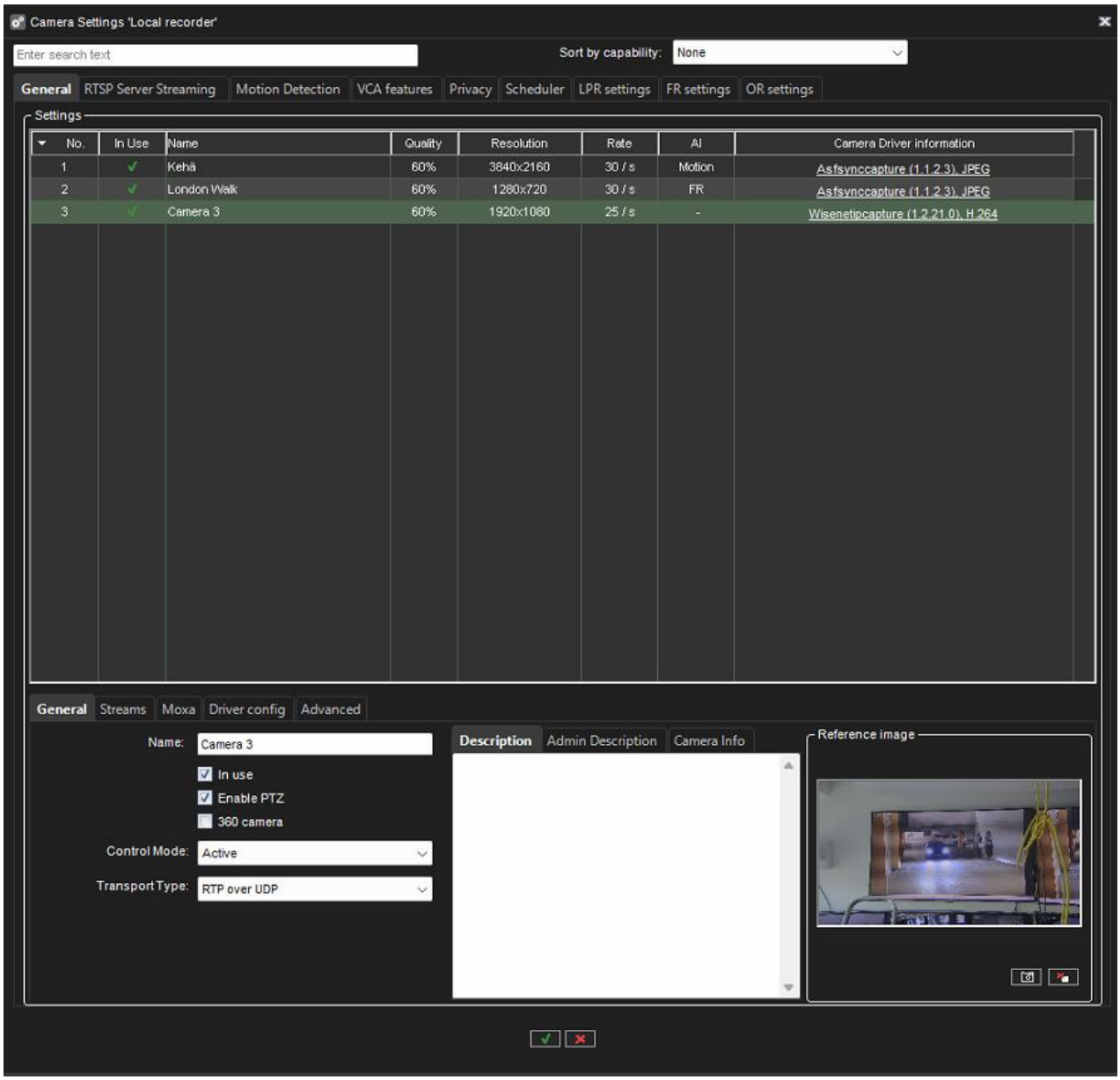
After the camera has been added to the server, the camera settings can be configured from the **Cameras** page.



10.6.1 Camera Settings contain settings for:

- General
- Motion Detection
- VCA features
- Privacy
- Scheduler

10.6.2 Camera settings



10.6.2.1 General settings

In General settings, the columns display the camera number, if the camera is in use, the camera name, quality, resolution, and rate, if the camera uses an AI service, which service, and which camera driver the camera uses. All columns can be sorted in ascending or descending order.

10.6.2.1.1 Name

The name of the camera. The system suggests the names like *Camera 1*, *Camera 2*, etc.

10.6.2.1.2 In Use

Clear this check box if no camera is connected to the camera input or if you want to disable the camera.

10.6.2.1.3 Enable PTZ

PTZ capabilities can be turned on or off for the camera with this option. This setting is visible only when the camera is detected to be a PTZ camera.

10.6.2.1.4 360 camera

This tells the Spotter client that the camera is a 360 camera, and Spotter will show the image de-warping options in the camera toolbar (if installed)

10.6.2.1.5 Control Mode

This setting has two options: Active (default) and Passive.
If multiple servers have the same camera configured, then one should be made Active, and the others should be Passive.
This way, only the Active server settings are communicated to the camera.

10.6.2.1.6 Transport Type

This setting controls how the media stream is transported from camera to server.
The available options are RTP over UDP (default) and RTP over RTSP.
If the camera seems to work poorly with one setting (for example, if there are holes in camera material or difficulty to get all frames from a camera), then the other set can be used.

10.6.2.1.7 Description

Here you can type a description of the camera shown to all users in the Spotter, given they have the user permissions to view this.

10.6.2.1.8 Administrative Description

Here you can type a description of the camera. The description will be shown in Spotter, given they have the user permissions to view this.

10.6.2.1.9 Camera Info

The “Camera info” tab has checkboxes for what should be automatically included in the Camera Info:

- VMS Server
- Server info
- IP address
- Camera model
- AI features used
- Resolution
- Frame rate settings

The information included by ticking the boxes for the camera will be automatically included in the Camera Description in Spotter for that Camera. All boxes are selected by default.

For the information to be shown in Spotter, permission must be given under User Group > Mirasys Spotter Enterprise role properties > Screen > Screen elements to **View Camera Info**.

10.6.2.1.10Reference image

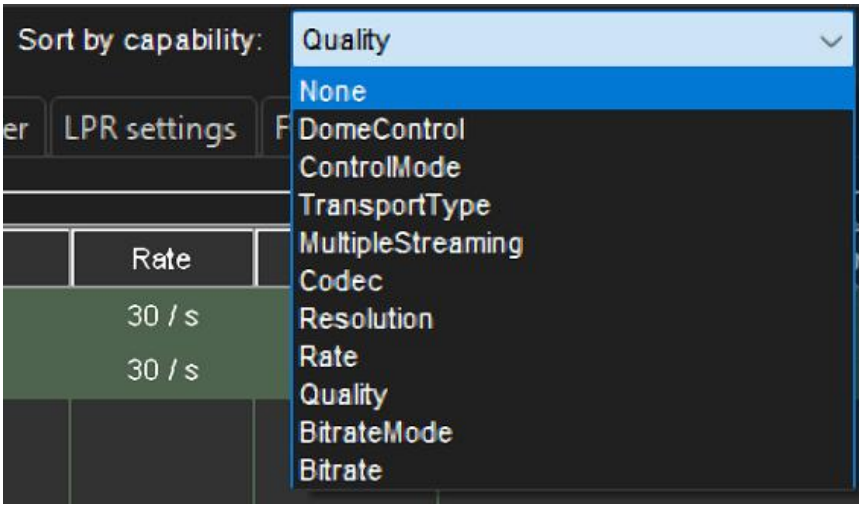
A reference image is an image captured from the camera, making it easier to identify the cameras.
In addition, in the Spotter program, the users can compare what they see in the video view against the reference image to ensure that the camera is pointed in the right direction.
To change the current reference image, click the Capture image button. To delete a reference image, click the Delete image button.

10.6.2.1.11Updating Camera Settings in bulk

Settings can be updated for multiple cameras simultaneously. This can be done by selecting multiple cameras (hold Ctrl and click the cameras in the list) and modifying the settings for one camera. Changes will apply to all selected cameras. Cameras that are updated simultaneously must share the same setting capabilities. Driver settings cannot be updated in bulk.

10.6.2.1.12Sort cameras by capability

Cameras can be grouped by capability in Camera Settings, which makes doing bulk updates for the settings easier. A grouping condition can be selected from the "Sort by capability" dropdown menu, and the cameras that fit the sorting criteria are selected from the list.



10.6.2.2 Streams

By default, Mirasys VMS receives recording quality stream from the camera.
Mirasys VMS server send recording stream by default to the Mirasys Spotter.



10.6.2.2.1 Codec

The codec is used for transmitting the video between the server and the client applications, and in the case of IP cameras, for transmitting the video between the IP camera and the server.
In the case of analogue cameras, the codec used by the system is JPEG.
In IP cameras, any codec supported by both the camera and the server software can be selected.
The codecs supported by the server software are JPEG, MPEG-4, H.264, H.265 and Mobotix MxPEG.

10.6.2.2.2 Bitrate mode.

This setting controls if the Variable bit rate (VBRMax) or Constant bit rate (CBR) is used.

10.6.2.2.3 Quality

Set this value between 0%-100%. A higher value means better image quality but also a large image data size.
To decrease the image data size, set the value lower. However, setting the value lower also decreases the quality of the images.
50% is usually sufficient. For wireless and low bandwidth connections, select 0%.

10.6.2.2.4 Resolution

For automatically configured IP cameras, the exact image resolutions supported by the camera model are displayed.

10.6.2.2.5 Record rate

The record rate defines how many frames the camera sends to the VMS and how many frames are recorded.
The maximum rate depends on the video standard and the camera type.
Multiple streaming (multi-streaming)

10.6.2.2.6 Multi-Streaming

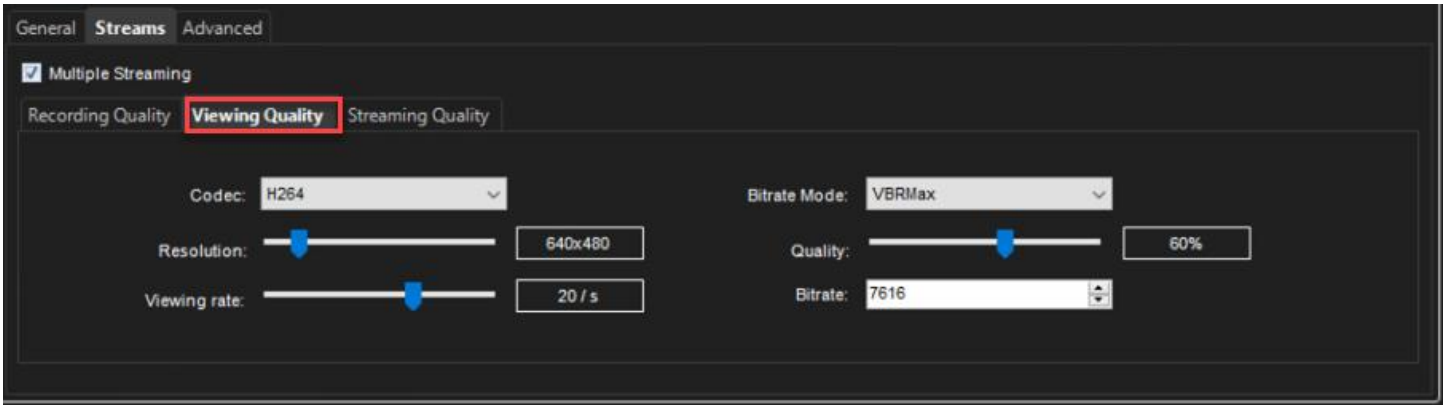
Multi-streaming enables separate feeds from a single camera.
The feature allows for separate streams to be used for recording and viewing.
The feature is available only if the camera and driver support it.

10.6.2.2.6.1 Recording Quality

By default, Mirasys VMS receives recording quality stream from the camera.
Mirasys VMS server send recording stream by default to the Mirasys Spotter



10.6.2.2.6.2 Viewing Quality



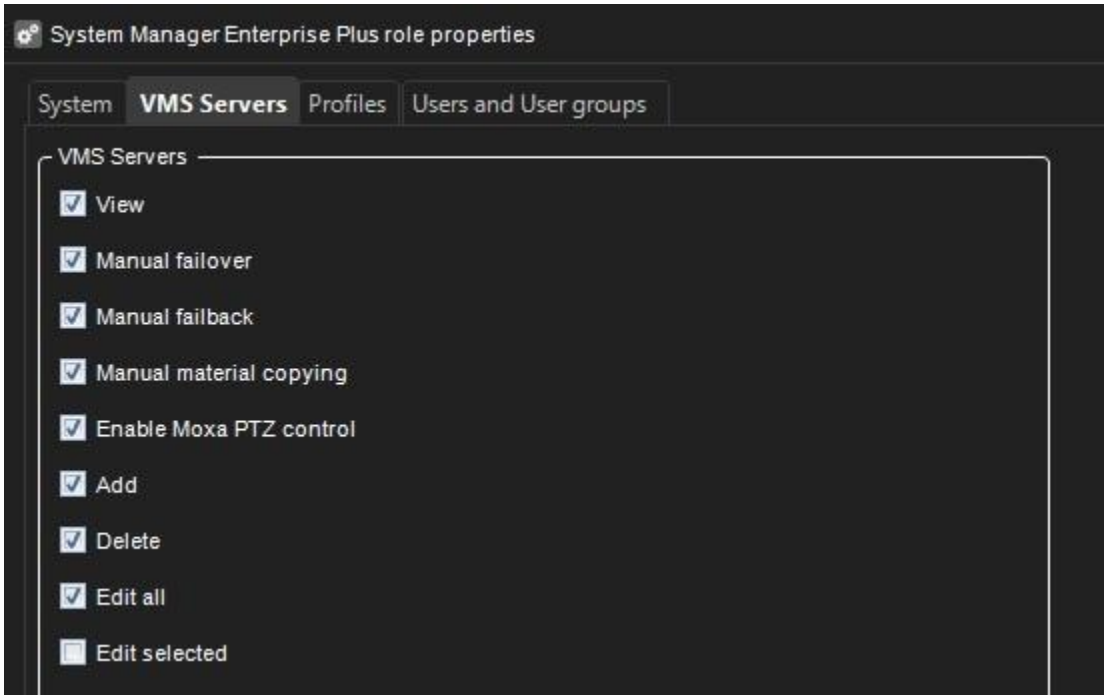
10.6.2.2.6.3 Streaming Quality



10.6.2.3 Moxa settings

10.6.2.3.1 Enable Moxa PTZ editing

In System Manager role properties / VMS Servers settings, Moxa PTZ settings editing for user group can be selected. If Enable Moxa PTZ control is not selected, Moxa PTZ settings under camera settings can be seen but those cannot be changed.



10.6.2.3.2 Moxa PTZ settings

In Camera settings, an additional Moxa settings tab is available for those cameras that have configured Moxa Ptz driver settings or if Moxa editing is enabled for users user group.

10.6.2.3.2.1 Device

Enable Moxa PTZ settings for the camera

- If the camera does not have PTZ settings, open the device and PTZ control tab pages with default values.
- If the camera has Moxa PTZ settings and **Enable** is not selected, the settings saving removes Moxa PTZ settings from the camera

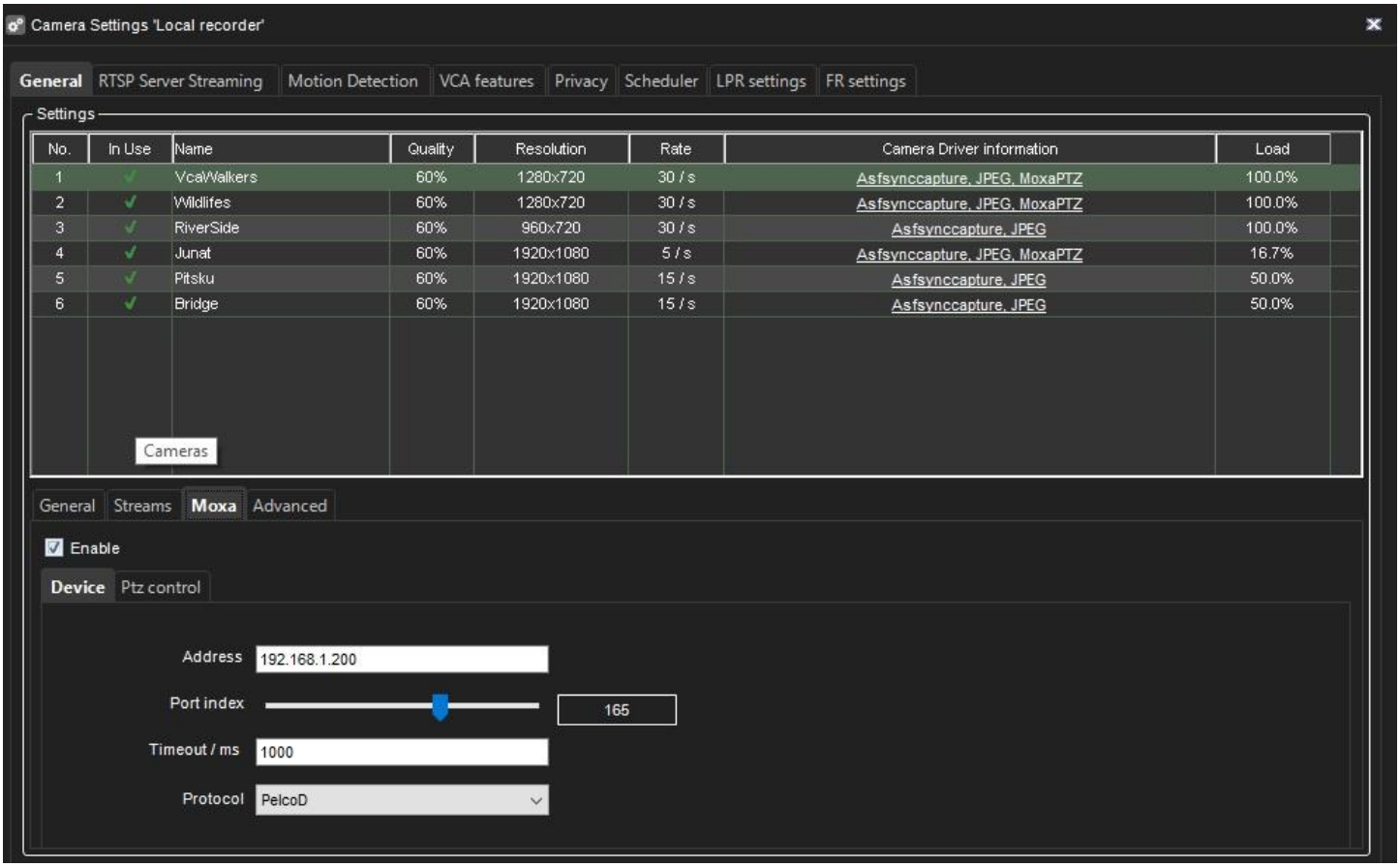
Address enter IP or DNS address of MOXA device.

Port index is the index of the serial port (1 - 255) in the MOXA device where the PTZ camera is connected.

Timeout/ms is the timeout in milliseconds for communications with MOXA device (5000 ms as default)

Protocol is the communication protocol with the PTZ camera from the following enumeration:

- { “PelcoD”, “BoschOSRD” }
    - Default value is “PelcoD“



10.6.2.3.2.2 PTZ control

Camera index - address of PTZ analog camera which is set in camera (usually it is hardware jumpers) (0 - 255)

Baud rate - serial port baud rate in bits per second. MOXA supports following set of baud rates:

- { 50, 75, 110, 134, 150, 300, 600, 1200, 2400, 4800, 6400, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 }.
- Default value is 38400 bps.

Data bits - (byte) - value from the following set:

- {5, 6, 7, 8 }
- Default value is 8.

Stop bit - (byte) - value from the following set:

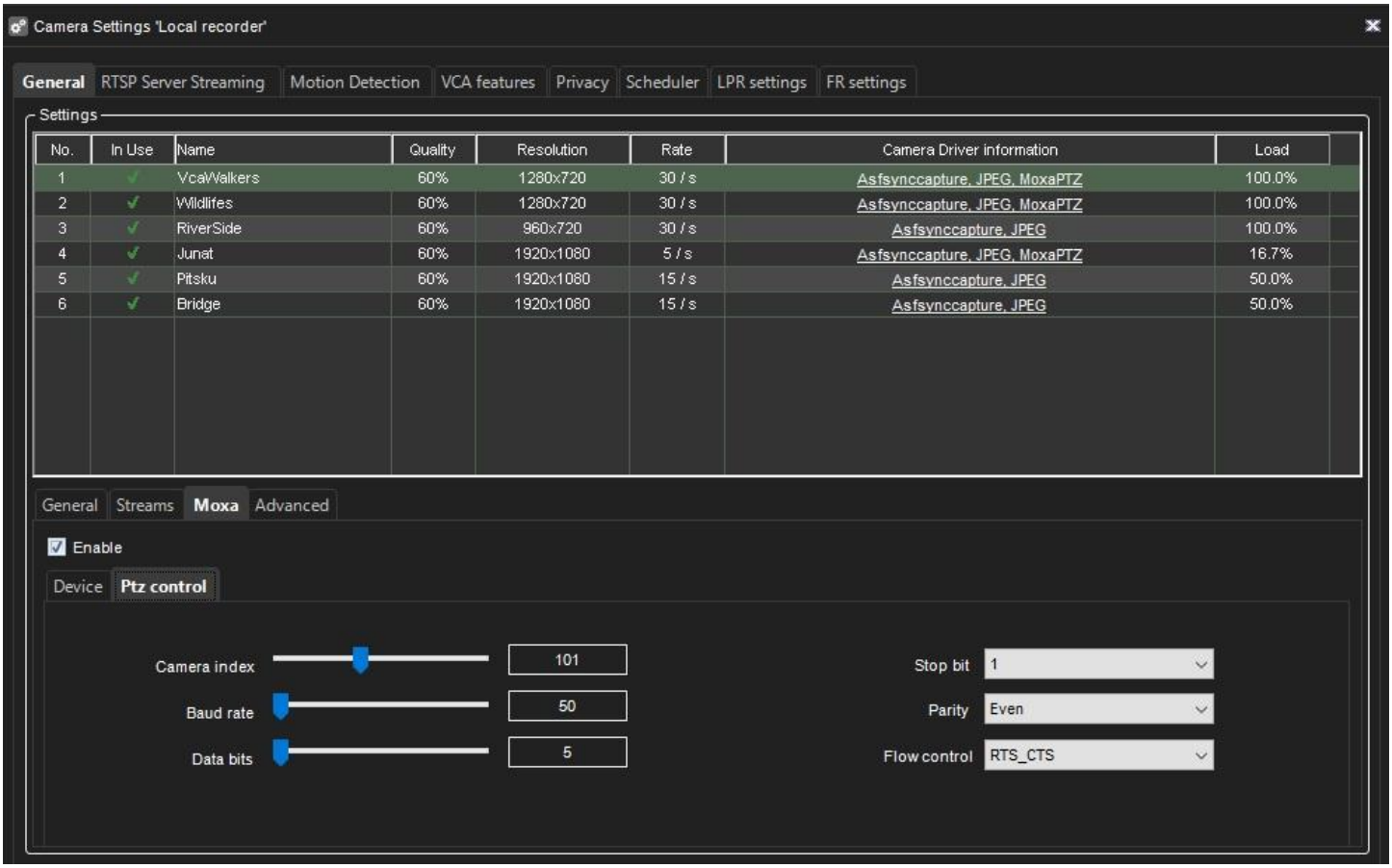
- { 1, 2 }
- Default value is 1.

Parity - value from the following enumeration:

- { “None” = 0, “Even” = 1, “Odd” = 2, “Mark” = 3, “Space” = 4 }
- Default value is “None“

Flow control - value from the following enumeration:

- { “None” = 0, “RTS / CTS” = 1, “XON / XOFF” = 2, “Both” = 3 }
- Default value is “None“



10.6.2.4 Driver config

This tab contains camera or driver-specific unique settings. A driver update may bring additional values to this tab. Selecting multiple cameras is possible with SHIFT or CTRL keys.
Please note that if you select more than one camera, you cannot set parameters not supported by all selected cameras.

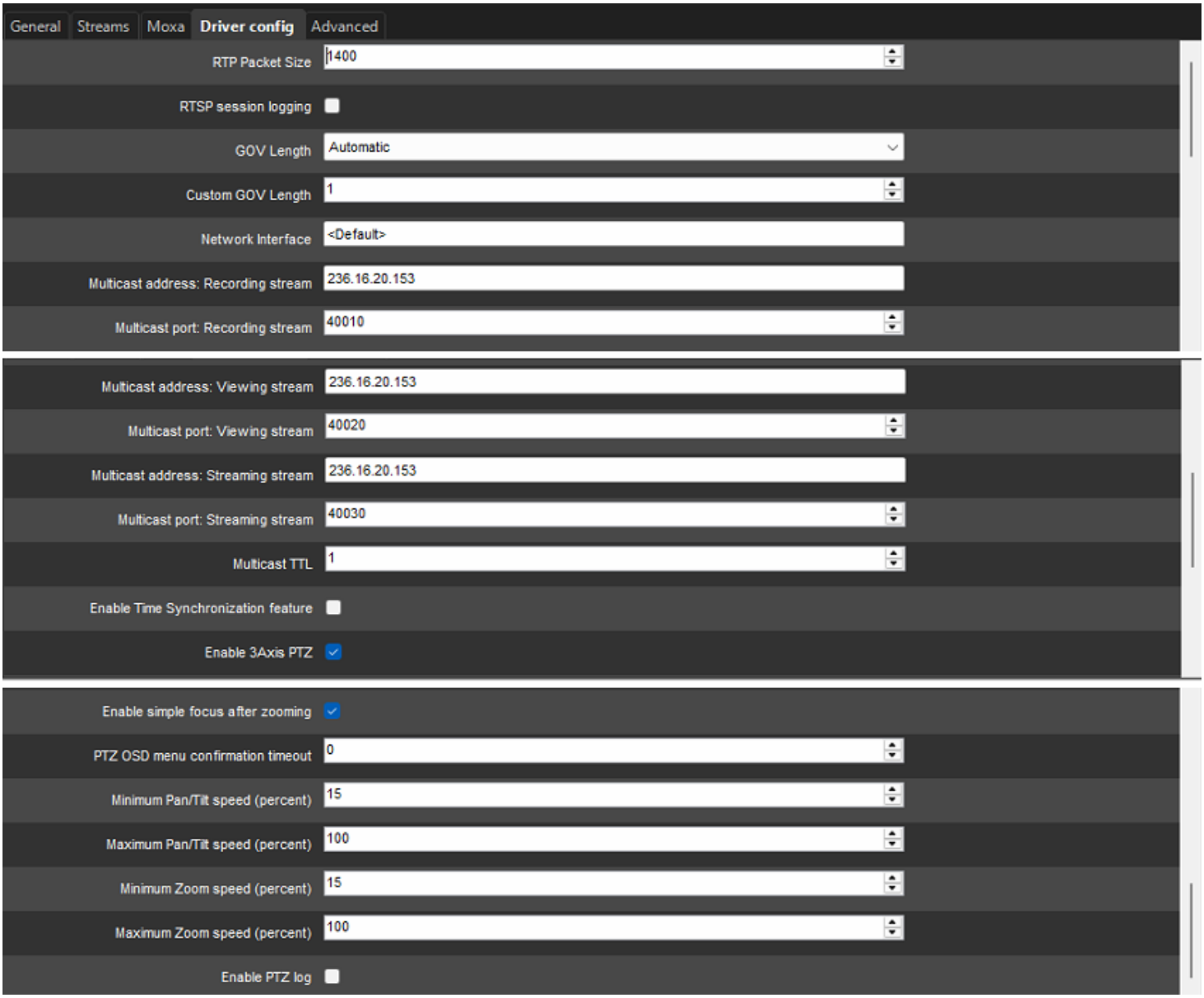
10.6.2.4.1 Configurable values

- RTP Packet Size

- RTSP session logging
- GOV Length
- Custom GOV Length
- Manage privacy mask by the driver
- Network interface
- Multicast address: Recording stream
- Multicast port: Recording stream
- Multicast address: Viewing stream
- Multicast port: Viewing stream
- Multicast address: Streaming stream
- Multicast port: Streaming stream
- Multicast TTL
- Enable Time Synchronization feature
- Enable 3-Axis PTZ
- Enable simple focus after zooming
- PTZ OSD menu confirmation timeout
- Minimum Pan/Tilt speed (percent)
- Maximum Pan/Tilt speed (percent)
- Minimum Zoom speed (percent)
- Maximum Zoom speed (percent)
- Enable PTZ log

Adjusting Pan/Tilt and Zoom speed is possible for the following camera drivers:

- ONVIF
- Bosch
- Hanwha
- Axis



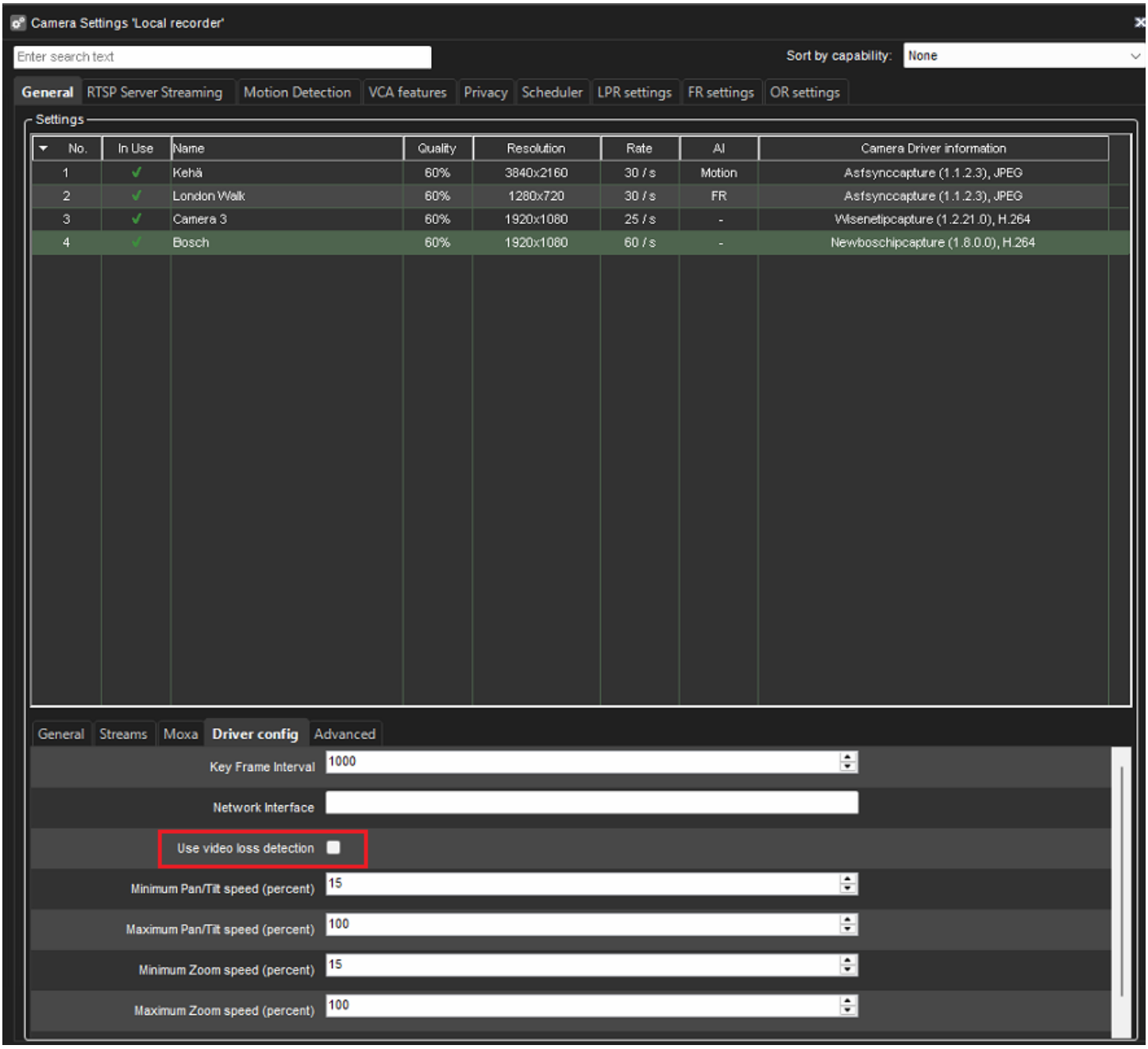
10.6.2.4.2 Signal Lost Event in Bosch Native Driver

A 'signal lost event' can be enabled in the Bosch native driver when utilizing Bosch encoders.

The setting is adjusted in the System Manager desktop application.

When a user sets this option to 'true,' it will remain so even after VMS updates or driver updates.

This ensures that user preferences for monitoring signal events are maintained consistently without reconfiguring settings post-update.



10.6.3 Advanced

This tab contains options for advanced camera settings.

10.6.3.1 Decompression codecs

Codecs are used for encoding and decoding video data.

10.6.3.2 Keyboard shortcut

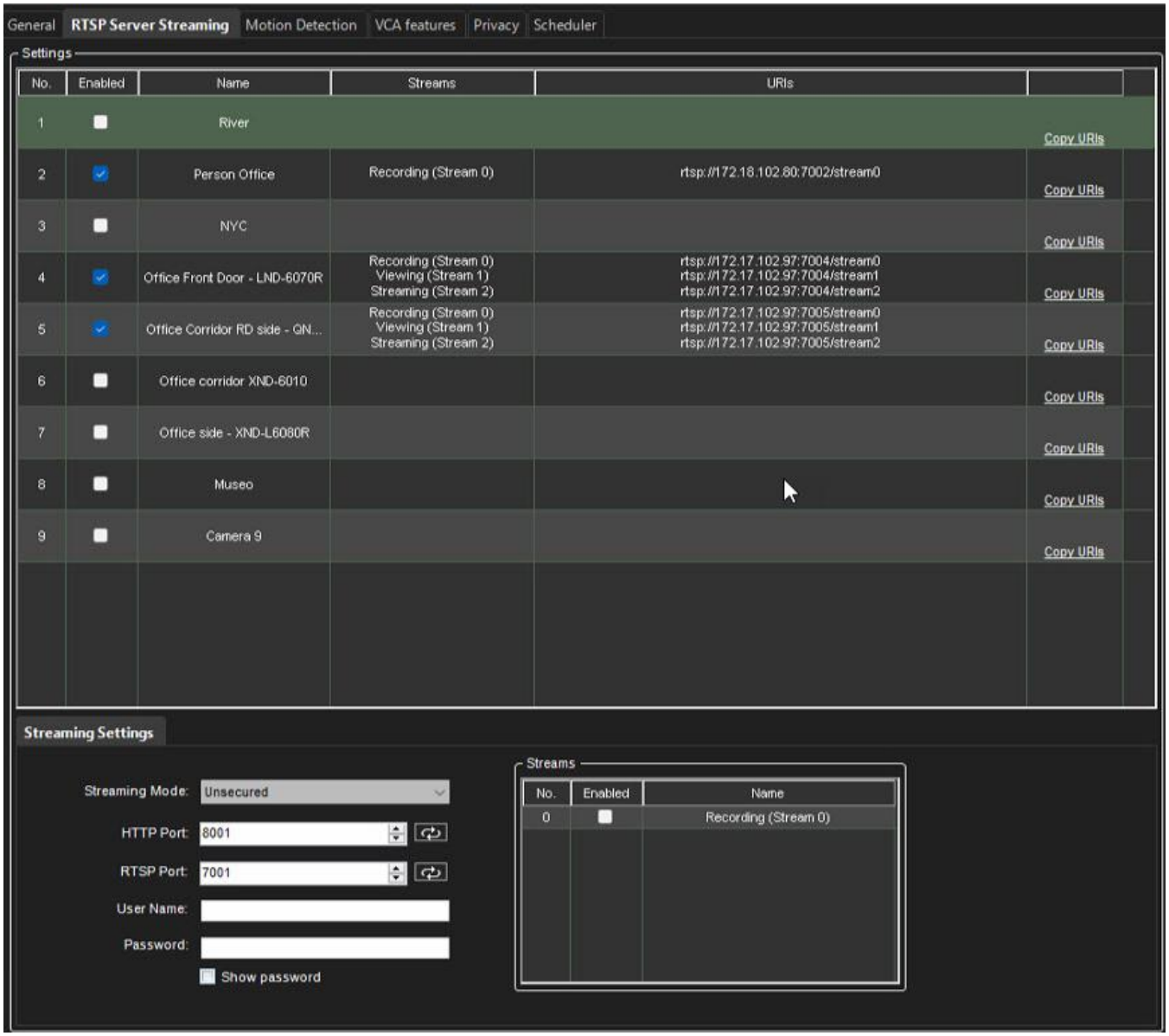
A keyboard shortcut can be set for a camera in the Device shortcut text field. The shortcut set in Camera settings is used as the default shortcut.

10.6.4 RTSP Server Streaming

RTSP/RTSPS server is used to stream video from the server to any third-party client that supports RTSP/RTSPS protocol.

10.6.4.1 Settings

- Camera number
- Enabled/disabled check-box - allow user to enable/disable streams from specified camera without changing the settings
- Camera name
- List of configured streams
- List of configured stream URIs
- Copy URIs link - to copy to clipboard URIs for specified camera



10.6.4.2 Streaming Settings

- Streaming mode - can be "Unsecured", Secured (UDP) and Secured (TCP). In secured mode instead of user name and password the certificate should be specified.
- HTTP Port - port for HTTP connection. Ports should be unique for each camera. User can use the "Test port" button to check if selected port is already used in recorder side.
- RTSP Port - port for RTSP connection. Ports should be unique for each camera. User can use the "Test port" button to check if selected port is already used in recorder side.

- Enabled/disabled check-box - allow user to enable/disable streams from specified camera without changing the settings
- User Name
- Password
- List of streams (multiple if multiple streaming is active) - each stream can be enabled/disabled separately

10.6.4.3 Enabling RTSP Server stream to the camera

1. Check the **Enabled** box from the selected camera
2. Select the line of the camera
3. Set **Streaming Mode**, **HTTP Port**, **RTSP Port**, **Username** and **Password**
4. Define used streams

10.6.5 Motion Detection

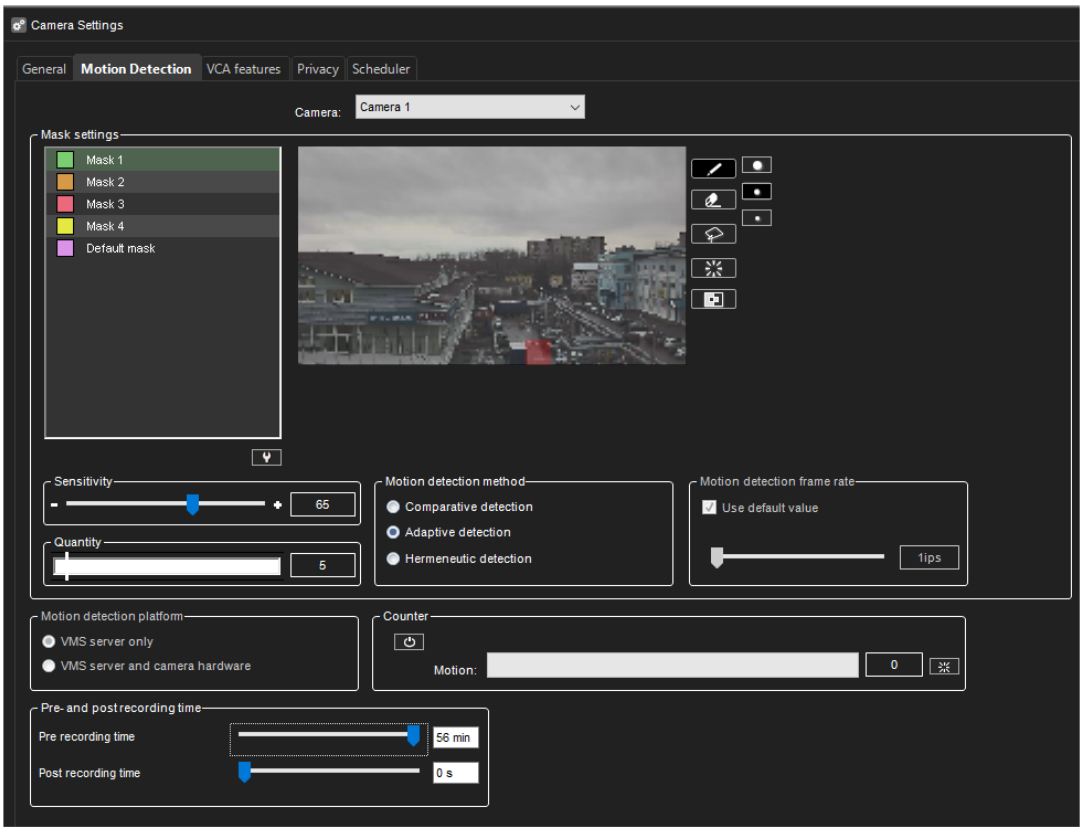
Our motion detection feature allows you to define which recordings will be stored in our file system and can be used to trigger alarms.

To start using motion detection, you need to configure motion masks which will then be used to define if motion is detected on the camera or video stream.

By using the scheduler, you can decide which motion masks will be used when storing recordings in the file system.

The information received through motion detection can be used in alarm settings to trigger alarms. In the alarm trigger settings, you define which motion mask motion detection should be used as an alarm trigger.

To access motion detection configuration in the System Manager, go to VMS Server Settings > Camera Settings > Motion Detection.



10.6.5.1 Sensitivity and quantity

The system detects motion based on Sensitivy and Quantity:

- Sensitivity: Pixels change more than the set limit
- Quantity: The specified number of pixels change

When there is a lot of background noise in the image (for example changes in lighting conditions), you can decrease the sensitivity by dragging the slider to the left or increase the quantity limit by dragging the slider to the right.

10.6.5.2 Motion detection methods

10.6.5.2.1 Comparative detection

Comparative detection compares an image to the image before it and can be used in most conditions.

If the differences exceed the set limits, the system detects motion.

When there is a lot of movement in the background, for example, rain, moving leaves, or changes in light levels, use adaptive motion detection.

10.6.5.2.2 Adaptive detection

Adaptive detection compares each image to a background image.

The system automatically learns the background image and the movement does not interpret, for example, moving leaves as motion.

If more than half of the pixels in an image change, the system concludes that the lighting conditions have changed, and as a result, it resets the reference image and starts learning it again.

10.6.5.2.3 Hermeneutic detection

Hermeneutic detection is a sophisticated motion detection system for challenging weather conditions, such as heavy rain, "noisy" background images, and situations in which external video content analytics (VCA) tools are used.

Hermeneutic detection requires more processing resources than the other detection methods.

10.6.5.3 Motion detection frame rate

Motion detection frame rate detects the frame rate used in motion detection.

It is generally recommended to use the default frame rate.

For IP cameras, motion detection uses intra-frames and matches the intra-frame rate. Typically, this is one image per second.

10.6.5.4 Motion detection platform

10.6.5.4.1 VMS server only

The VMS server receives all video frames from the camera. The VMS server utilizes the configured motion masks or continuous recording based on the scheduler settings.

10.6.5.4.2 VMS server and camera hardware

The VMS server receives those video frames from the camera that have been detected to include motion by the camera's motion detection. The VMS server utilizes the configured motion masks or continuous recording based on the scheduler settings:

- Motion detection masks: both cameras and the VMS server motion detection are used to avoid recording video when streams are opened for viewing from client applications.
- Continuous recording: only the camera's motion detection is used. Note that the video that is passed to the client applications for viewing is also recorded.

10.6.5.5 Motion Detection Configuration

To access motion detection configuration in the System Manager, go to VMS Server Settings > Camera Settings > Motion Detection.

1. Select the camera in the Camera drop-down menu.

2. Under Mask settings, select the mask you want to configure.
   You can change the name of the mask. Click Change Mask Name and type a new name for the mask.
   Please note that the Default mask configuration cannot be changed.
3. Draw the mask on top of the image to select for which area the motion detection feed will be calculated. Use the drawing tools to the right of the view, and with the drawing tools you, paint the areas red where you want the system to detect motion and you remove the red from areas where you want to ignore motion.

10.6.5.5.1 Drawing Tools

Tool	Name	Description
	Pencil	Use to set the motion detection area. Select the pencil size by clicking one of the tool size buttons (large, medium, small).
	Eraser	Use to erase selected areas that you do not want to include. Select the eraser size by clicking one of the tool size buttons (large, medium, small).
	Lasso	Use to select areas using straight lines. If the pen tool is selected, using this tool adds to selected areas. If the eraser tool is selected, this tool removes from the selection. Click the image where you want to start the selection. Click again where you want to anchor the line and change direction. To complete the selection, click the starting point. The selected area is painted red, or the red colour is removed.
	Fill/Clear	If the pen tool is selected, clicking this button selects the total image area. If the eraser tool is selected, clicking this button removes all selections.
	Invert	Reverses selected and unselected areas. Sometimes it is easier to select the area you do not want to mask and then invert the selection.
	Tool Size	Click one of the buttons to select the size of the pencil or eraser (large, medium, small).

1. Set the detection sensitivity by using the slider.
2. Set the minimum quantity of motion by using the slider.
3. Select the motion detection method. You can select comparative, adaptive, or hermeneutic motion detection. For a more in-depth description of these options please see the previous page.
4. Select either to use the default value for Motion detection frame rate, or use the slider.
5. Select the Motion detection platform, either only the VMS Server or the VMS Server and camera hardware.

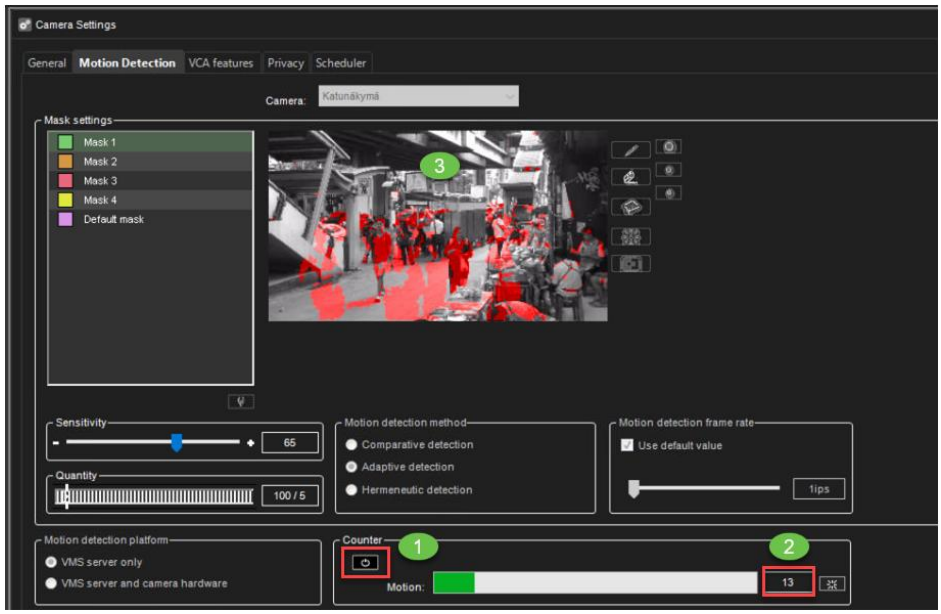
6. Once the configuration is finalized, the motion detection masks must be taken into use by using the scheduler. To access motion detection configuration in the System Manager, go to VMS Server Settings > Camera Settings > Scheduler. Please see the next document for instructions on how to use the Scheduler.

10.6.5.5.2 Counter

To test motion detection, you can use the counter. When you enable the counter, the video will be streamed from the camera and the motion detection is calculated. The result of the motion detection is shown on top of the image. The counter values increases everytime motion is detected, based on your configuration.

To use the Counter:

1. Enable **Counter**
2. Check the motion values
3. The camera image shows which area of the camera image causes motion detection recording



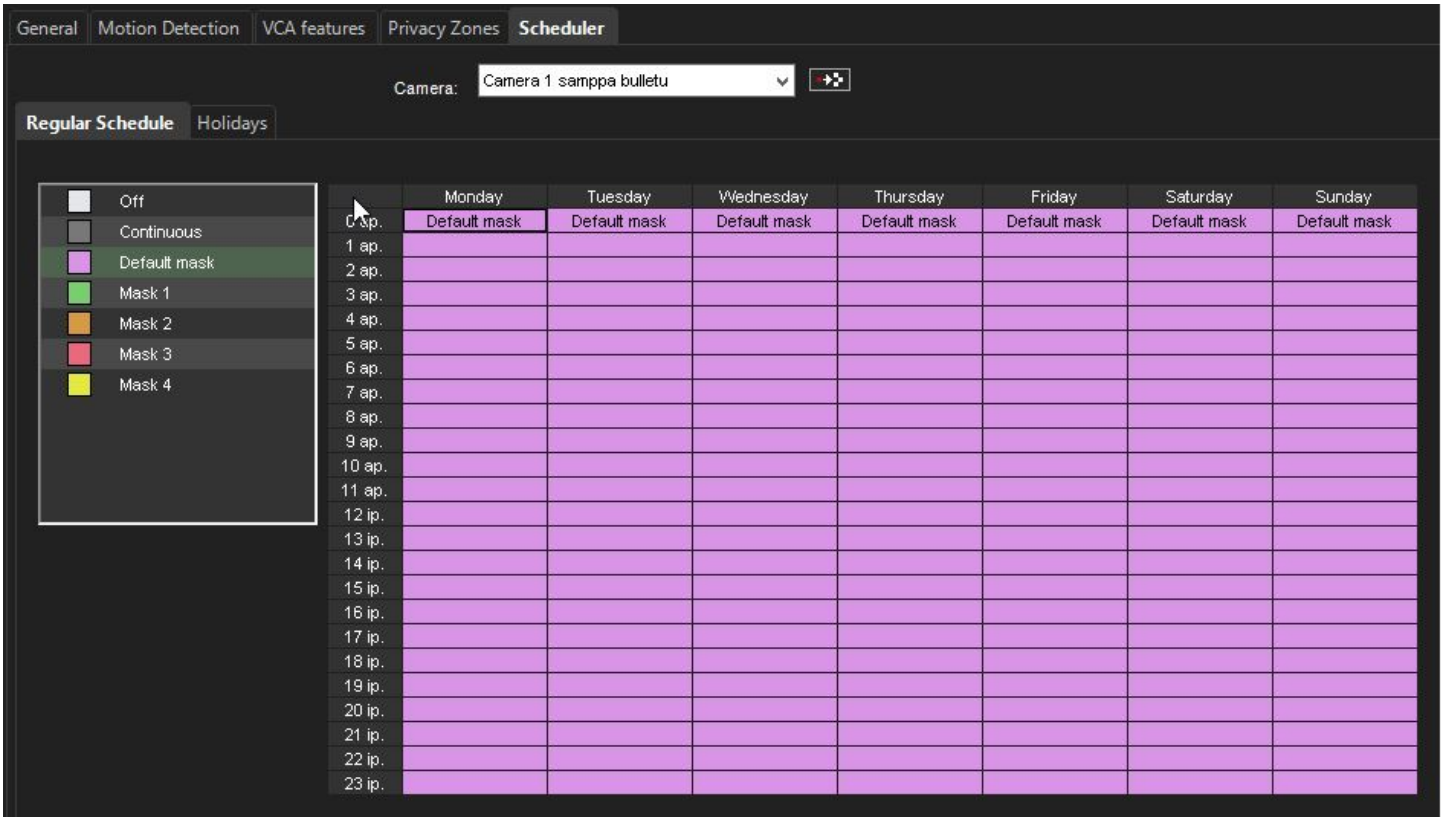
10.6.5.5.3 Pre- and Post- recording time

If you want recorded material before and after the motion, use Motion pre- and post-recording.

- Each mask can be configured separately.
- Values are from 0s to 60 minutes.
- You can copy selected values to the all cameras using button **Copy pre-and post recording time for all cameras.**

10.6.5.6 Scheduler

The Scheduler defines which motion mask is used for each camera at what time. You can select active days for a motion mask, or even more granular, active hours. By default, video is recorded when the system detects motion in the default mask. The default mask is active 24/7 by default.



For each hour of the week, you can set different options, like using different motion detection masks during the day and the night. The Scheduler has the following options:

- **Off**
  Video is not recorded. However, possible alarms are recorded. Alarms are configured in **Alarm Settings**.
- **Continuous**
  The camera records all images. This option uses a lot of disk space.
- **Default mask**
  The camera records video using the default motion detection mask and default motion detection parameters.
- **Custom mask**
  The camera records video using a custom mask. Each camera can have as many as four custom masks.

10.6.5.6.1 How to use the Scheduler

1. Set the regular weekly schedule in the **Regular Schedule** tab.
2. Set holiday schedules on the **Holidays** tab, if needed.
3. To change the schedule, click on the motion mask you want to select.
4. Click on the scheduled hour where you want the motion mask to be used.
    - To change more than one hour at the same time, drag with the mouse or click the first cell, keep the SHIFT key pressed, and then click the last cell.
    - To change all hours in a column or a row, click the column or row heading.
    - To change all hours of the week, click the cell above the hour's column (on the left side of the weekday heading row).
5. Click the Save icon ✔ at the bottom of the page to save all Camera settings.

10.6.5.6.2 Copy a schedule for all cameras

You can copy the currently selected recording schedule for all cameras in the system.

1. Click the Copy Schedule icon.



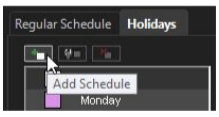
2. When asked for confirmation, click **OK**.

10.6.5.6.3 Exception days settings for holidays

You can use alternative recording schedules for holidays, and apply a daily schedule from the **Regular Schedule** or use an **Exception days** schedule.

10.6.5.6.3.1 Adding a schedule for exception days

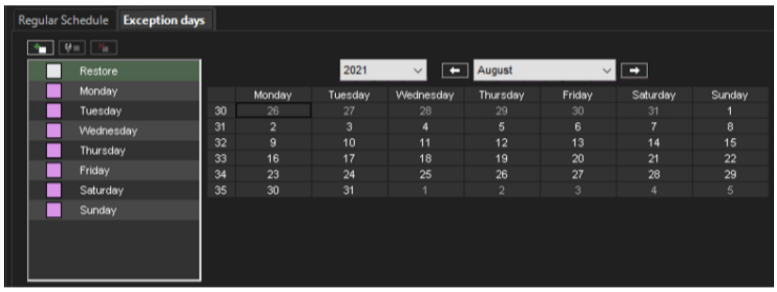
1. Click **Add Schedule**



1. Select a name for the schedule and use the text box to name it.
2. Click the motion mask you want to apply.
3. Click the hours you want to apply the motion mask.
4. Click **OK**.

10.6.5.6.3.2 Using exception days schedules

1. Click the **Exceptions days** tab.
2. Select the year and month.
3. In the left panel, click the schedule that you want to apply.
4. Click the holiday in the calendar.



10.6.5.6.3.3 Editing a custom schedule

1. Select the schedule.
2. Click **Edit Schedule**.
3. Make the changes you wish to apply.
4. Click **OK**.

10.6.5.6.3.4 Deleting a custom schedule

1. Select the schedule from the left pane.
2. Click **Delete Schedule**.
3. Confirm that you want the schedule to be deleted.

10.6.5.6.4 Restore the original schedule

1. Click **Restore**
2. Click the day that you want to restore.
3. Click ✔ to Save.

10.6.6 VCA features

If the software license includes Video Content Analytics (VCA) functionality, it can be administered on a camera-specific basis on the **VCA Features** -tab.
Depending on the license, specific VCA functionalities can be enabled or disabled on the tab.
It is possible to control which stream (in a configured camera to use multiple streaming) is used for VCA.
This is achieved from the pull-down menu below the camera selector (see the following mage)

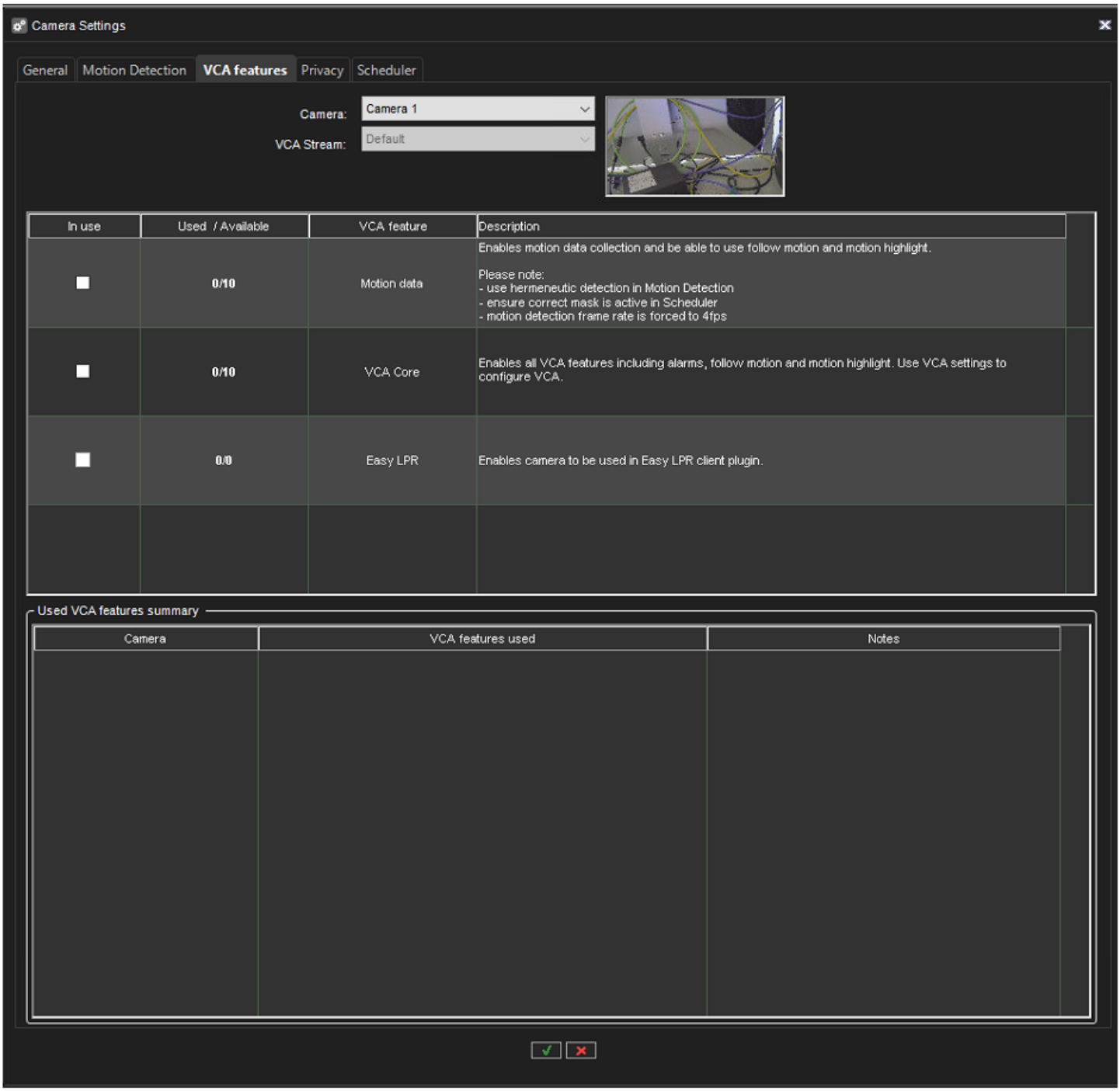


Figure 15 The VCA Features tab

In the primary state, the tab contains the following VCA features:

- **Motion data:** Internal VCA motion data, enabling data collection, motion following, and motion highlighting. Visualized in **Mirasys Spotter**.
- **VCA Core:** enables full VCA functionality. Configured through VCA settings in system manager.
- **Easy LPR**: Enables the camera to be used in the Easy LPR Client plugin

Please note that the VCA features are only available if enabled through the license.

10.6.7 Privacy

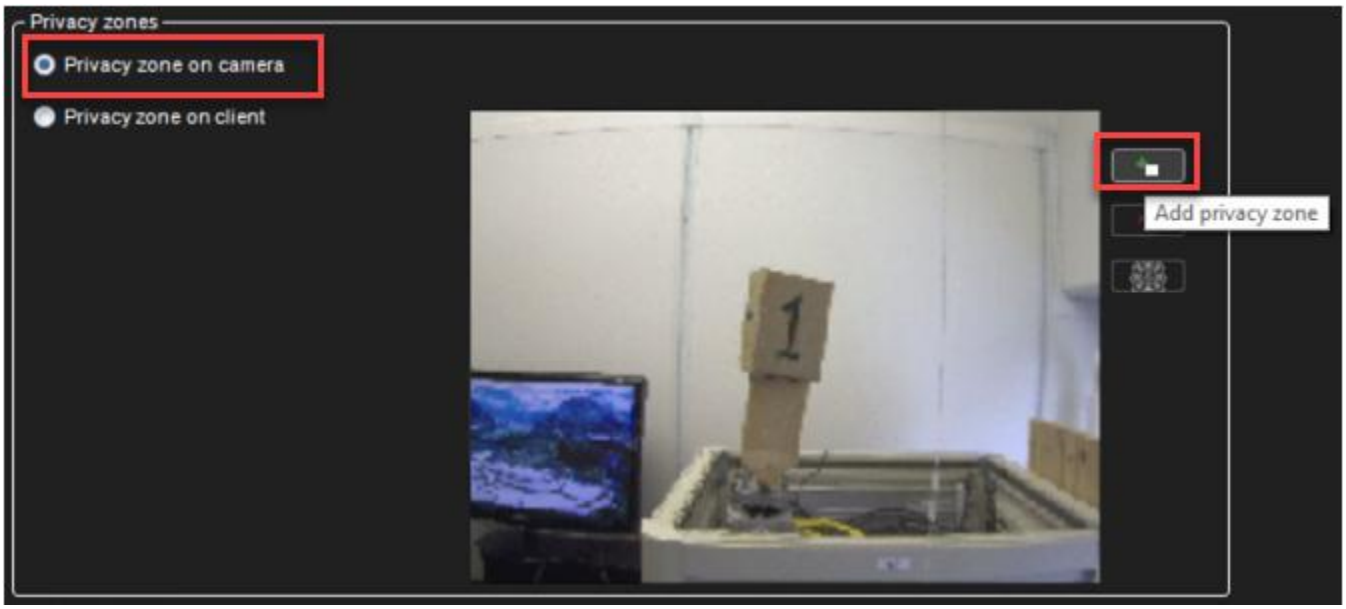
Under the Privacy menu, you can control the privacy zones of the camera and the facial- and movement blurring functionality.

To be noted: the content of the privacy functionalities is available (for the user) only if they are defined for the camera.
(I.e. if the camera does not have, e.g. the facial blurring defined, this camera shall not have the faces blurred – even if the user group of the end-user would have permission level set to view only unblurred materials.
This also applies when exporting the materials.

10.6.7.1 Privacy zone on the camera

10.6.7.1.1 Adding privacy zone

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select **Privacy zone on the camera**
3. Click **Add privacy zone**.
4. Paint the privacy zone onto the camera view. The newly created zone is displayed in semi-transparent light grey. You can resize and move the zone by dragging it.
5. Repeat steps 1-3 to create as many private zones as required.
6. Click **OK**.



10.6.7.1.2 Removing the privacy zone

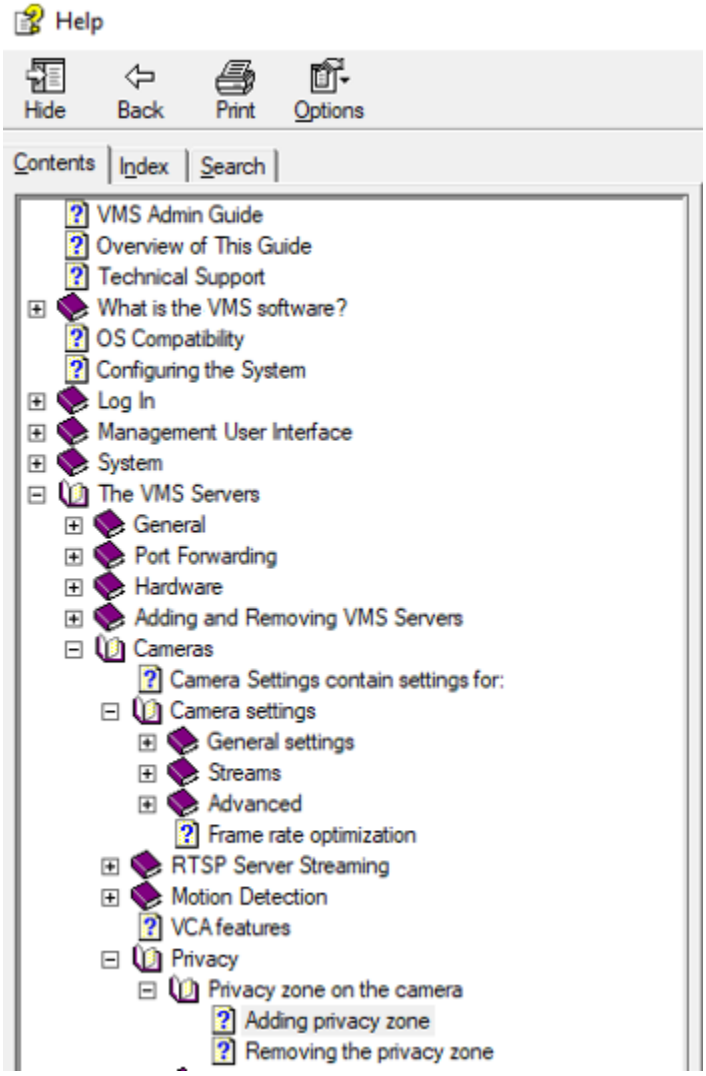
To remove privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click on a privacy zone in the camera view.
3. Click **Remove privacy zone** or **Remove all privacy zones**.
4. Click **OK**.

10.6.7.1.3 ONVIF Profile T privacy masking support

The ONVIF automatically detects if a Profile T device supports privacy masking. This feature provides greater control over video surveillance content and allows users to add, remove, or modify privacy masking for our VMS in the System Manager.

For more information, see the System Manager Desktop Application's **Help tab** > **Help Topics** > **VMS Admin Guide** > **The VMS Servers** > **Cameras** > **Privacy**



Adding privacy zone

10.6.7.2 Privacy zone on the client

On the Spotter client: these privacy zones are implemented only on the viewing client.
This allows the complete video to be recorded and exported, but the privacy-screened areas are only accessible for users who have the right to do so.

10.6.7.2.1 Adding privacy zone

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select **Privacy zone on the client**
3. Click **Add privacy zone**.

4. Paint the privacy zone onto the camera view. The newly created zone is displayed in semi-transparent light grey. You can resize and move the zone by dragging it.
5. Repeat steps 1-3 to create as many private zones as required.
6. Click **OK**.



10.6.7.2.2 Removing the privacy zone

To remove privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click on a privacy zone in the camera view.
3. Click **Remove privacy zone** or **Remove all privacy zones**.
4. Click **OK**.

10.6.7.3 Object Blurring

"Blur faces" and "Blur moving objects" settings are available to be set up as additional privacy.
If the facial- or motion-based blurring is enabled for a camera, these are also available on the Spotter side (provided that the user has sufficient permissions.)
The blurring will not be functional on the spotter side- or for exports of the video material for the cameras if they have not been selected on the system administrator side.
Higher resolutions used for the algorithms mean higher accuracy for the algorithms- but also higher CPU loads.

10.6.7.3.1 Blur Faces

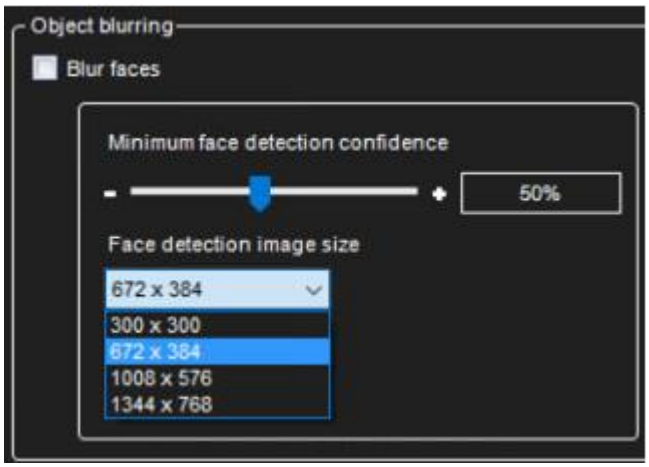
10.6.7.3.1.1 Minimum face detection confidence

10.6.7.3.1.2 Face detection image size

Using a small face detection size value, a person face must be closer to the camera. Face detection will be faster.

Using bigger face detection size value. a person's face is detected more away from the camera.

- 300x384
- 672x384
- 1008*576
- 1344x768



10.6.7.3.2 Blur Moving objects

10.6.7.3.2.1 Motion detection sensitivity

How sensitively pixel in the image is detected as motion pixel

10.6.7.3.2.2 Background image detection history length

How quickly stationary objects are detected as background

10.6.7.3.2.3 Motion detection input image size

The smaller size is quicker to process but outputs the worse results.

- Original size
- 1:2 size
- 1:4 size

- 1:8 size



10.6.8 License Plate Recognition (LPR) settings

System Administrator settings enabling Operators to use License Plate Recognition in Spotter Smart Search, and Spotter Smart Recognition.

> The **Smart LPR** feature requires an **RTSP Server Streaming** license.

10.6.8.1 License Plate Recognition Settings

License Plate Recognition Settings can be found in System Manager under the **VMS Server** tab > **Cameras**.

In the Camera settings window, go to the **LPR Settings** tab.

> If your license does not support the **Smart LPR** feature, the **LPR settings** tab will be hidden.

10.6.8.1.1 Select camera, stream, and enable LPR

1. Select the **Camera** from the drop-down menu in LPR
2. If there is more than one **Stream**, you can select the stream. If there is only one stream, there is a default stream like in the picture above, and the drop-down menu is disabled.
3. You can only choose a Service after you have enabled the service by clicking the box **Enable LPR for selected camera**.
4. If the **Enable LPR for selected camera** is not ticked, the **Service** drop-down menu is disabled.
5. The license text box shows number of used licenses and maximum number of licenses.



10.6.8.2 Detection Parameters

After the camera, its stream and the LPR detection service are selected, license plate detection settings can be adjusted. Plate detection settings can be found in the **Detection Parameters** group box in the **LPR settings** tab in the **Camera Settings** window.

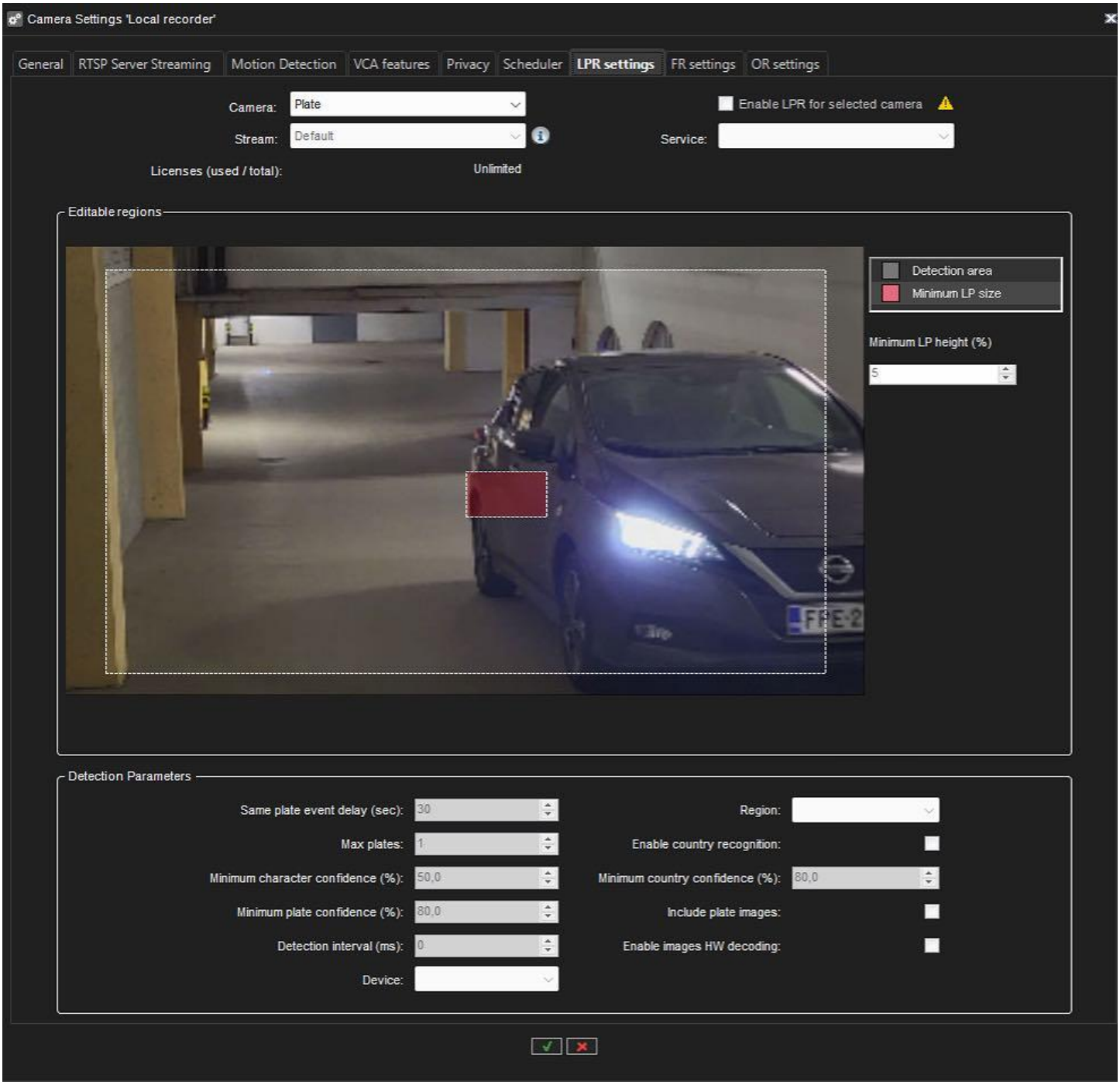


Plate detection settings are used for configuring the plate recognition detector.

- **Region of interest** - define the area where the detections are made.
- **Same plate event delay** - the number of seconds that should elapse before reading the same plate twice.

Tel +358 (0)9 2533 3300 Email info@mirasys.com https://www.mirasys.com

- **Max plates** - maximum number of plates to detect. Detected plates are sorted by plate confidence number in descending order.
- **Minimum character confidence** - plate characters recognizer confidence level. Valid values are between 25% - 95%.
- **Minimum plate confidence** - recognizer confidence level. Valid values are in the range of 25% - 95%.
- **Minimum plate height** - minimum plate height in %. Valid values are in the range 1% - 50%. The default value is 5%.
- **Detection interval** - the number of milliseconds that describes how often plate detection is done: if it is, for example, 250ms, then plate detection is done 4 times in a second (even if the video stream frame rate is much higher, like 30 fps).
- **Device** - is used for inference. Available devices depend on the hardware of the actual service.
- **Region** - The detection model (Eurasia or Americas) to be used for detection.
- **Minimum country confidence** - country recognizer confidence level. Valid values are between 25% - 95%.
- **Enable country recognition** - enable or disable country detection. Enabling country detection can improve plate number detection in some cases.
- **Include plate images** - include plate images or not in returned data.
- **Enable images HW decoding** - enable to decode input images with the most suitable computing platform (CUDA, DXVA, or DirectX).

10.6.8.3 Save settings

1. Click the **OK** button with the green checkmark icon at the bottom of the **Camera Settings** window.
2. Click the **Cancel** button with the red cross icon to cancel saving LPR settings and return to the settings values loaded after opening the **System Manager** application.
3. LPR settings for the selected camera are temporarily saved after switching on other cameras, streams, or tabs.

If you need to delete stream settings for the selected camera and detection stream, then select “None” in the **Service name** Combobx for the selected camera and detection stream.

10.6.8.4 Influence on settings

The following actions affect the service settings regardless of the actions on the **LPR settings** tab:

- *Deleting a recorder:* in case of deleting a recorder, all streams are deleted in the settings of all LPR services that worked with the remote recorder and saving the LPR settings.

- *Deleting a camera:* in case of deleting a camera, the stream is deleted in the settings of all LPR services that worked with this camera and saving LPR settings. There is a rule - one camera with one stream can only be used by one LPR service, but one LPR service can work with multiple cameras.
- *Changing the image size and compression type on the **Streams** subtab of the **General** tab:* in case of changing the resolution or compression type for the camera and stream, which are present in the settings of any LPR service, the LPR service settings are changed and saved when the **Camera Settings** window is closed.
- *Changing the RTSP streaming settings in the **Streaming Settings** group of the **RTSP Server Streaming** tab:* in case of changing the "Password," "User Name", "RTSP Port", "Streaming Mode" (security type) for the selected camera and stream, which are present in the settings of any LPR service, the LPR service settings are changed and saved when the **Camera Settings** window is closed.
- *Changing the image size in the **Device Settings** group of the **Video** tab in the **Hardware Settings** window:* in case of changing the resolution for the selected camera (here is possible to change the resolution for ***Recording*** stream only), which is present in the settings of any LPR service, the LPR service settings are changed and saved when the **Hardware Settings** window is closed.
- *Changing the camera by clicking on the **Edit IP camera** button on the **Video** tab in the **Hardware Settings** window:* in case of changing the camera by clicking on the ***Edit IP camera*** *button* resolution and compression type for the new camera (for ***Recording*** stream only) will be rewritten in LPR services settings, where camera ID is presented, the LPR service settings are changed and saved when the **Hardware Settings** window is closed.

10.6.9 Face Recognition (FR) Settings

System Administrator settings enabling Operators to use Face Recognition in Spotter Smart Search and Spotter Smart Recognition.

> The feature requires an **RTSP Server Streaming** license.

10.6.9.1 Face Recognition Settings

Face Recognition Settings can be found in System Manager under the **VMS Server** tab > **Cameras**.

In the Camera settings window, go to the **FR Settings** tab.

> If your license does not support the **Smart FR** feature, the **FR settings** tab will be hidden.

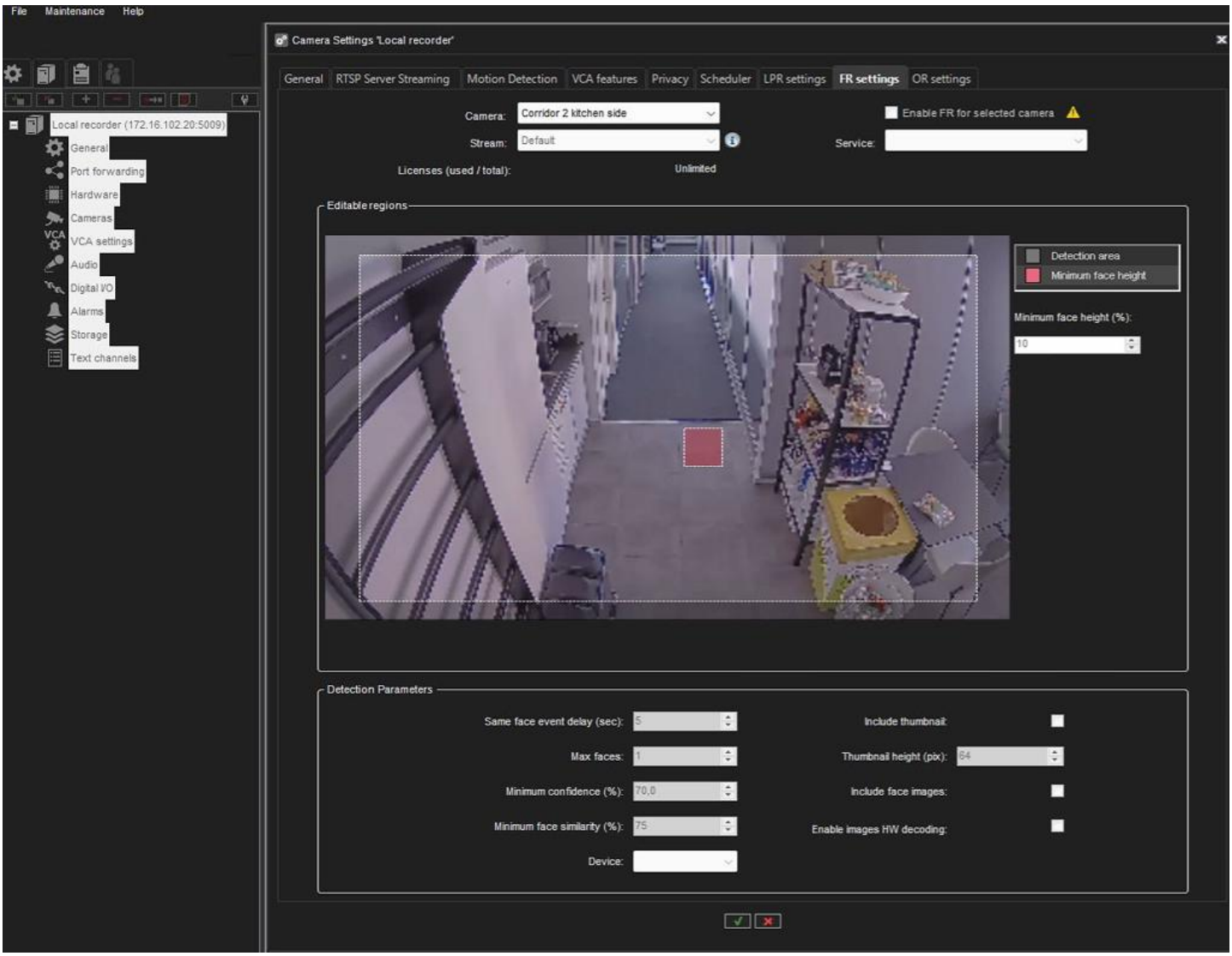
10.6.9.1.1 Select camera, stream, and enable FR

1. Select the **Camera** from the drop-down menu in FR
2. If there is more than one **Stream**, you can select the stream. If there is only one stream, there is a default stream like in the picture above, and the drop-down menu is disabled.
3. You can only choose a Service after you have enabled the service by clicking the box **Enable FR for selected camera**.
4. If the **Enable OR for selected camera** is not ticked, the **Service** drop-down menu is disabled.
5. The license text box shows number of used licenses and maximum number of licenses.



10.6.9.2 Face detection settings

After the camera, its stream, and the FR detection service are selected, face detection settings can be adjusted.



10.6.9.3 Detection Parameters

Face detection settings are used for configuring the face recognition detector.

- **Region of interest** - define the area where the detections are made.
- **Max faces** – maximum number of faces to detect from the image. The value should be between 1 and 20.
- **Minimum confidence** – recognizer confidence level. If confidence for the detected face is below this threshold, then the face is ignored. Valid values are between 25% - 95%.
- **Minimum face height** – minimum face height in %. Valid values are from 5 to 50%%. Default value 10%.
- **Minimum face similarity** – If the similarity is greater than or equal to this value, then it is the same face. The value should be between 50% and 95%.

- **Same face event delay** – the number of seconds that should elapse before arising an event with the same face.
- **Device** – is used for inference. Available devices depend on the hardware of the actual service.
- **Thumbnail height** – the height of the thumbnail image in pixels. The value should be between 32 and 128 pixels.
- **Include thumbnail** – include detection source image thumbnail or not in returned data.
- **Include face images** – include face images or not in returned data.
- **Enable images HW decoding** – enable to decode input images with the most suitable computing platform (CUDA, DXVA or DirectX).

10.6.9.4 Save settings

Click the **OK** button with the green checkmark icon at the bottom of the **Camera Settings** window to save.

Click the **Cancel** button with the red cross icon to cancel saving FR settings and return to settings values loaded after opening the **System Manager** application.

When deleting stream settings for the selected camera and detection stream, the "None" value should be selected in the **Service name** Combobox for the selected camera and detection stream.

10.6.9.5 Influence on settings

The following actions affect the service settings regardless of the actions on the **FR settings** tab:

- *Deleting a recorder:* in case of deleting a recorder, all streams are deleted in the settings of all FR services that worked with the remote recorder and saving the FR settings.
- *Deleting a camera:* in case of deleting a camera, the stream is deleted in the settings of all FR services that worked with this camera and saving FR settings. There is a rule - one camera with one stream can only be used by one FR service, but one FR service can work with multiple cameras.
- *Changing the image size and compression type on the **Streams** subtab of the **General** tab:* in case of changing the resolution or compression type for the camera and stream, which are present in the settings of any FR service, the FR service settings are changed, and saved when the **Camera Settings** window is closed.
- *Changing the RTSP streaming settings in the **Streaming Settings** group of the **RTSP Server Streaming** tab:* in case of changing the "Password," "User Name", "RTSP Port", "Streaming Mode" (security type) for the selected camera and stream, which are present in the settings of any FR service, the FR service settings are changed and saved when the **Camera Settings** window is closed.

- *Changing the image size in the **Device Settings** group of the **Video** tab in the **Hardware Settings** window:* in case of changing the resolution for the selected camera (here is possible to change the resolution for ***Recording*** stream only), which is present in the settings of any FR service, the FR service settings are changed and saved when the **Hardware Settings** window is closed.
- *Changing the camera by clicking on the **Edit IP camera** button on the **Video** tab in the **Hardware Settings** window:* in case of changing the camera by clicking on the ***Edit IP camera*** *button* resolution and compression type for the new camera (for ***Recording*** stream only) will be rewritten in FR services settings, where camera ID is presented, the FR service settings are changed and saved when the **Hardware Settings** window is closed.

10.6.10 Object Recognition (OR) Settings

System Administrator settings enabling Operators to use Object Recognition in Spotter Smart Search.

10.6.10.1 Object Recognition Settings

Object Recognition Settings can be found in System Manager under the **VMS Server** tab > **Cameras**.

In the Camera settings window, go to the **OR Settings** tab.

> If the user license does not support the Object Recognition feature, the OR settings tab will be hidden.

10.6.10.1.1 Select camera, stream, and enable OR

1. Select the **Camera** from the drop-down menu in OR
2. If there is more than one **Stream**, you can select the stream. If there is only one stream, there is a default stream like in the picture above, and the drop-down menu is disabled.
3. You can only choose a Service after you have enabled the service by clicking the box **Enable OR for selected camera**.
4. If the **Enable OR for selected camera** is not ticked, the **Service** drop-down menu is disabled.
5. The license text box shows number of used licenses and maximum number of licenses.

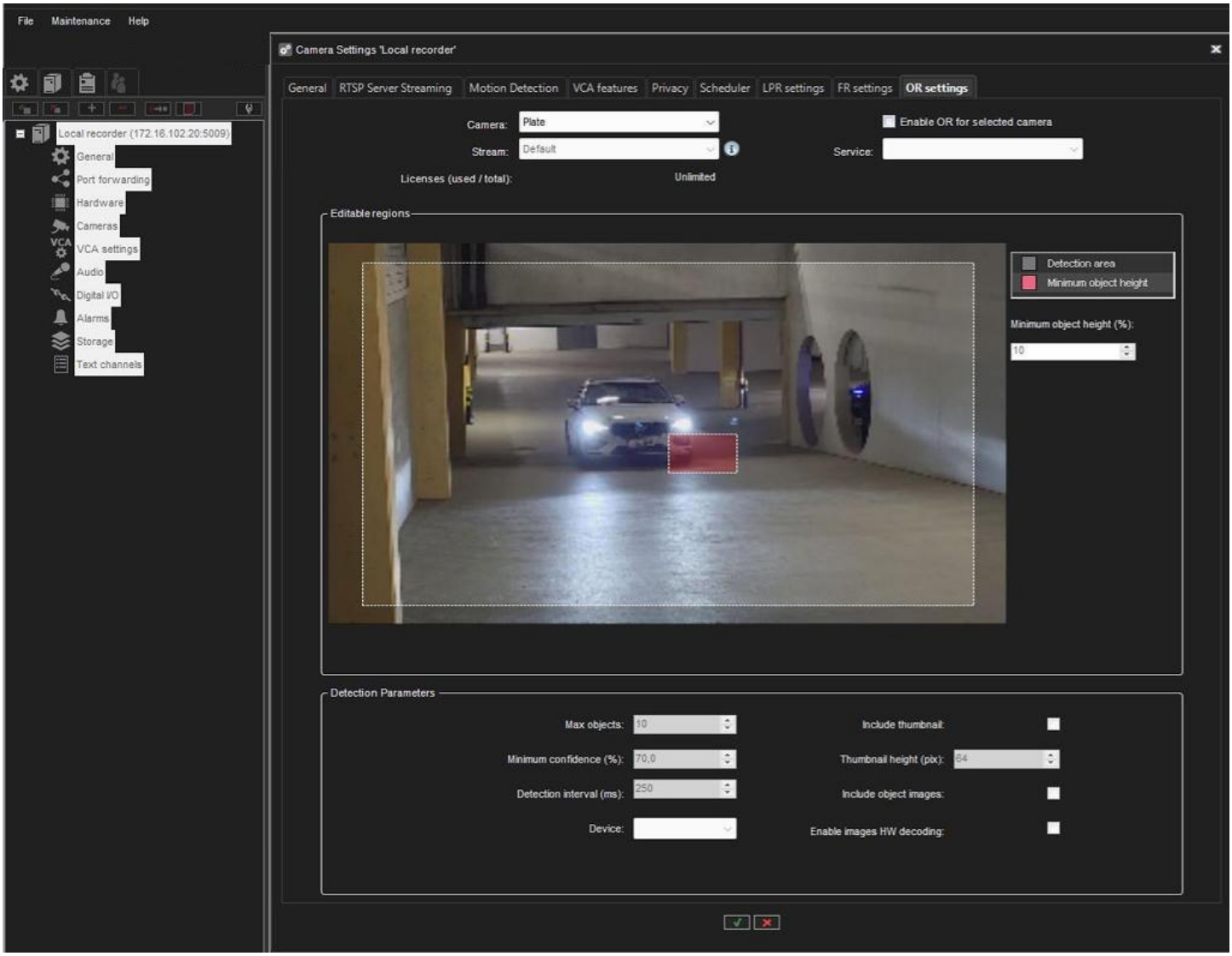


> If the camera does not support OR or there is no Service active for it, then it is not possible to enable the service at all.
> The yellow icon indicates that, and if the user hovers over it, there is a tooltip with the text **There's no active OR service for this camera**.

10.6.10.1.2Detection Area / Minimum Object Size

An image in the **Detection Area** is uploaded immediately after the current camera is selected in the **Camera** Combobox. The minimum object size can be adjusted in two ways:

- Adjust the percentage in Min. object height (%)
- Adjust it in the frame with the indicated square for Minimum object size. The square will have the same color as in the selector to the right of the frame.
- The minimum size cannot be less than 10%.



10.6.10.1.3Detection Parameters

- **Max objects** – maximum number of objects to detect from the image. The value should be between 1 and 100.
- **Minimum confidence (%)** – recognizer confidence level. If confidence for the detected object is below this threshold, then the object is ignored. Valid values are between 25% - 95%.
- **Detection interval (ms)** - the number of milliseconds that describes how often object detection is done: if it is, for example, 250ms, then object detection is done 4 times in a second (even if the video stream frame rate is much higher, like 30 fps).
- **Device** – is used for inference. Available devices depend on the hardware of the actual service.
- **Include thumbnail** checkbox – include detection source image thumbnail or not in returned data.
- **Thumbnail height (px)** – the height of the thumbnail image in pixels. ONLY enabled if the **Include thumbnail** box is checked. The value should be between 32 and 128 pixels.
- **Include object images** checkbox – include object images or not in returned data.
- **Enable images HW decoding** checkbox – enable to decode input images with the most suitable computing platform (CUDA, DXVA or DirectX).

WARNING: Using high limits may lead to unintended mass data deletion and increased system load. It is recommended to start with smaller limits and verify the results before executing larger operations.

Settings for Object Data Store can be found in **System Settings** > **Object Data Store Settings** in System Manager.

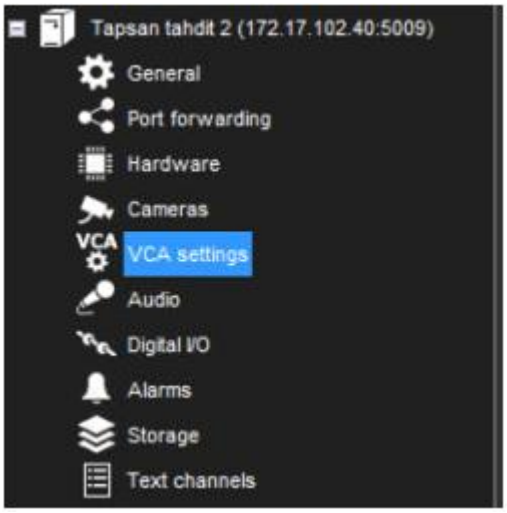
10.6.10.1.4Recommended configuration for OR settings

The following streaming and detection settings are recommended for OR:

- Use CBR (Constant Bit Rate) for streams – with CBR, OR gets a full image/I-frame only containing the changed images. This makes the system work better and produce better results. Note that there may be a need to limit the streaming Mbps to prevent network performance from being affected.
- Detection interval should preferably be 2000ms or 1000ms per different cameras for up to 10-15 objects.
- Thumbnail height should be set to 64px or lower. Larger values can kill the storage.
- When the minimum object height is being determined, note that larger values are the best for clear images.

Using the recommended settings helps optimize OR performance. For example, disk usage and GPU usage can be notably lowered when OR is configured correctly.

10.7 VCA SETTINGS



Please see the Mirasys VCA Guide.

In some cases detection may not work correctly. Please try to increase image quality or move/zoom camera image to closer wanted detection area.
Models are trained using clear images and some cases when using black/white image or thermal camera image this may cause that detection is working correctly. For this you can try use Deep Learning Filter with Object Tracker.

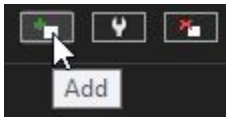
10.8 AUDIO

10.8.1 Adding, Editing and Removing Audio Devices

The system supports three basic types of audio components: one-way analog and IP audio channels, two-way IP audio channels, and a single audio communication channel.

To configure audio devices:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the **Add**-option



5. Select the capture driver from the list.
6. Select one of these options:

1. **Mono**. Select to use two mono channels.
2. **Stereo**. Select to combine two mono channels into one stereo channel.

1. Click **OK**.

Note: *IP camera-based IP audio input and output channels are added to the system primarily through the automated camera search tools.If an IP camera-based audio channel cannot be added through the camera search tools, or if the channel is added belatedly, follow the instructions above to add the audio channel.*

10.8.1.1 To edit an audio device:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the audio channel.
5. Click **Edit Audio Channel** in the lower right corner of the tab. The **Configure Audio** dialogue box is shown.



6. Edit the information fields.
7. Click **OK**.

10.8.1.2 To remove an audio device:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the audio channel.
5. Click **Remove Last Audio Channel from the List**in the lower right corner of the tab.**Note:** *You cannot remove an audio device from the middle of the list; only the most recently added audio device can be removed.*

6. The last audio device on the list is removed from the server.

10.8.2 Audio Settings

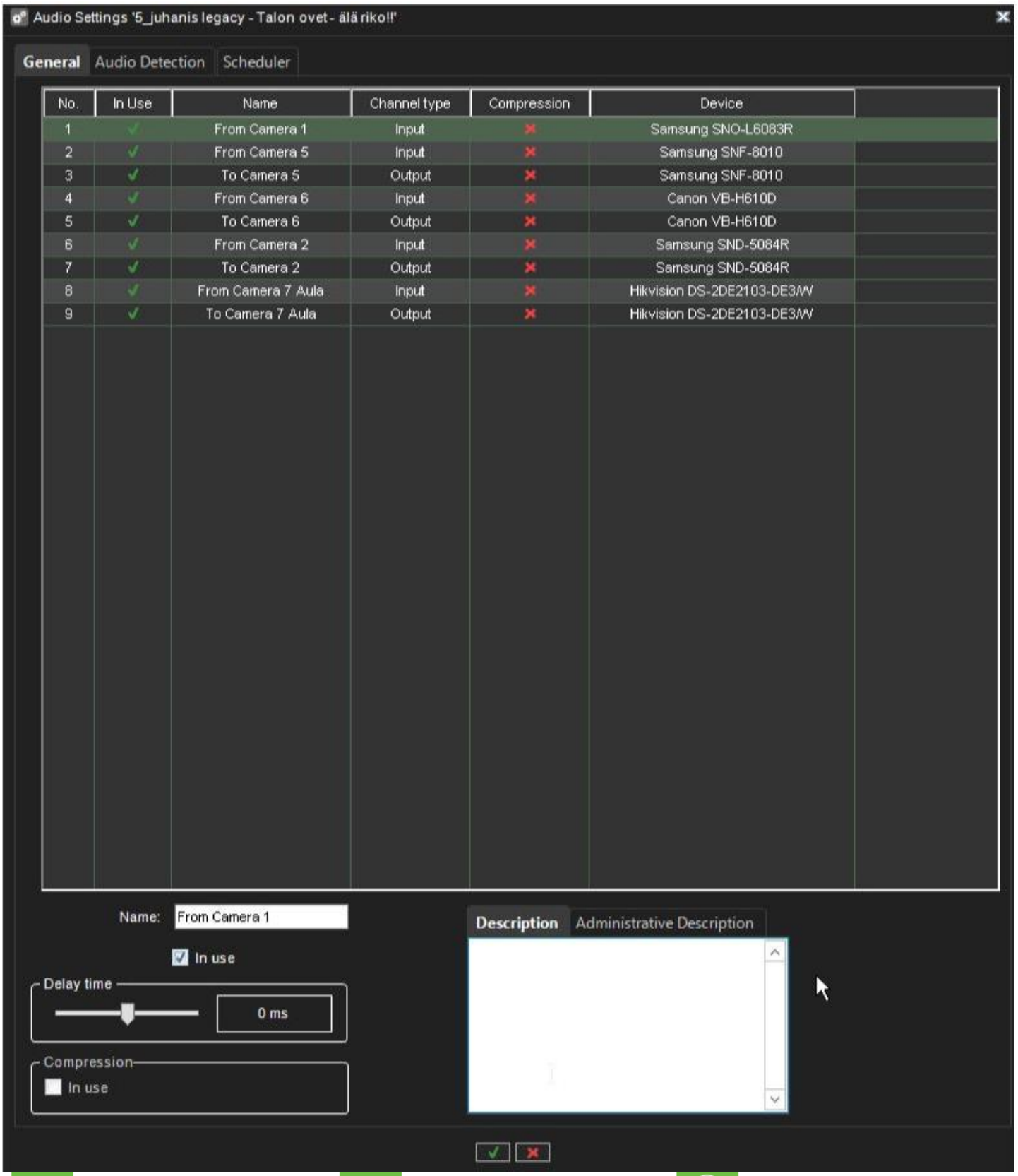
The system supports three basic types of audio components:

- **One-way analogue and IP audio channels:** These include mainly camera-based and separate microphones.
- **Two-way IP audio channels:** Two-way IP audio channels require an IP camera with an audio input and output channel.
    - Two-way IP audio channels are used for communication between the camera site and a Spotter client.
    - Only one Spotter client can be used for communication at any time, but other clients in the system can listen to the channel and take over the communication if required.
    - All communication that passes through a two-way IP audio channel is recorded in the system.
- **A single audio communication channel:** An older communication model. Each system contains one communication channel.
    - The drawback in using the audio communication channel is that the signal bypasses the server, meaning that the communication is not recorded in the system.

10.8.3 General Settings tab



MIRASYS



Tel +358 (0)9 2533 3300 Email info@mirasys.com https://www.mirasys.com

The **General** tab in the **Audio** page lists the basic settings of all audio channels:

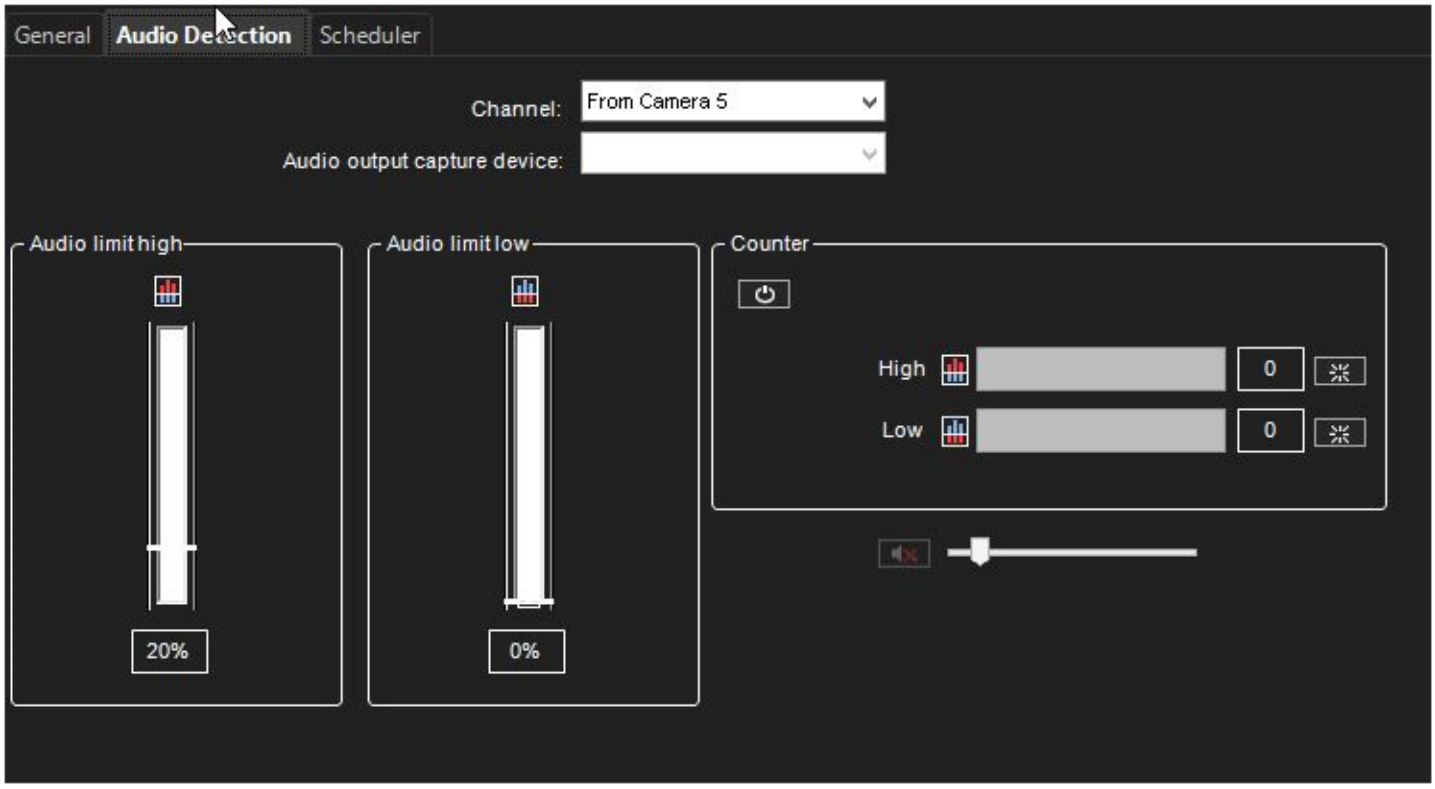
- **No.** The number of the channel.
- **In Use.** Shows if a channel is enabled or disabled.
- **Name**. The name of the channel.
- **Mono / Stereo**. Shows if a channel is a mono or stereo channel.
- **Compression**. Shows if compression is on or off. A checkmark means that compression is used.
- **Capture Driver**. Shows what capture driver is used. Select the driver in **Hardware Settings**.

To change general settings:

1. Select the channel from the list.
2. You can change these settings in the lower part of the window:

1. **Name**. The name of the channel.
2. **In use**. Select to enable the channel. Clear the check box to disable the channel.
3. **Delay time**. Sets the delay time in synchronizing the audio stream with other devices.
4. The delay time can be used to optimize the audio and video stream synchronization to, for example, enable better lip synchronization.
5. **Compression**. Select to use compression. Compressed audio files use less disk space, but the quality of the audio is a bit lower. Clear the check box to not use compression.
6. **Description**. Here you can type a description of the channel that will be shown to the users in the Spotter program.
7. **Administrative Description**. Here you can type a description of the channel that will be shown in the Spotter program to only system administrators.

10.8.4 Audio Detection



On the **Audio Detection** tab on the **Audio** page, set the high and low limits for audio detection.
The system records audio when the audio level exceeds the high limit.
In addition, you can set the system to give an alarm when the audio level exceeds the high limit or drops below the low limit.

To set the limits:

1. Select the audio channel from the list.
2. Click **Turn Audio Counter On/Off**.
    a. The system shows the audio level in the **Audio Limit High** and **Audio Limit Low** indicators, and the counters increment each time audio detection is activated.
    b. The top counter increments when the audio level exceeds the high limit. The lower counter increments when the audio level drops below the lower limit.
3. Set the high limit so that in usual conditions, the audio level stays below the limit.
    a. Audio detection is activated when the level exceeds the limit.
4. Set the low limit so that in usual conditions, the audio level stays above the limit.

a. Audio detection is activated when the level drops below the limit.

5. To reset the counters, click the reset buttons.
6. Turn the counters off by clicking the **Turn Audio Counter On/Off** button.
7. To save the settings, click **OK**.

You can adjust the volume of audio and also mute the audio channel.

These settings are not saved; they only change how audio is played in the audio settings.

- **Mute**. Mutes the audio channel.
- **Adjust Volume**. Adjusts the audio volume.

10.8.5 Scheduler (Audio)

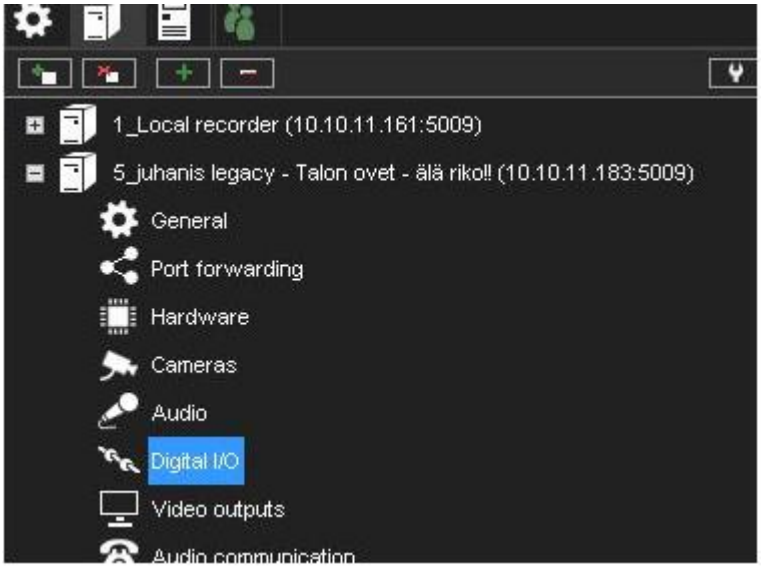
By default, audio is recorded when the detected level of audio exceeds the default detection limit (**Audio limit high**).

Similarly, to the video scheduler, it is possible to control the audio recording with the following options both for regular weeks and holidays.

1. **Off.** Audio is not recorded. However, possible alarms are recorded.
2. **Continuous.** All audio is recorded.
3. **Audio detection.** Audio is recorded when the measured level of audio exceeds the limit **Audio level is high.**
    a. Set the limit on the Audio Settings

The functionality of this view is similar to the video scheduler.

10.9 DIGITAL I/O

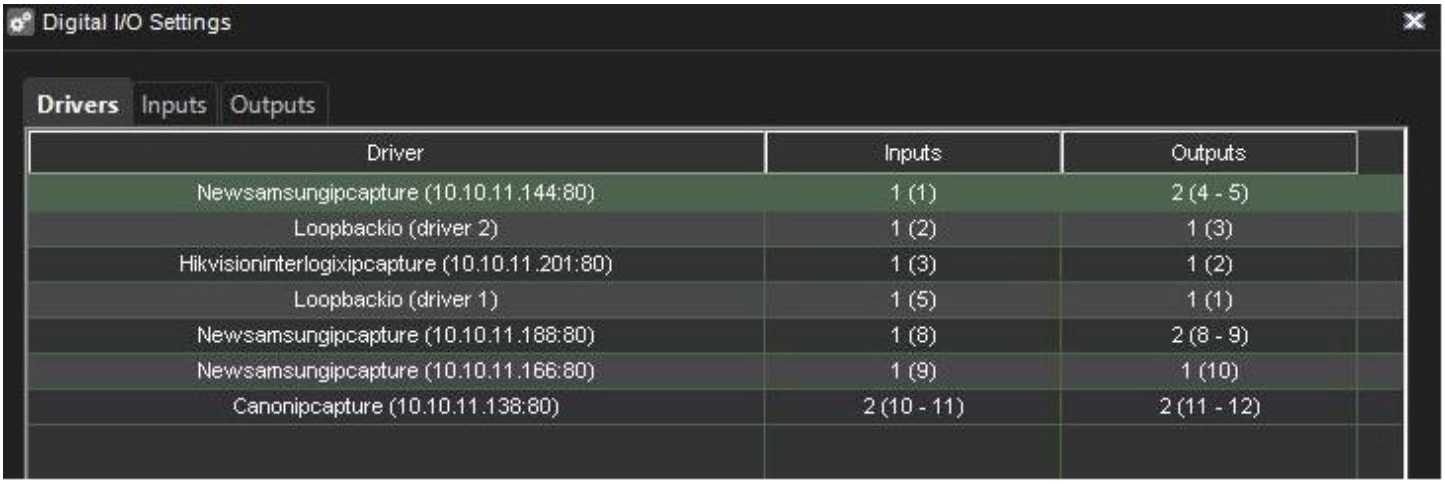


10.9.1 Digital I/O Settings

In **Digital I/O** settings, you can add digital input and output devices and configure the input and output settings. These sections describe how to set up digital I/O devices.

10.9.1.1 Drivers

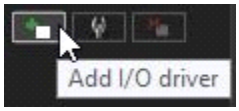
In addition to the default digital I/O drivers included in the system, new drivers can be added to the system by installing them as plugins.
Once an I/O device driver has been added to the system, the device can be configured and taken into use through the **Drivers** tab.



To take an I/O device driver into use:

1. If necessary, install the device driver package.

2. Open the **VMS Servers** tab.
3. Select the correct server and open the **Digital I/O** page from the menu.
4. Click **Add I/O driver** in the lower-right corner of the screen.



5. Select the driver from the **Model** drop-down menu.
6. Configure the device settings in the **Properties** list.
7. To save the settings, click **OK**.

Note: *After configuring a digital I/O device driver, you may need to configure the inputs and/or outputs.*

To edit I/O device driver settings:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Double click on the device driver you want to edit.
4. Edit the device settings in the **Properties** list.
5. To save the settings, click **OK**.

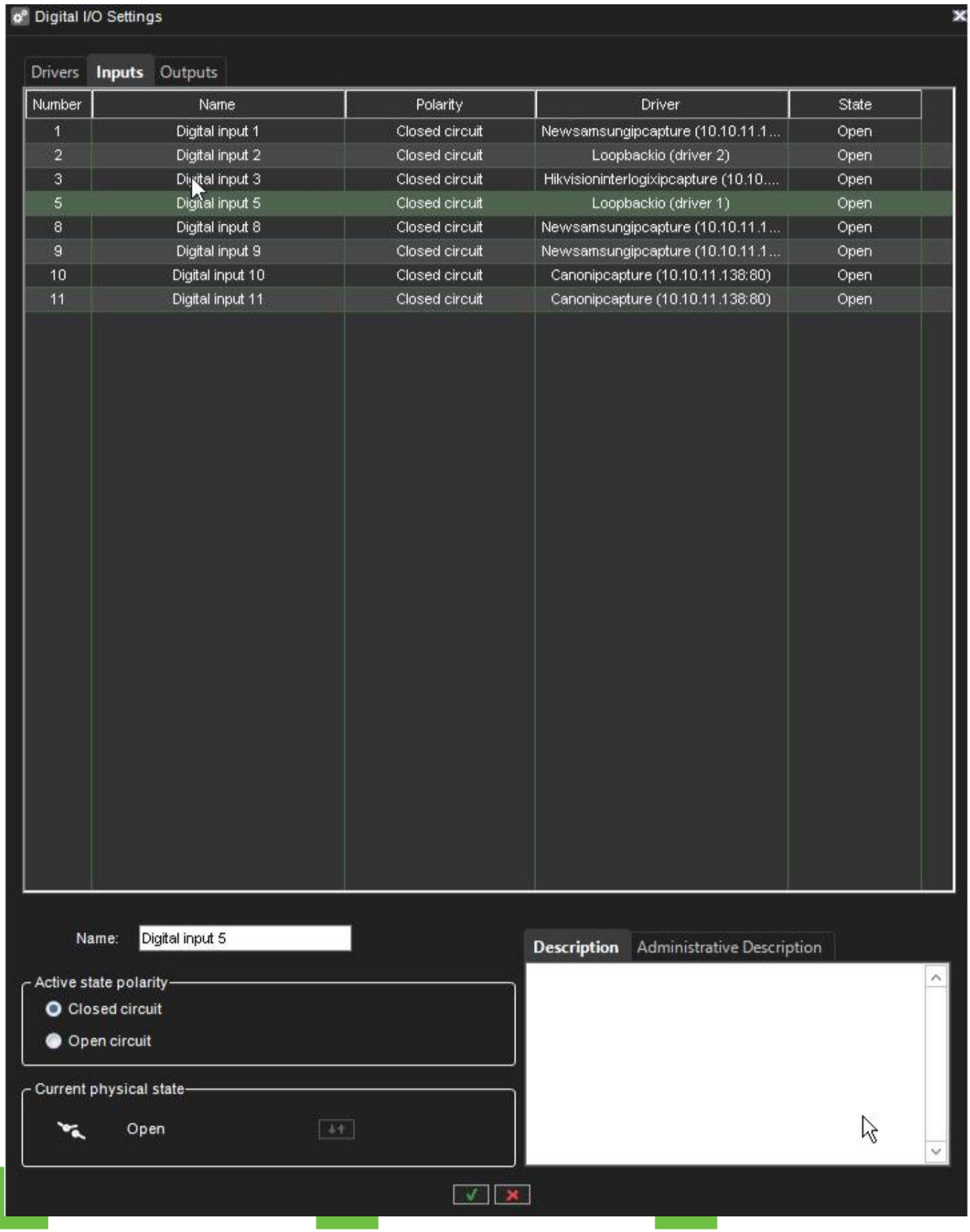
To delete an I/O device driver:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Click on the I/O device driver you want to delete.
4. Click **Delete I/O driver** in the lower right corner of the screen.
5. Click **Ok** to confirm the deletion.

10.9.1.2 Digital Inputs

You can use digital inputs to activate alarms.
In digital input settings, set the polarity of the inputs. Set the alarm actions in alarm settings.

MIRASYS


Digital I/O Settings
Drivers
Inputs
Outputs
Number
Name
Polarity
Driver
State
1 Digital input 1 Closed circuit Newsamsungipcapture (10.10.11.1... Open
2 Digital input 2 Closed circuit Loopbackio (driver 2) Open
3 Digital input 3 Closed circuit Hikvisioninterlogixipcapture (10.10.... Open
5 Digital input 5 Closed circuit Loopbackio (driver 1) Open
8 Digital input 8 Closed circuit Newsamsungipcapture (10.10.11.1... Open
9 Digital input 9 Closed circuit Newsamsungipcapture (10.10.11.1... Open
10 Digital input 10 Closed circuit Canonipcapture (10.10.11.138:80) Open
11 Digital input 11 Closed circuit Canonipcapture (10.10.11.138:80) Open
Name:
Digital input 5
Description
Administrative Description
Active state polarity
Closed circuit
Open circuit
Current physical state
Open

Name. To rename an input, select the input and then type a new name for the input in **Name.Active state polarity.** Select the input and then select if the input is activated when the circuit is opened or closed.
Current physical state. Shows the state of a relay in real-time (**Open** or **Closed**).
Description. Here you can type a description of the selected input shown to all users in the Spotter program.
Administrative Description. Here you can type a description of the selected input shown in the Spotter program to only system administrators.

10.9.1.3 Digital Outputs

In digital outputs, select if a relay is opened or closed (polarity) when the output is triggered.

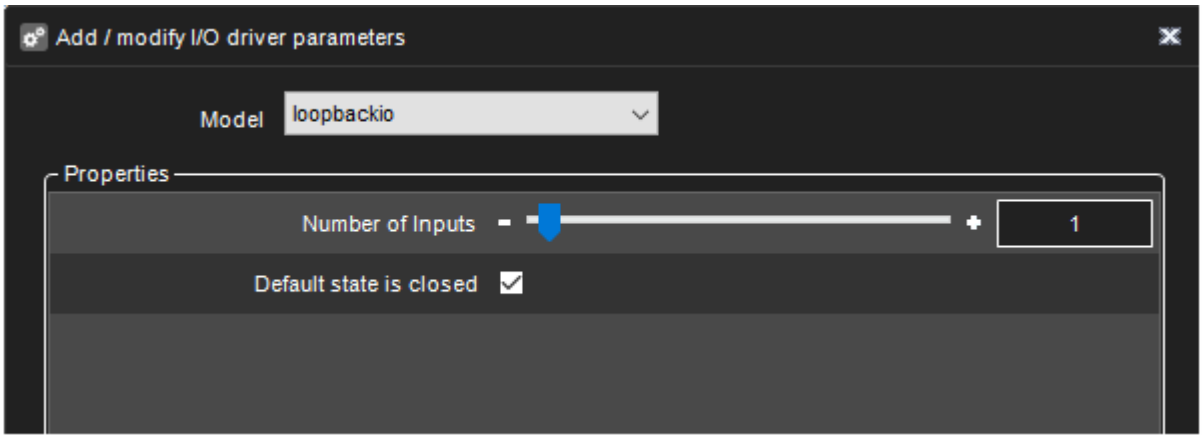
Name. To rename an output, select the output and then type a new name for the output in **Name**.
Active state polarity. Select the output and then select if the output is closed or opened when it is activated.
Current physical state. Shows the state of a relay in real-time (**Open** or **Closed**).
Description. Here you can type a description of the selected output shown to all users in the Spotter program.
Administrative Description. Here you can type a description of the selected output shown in the Spotter program to only system administrators.

To test a digital output, click the **Change State (Toggle)** button.

10.9.2 LoopBack I/O

The LoopBack I/O allows you to create virtual I/O devices where the input is directly connected to the output.

This driver enables you to create buttons in the Spotter application to trigger alarms manually.



10.9.3 Logical I/O

With Logical I/O, it is possible to create actions based on the OR and AND operators.

The I/O driver emulates an external I/O that is connected to itself. Example:

For example, if the customer wants to confirm that an Automatic Number Plate Recognition (ANPR) event is triggered when a car is in front of the camera, the Logical I/O can be used to create a “rule” that results in action only when VCA detects a car, AND at the same time, there is an ANPR read event.

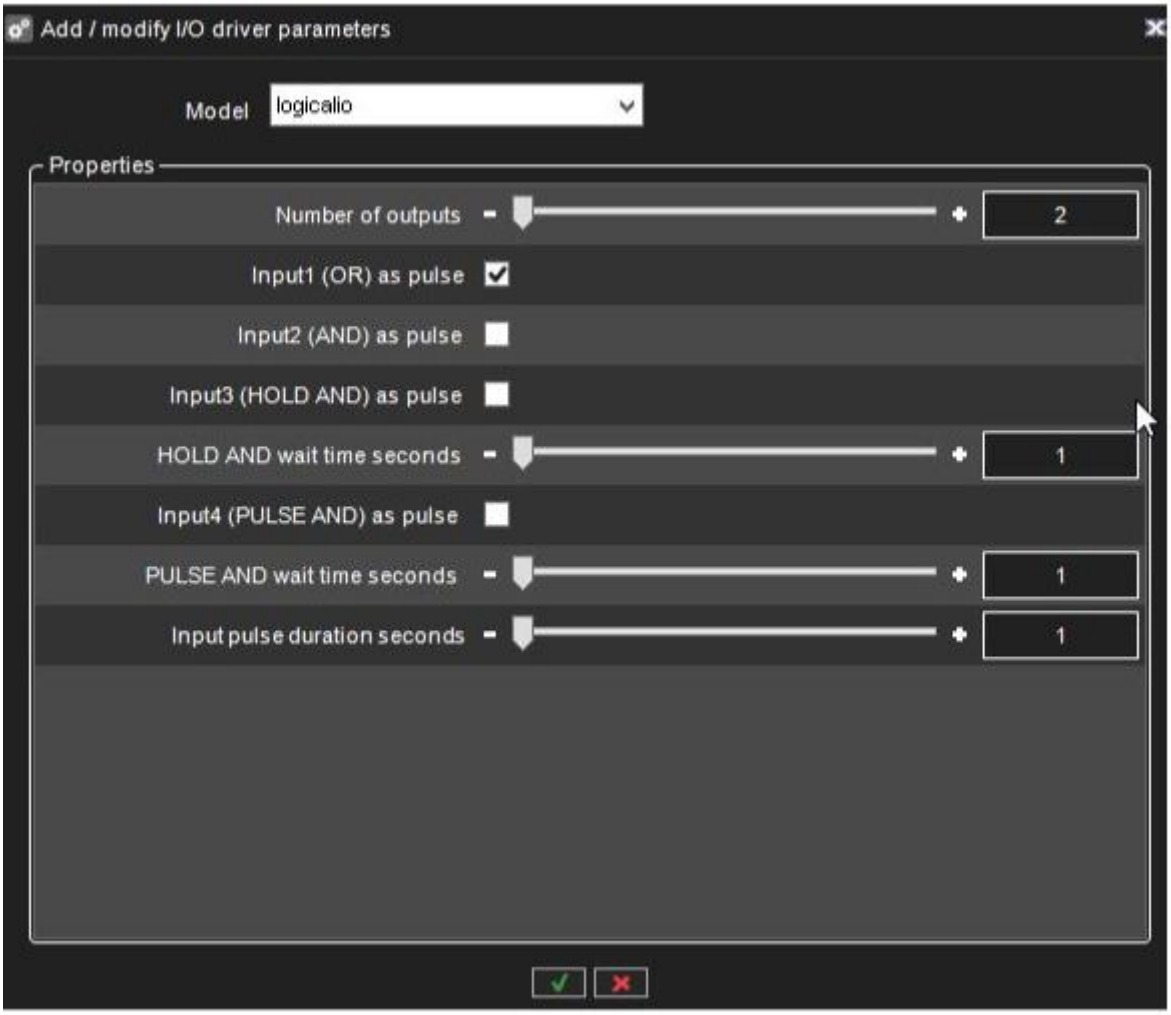
Another example could be that an entry “gate” with two doors only allows the second door to be opened when the first one is closed.

Logical I/O can be operated from the same interface as the rest of the Digital I/O in System Manager.

A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

When a new Logical I/O is being added, the first option in the dialogue is how many output states are used as operands in the AND/OR decision making.

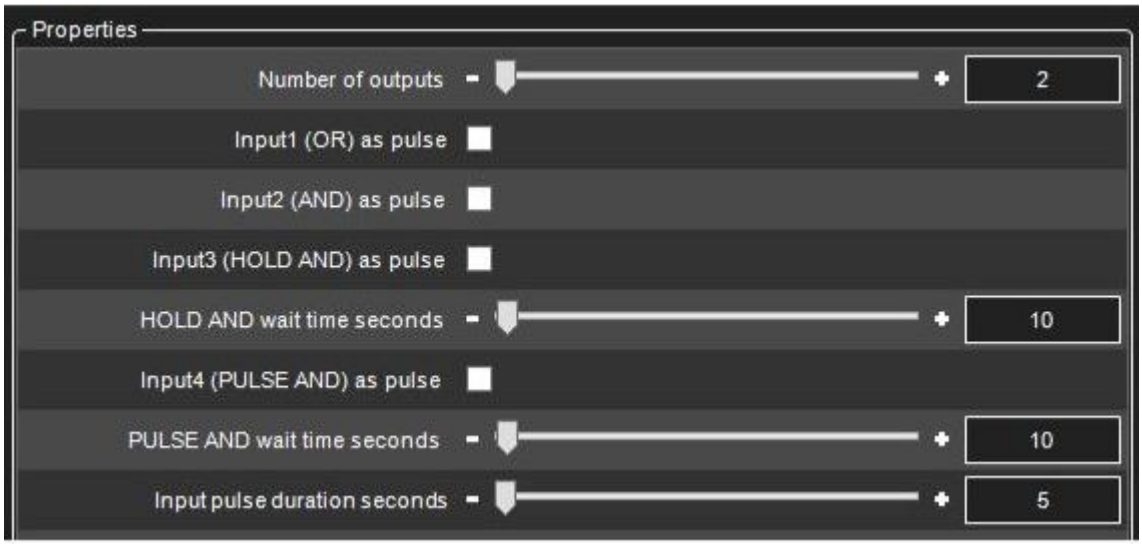
The minimum number is two, and the maximum is 32.



All Logical I/Os will automatically generate four inputs that can be used.

Input	Type
1	OR
2	AND
3	HOLD AND
4	PULSE AND

The following sections will describe the different inputs in more detail by using the below example:

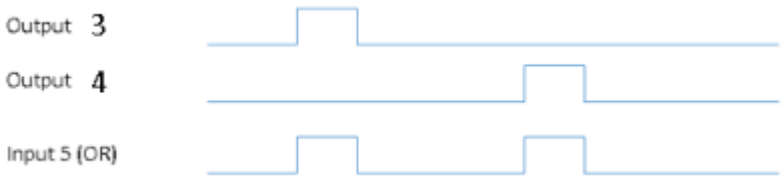


The example has 2 outputs that are the operands. These can be seen in the IO list as outputs 3 and 4.

The automatically created 4 inputs are seen in the list as inputs 5,6,7 and 8.

10.9.3.1 "OR" Input

The first input that the Logical I/O will generate is OR signal. If any of the outputs are on, the OR input will be turned on.

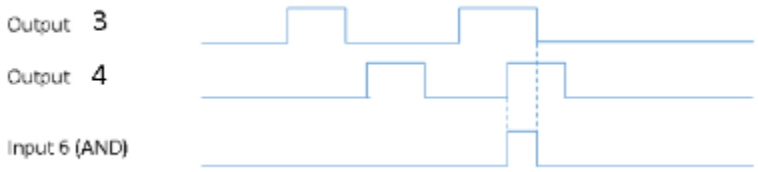


In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, input 5 will be turned on as a result.

Input will remain on as long as any of the outputs remains on. (Unless pulse mode is selected, see below for details)

10.9.3.2 "AND" Input

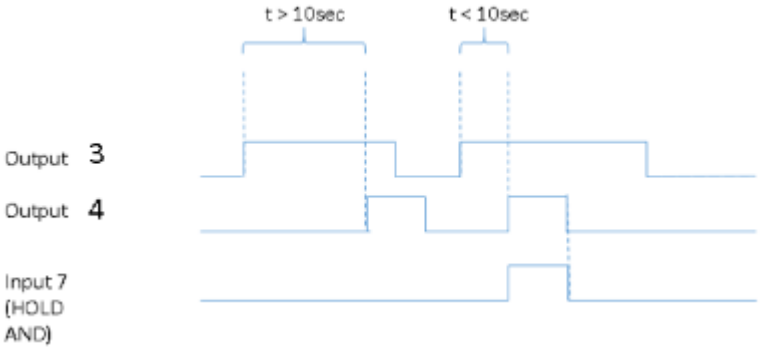
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on simultaneously, input 6 will be turned on.



Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details)

10.9.3.3 "HOLD AND" Input

HOLD AND input become active if all the outputs are active simultaneously, and the time from the first activation to the last activation is less than the time defined in the HOLD AND wait time slider.



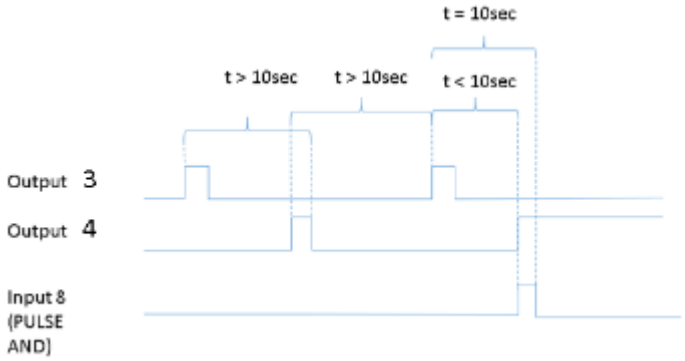
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details

10.9.3.4 "PULSE AND" Input

PULSE AND input will become active if all outputs *have been* active within a specified time.

In our example, if output 3 has been active inside 10 seconds, and output 4 becomes active, then input 8 will be turned on.



Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

In our example, when 10 seconds have elapsed from output 3 activation, input 8 will be turned off.

10.9.3.5 Pulse Mode For Inputs

For each of the four inputs, it is possible to define pulse mode to be in use.



and



The pulse duration can also be adjusted.

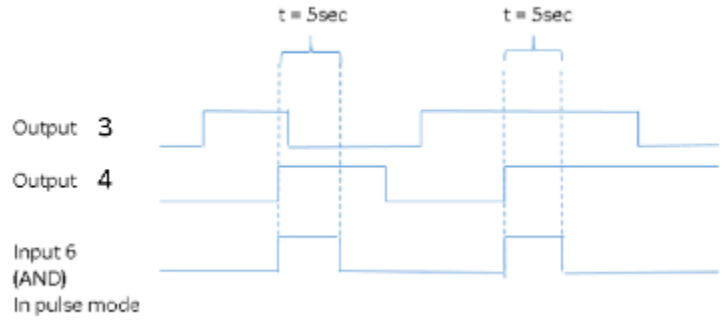


If the pulse mode is in use, the input will turn off after the set pulse duration.

If in our example, we would set the AND input to be in pulse mode like this:



It would mean behaviour like this:



10.9.4 Countdown I/O

With Countdown I/O, it is possible to create actions based on whether some events happen or do not happen at a defined period.

When a new Countdown I/O is created in System Manager, it automatically creates 4 inputs and 4 outputs.

Countdown I/O has two basic modes. The first two input/output pairs are of type 1, and the last two pairs are of type 2.

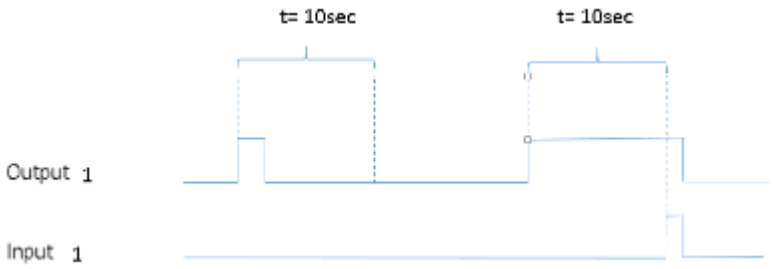
A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

10.9.4.1 Event Duration Exceeded Mode (Type 1)

Firstly, it is possible to trigger an alarm if some event takes longer than the planned duration.

For example, let's say the time is 10 seconds. If output one is triggered and stays active for less than the defined duration, there is no alarm.

If the output is triggered and stays active for longer than the defined duration, there is an alarm.



When creating a new Countdown I/O, the first two input-output pair is of this type.

10.9.4.2 Expected Trigger Mode (Type 2)

Secondly, it is possible to trigger an alarm if an expected pulse is not received inside the defined time.

For example, the time is 10 seconds, and we expect the regular operation to get pulses from output 3 every 2-3 seconds.

When the pulse is missing for longer than 10 seconds, the input state is changed to active. It stays active until the next output trigger is received.



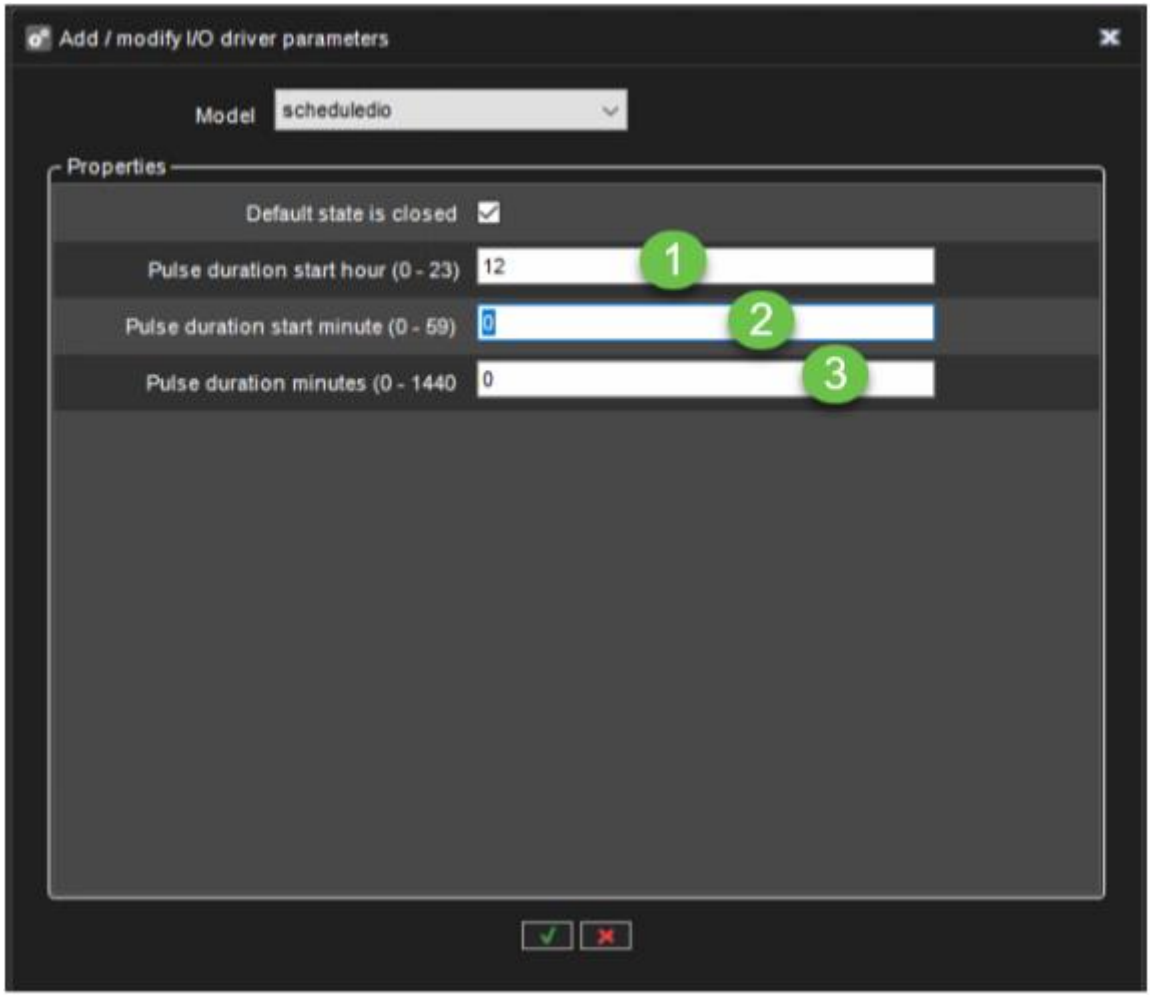
When creating a new Countdown I/O, the last input-output pair is of this type.

10.9.5 Scheduled IO

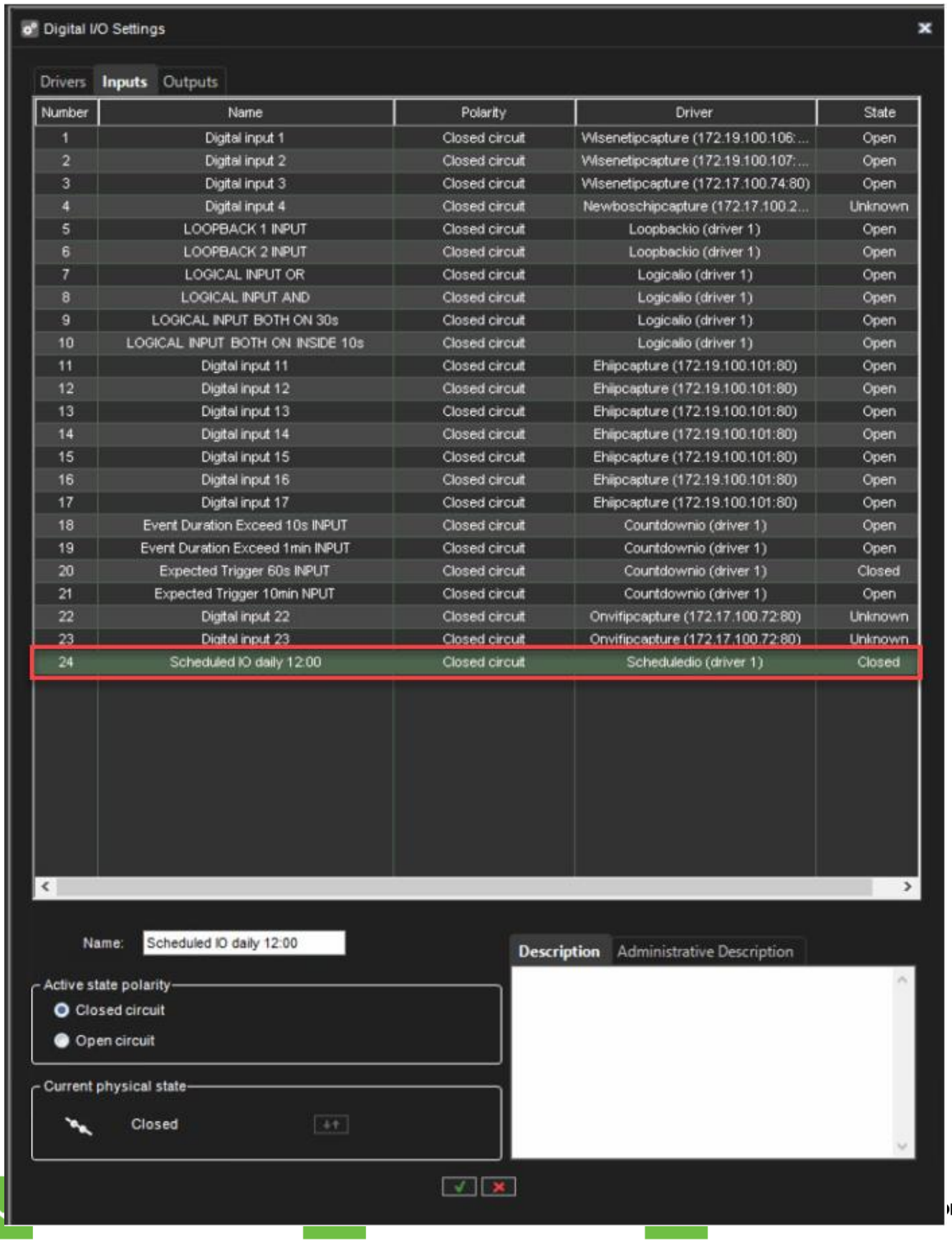
With the Scheduled IO is possible to create a schedule for any digital output, which is connected to the VMS server.

Only the same VMS server digital outputs can be scheduled.

1. Set Pulse duration start an hour
2. Set Pulse duration start minute
3. Set Pulse duration minutes



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com


Digital I/O Settings
Drivers
Inputs
Outputs
Number
Name
Polarity
Driver
State
1 Digital input 1 Closed circuit Wisenetipcapture (172.19.100.106:... Open
2 Digital input 2 Closed circuit Wisenetipcapture (172.19.100.107:... Open
3 Digital input 3 Closed circuit Wisenetipcapture (172.17.100.74:80) Open
4 Digital input 4 Closed circuit Newboschipcapture (172.17.100.2... Unknown
5 LOOPBACK 1 INPUT Closed circuit Loopbackio (driver 1) Open
6 LOOPBACK 2 INPUT Closed circuit Loopbackio (driver 1) Open
7 LOGICAL INPUT OR Closed circuit Logicalio (driver 1) Open
8 LOGICAL INPUT AND Closed circuit Logicalio (driver 1) Open
9 LOGICAL INPUT BOTH ON 30s Closed circuit Logicalio (driver 1) Open
10 LOGICAL INPUT BOTH ON INSIDE 10s Closed circuit Logicalio (driver 1) Open
11 Digital input 11 Closed circuit Ehiipcapture (172.19.100.101:80) Open
12 Digital input 12 Closed circuit Ehiipcapture (172.19.100.101:80) Open
13 Digital input 13 Closed circuit Ehiipcapture (172.19.100.101:80) Open
14 Digital input 14 Closed circuit Ehiipcapture (172.19.100.101:80) Open
15 Digital input 15 Closed circuit Ehiipcapture (172.19.100.101:80) Open
16 Digital input 16 Closed circuit Ehiipcapture (172.19.100.101:80) Open
17 Digital input 17 Closed circuit Ehiipcapture (172.19.100.101:80) Open
18 Event Duration Exceed 10s INPUT Closed circuit Countdownio (driver 1) Open
19 Event Duration Exceed 1min INPUT Closed circuit Countdownio (driver 1) Open
20 Expected Trigger 60s INPUT Closed circuit Countdownio (driver 1) Closed
21 Expected Trigger 10min NPUT Closed circuit Countdownio (driver 1) Open
22 Digital input 22 Closed circuit Onvifipcapture (172.17.100.72:80) Unknown
23 Digital input 23 Closed circuit Onvifipcapture (172.17.100.72:80) Unknown
24 Scheduled IO daily 12:00 Closed circuit Scheduledio (driver 1) Closed
Name:
Scheduled IO daily 12:00
Description
Administrative Description
Active state polarity
Closed circuit
Open circuit
Current physical state
Closed

10.9.6 Properties

HTTP Method(Opened)

- GET
- PUT
- POST
- DELETE

URL(Opened)

Content(Opened)

User(Opened)

Password(Opened)

HTTP Method(Closed)

- GET
- PUT
- POST
- DELETE

URL(Closed)

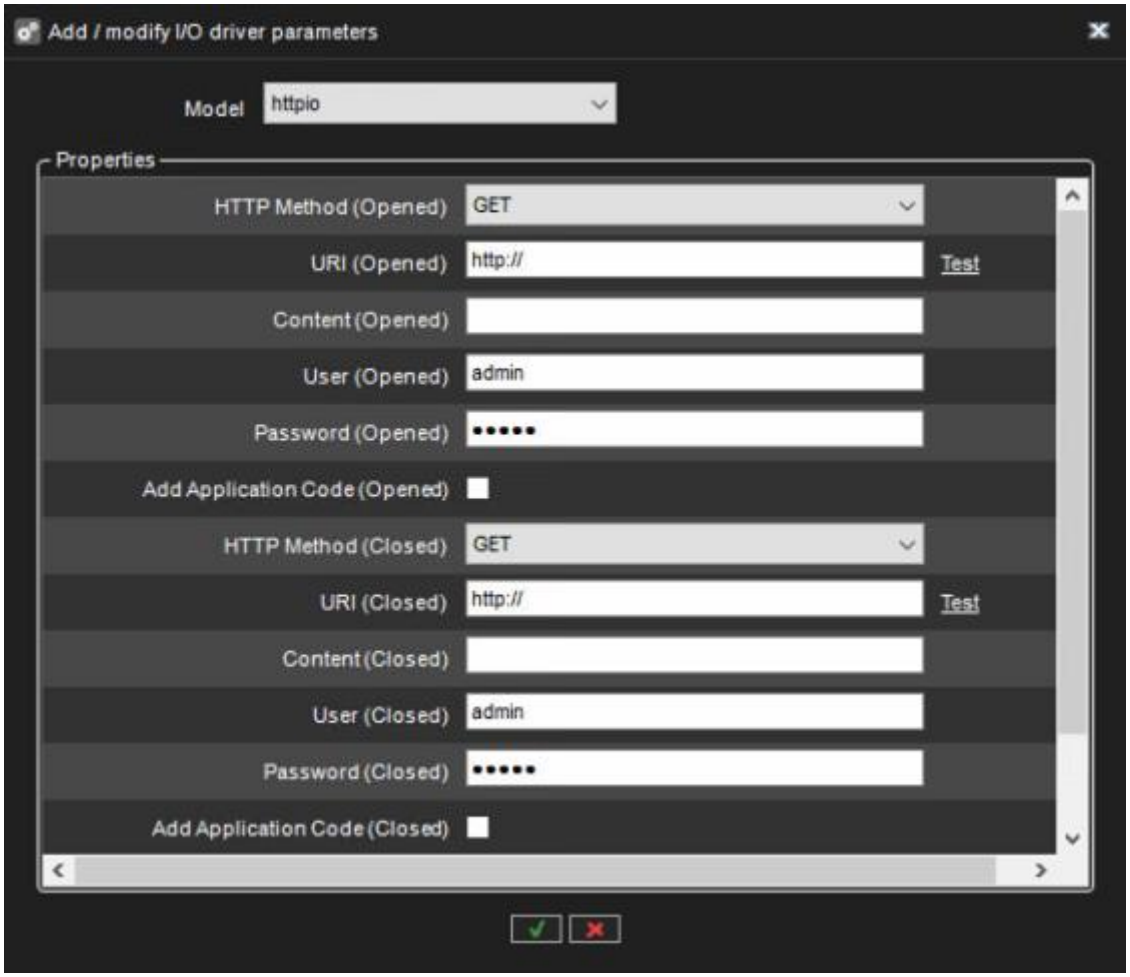
Content(Closed)

User(Closed)

Password(Closed)

Authentication

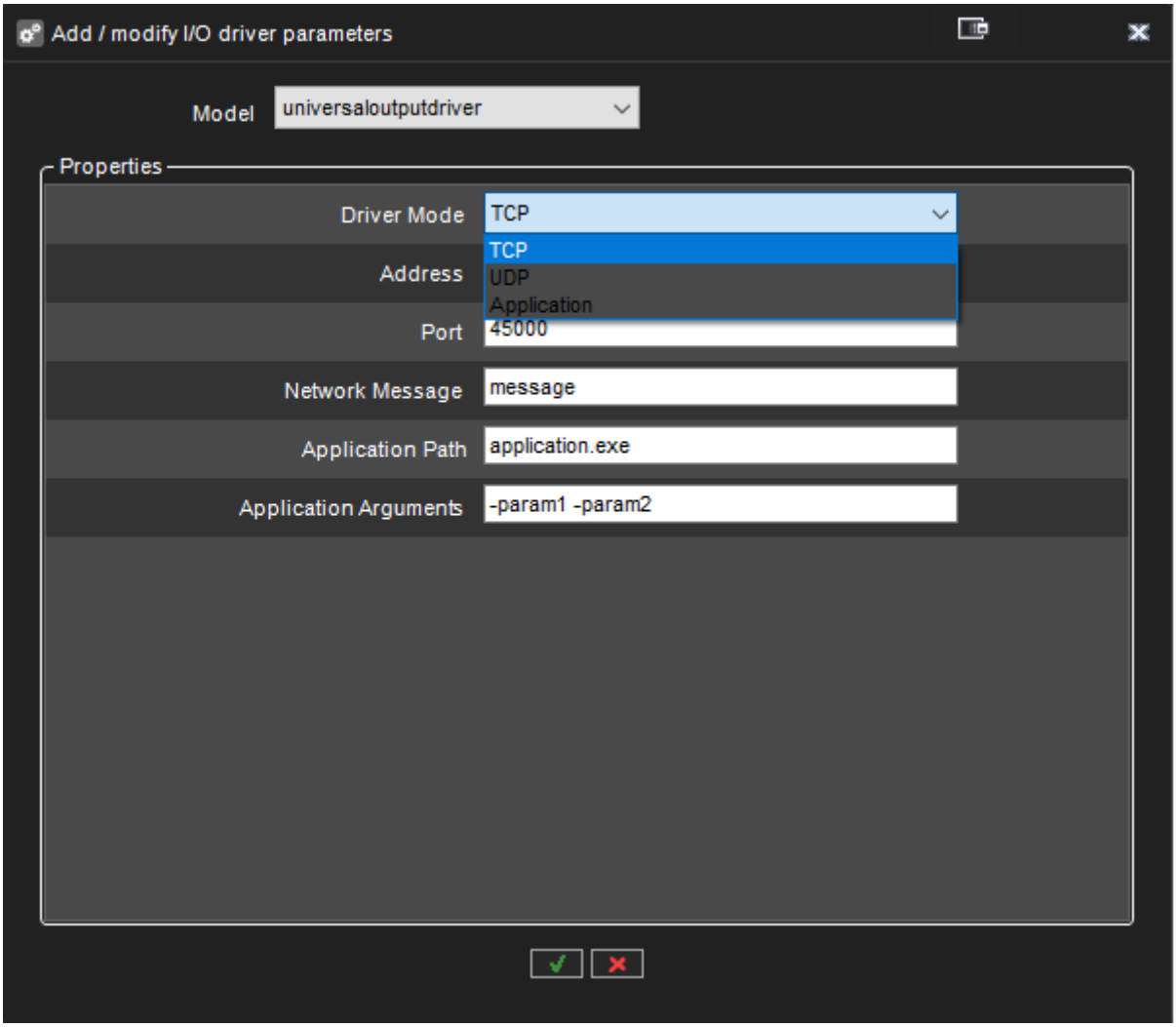
- BASIC
- DIGEST



10.9.7 UniversalOutputDriver

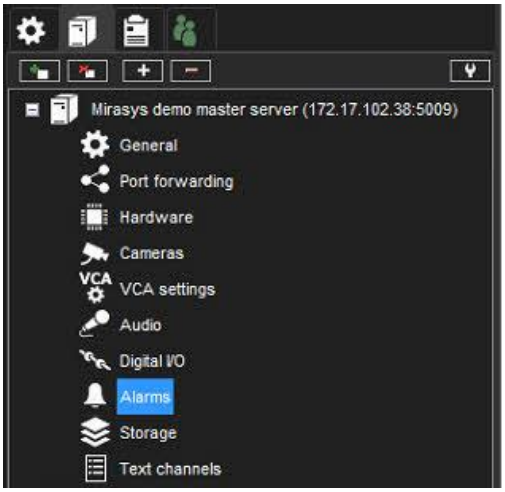
This driver enables you to send data to 3rd party systems or start applications on the server or remote systems.

Please see additional documentation for this driver from our extranet or contact support.



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

10.10 ALARMS



10.10.1 Alarms settings

System Administrators can create, edit, and delete server-specific alarms based on various triggers in System Manager > VMS Servers > Alarm Triggers.

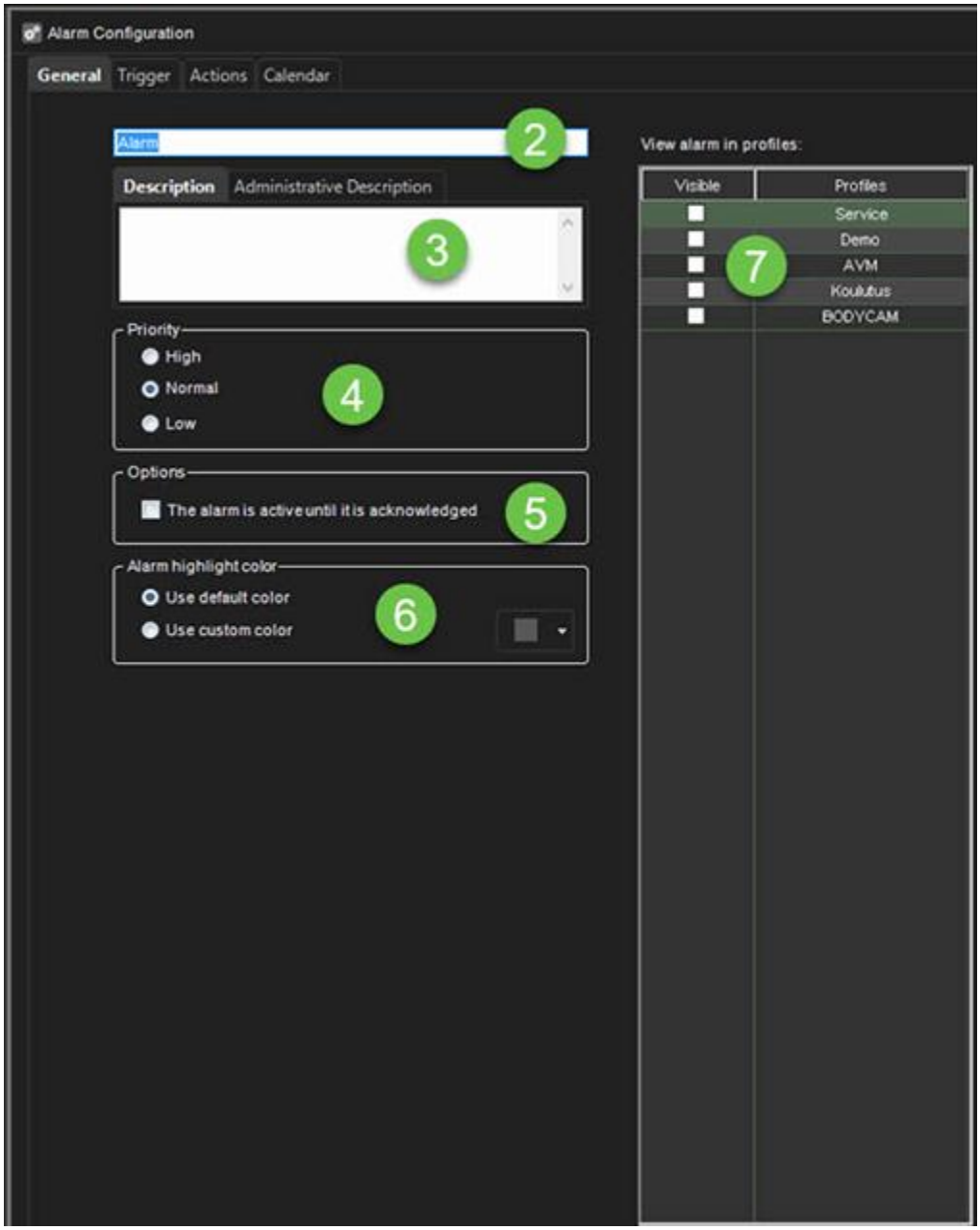
10.10.1.1 Add, Delete, Modify and Copy Alarms

10.10.1.1.1 Adding a new alarm

1. Click **New Alarm** at the lower-left corner of the Alarms screen.



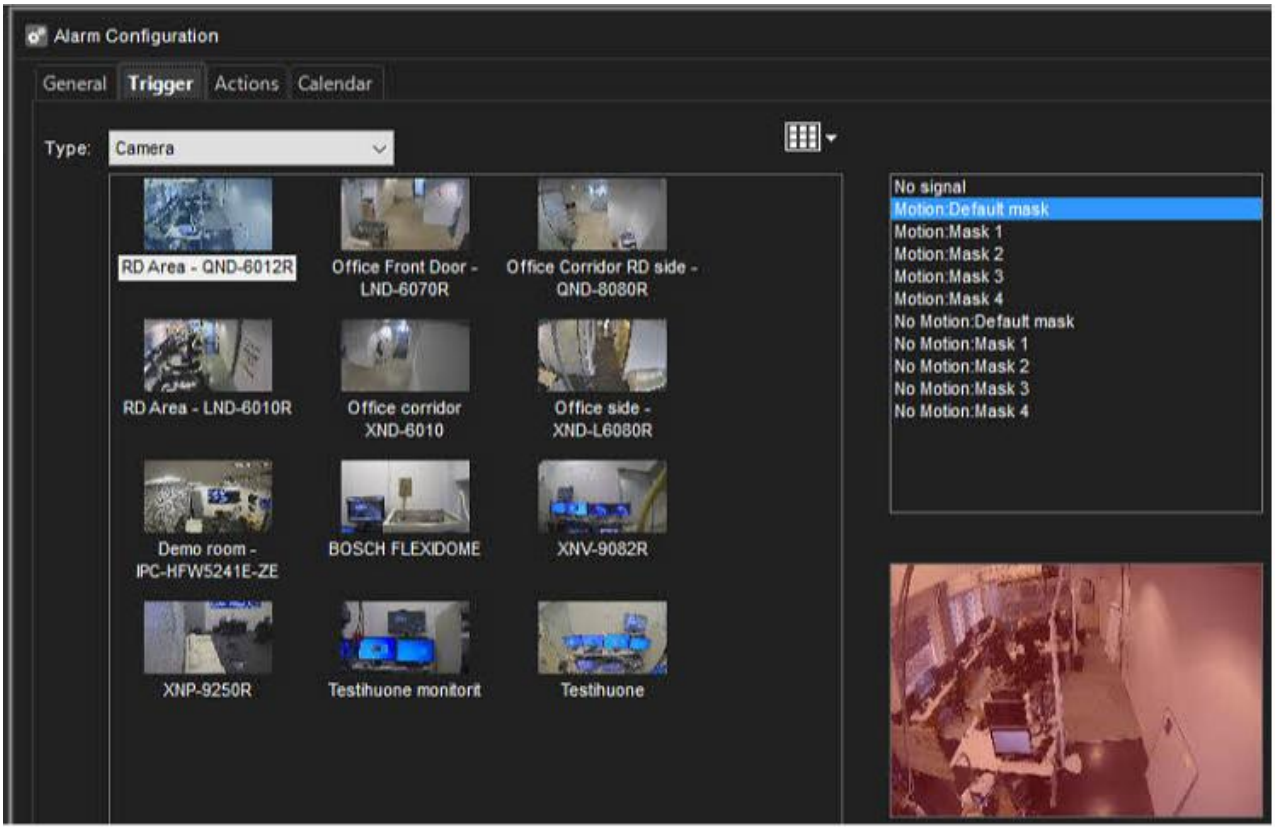
1. Type the name of the new alarm in the **Name** field.
2. Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.
3. Select whether the alarm is of **high**, **average** or **low priority**. The priority is used to define the order in which alarms are executed in case of multiple simultaneous alarms.
4. Select **The Alarm is active until it is acknowledged** to create the alarm as continuous; if the option is selected, the alarm will continue until a user acknowledges it through the **Spotter** application.
5. **Alarm highlight colour** allows administrators to define a custom colour for each alarm separately.
6. In the **View Alarms in Profiles** menu, select the profiles in which the alarm will be used.



Alarms can also be added to profiles through the **Profiles** tab.

10.10.1.1.1.1 Select trigger

1. Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.

2. 

Select the trigger **Type** from the drop-down menu.

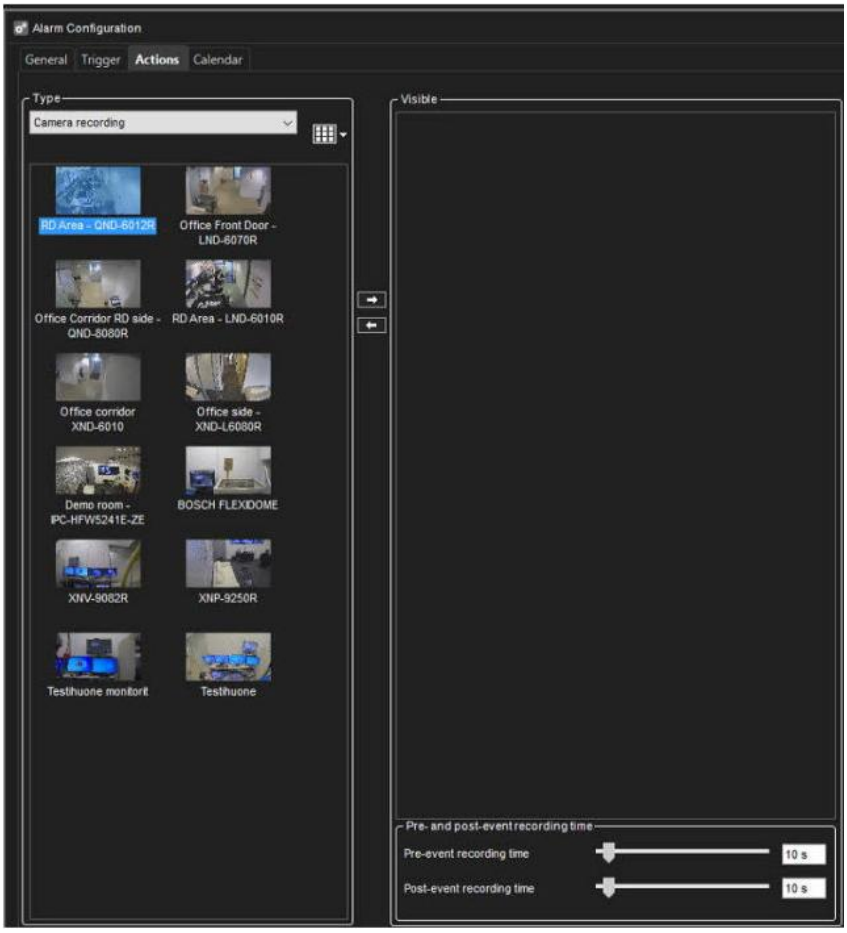
- Camera
- Audio
- Text data
- Digital input
- Metadata
- External (Customized triggers, created under VMS Servers > Alarm Triggers)

3. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.
4. Select the triggering condition from the condition list on the right side of the screen.
    - For camera-based triggers, you can select the mask used in motion detection to trigger the alarm.
    - For audio-based triggers, you can set the alarm to trigger based on a high or low audio level.
    - For text data based (e.g., VCA, metadata, etc.) triggers, you can set the alarm to trigger based on a text data string.

- In addition, you can set an optional alarm ending trigger by marking **Define ending input** and selecting a string for ending the alarm.
- For digital input-based triggers, the alarm is triggered based on the change of the input's polarity.
- For External triggers, you can select the triggers created under Alarm Triggers. For channel based triggers, you can also select the channel.

10.10.1.1.1.2 Actions

1. Open the **Actions** tab. The **Actions** tab is used to define the actions performed by the alarm when it is triggered.



1. Select the action type from the **Type** drop-down menu. The action type defines the basic functionality of the alarm. See more about Action types and settings on the next page.
2. Determine the schedule of the alarm on the **Calendar** tab if needed.
3. Click **OK**.

4. Click **OK** in the alarm list view to save changes.

10.10.1.1.2Deleting an alarm

1. On the **VMS Servers** tab, select the server
2. Double-click on **Alarms**
3. Select the alarm you want to delete by clicking on its name
4. Click **Remove Alarm** at the lower-left corner of the **Alarms** screen



5. Click **OK** in the alarm list view to save changes

10.10.1.1.3Modifying an alarm

1. Go to **Alarms**
2. Select the alarm to be modified
3. Click **Modify Alarm**



4. Make the needed changes and click **OK**
5. Click **OK** in the alarm list view to save changes

10.10.1.1.4Copy and paste alarms

An existing alarm configuration can be copied and pasted to create a new, similar alarm. The user only needs to define the name, description, and trigger for the new copy, making the alarm configuration process quick and efficient.

1. Go to **Alarms**
2. Select the alarm to be copied
3. Click **Copy alarm**



1. Define the name, description, and trigger for the new alarm
2. Click **OK**
3. Click **OK** in the alarm list view to save changes

10.10.1.2 Action Types and Settings

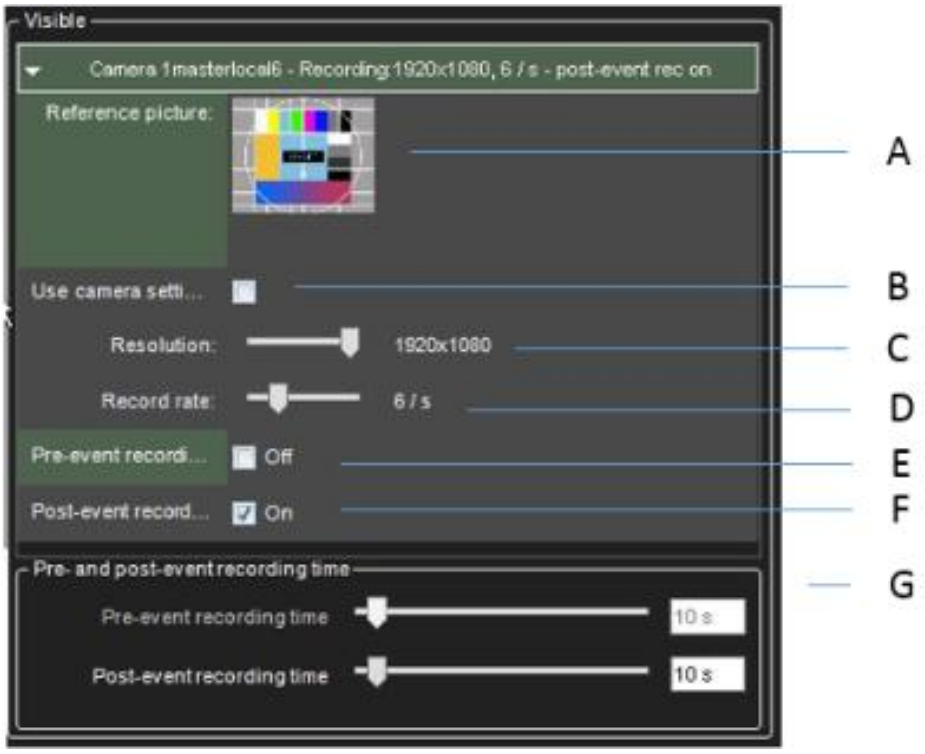
About default action types and their parameters.

> Some of the action types listed below may not be available on all systems.
> In addition to the default actions, the system may include alarm actions installed through third-party modules.

10.10.1.2.1 Camera Recording

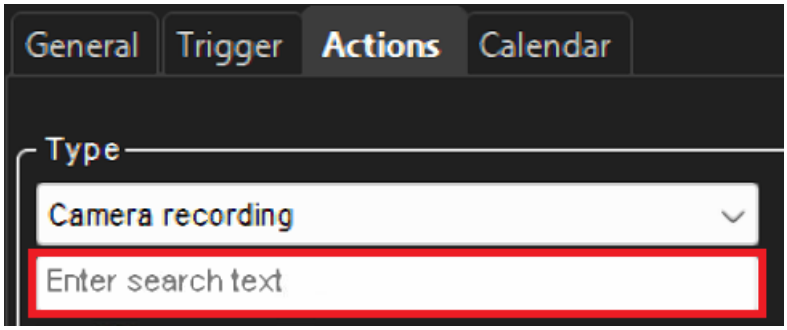
Camera recording is the default action for cameras. When an alarm that contains this action type is triggered, the recording settings defined by the alarm type will be used instead of the camera's default settings.

In **Spotter**, if alarm pop-up windows are enabled for the user profile, devices used with the **Camera recording** action are displayed in the alarm pop-up view when the alarm is triggered.



10.10.1.2.2Searching actions

To search for an action, type the name of the action you are searching for in the search bar.



The action includes the following fields and parameters:

10.10.1.2.2.1 Reference picture

This static field contains the reference picture (image) of the camera (A).

10.10.1.2.2.2 Use camera settings

The alarm recording will be performed using the camera-specific resolution and record rate setting by marking this checkbox (B).

10.10.1.2.2.3 Resolution

Use the slider to change an IP camera's resolution during alarm recording. The slider is active only for IP cameras (C).

10.10.1.2.2.4 Record rate

Use the slider to change the camera's IPS rate during alarm recording. The slider is inactive if the **Use camera settings** checkbox is marked (D).

10.10.1.2.2.5 Pre-event recording

Mark this checkbox to set the pre-event recording on. The duration of the pre-event recording can be set through the **Pre-event recording time** slider (E).

10.10.1.2.2.6 Post-event recording

Mark this checkbox to set post-event recording on. The duration of the pre-event recording can be set through the **Post-event recording time** slider (F).

10.10.1.2.2.7 Pre- & post-event recording duration

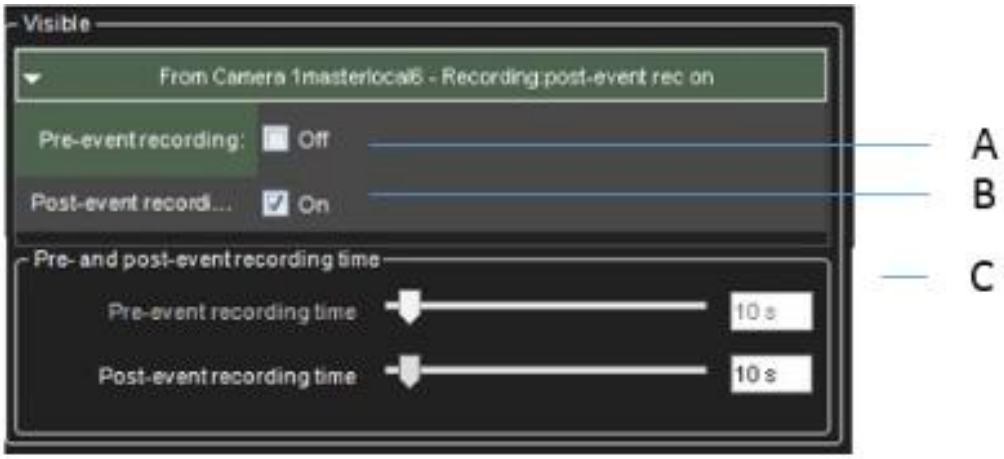
These sliders can be used to set the pre-and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated (G).

All devices (cameras and microphones) are connected to the alarm and have their pre-and post-event recording activated to share the same pre-and post-event recording durations.

10.10.1.2.3Audio Recording

Audio recording is the default action for microphones. When an alarm that contains this action type is triggered, the recording settings defined by the alarm type will be used instead of the microphone's default settings.

In **Spotter**, if alarm pop-up windows are enabled for the user profile, devices used with the **Audio recording** action are displayed in the alarm pop-up view when the alarm is triggered.



The action includes the following fields and parameters:

10.10.1.2.3.1 Pre-event recording

Mark this checkbox to set the pre-event recording on. The duration of the pre-event recording can be set through the **Pre-event recording time** slider (A).

10.10.1.2.3.2 Post-event recording

Mark this checkbox to set post-event recording on. The duration of the pre-event recording can be set through the **Post-event recording time** slider (B).

10.10.1.2.3.3 Pre- & Post Recording duration

These sliders can be used to set the pre-and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated (C).

All devices (cameras and microphones) connected to the alarm and have their pre-and post-event recording activated to share the same pre-and post-event recording durations.

10.10.1.2.4Digital output

The d**igital output** is the default action for digital I/O devices. When an alarm that contains this action type is triggered, the I/O device is activated.

Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

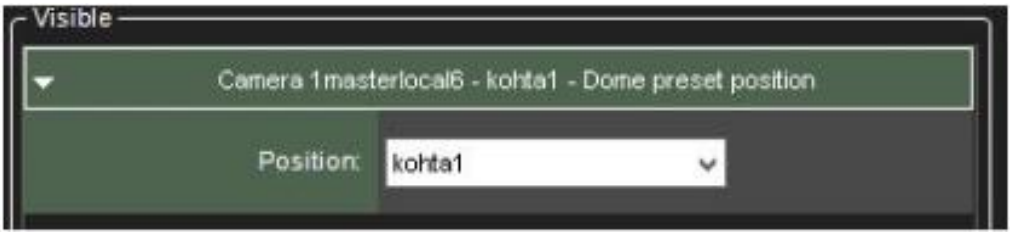
10.10.1.2.5PTZ (Dome) Preset Position

The **PTZ preset position** action can be used to set a PTZ camera to a specified preset position.

When an alarm that contains this action type is triggered, the PTZ camera will automatically move to the selected preset position.

Please see Mirasys VMS Spotter User's Guide for information on setting PTZ camera preset positions.

It should be noted that this action moves the PTZ camera to a preset position but does not result in the video feed from the PTZ camera being displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording,** has been selected for the PTZ camera.



The action includes the following parameters:

10.10.1.2.5.1 Position

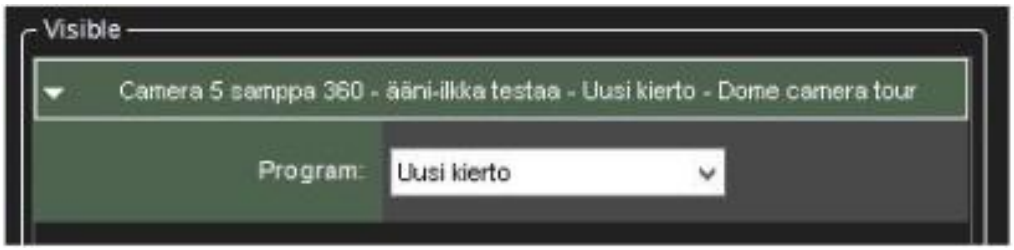
Use the drop-down menu to select the preset position to which the PTZ camera will move during the alarm.

Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

10.10.1.2.6PTZ (Dome) Camera Tour

The **PTZ camera tour** action can be used to set a PTZ camera to start a pre-programmed PTZ camera tour. When an alarm that contains this action type is triggered, the selected PTZ camera tour is started. Please see *Mirasys VMS Spotter User's Guide* for information on setting PTZ camera tours.

It should be noted that this action starts the PTZ camera tour but does not result in the video feed from the PTZ camera being displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording,** has been selected for the PTZ camera.



The action includes the following parameters:

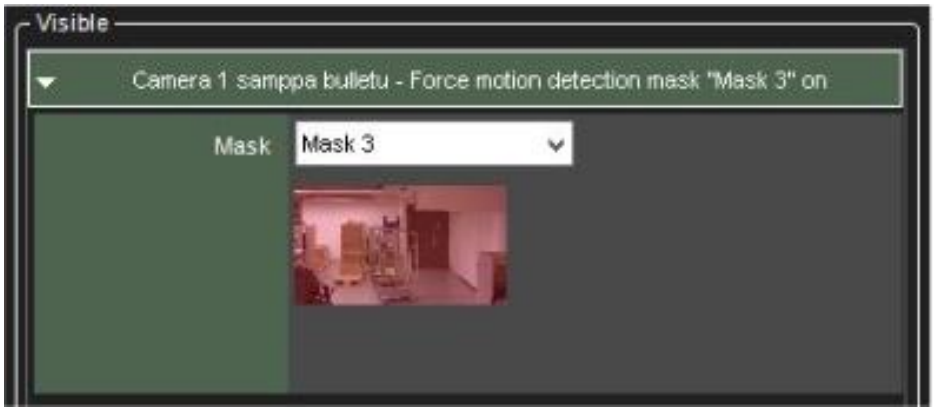
10.10.1.2.6.1 Program

Use the drop-down menu to select the PTZ camera tour, starting when the alarm is triggered.

> Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

10.10.1.2.7Set Motion Detection Mask

The **Set motion detection mask** action can change the motion detection mask used by a specific camera during the alarm. When the alarm occurs, the motion detection mask used for the designated camera is changed to the alarm specific mask. After the alarm ends, the system restores the default mask.



The action includes the following parameters:

10.10.1.2.7.1 Mask

Use the drop-down menu to select the motion detection mask that will be used during the alarm.

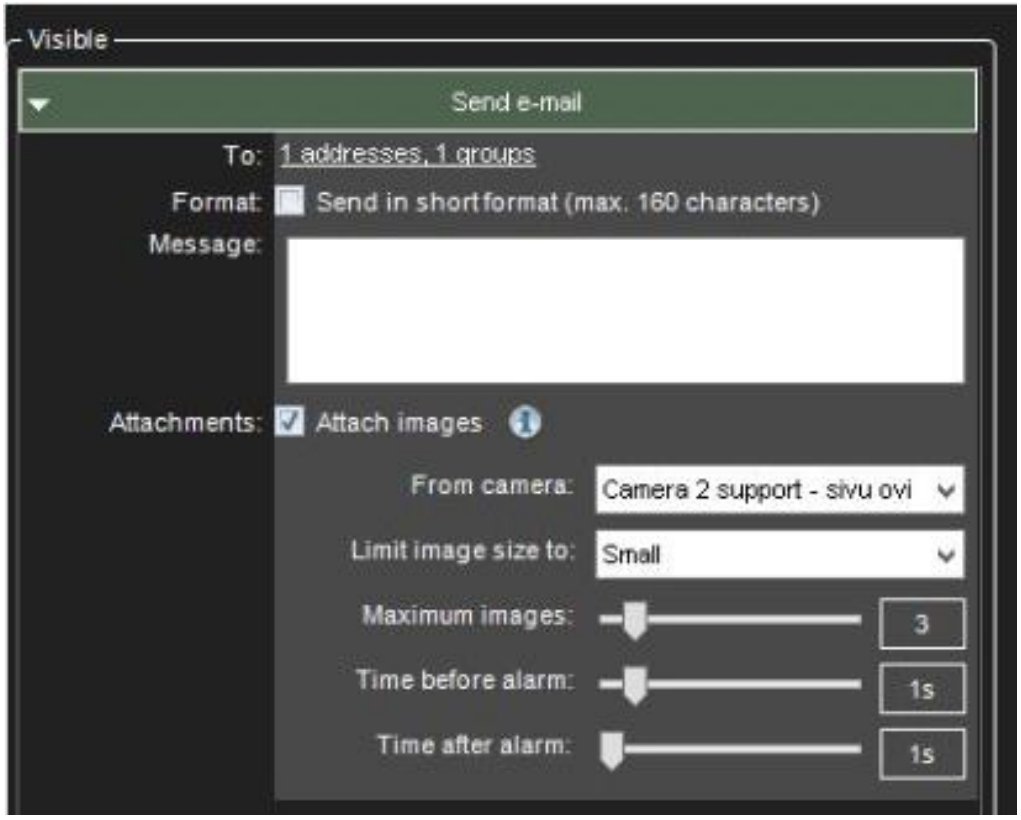
> Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

10.10.1.2.8Send E-Mail

The **Send e-mail** action can be used to send e-mail to any email address or group configured in the **E-mail settings** in the **System** tab.

You can choose which recipient or group should receive the alarm.

You can also include one or more unscaled or scaled-down images in the alarm email. To do this, uncheck the **Send in a short format** -option and check the **Attach images** –option



After this, you can choose a camera, size for the image scaling, desired number of images, and the time span from which the images are fetched.

- The number of images in this configuration is the maximum amount delivered. Fewer images might arrive.
- Attaching images to alarm emails might lead to high data traffic, so it is recommended to test the configuration settings to find the optimum setting.
- If you experience issues that no images are arriving with the default settings, it is recommended to select more than one image to the "maximum images" setting and adjust the sliders slightly to have a longer duration of time where the images are being fetched.

The action includes the following parameters:

10.10.1.2.8.1 Format

Defines the message format as short or usual.

A short message will contain only up to 160 characters and cannot contain additional message text or image attachments (see below).

10.10.1.2.8.2 Message

This field contains the message that will be sent to the recipients if the alarm occurs. The message field is active only if the e-mail format has been set as long.

Unlike other alarm actions, the **Send e-mail** action can be selected only once for each alarm. Once selected, the action will disappear from the list of available actions.
The message will have the alarm name in the title.

10.10.1.2.9Adjust settings for all alarm actions at once

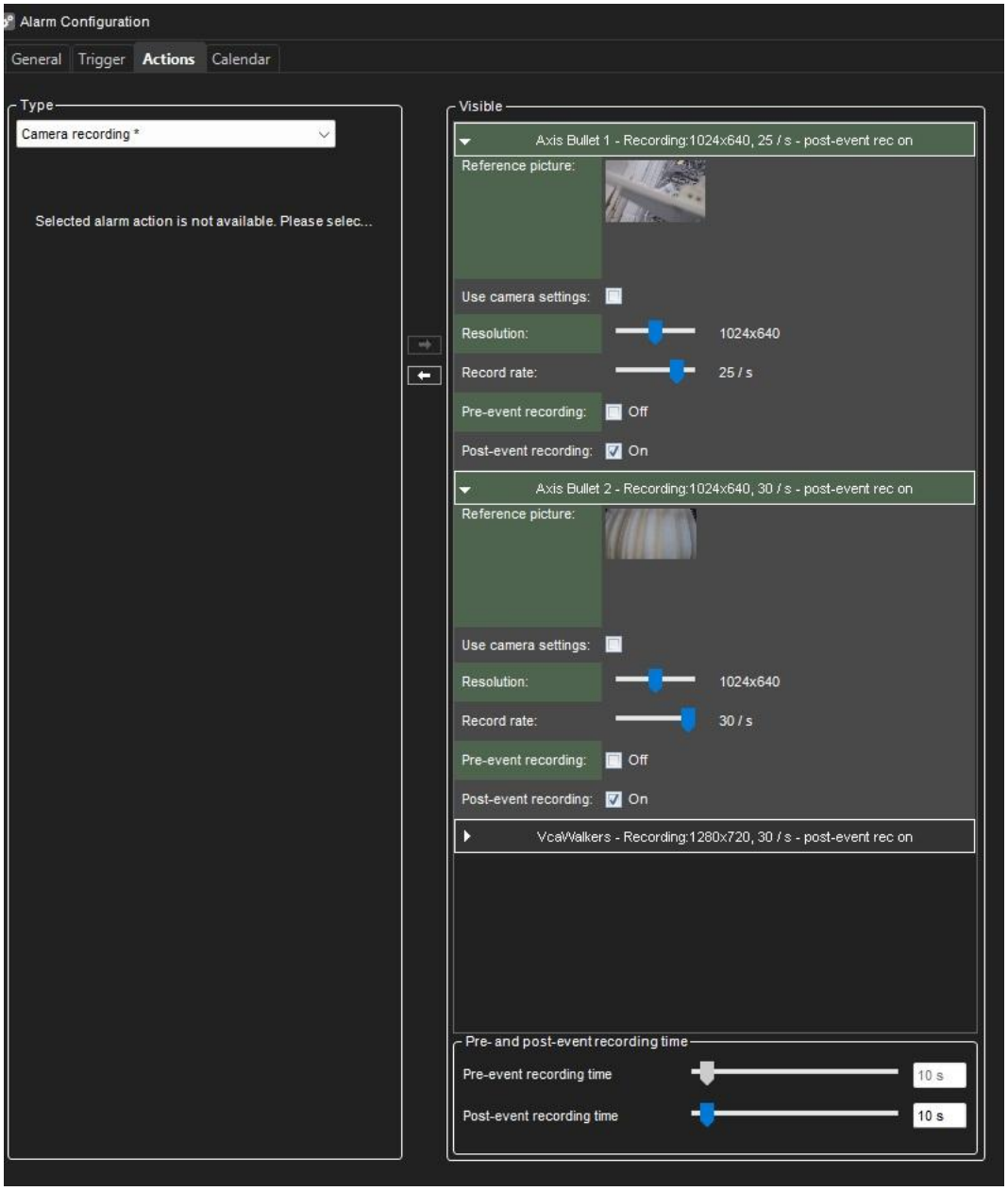
Settings for multiple alarm actions can be adjusted simultaneously in Alarm Configuration. This option speeds up the configuration when alarms have similar actions, as the settings don't have to be adjusted separately for each action. For example, in the picture below, the alarm action settings can be adjusted for both of the selected cameras simultaneously.

To adjust settings for multiple actions at once, all selected actions must share the same action type.

Adjusting the settings for all alarm actions at once:

1. Open **Alarms**
2. Open the **Actions** tab in Alarm Configuration
3. Select the correct action type from the dropdown menu and add desired actions

4. Select the added actions from the list (you can choose multiple by holding Ctrl while clicking the items)
5. Adjust the settings of one of the selected actions: the same changes are automatically applied to all selected actions



10.10.1.2.10 Disable Alarms

The **Disable alarms** action can be used to send disable alarms based on one alarm. The configuration can be done so that all alarms are disabled, low and medium priority alarms, or low alarms.

This option allows specific alarms to remain active while others are suppressed.

The alarms are disabled only while the alarm that disables them is active.

10.10.1.3 ONVIF Profile M

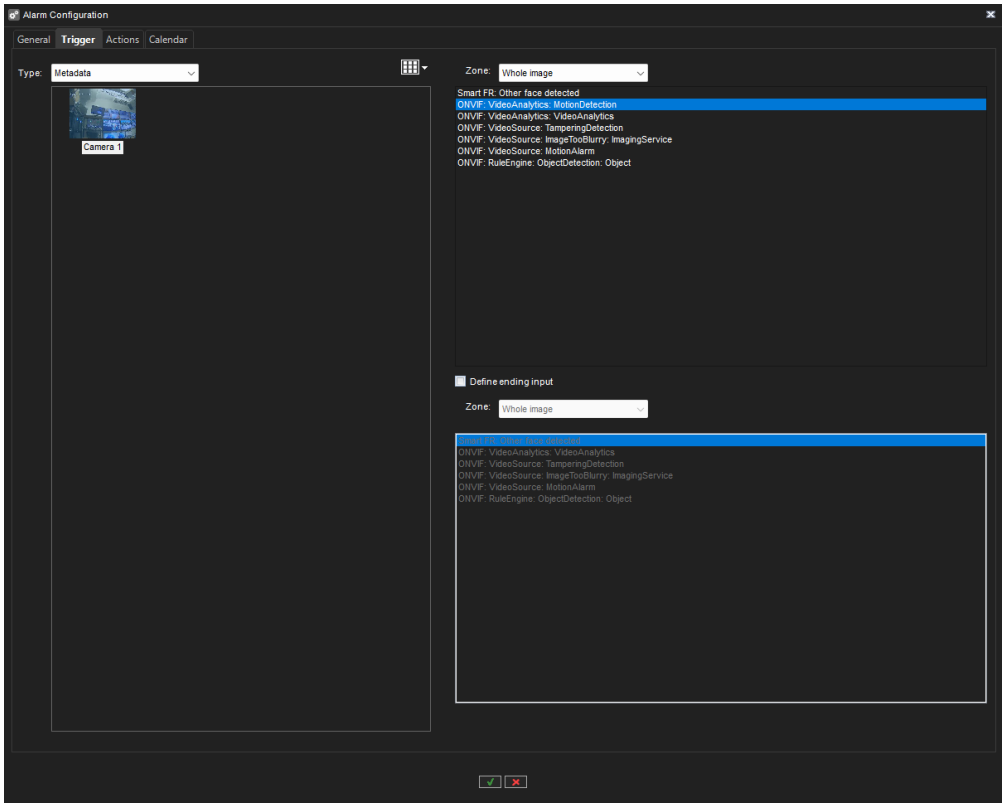
ONVIF profile M support enables our system to respond to the triggering of an alarm generated by camera analytics.

> See ONVIF Profile M Custom Alarm Triggers for how to create customized triggers

10.10.1.3.1 ONVIF alarm

When you have added a device that supports ONVIF Profile M, you do not need to take any special steps to enable or disable these triggers. They are automatically added to the camera's metadata triggers.

In the Alarm Configuration in System Manager, this will be displayed in the **Trigger tab** and listed as ONVIF. You can use these to create new alarms.



10.10.1.3.2Creating an ONVIF alarm trigger

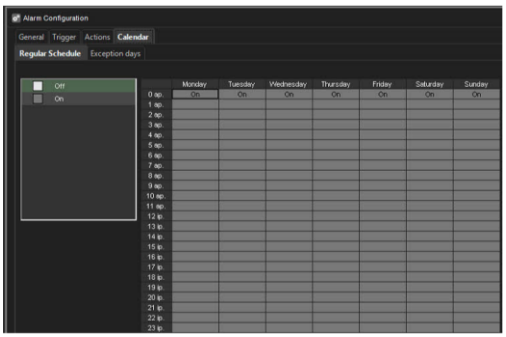
Note that device alarms/triggers itself should be configured using device web interface, not in the System Manager.
This configuration should be done **before** you add device to VMS. Otherwise device capabilities should be refreshed in System Manager for it to include the changes in device.

1. Start the System Manager desktop application.
2. Add a device with ONVIF Profile M support.
3. Go to the VMS Servers tab.
4. Select **Alarms**.
5. Select a **New Alarm**.
6. The **General** tab opens. Name the alarm in the general tab, and select which profiles will use the alarm.
7. Go to the **Trigger** tab.
8. Select **Metadata** as the type.
9. Select the type of ONVIF metadata you want to use to trigger the alarm.
10. Go to the **Actions** tab and select the desired action for the alarm.
11. Go to the **Calendar** tab and select which days/hours are enabled for the alarm. By default, the alarm is active 24 hours each day.
12. Click the OK checkmark ☑ at the bottom of the page

10.10.1.4Alarms Calendar

In VMS Servers > Alarms > Calendar, you can define when the alarm should be active.

1. Define that when the alarm is active
2. Click **OK**



10.10.1.4.1Holiday Schedules

Alarm specific holiday schedules can create schedules for specific dates or set a specific date to use an alarm schedule designed for another weekday. The **Holidays** sub-tab can be accessed through the alarm's **Schedule** tab.

10.10.1.4.2Set a specific date to function with another weekday's schedule

1. Select the weekday from the schedule list on the left side of the screen.
2. Select the desired year and month from the drop-down menus above the calendar.
3. Click on a date in the calendar to add the schedule.

10.10.1.4.3Create a custom schedule

1. Click Add at the upper left side of the screen.



2. Type the name of the holiday schedule in the **Schedule name** field.
3. To create the schedule, select **Off** from the **On/Off** list on the left side of the screen and mark the hours the alarm is switched off for the day.
4. Click **OK** to save the schedule.
5. Select the desired year and month from the drop-down menus above the calendar.
6. Click on a date in the calendar to add the schedule.

10.10.1.4.4Edit a custom schedule

1. Select the custom schedule from the schedule list on the left side of the screen.
2. Click **Edit** at the upper left side of the screen.



3. Edit the schedule.
4. Click **OK** to save the changes.

10.10.1.4.5Delete a custom schedule

1. Select the custom schedule from the schedule list on the left side of the screen.
2. Click **Remove** at the upper left side of the screen.



10.10.1.4.6Restore the original schedule

1. Click **Restore** in the schedule list on the left side of the screen.
2. On the calendar, click the day that you want to restore.

10.10.2 Custom Alarm Triggers

System Administrators can create custom alarm triggers in System Manager > VMS Servers > Alarm Triggers. Under this tab, you can view all custom alarm triggers created in table format displayed by Trigger name, type, Unique ID, and Camera.

10.10.2.1 Web API Custom Alarm Triggers

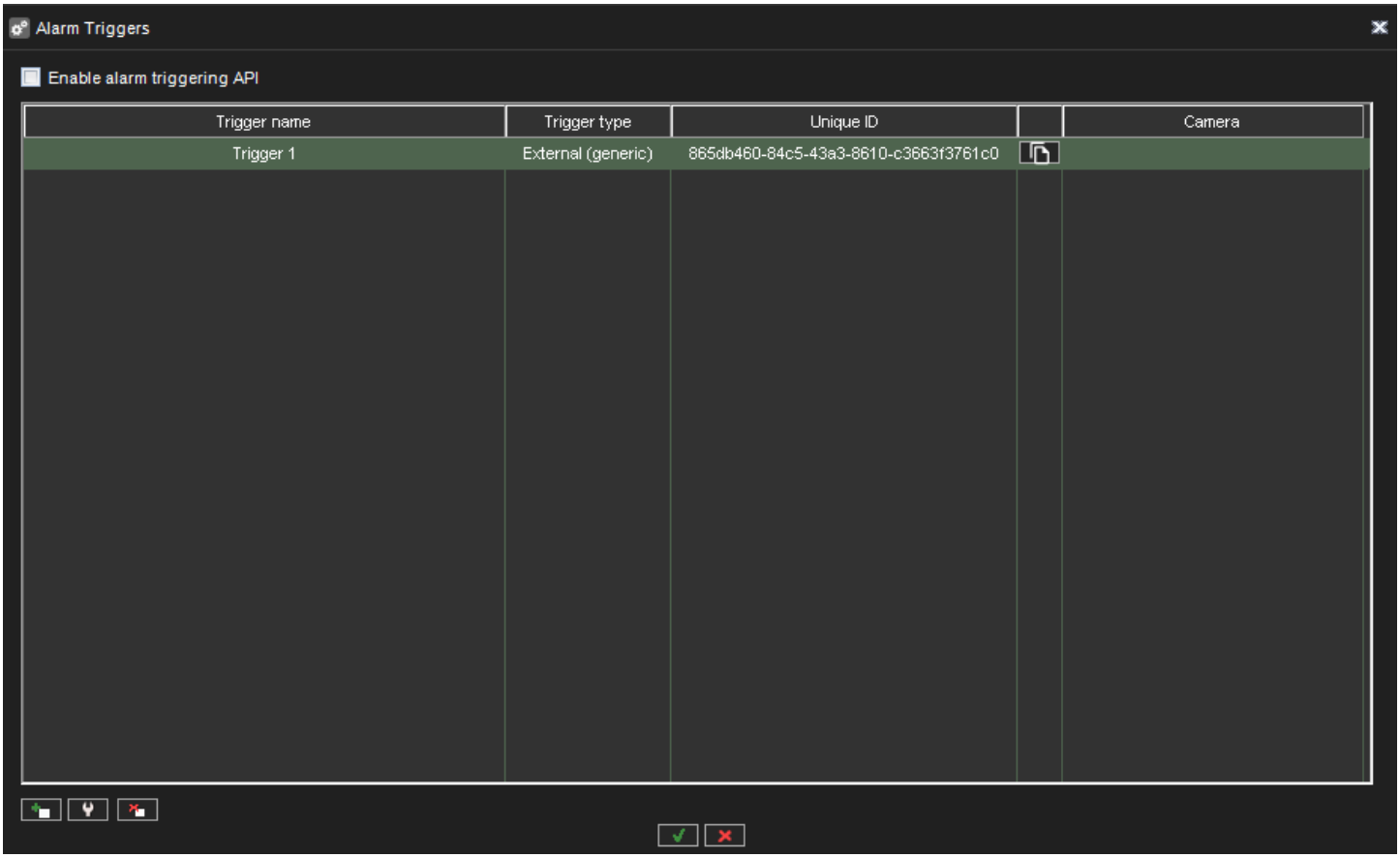
When using Mirasys Alarm API to integrate into our system, System Administrators can create custom alarm triggers in System Manager > VMS Servers > Alarm Triggers.

Under this tab, you can view all custom alarm triggers created in table format displayed by Trigger name, type, Unique ID, and Camera.

When you **Enable alarm triggering API** in the Alarm Triggers window, you will see all alarm triggers created from Mirasys Alarm API.

10.10.2.1.1Create an alarm trigger

1. To create an alarm, go to **VMS Servers**, and select recorder.
2. Open **Alarm Triggers**.
3. Click the green + sign at the bottom-left of the window to **Add an API trigger**. A new dialog to **Add new alarm trigger** will open.
4. Select trigger type **Mirasys Alarm API**.
5. Write the **Trigger Name** in the free text field.
6. Select Type, which is either **Generic Alarm** or **Channel**.
    - For **Channel**, please define the Channel range.
7. Click **Save**. The system will generate a unique ID for the trigger, and it will be displayed in the **Alarm Triggers** table.
8. Click the green checkmark to **Save** the **Alarm Triggers** settings.



10.10.2.1.2Edit an alarm trigger

1. To modify an alarm trigger, go to **VMS Servers**, and select recorder. Under **Alarms**, open **Alarm Triggers**.
2. Select the trigger you want to modify from the list.
3. Click the **Modify** button.
4. You can change the trigger name and select Channel or Generic Alarm. For Channel, please define the Channel range. The system will generate a unique ID for the trigger.
5. Click **Save Changes**.

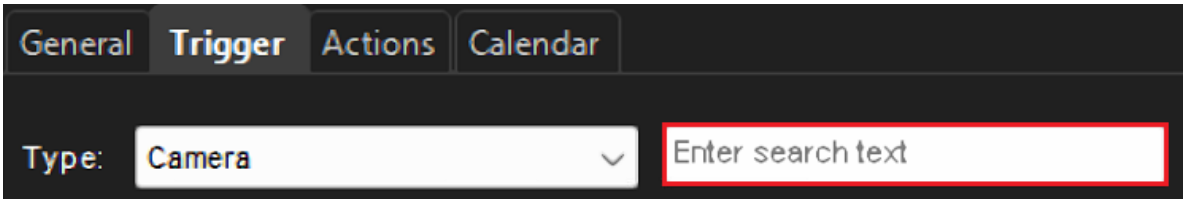
10.10.2.1.3Delete an alarm trigger

1. To delete an alarm trigger, go to **VMS Servers**, and select recorder. Under **Alarms**, open **Alarm Triggers**.
2. Select an alarm from the trigger list.
3. Click the **Delete** button.

4. Confirm the deletion in the confirmation modal.

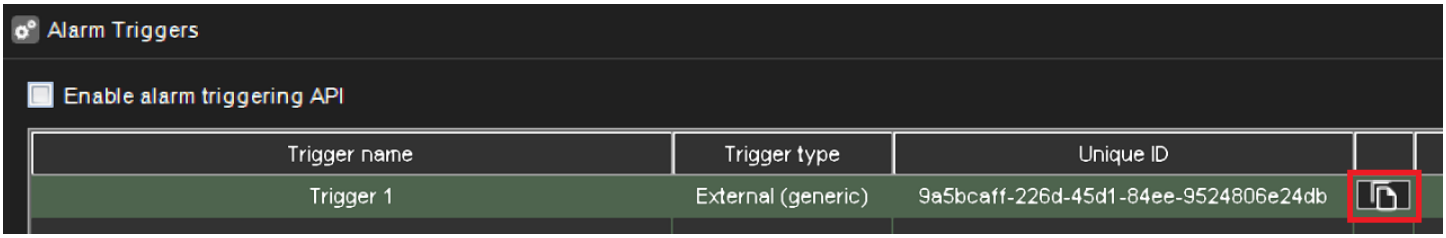
10.10.2.1.4Search for alarm triggers

1. Go to **Alarms** and double-click on an alarm
2. Open the **Trigger** tab
3. Type the name of the trigger you are searching for in the search bar



10.10.2.1.5Copy an alarm trigger ID

1. Go to the **VMS Servers** tab in System Manager
2. Double-click **Alarm Triggers**
3. Click the **Copy** button next to the ID of the trigger



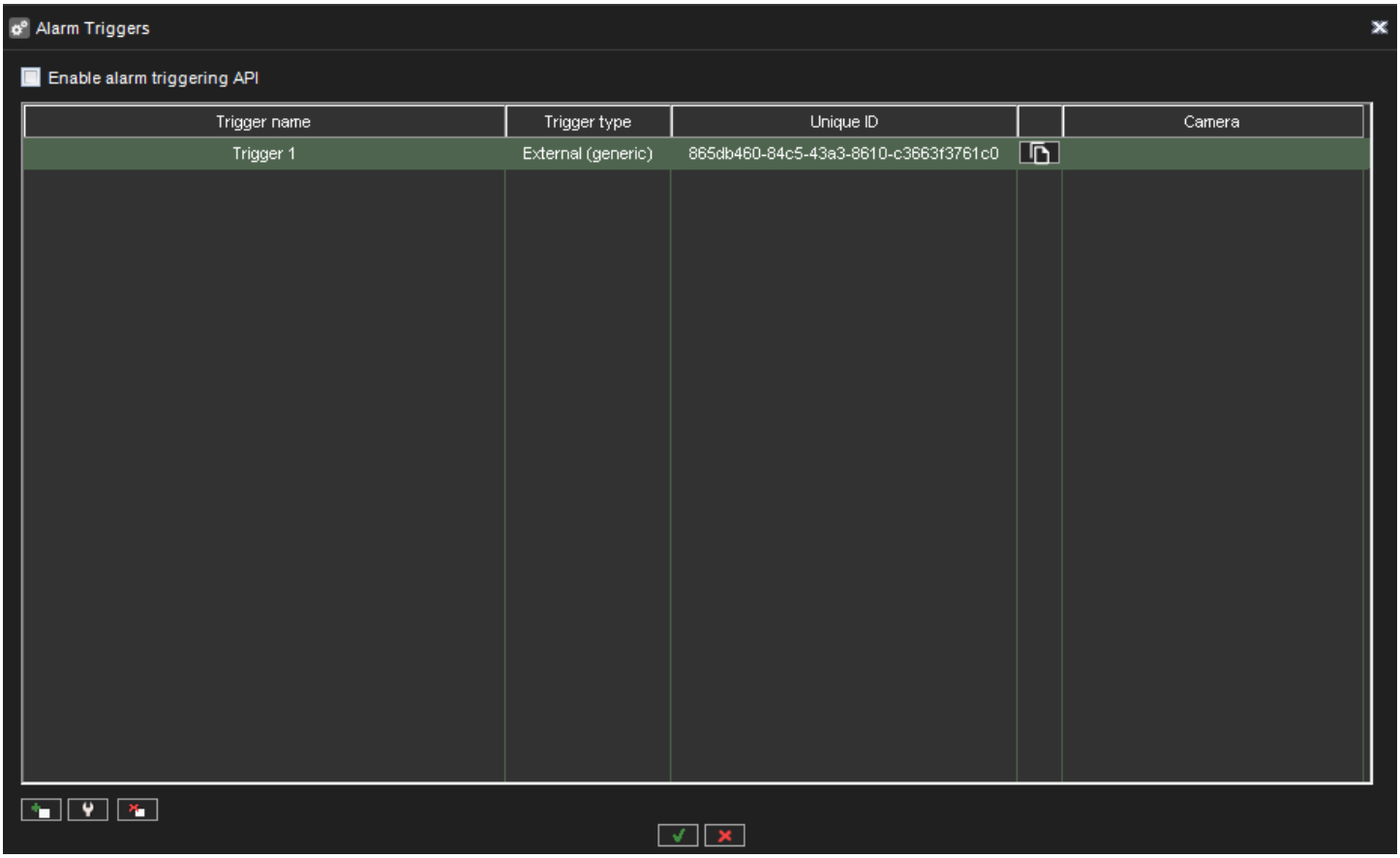
The trigger ID can also be copied when adding or modifying a trigger by selecting the text in the ID field and pressing Ctrl + C or by right-clicking on top of the text and selecting “Copy”.

The ID is copied to the clipboard and thus can be easily pasted in external applications.

10.10.2.2 ONVIF Profile M Custom Alarm Triggers

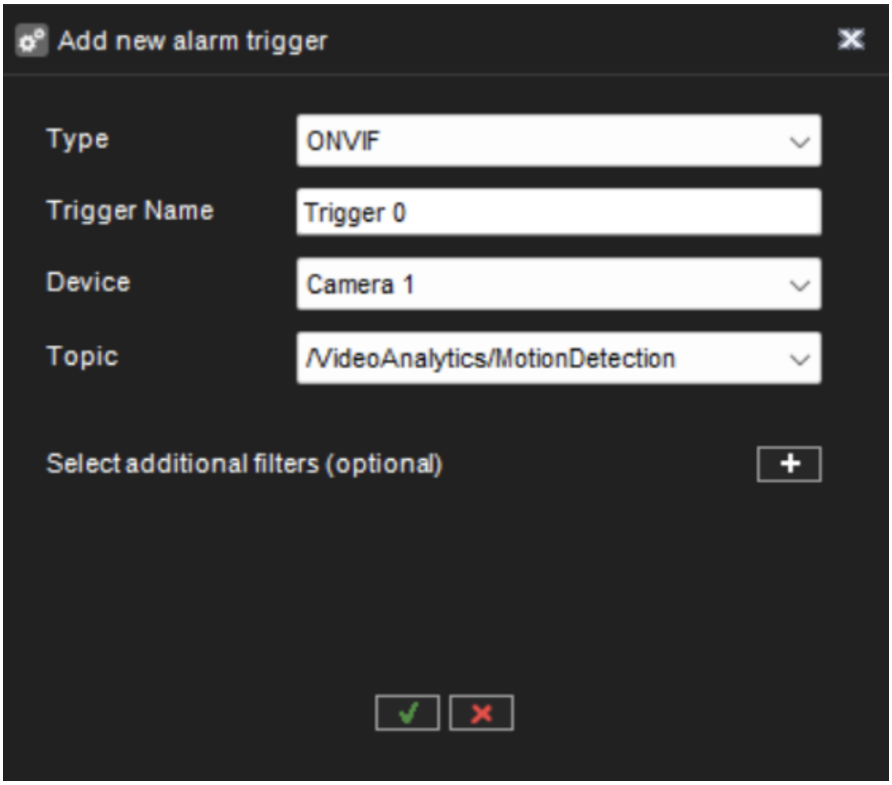
When using ONVIF Profile M conformant devices, System Administrators can create alarm triggers in our VMS based on the metadata available on the camera side.

Go to System Manager > VMS Servers > Alarm Triggers



10.10.2.2.1Create an alarm trigger

1. Open Alarm Triggers. A table of your custom alarm triggers will be displayed.
2. Click the + sign in the bottom-left corner to add an alarm trigger.
   This will open the **Add new alarm trigger** dialog.
3. Select the trigger **Type** ONVIF.
4. Write the **Trigger Name** you have chosen for the trigger.
5. Select a camera in the drop-down **Device** menu.
6. Select a **Topic** for the trigger in the drop-down menu, such as Motion Detection.



1. **Select additional filters** by clicking the + sign.

10.10.2.2.2Filter by source and parameter

We highly recommend selecting optional filters by source and parameter for specifying which alarms to receive.

In the Filter by source and parameter System Administrators can add as many filters as they would like.

To **Add Source**, click the + sign. Select the source from the available sources in the drop-down menu **Name**s. Define the **Value**. Define the **Operation**.

To **Add Parameter**, click the + sign. Select the parameter from the available parameters in the drop-down menu Names. Define the **Value**. Define the **Operation**. Select **Greater or equal** or **Less or equal** under operation to define a value range.

To remove sources and parameters, there is a red - sign to the right of each row. Click to remove.

Click ✓ to **Save**. You will return to the Add new alarm trigger dialog.

If you have not entered the value, the save ✓ functionality is disabled.

1. Click ✓ to **Save**.

10.10.2.2.3Edit an alarm trigger

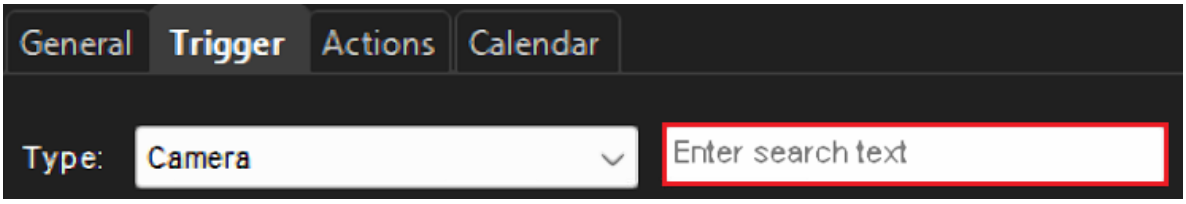
1. To modify an alarm trigger, go to **VMS Servers**, select recorder, and under alarms, open **Alarm Triggers**.
2. Select the trigger you want to modify from the list.
3. Click the **Modify** button at the bottom left (wrench symbol).
4. See Create an Alarm Trigger above for instructions on how to make modifications.
5. Click ✓ to **Save** changes.

10.10.2.2.4Delete an alarm trigger

1. To delete an alarm trigger, go to **VMS Servers**, and select recorder.
2. Open **Alarm Triggers**.
3. Select an alarm from the trigger list.
4. Click the red X button at the bottom left to **Delete**.
5. Confirm the deletion in the confirmation modal.

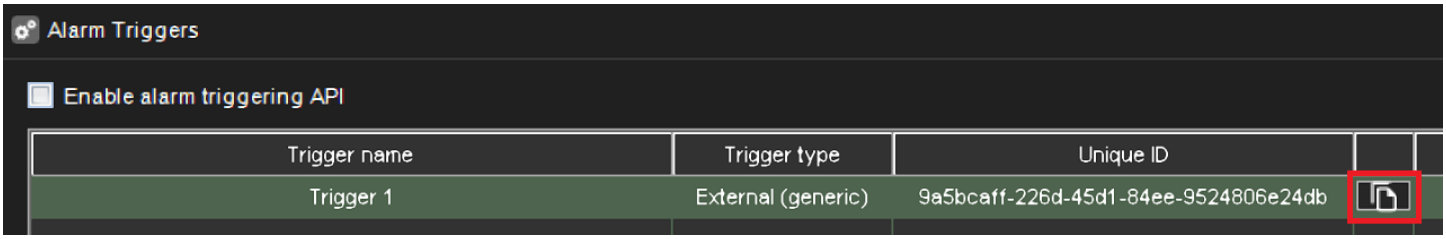
10.10.2.2.5Search for alarm triggers

1. Go to **Alarms** and double-click on an alarm
2. Open the **Trigger** tab
3. Type the name of the trigger you are searching for in the search bar



10.10.2.2.6Copy an alarm trigger ID

1. Go to the **VMS Servers** tab in System Manager
2. Double-click **Alarm Triggers**
3. Click the **Copy** button next to the ID of the trigger



The trigger ID can also be copied when adding or modifying a trigger by selecting the text in the ID field and pressing Ctrl + C or by right-clicking on top of the text and selecting "Copy".

The ID is copied to the clipboard and thus can be easily pasted in external applications.

10.11 Storage

In storage settings, you can set the storage time of the recorded video, audio and text data, and alarm data.

In addition, after adding a hard disk to a server, you can set it as additional data storage through the storage settings.

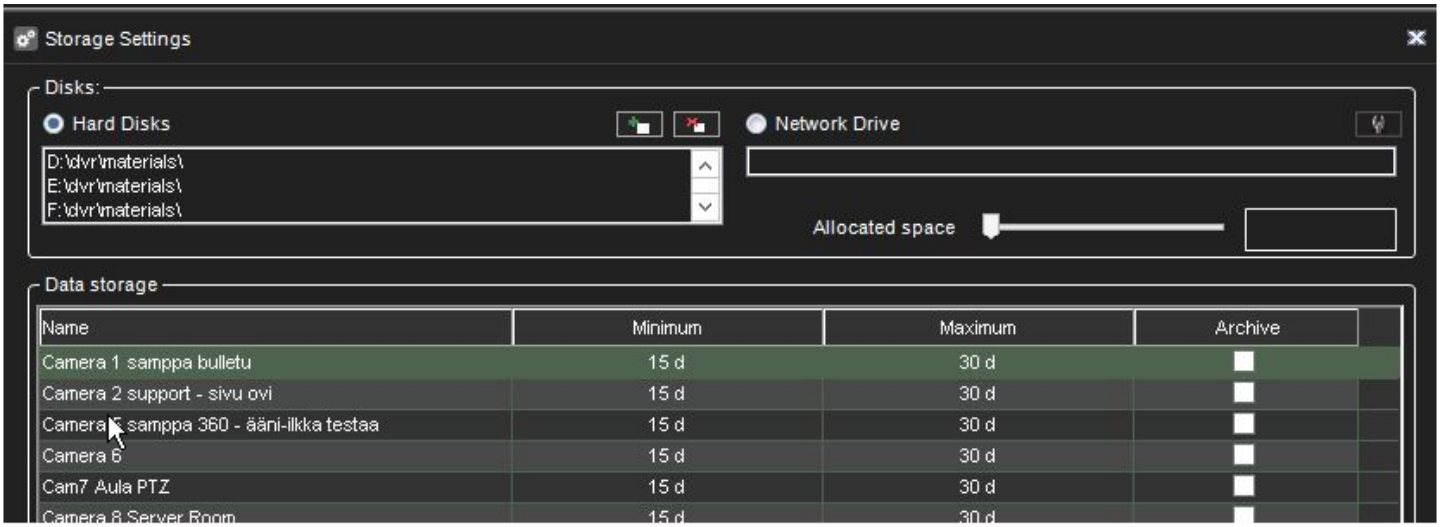
The storage settings are also used to configure the automatic archiving functionality, enabling the creation of backup copies of the server-specific video, audio, and text data daily or weekly.

Video, audio, text data, and alarm recordings are kept until their defined **Maximum** date has been exceeded or until the allocated storage space has run out.

10.11.1 Adding Storage Space

If additional storage space is required, you can add new hard disks or map a network drive for data storage (i.e., NAS support).

There can be multiple network storage disks, and local disks used simultaneously, as seen in the picture.



Note: *When adding storage drives to legacy Mirasys filesystem (VMS server version 7.5.x or earlier), the storage drives are recommended to be all of the same capacity, and any single disk should be less than 10TB in size, and the total amount per VMS server should be less than 25 TB in size.*

The use of multiple storage disks has the benefit of allowing material write to be distributed to all the drives, making a loss of any single material drive less likely to wipe out large parts of the stored material.

10.11.1.1 To add a hard disk:

1. Install the new disk.
2. In Storage Settings, click **Add Disk**.



3. The Add Disk dialogue box is shown. The Minimum free space on the new disk box shows how much free space the new disk must-have.
4. Select the disk from the list and click **OK**.

10.11.1.2 To map a network drive:

1. In **Storage Settings**, mark the **Network drive** checkbox.
2. If needed, click **Define network drive** to open the network drive configuration screen.



3. Type the network drive username and password into the **Username** and **Password** fields.

4. Type the location of the network drive into the **Network drive path** field.
5. Click **OK**.
6. Use the **Allocated space** slider to set the space reserved on the network drive for data storage.

10.11.1.3 To map multiple network drives:

1. Install and configure the networks storage to work as a locally mapped drive (for example, use iSCSI initiator or similar).
2. In Storage Settings, click **Add Disk**.



The Add Disk dialogue box is shown.

3. Storage size cannot be configured for iSCSI disks.
4. Click ok to store settings. Repeat for other disks.

10.11.2 Video, audio and text data storage settings

10.11.2.1 Minimum

To prioritize recordings from one or more video, audio or text data channels, ensure that the minimum values are sufficiently low for other channels.

Then set the value higher for the high priority channel or channels.

If you select **Automatic**, the system deletes recordings from channels that use the most storage space.

10.11.2.2 Maximum

The system examines the recordings daily and deletes those that are older than the maximum number of days.

If you select **Automatic**, the recordings will be deleted only when the free space is not sufficient.

***Note**: If the minimum values are too high for some channels while, at the same time, they are not set for other channels, the system will delete recordings from the channels with no set minimum.*

10.11.2.3 Alarm limits

10.11.2.3.1 Minimum

The system deletes alarms that are older than the minimum value.

If you select **Automatic**, the system deletes alarm recordings from channels that use the most storage space.

10.11.2.3.2 Maximum

The system examines the alarm recordings daily and deletes them older than the maximum number of days.

If you select **Automatic**, the recordings will be deleted only when the free space is not sufficient.

10.11.2.3.2.1 Log entries

This value specifies how many alarm events will be kept in the alarm log at the most.

The system examines the number of log entries hourly and deletes the oldest entries if they are exceeded.

10.11.2.3.2.2 % maximum

This value specifies how much storage space alarm recordings are allowed to use of all storage space.

As long as all storage space is not used, alarm recordings can use more space than this value.

The system first deletes the oldest alarm recordings before deleting other video or audio recordings if all storage space is used.

10.11.3 Automatic Deletion of Video, Audio and Text Data

After exceeding the defined maximum storage time, stored video, audio, text, and alarm data is automatically deleted—the maximum storage time for data the system checks daily.

As the size of a stored data stream can vary significantly due to movement in the video image, changes in audio levels, or the number of text data events, it may be hard to predict storage space requirements accurately.

Thus, sometimes the system may deem it necessary to ensure free storage space by automatically deleting old material regardless of the maximum storage time.

If data needs to be deleted to ensure free storage space, the deletion process proceeds through the following pattern:

In simple words this retention process goes like this when FS need a new free file:

1. Check alarm quota, if alarm material files count in more then set in quota (% from all data) we cleanup oldest alarm file and reuse it
2. Check min settings for alarm data - if alarm channels have data that exceed min alarm settings – we take the oldest file from those, cleanup it and reuse
3. Check min settings for all material channels (video, audio, data) - if some channels have data that exceed min settings – we take the oldest file from those, cleanup it and reuse
4. Check the oldest file from channels with auto min settings if they are present, if so - we take the oldest file from those, cleanup it and reuse
5. If still, nothing is found – we just take the oldest file from all channels (material and alarm), clean up it and reuse

Also, we have a background task that cleans up material files according to max settings.

The launch period is set to a minimum max setting from all channels (material and alarm).

Note: *To ensure that the need for automatic deletion due to a lack of disk space is minimized, it is good to monitor the disk usage regularly and alter the maximum storage time and allocated disk space.*

It is advisable to use manual or automatic archiving tools to ensure that no relevant data is deleted in storage space issues.

Hint: *You can set a Watchdog event to notify you if the storage space runs low.*

10.11.4 Archiving

You can set the system to automatically archive video, audio, and text data daily or weekly.

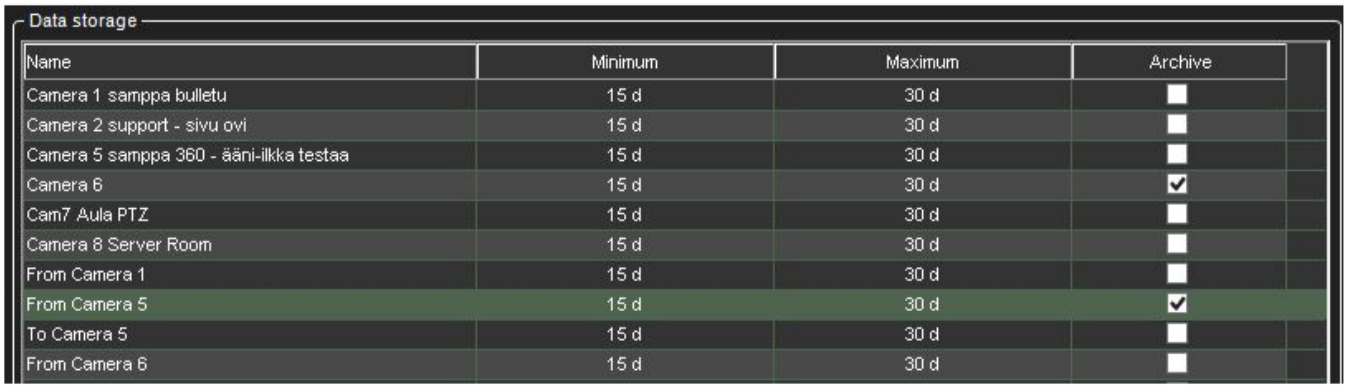
The archive files can be automatically created on the server's hard disks or a network drive.

The archive files can be opened on any Spotter client.

Note: *Archive files can be huge, and thus they can fill storage space quickly. Archive files should be regularly copied and removed from the server hard disks or network drives on which they are automatically saved.*

10.11.4.1 To set an automatic archiving schedule:

1. In the **Data storage** pane, click on the devices you want to include in the automating archiving process.
   TIP: Select adjacent devices or folders, hold down the SHIFT key and then click the first and last device you want to select.
   a. To add a device to a selection or remove it from a selection, keep the CTRL key pressed and then click the device you want to add or remove.
      Note: *Selecting a device group (folder) also selects its contents.*
2. Mark the **Archive** checkbox.



3. Click **Modify archive settings**



4. Set the archive password by clicking **Change archive password**

5. Select whether to create the archive daily or weekly by selecting **Every day or Once a week**

6. If you set archiving to occur daily, use the **Archiving time** drop-down menu to select the time on which the archive files are created.

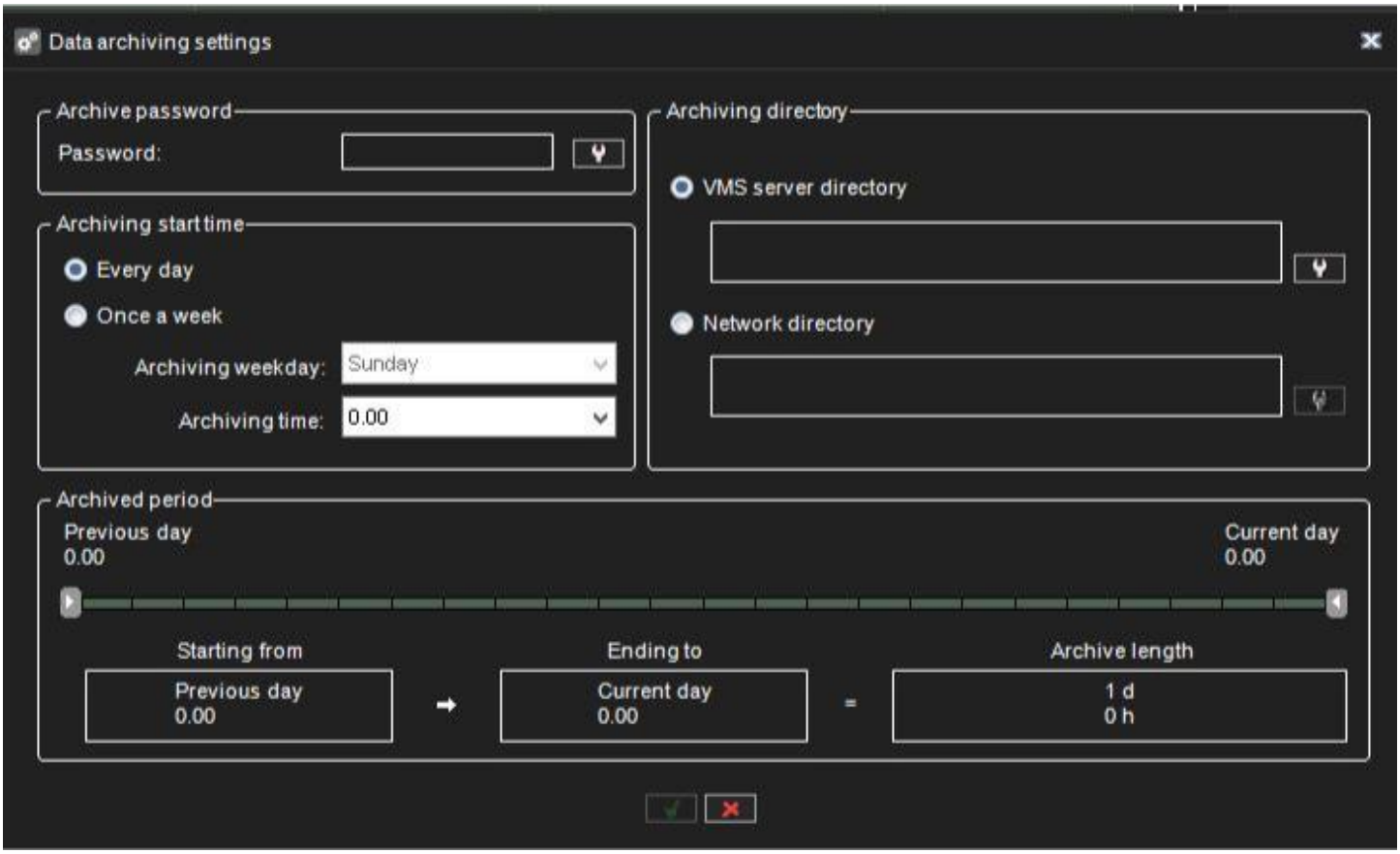
7. If you set archiving to happen every week, use the **Archiving weekday** and **Archiving time** drop-down menus to select the date and time on which the archive files are created.

8. Use the **Archived period** slider to set the period used in the archive files.

9. Select whether to create the archives on a local drive (on the server) or a network drive by selecting the **VMS Server directory** or **Network directory**.

10. Click the **Change directory** or **Change network drive** button to set the directory to save the archives.

11. Click **OK** to set the archiving schedule



10.11.5 Use OS cache

DVMS 8. x and newer have the possibility to enable OS cache usage when accessing the physical disk.

DVMS 9.4 and newer have the possibility to set maximum OS cache size.

Any software can access the disk in direct access mode when OS doesn't use any caching and using OS cache.

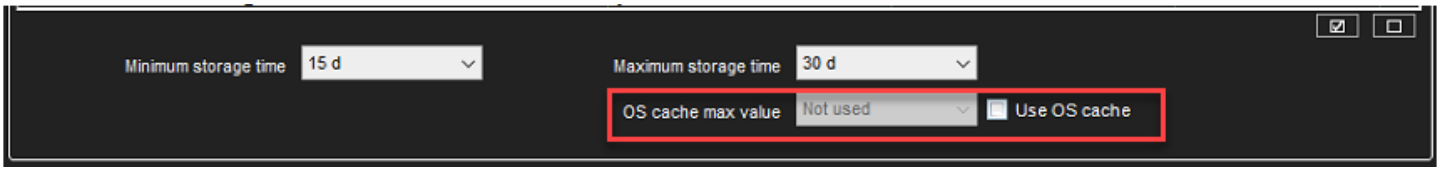
The last one helps to deal with unstable load to HDD and caching most used parts of data.

Windows Server and Windows desktop versions have different priorities for applications - Windows Service priorities background services and desktop version priorities UI applications.

Also, Windows Server uses more system resources to cache e.g. HDD access and can use up to 90% of RAM for this.

To avoid situations when all RAM is occupied by file system cache DVMS 9.4 and newer has an option to limit max OS cache size.

Max OS cache setting is valid until PC reboot, so they are set each time recorder starts.

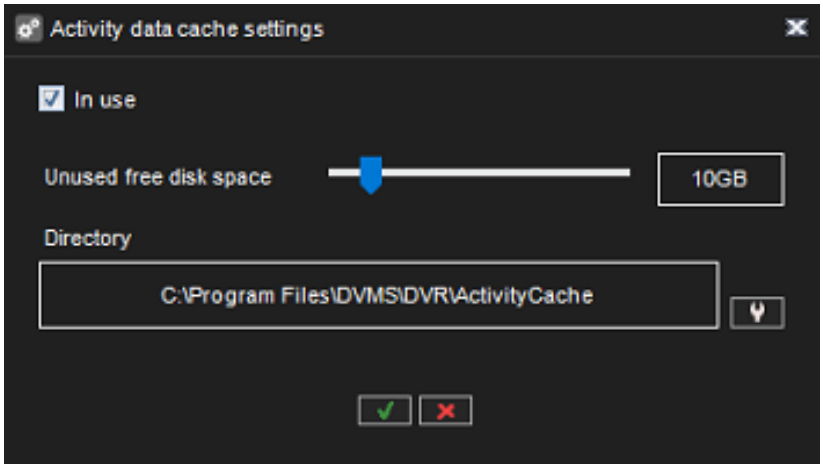


10.11.6 Activity data cache

You can edit activity data cache settings by clicking **Edit activity cache settings**.



In the settings dialog, you must first check **In use** to enable the feature, after which you can modify the settings.



You can edit the following settings:

- **Unused free disk space**: Use the slider to set how much disk space should remain free (default: 10GB)
- **Directory**: Select the directory where cache files are stored

To apply the changes, click **OK** in the Activity data cache settings dialog and in the Storage Settings view.

10.12 Text Channel Settings

The servers can receive text data from devices such as cash registers or gas station pumps.

The driver specifies what text data is recorded and what is shown to the users. It also specifies custom events and searches criteria.

In addition to the default text data drivers included in the software, new drivers can be installed.

In-text channel settings, you can change the name of a text channel and add or edit its description.

In profile **settings**, you can set the user rights and the device window options for each channel and each profile.

An additional document for UniversalData drivers can be downloaded from our extranet or contact support. This driver opens endless possibilities for integration to 3rd party systems.

10.12.1 To add text data channels:

1. Click **Add channels** in the lower right corner of the **Text channel settings** screen.



2. Select the text data channel driver from the **Model** drop-down menu.



3. Use the **No. of data channels** slider control to select the number of channels you want to create.

4. Fill the driver-specific information into the fields in the **Properties** list.

5. Click **OK** to save the channels.

10.12.2 To edit text channels:

10.12.2.1 To edit the name and description of a text data channel:

1. Select a text data channel from the channel list.

2. Type a name for the channel into the Name field.
3. Type general and administrative descriptions of the channel into the respective fields.
    a. All users can see the general description, whereas only system administrators can see the administrative description.
4. Mark the **In use** checkbox to set the channel as active, or unmark the checkbox to set the channel as inactive.

10.12.2.2 To edit the configuration setting of a text data channel:

1. Select a text data channel from the channel list.
2. Click **Modify channels**.



3. Edit the driver-specific information to the fields in the **Properties** list.
4. Click **OK** to save the changes.

Note: *When editing the configuration settings of a text data channel, the settings are changed for all text data channels that use the exact driver.*

10.12.3 To remove all text channels that use the same driver:

1. Select a text data channel from the channel list.
2. Click **Delete channels** in the lower right corner of the **Text channel settings** screen.



3. All text data channels that use the same driver as the selected text data channel are removed.

Note: *To remove text data channels without deleting all channels that use the specific driver, click* ***Modify channels*** *and specify the new number of text data channels using the* ***No. of channels slider****.*

11 PROFILES

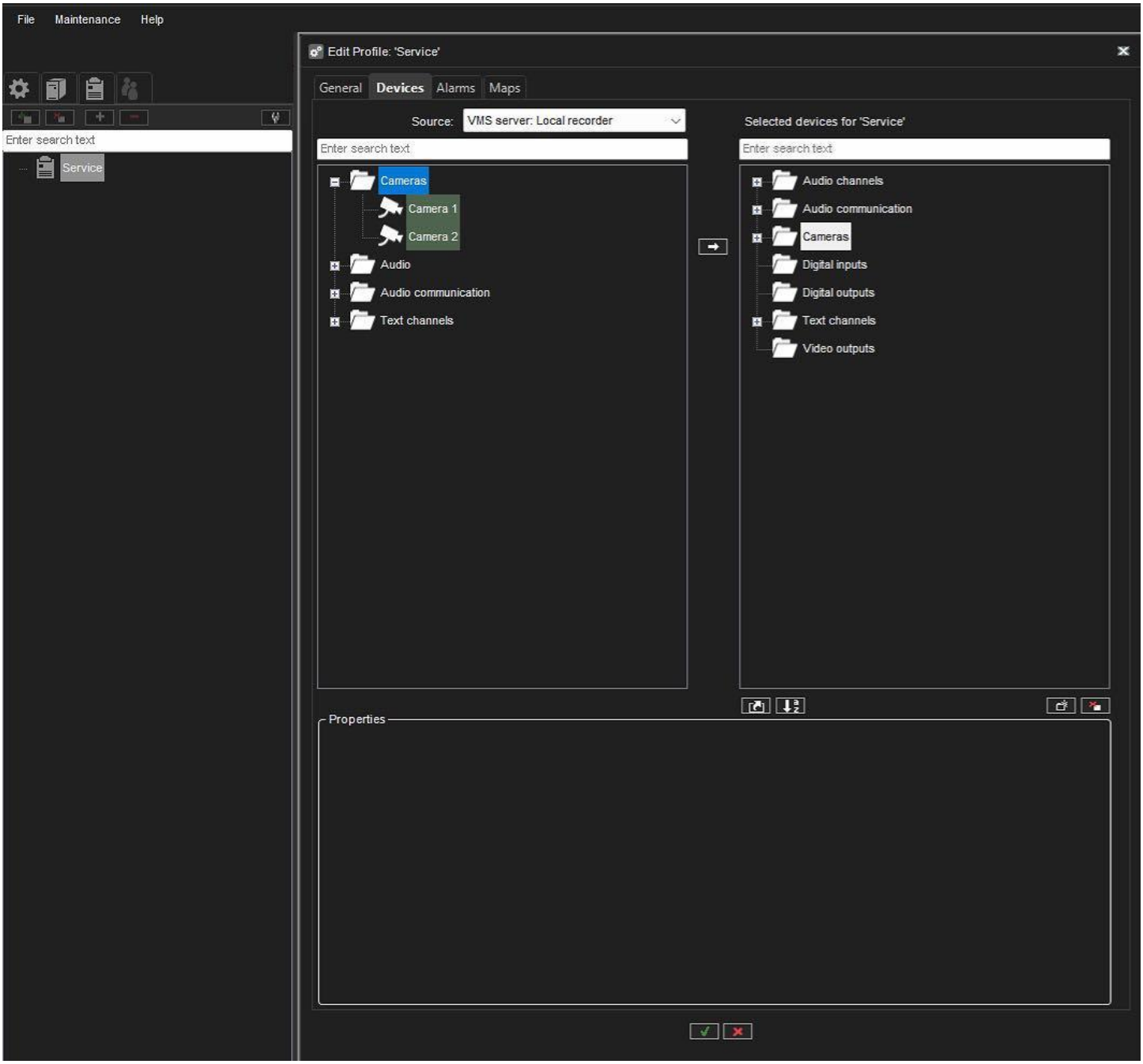
In Mirasys VMS, Profiles define which VMS components the user has access to and what kind of user rights the user has for the components. The system has one default profile, Service. The default profile contains the devices that the license key of the Main Server specifies.

The devices are grouped by device type. For example, all cameras are in one group and all audio channels are in a different group.

A profile sets a user's rights in the system. Each user can have 1 to 5 profiles that contain these *devices*:

- Cameras (fixed cameras and PTZ cameras)
- Audio channels
- Audio communication channel
- Digital inputs (alarm inputs)
- Digital outputs (control outputs)
- Video outputs
- Text channels
- Alarms
- Plugin instances
- Web browser home pages

To see the content of a profile, double-click the profile and the content will load in the main screen.



You can use the default profile as such or edit it freely, for example, group cameras at the exact location or you can add new profiles. A profile can contain devices from different servers.

You can add as many as 2,000 groups and devices to a profile. Furthermore, you can put the devices into groups as you like.

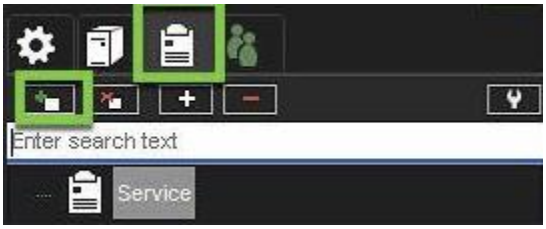
Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

11.1 Creating a customer-specific profile

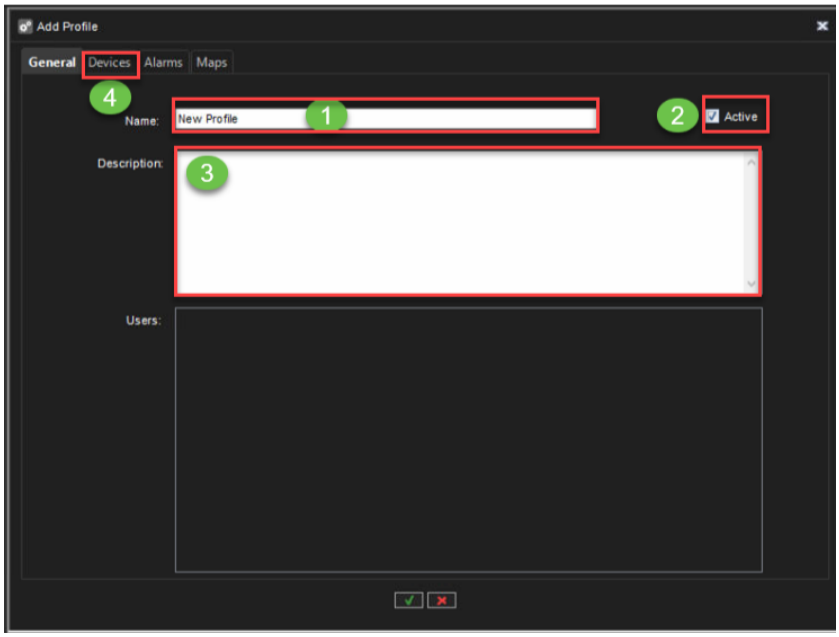
The profile defines a set of devices in a structured (tree) format with profile-level rights. The System Manager profile settings can be used to add new profiles and edit existing ones.

11.1.1 Adding a profile

1. Click **Add Profile**



1. Set the name of the profile.
2. Set profile status: **Active** or **Disabled**
3. Set description, if needed. The description is shown only in the System Manager.
4. Open **Devices** and see instructions on the following pages.



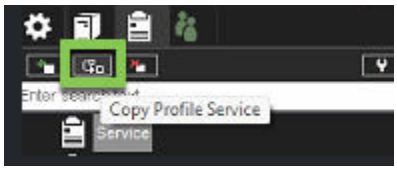
11.2 Duplicate an existing Profile

You can copy an existing Profile in System Manager to make it easier to create new profiles based on existing ones.

The copied profile will include identical **Device**, **Alarm**, and **Map** settings.

Please note that General settings such as description and user groups will not be copied.
The new profile will be active by default and can be edited and deleted.
Only System Administrators with the "can add profile" ability enabled in the System Manager role can copy the profile.

1. Select a profile in System Manager > Profiles.
2. Click the "copy profile" button located between "add profile" and "remove profile".



Please note that this button will only be active when a profile is selected.

3. When clicking "copy profile, a new profile is created with device, alarm, and map settings identical to the copied profile.



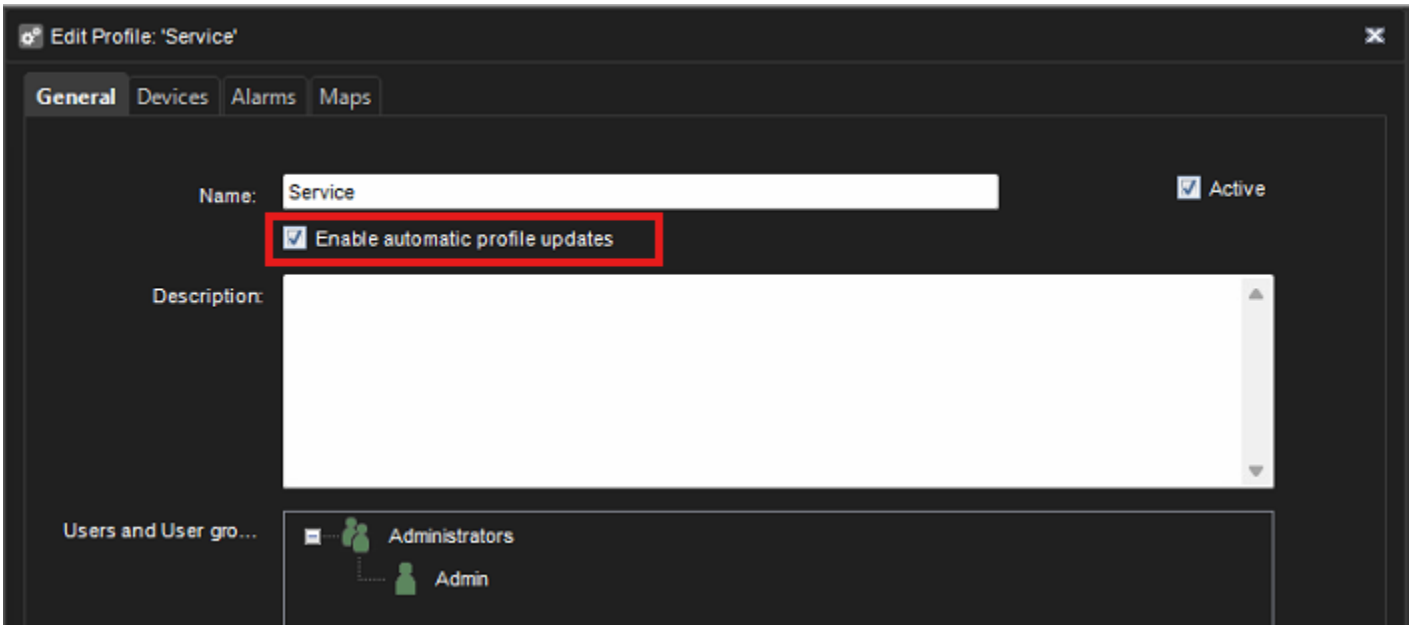
The new profile copy is below the copied profile with a number after the name: If the profile name is Service, the copy will be "Service 1". If there is already a "Service 1" profile, it will be "Service 2", and so on.

4. In General settings, the name can be edited, the profile can be activated or deactivated, and a description can be added. The new profile copy will be active by default.
5. Click ✓ to Save. The profile will now be visible in SM > User groups and can be added to user groups.

11.3 AUTOMATIC PROFILE UPDATES

11.3.1 Enable automatic profile updates

The **General** tab of a profile includes the **Enable automatic profile updates** option. The setting is enabled by default.



The behavior of the setting in an enabled/disabled state is described below.

11.3.2 Automatic profile updates enabled

I.e., the setting checkbox is ticked.

Profile nodes are removed automatically from the profile when the linked device is removed.

11.3.3 Automatic profile updates disabled

I.e., the setting checkbox is not ticked.

If a system administrator disables the setting and thus "locks" the profile, only manual changes in the System Manager profile settings are applied.

Profile nodes are not removed automatically when linked devices are removed, and profiles can contain broken links to devices.

Profile nodes can be added or removed only manually in System Manager's Profile settings, or for alarms in Alarm settings.

11.3.3.1 Broken profile nodes

All applications function correctly regardless of broken profile nodes. Backing up and restoring the system also work normally.

Broken profile nodes are inaccessible to users and not displayed in the profile tree in any application except for System Manager's Profile Settings. Though the nodes are not displayed, they remain in the system data.

System Manager's Profile settings display the following information for broken links:

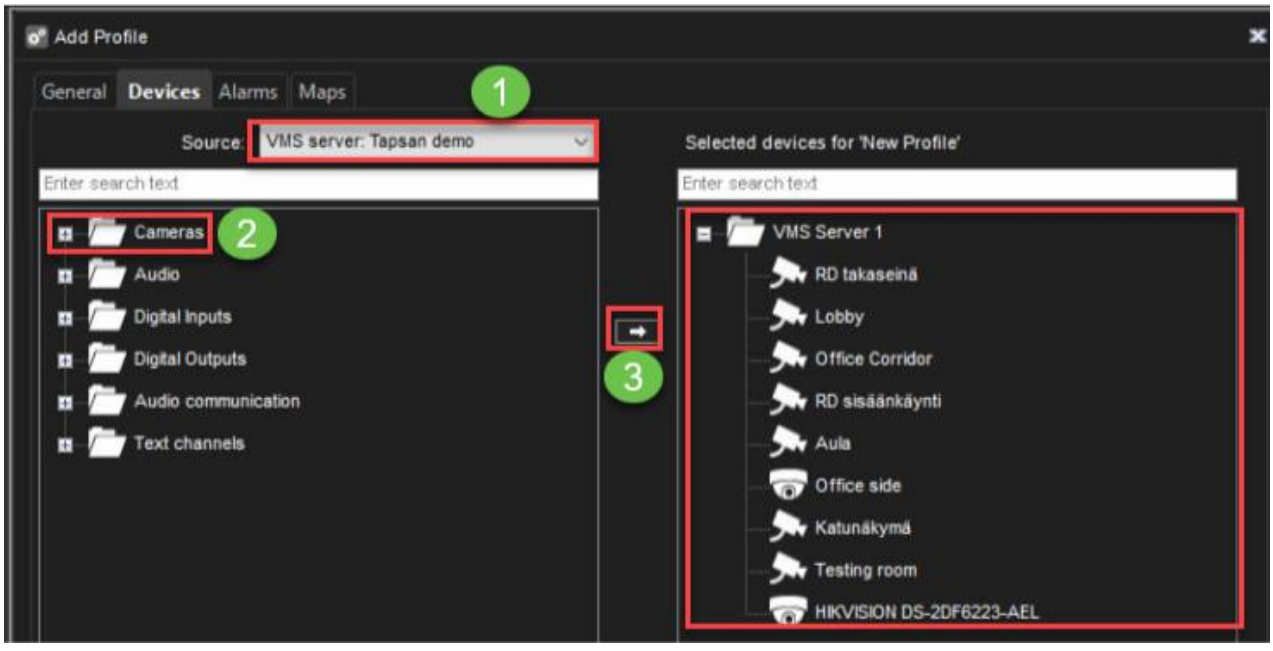
- Recorder name and address
- Device name
- Information that the device link is broken

When a linked device is re-added, the link between the profile node and the device is restored. All clients regain access to the profile node and the device.

11.4 DEVICES PROFILE SETTINGS

11.4.1 Add devices to a profile

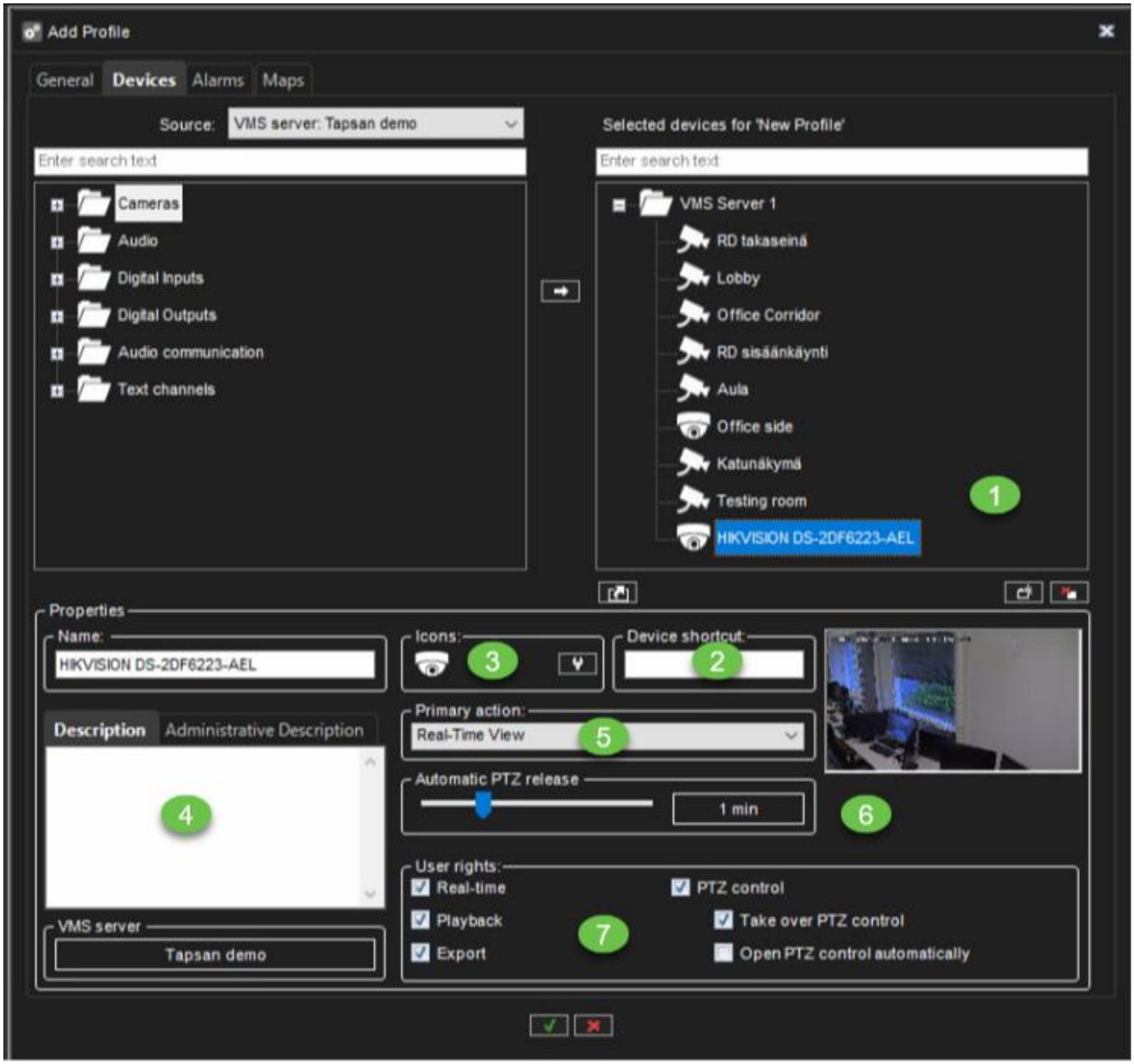
1. From the Source drop-down list select **VMS server or another profile**
2. Select needed components or device groups from the left box
3. Click **Add**
4. To change selected components properties, please go to **Selected Devices**



11.4.2 Selected Device Properties

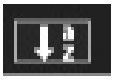
1. Select component from the list of the selected device
2. Set **Device shortcut**
3. Change the device icon by clicking **Change Icon**

4. Set **Description** and **Administrative Description**, if needed
5. Select the **Primary action**, select the action that will occur when a user double-clicks the device in Spotter.
6. Set **Automatic PTZ release**(only for the PTZ cameras)
7. Set user rights for the component
    a. **Real-time**
    b. **Playback**
    c. **Export**
    d. **PTZ Control**(only for the PTZ cameras)
        i. **Take over PTZ control**
        ii. **Open PTZ control automatically**
8. Click **OK** to finalize the profile creation



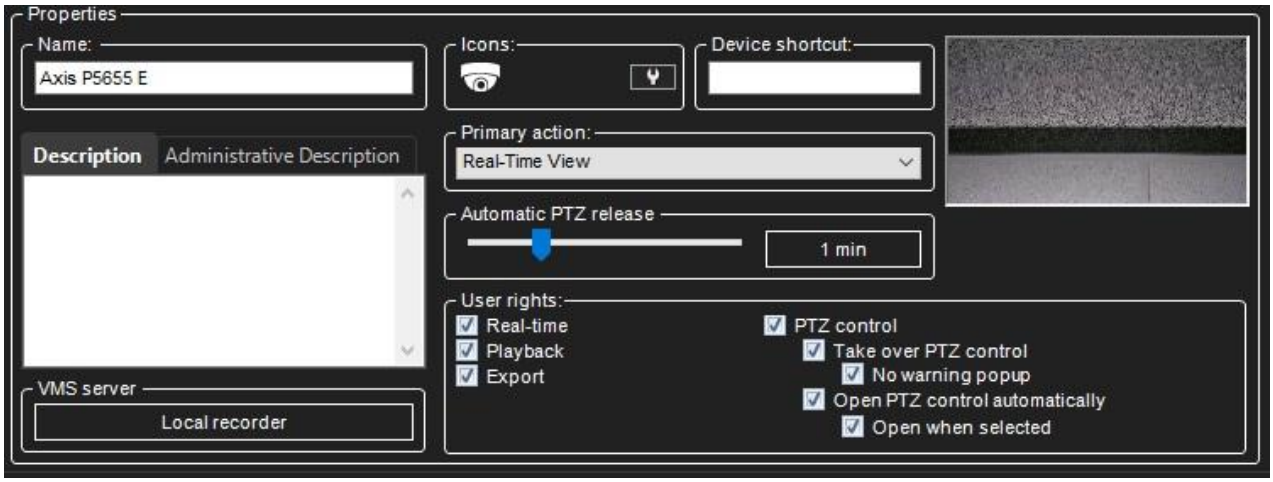
11.4.3 Sort selected device nodes

Alphanumeric sorting (a -> z) of selected folder profile nodes is executed when pressing sort button, second press will execute reverse sorting (z -> a).



11.4.4 PTZ camera profile settings

In System Manager camera profile settings in PTZ camera user rights, selection **Open when selected** is added.

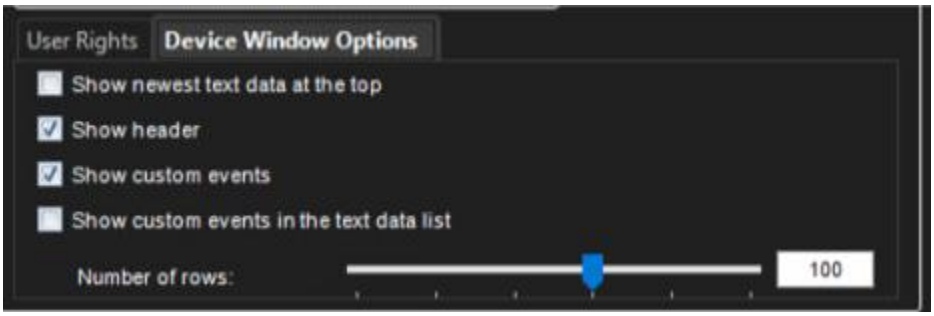


If **Open when selected** is selected, then PTZ camera control is automatically activated when PTZ camera view is selected in Spotter.

11.4.5 PTZ control

- Automatic dome release
    - Values: 1 min, 2 min, 3 min, 4 min, 5 min, 10 min, 15 min, 30 min, 45 min, 1 h, 2 h, 4 h, 8 h, 12 h, 1 d
- Take over PTZ control
    - No warning popup
- Open PTZ control automatically

11.4.6 Text channel Device Window Options



In Device Window Options, you can select how text data is shown to users. These options are available:

11.4.6.1 Show the newest text data at the top.

By default, the newest text data is added to the bottom of the text data list. Select this option to show the newest text data at the top of the text data list instead.

11.4.6.2 Show header

Select to show identification data specified by the text data capture driver.

11.4.6.3 Show custom events

Select to show custom events specified by the text data capture driver.

11.4.6.4 Show custom events in the text data list

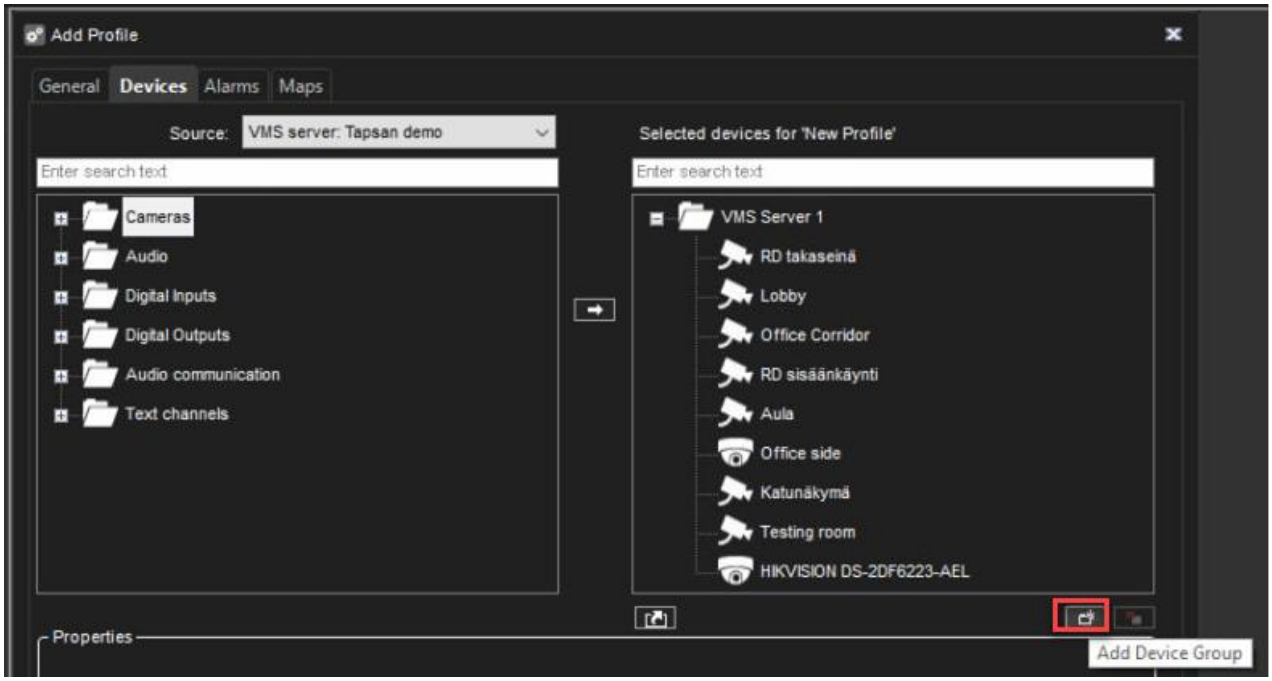
Select to show custom events in the text data list (instead of the custom event list).

11.4.6.5 The number of rows

Specify the number of rows that are shown in the text data list at the most.

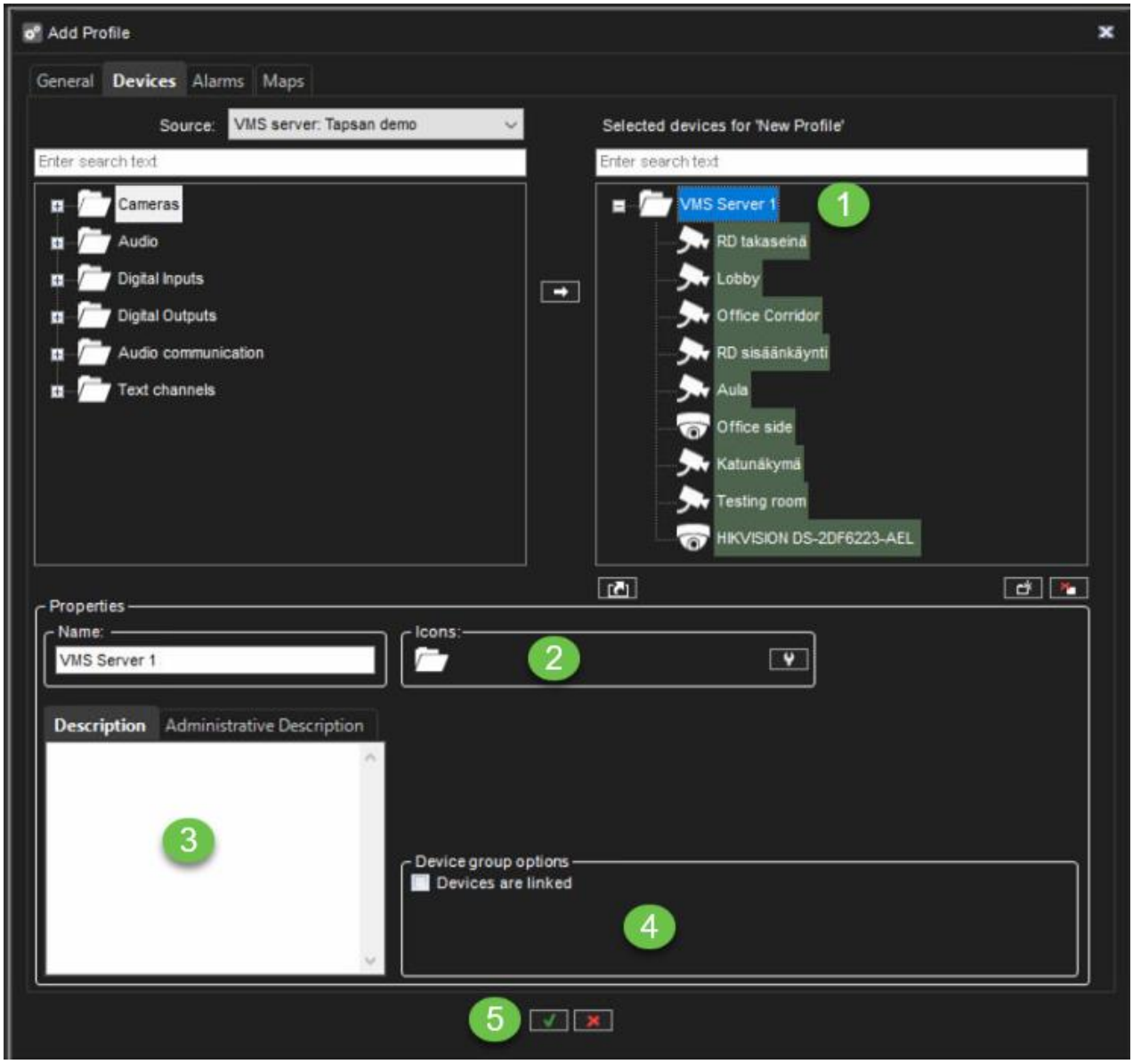
11.4.7 Adding Device Groups to the list of the selected device

1. Click **Add Device Group** below the **Selected devices** panel. A new device group is shown.



Note: A new device group is always added under the selected device group. To add a device group to the top level, make sure that none of the existing device groups is selected.

1. Click the device group and type a name for it
2. To change the icon that is used for the device group, click **Change Icon**. Then select the icon that you want to use.
3. Type a description of the device group in **Description**.
4. Set Device group options, if needed(**Devices are linked** to automatically open all device views from the same group when the user opens one of the device views).



11.4.8 Sort Alphabetically

Sorting rules:

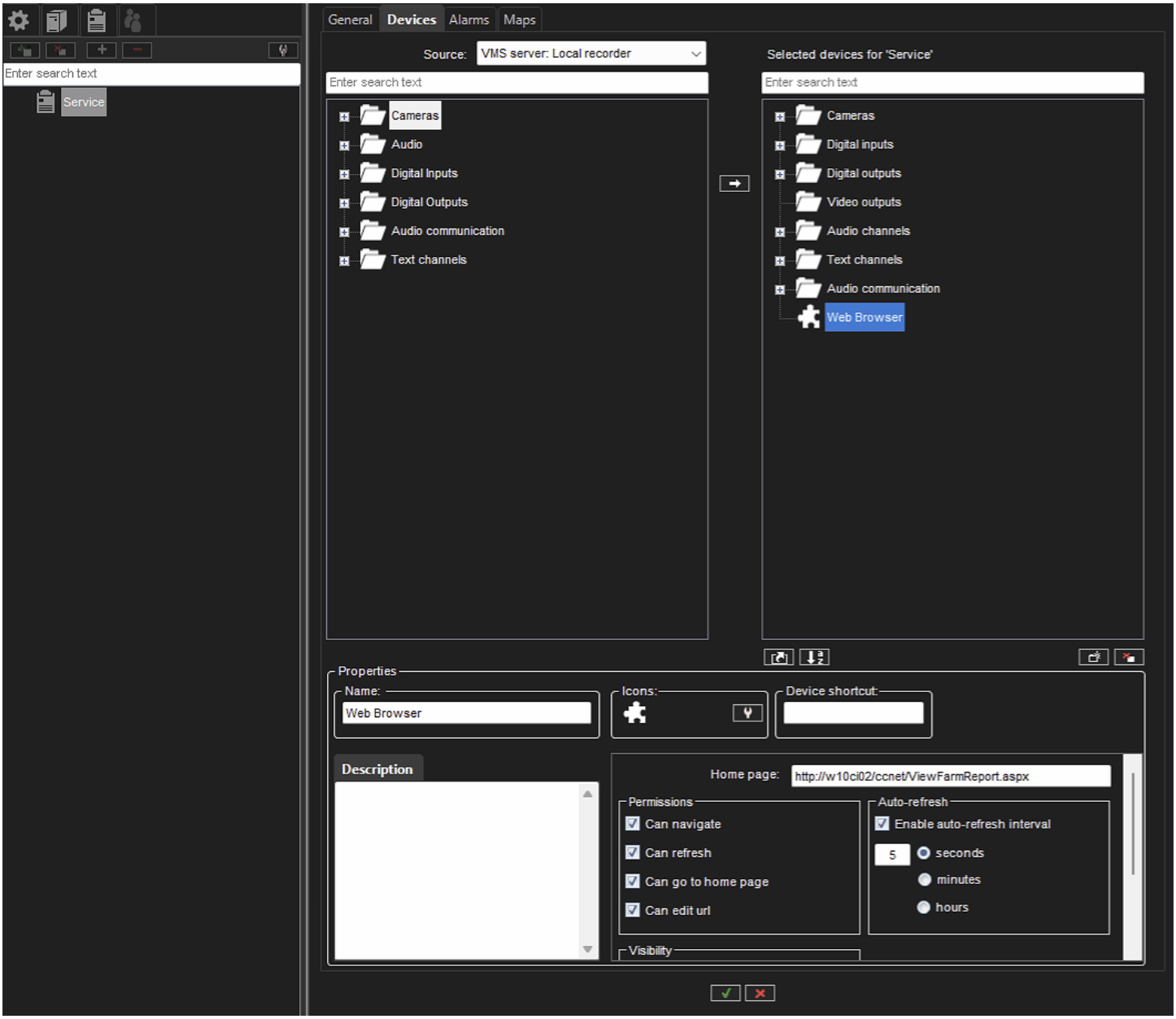
- to the folder or root level where the currently selected component is located (but not to subfolders)
- to the selected folders (but nor to subfolders)
- if no profile node is selected, root nodes are sorted (but nor subfolders)
- if multiple folders are selected from same level, all selected folders are sorted (but not subfolders)

11.4.9 Client Plugins

11.4.9.1 Web browser plugin

The web browser is configured in System Manager > Profiles > Select and open Profile > Devices.

1. To add webpages as channels, change the source to **Client Plugins**. Select the Web Browser plugin, and add it to Devices.
2. Select the Web Browser, and add the name, a description if you want one, and change the icon if you want to.
3. Under Home page, add the web page address.
4. Set permissions:
    - Can navigate
    - Can refresh
    - Can go to home page
    - Can edit URL
5. You can select to enable an Auto-refresh interval, and set the interval in either seconds, minutes, or hours.
6. Click ✓ to Save.



11.4.9.2 VLC Player plugin

VLC Player configuration is done in System Manager > Profiles > Select and open Profile > Devices.

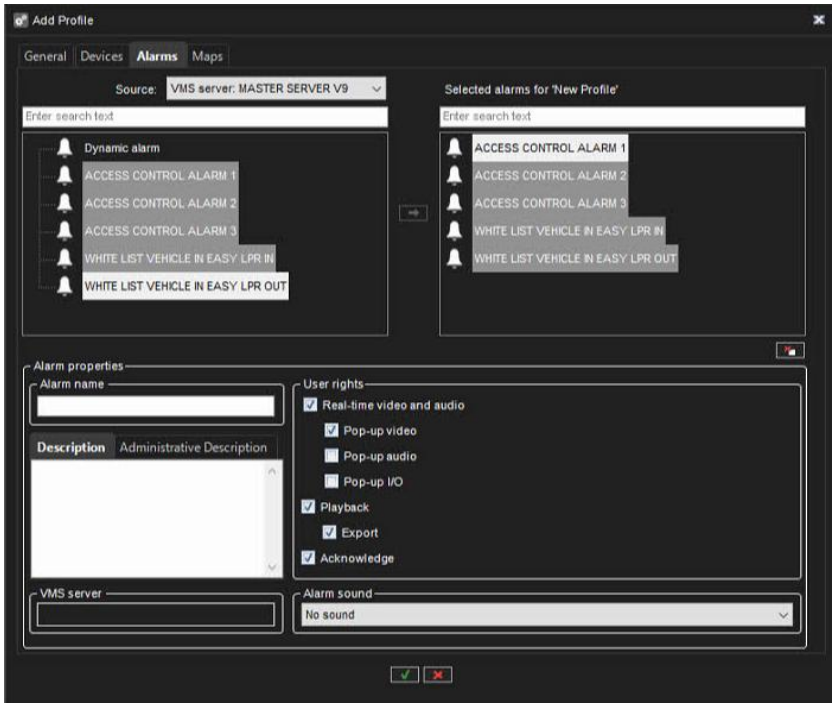
To configure the VLC Player plugin:

1. Click the **Devices** tab in Profile settings.
2. Select **Client plugins** from the Service drop-down menu.

3. Select VLC Player.
4. Click the **arrow** ➡ pointing to the right to add the VLC Player to the profile tree.
5. **Name** the Player instance under Properties.
6. Add a **Description** if needed.
7. Select an icon for the Player under **Icons** if needed.
8. Add a **Device shortcut** if needed.
9. Enter the VLC Player **URL** that you want to play.
10. Tick the box **Show URL** if you want the URL displayed in Spotter.
11. Tick the box **Auto-play** if you want VLC Player to play the URL when opened in Spotter.
12. Click ✓ to Save.

11.5 ALARMS PROFILE SETTINGS

11.5.1 Editing Profile Specific Alarm Settings



On the **Alarms** tab, you can select the alarms you want to include in a profile and edit the alarms' profile-specific user rights.

The Trigger Type for Alarm Triggers created by the System Administrator for ONVIF Profile M conformant devices, and for the Alarm Triggering Web API is External.

11.5.2 Adding alarms to a profile

1. Open the **Alarms** tab.
2. Select a server from the **Source** drop-down menu. The available alarms are shown in the left pane.
3. Select the alarm or alarms that you want to add and then click the right arrow. You can also drag alarms from the left pane to the right.
4. Save the profile by clicking **OK**.

Note: *You can also add alarms to profiles through the alarm creation/editing screen.*

11.5.3 Editing profile-specific alarm user rights

1. Open the **Alarms** tab.
2. Click on an alarm in the **Selected alarms** pane.
3. Set the user rights for each alarm. The user rights settings are located on the bottom right side of the **Alarms** tab.
    a. You can set individual rights for each alarm or select multiple alarms (by holding the shift or control keys down while selecting alarms) and set the same options for multiple alarms.
4. To have the computer play a sound when an alarm occurs, select **Alarm sound** and then select the played sound. To test the sounds, select the sound from the list and click **Play**.
5. Save the settings by clicking **OK**.

The user rights include:

- **Real-time video and audio**. Select to let the users see real-time alarm video or audio.
- **Pop-up video**. Select to let users receive alarm video automatically.
- **Pop-up audio**. Select to let users receive alarm audio automatically.
- **Playback**. Select to let the user's playback alarm video.
- **Export**. Select to let the users save alarm video on local media.
- **Acknowledge**. Select to let the users acknowledge alarms.

11.5.4 Deleting an alarm from a profile

1. Open the **Alarms** tab.

2. Click on an alarm in the Selected alarms pane.
3. Click **Delete Alarm**.

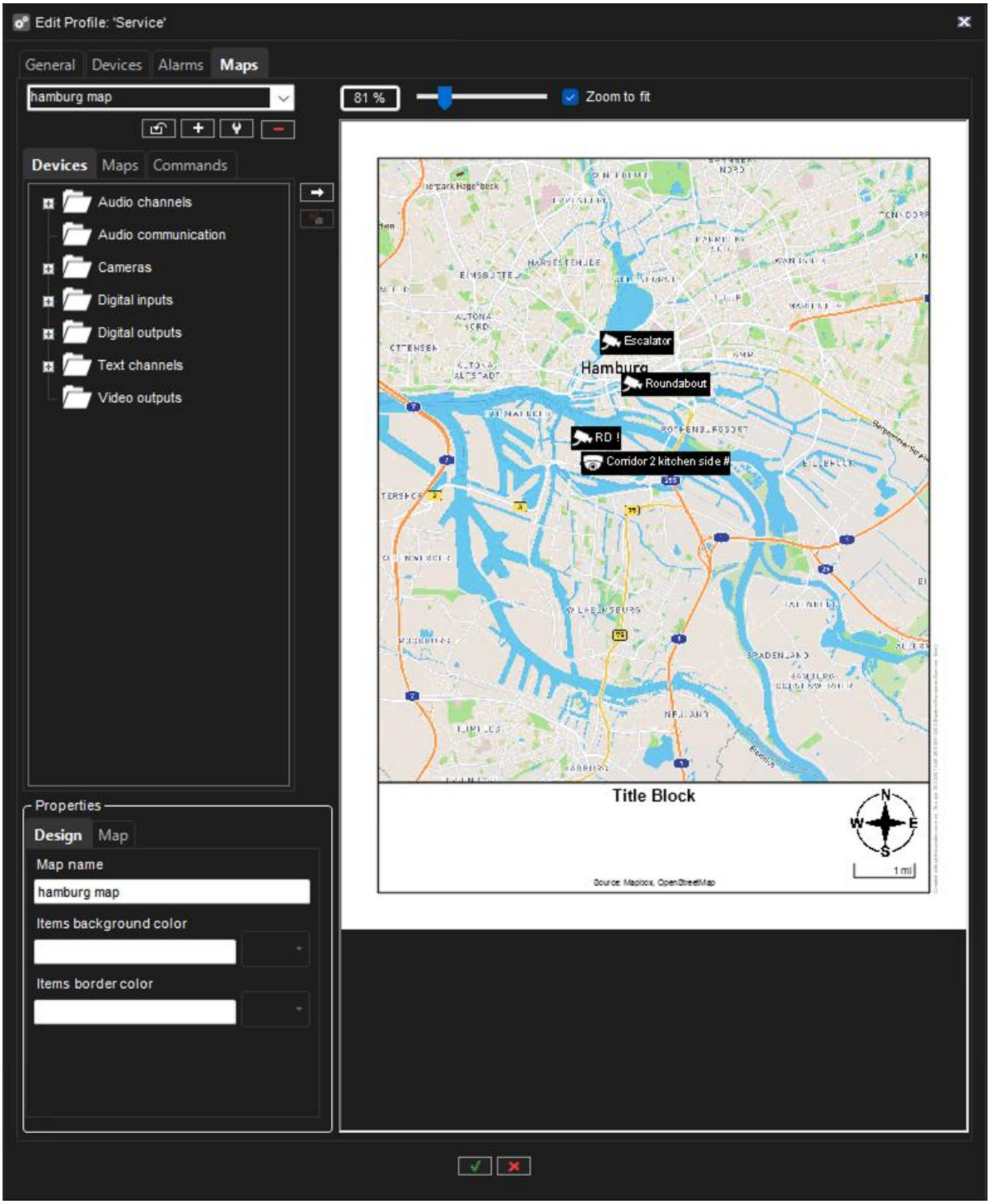


If an alarm lacks a trigger or actions, it remains visible in the profile's Alarms tab but not in the recorder's Alarms settings. Changing the alarm settings removes their configuration, including profiles.

11.6 MAPS PROFILE SETTINGS

When adding a map in profile settings, we support the following formats:

- JPG / JPEG (Joint Photographic Experts Group)
- BMP (Bitmap)
- PDF (Portable Document Format)
- SVG (Scalable Vector Graphics)
- PNG (Portable Network Graphics)



11.6.1 Adding Maps to Profiles

1. Click the **Change Level** button and then select the device group to which you want to attach a map.

- The devices that belong to the selected group are shown in the left pane.
- Subgroups are also shown. You can also double-click the subgroup icons in the left pane to move to a lower level.

2. Click **Add Map** and find the image that you want to use as a map.
3. **Zoom to fit** above the map is selected by default. You can also unselect Zoom to fit to adjust the zoom with the slider above the map manually.
4. From the left pane, select the devices and device groups you want to add to the map and click the **Add to Map** arrow.
   - Items that are already on the map appear dimmed in the left pane. If you add subgroup icons to the map, the icons will act as links to the subgroup maps.
   - Users can move to a lower-level map by double-clicking the subgroup icon.

Tip: To select multiple devices simultaneously, keep the SHIFT or CTRL key pressed.

1. Select a device or device group from the map, and then, under **Device properties,** you can set these options:
2. You can select the direction the camera icon points to for cameras.
3. By default, the name label of each device is shown on the map. To avoid label clutter, clear the check box **Label**. The name will be shown as a popup label instead.
4. You can use placemarks if you need to fit several device icons in a small space.
5. Select the **Placemark** check box. A placemark (x) and a connecting line are shown on the map. Drag the placemark (x) to the device's correct position.
6. Then, drag the icon to a convenient position on the map.
7. Click ✓ to Save.

11.6.2 To remove a site map:

- Display the map that you want to remove and click **Remove Map**

11.6.3 To remove an icon from the map:

- Select the icon and click **Remove**

12 USERS AND USER GROUPS

All users belong to a user group (see below), through which their use rights are defined and managed.

The administrator can add new user groups, set varying use rights for the groups, and add users.

The system supports domain-level user rights integration (LDAP), enabling users to be synchronized from domain groups.

Each user group must have at least one profile that sets the user group's devices in the system.

One user group can have five profiles at the most.

A username and a password protect all user accounts.

12.1 Logging Users Off

If you have administrative rights, you can log a user off from the Spotter program.

12.2 To log a user off:

Right-click the username on the Users tab and click **Log User Off.**

NOTE:
Please change always the Admin user password after you have finalized the installation.
You should never leave default passwords in the Mirasys VMS system.

12.3 Monitoring Users

The **Users** tab shows if users are logged on to the system:

Icon	Description
	(Green). The user is logged on. Click the plus sign (+) to see the name of the program the user is logged on to and the IP address of the user's computer. In addition, the date and time of logon are shown.
	(Red). The user is not logged on.
	(Grey) The user account is disabled.

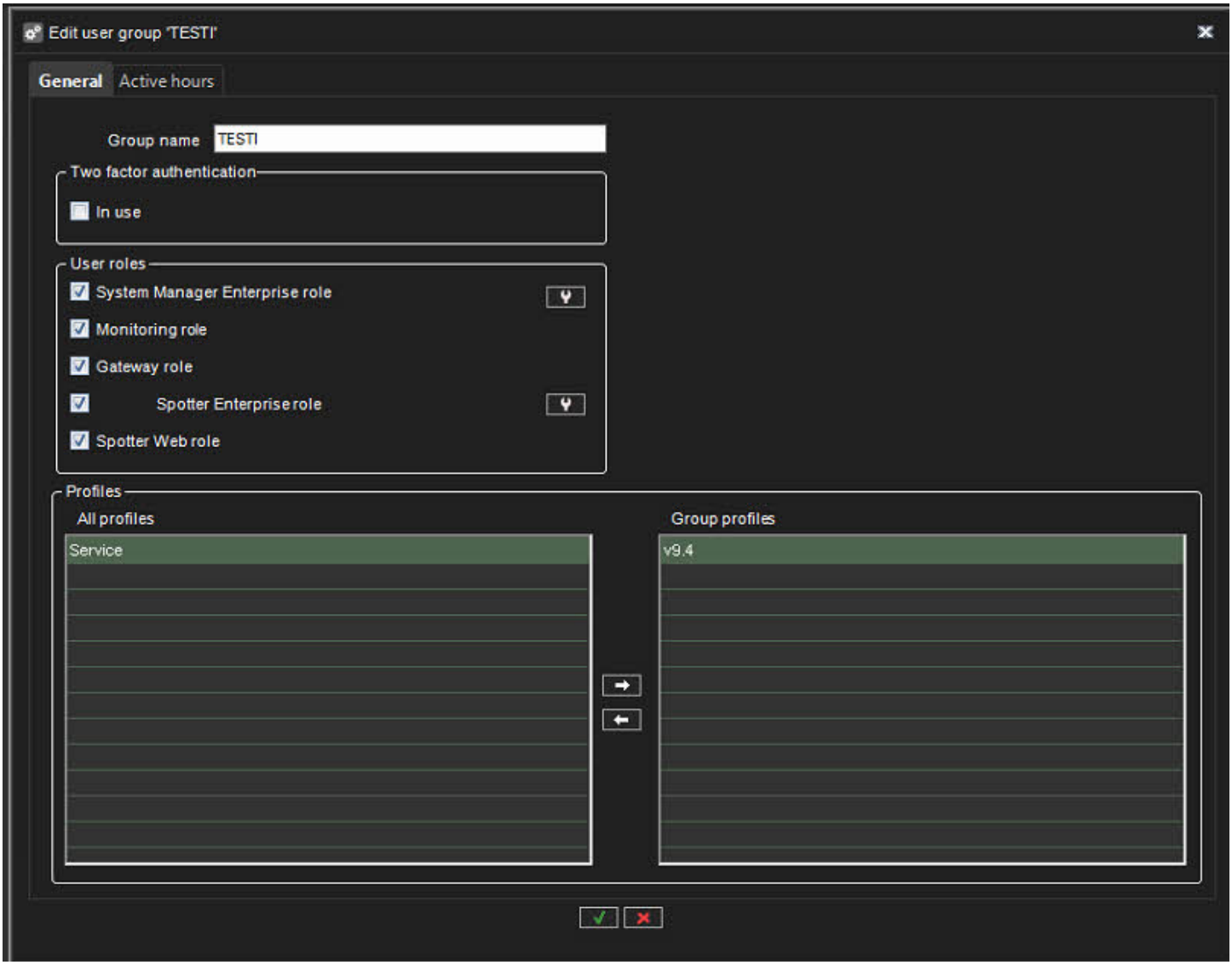
12.4 USER GROUP

The user group defines which Mirasys VMS applications the user group has access to and what kind of permissions the user group has regarding the applications.

12.4.1 User Roles

The system supports the following types of user roles (defined through user groups)

- **System Manager role:** Administrators are allowed to log in to System Manager and change all settings, such as changing camera settings or adding new profiles or user accounts.
- **Monitoring role:** Users with monitoring rights are allowed to log in to System Manager and monitor the system on the **System** tab, but they are not allowed to change the settings.
- **Gateway role:** if this role is active, the user group can access the DVMS gateway
- **Mirasys Spotter Enterprise role:** End users can log in to Spotter but not to System Manager.
- **Spotter Web role:** End users can log in to the Spotter Web



12.4.1.1 User group level automatic lock / log off

12.4.1.1.1 Possibility to force other user log off when starting System Manager

- Enabled only if System Manager Enterprise Plus role is enabled
- Possible values for Wait time: 0s, 10s, 20s, 30s, 45s, 1 min
- When creating new group, default value is 10 seconds

12.4.1.1.2 Functionality at log on

There is changes from previous versions only if other user log off is enabled and there is other user logged in System Manager with administrator rights.

When trying to log on, following choices will appear:

- Kick off current user: start sequence to kick off current user with administrator rights in System Manager
- Login with limited system monitoring rights: continue login with monitoring rights, no effect to current System Manager users
- Cancel login: go back to start login page (cancel button has this same effect)

Kick off current user

Current user is selected, new processing window is opened:

This processing window is open until:

- Other user is logged off
- Other user has cancelled force log off
- Cancel button is pressed

12.4.1.1.2.1 Other user is logged off
User is automatically logged in with administrator rights.

Other user has cancelled force log off

12.4.1.1.2.2 Other user has cancelled force log off
After OK button, go back to login page, other user with administrator rights continue logged in.

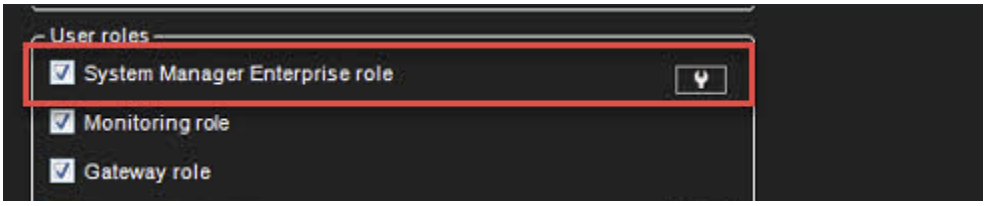
12.4.1.1.2.3 Cancel button is pressed
Go back to login page, other user with administrator rights continue logged in.

12.4.1.1.2.4 Other (already logged with Administrator rights) side
If there is timeout in forced log off settings, warning of coming forced log off appears:

Remaining seconds before forced log off is updated. During this timeout, user can cancel forced log off by cancel button.

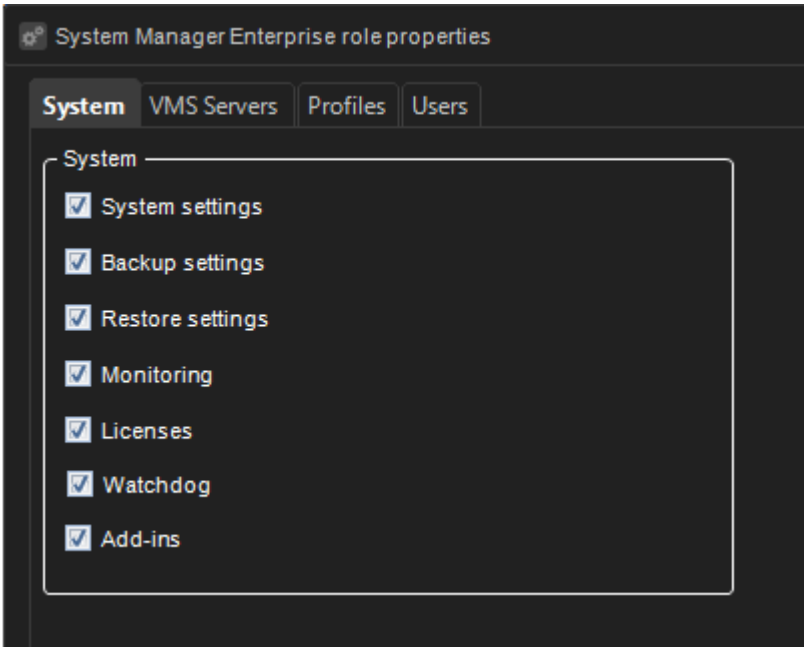
If timeout is past or Ok button is pressed, current user session is logged off.

12.4.1.2 System Manager Enterprise role
It is possible to set explicit permissions for the system manager for different user groups.
This allows, for instance, implementing functionality for allowing different user groups for hardware maintenance and user administration, which is helpful for large scale systems.
To enable the functionality - check the "System manager enterprise role" tickbox for the user group and click the "wrench" icon to edit the details for this group.



12.4.1.2.1 System

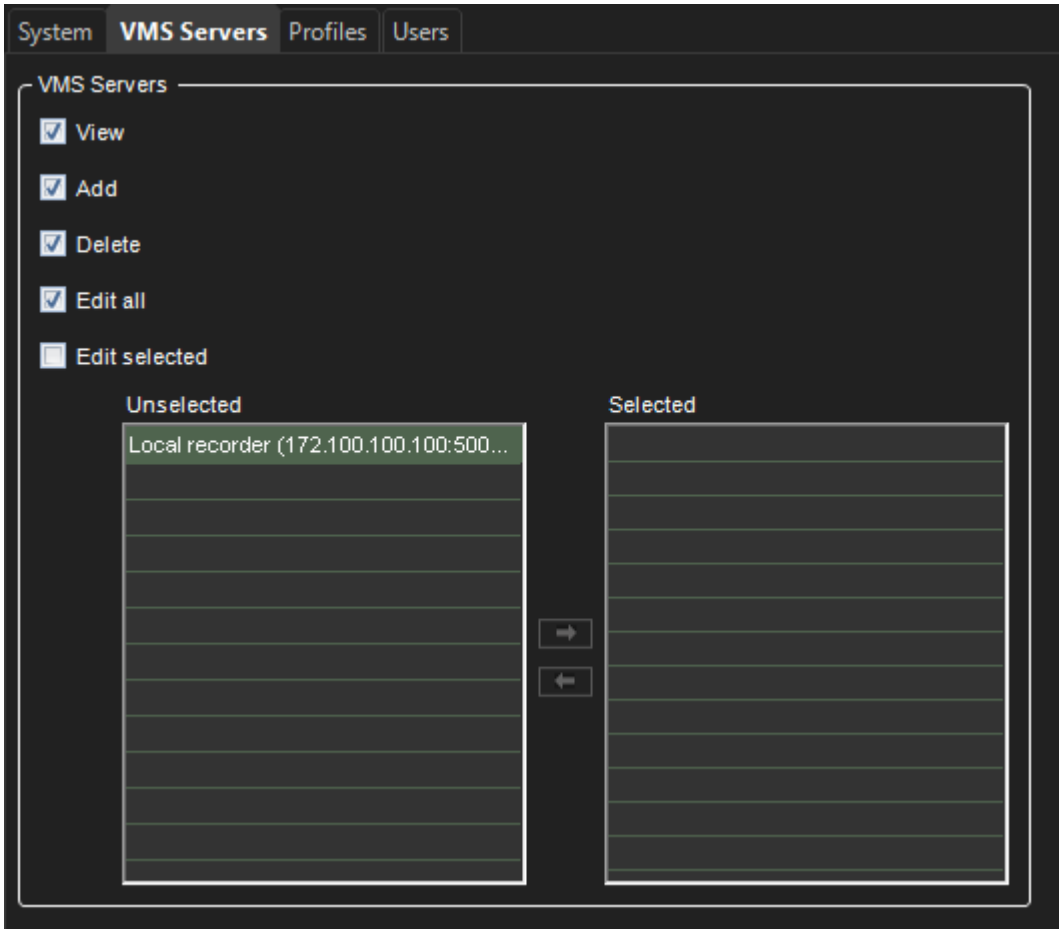
The System tab permissions can be enabled or disabled for a user group, disabling, for example, System settings hides system settings for all users in the user group



12.4.1.2.2 VMS Servers

The VMS servers tab allows permissions for a user group to View, Add, Delete and edit either all or only selected VMS Servers to be noted: if "Edit selected" is checked, the shuttle box below enables defining which specific servers this user group has access to.

This is convenient in large installations if specific user groups are working with specific servers (e.g. if there are separate maintenance groups for different sites - and the recording servers are site-specific.)



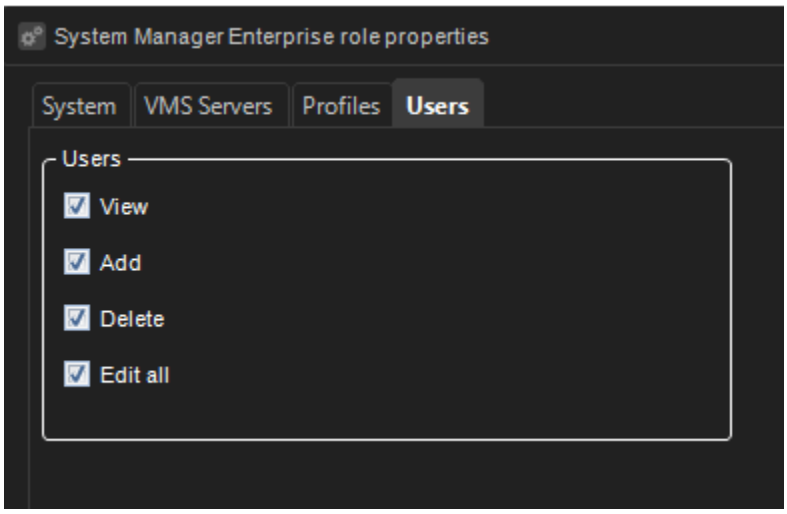
12.4.1.2.3 Profiles

The Profiles tab/permissions that can be set for the user group:

“Edit selected” enables you to decide to which profiles the functionality applies (similar to the "servers" permission configuration).

12.4.1.2.4 Users

The user tab/permissions that can be set for the user group:



Edit all or Edit selected must be enabled for a user group for users to add and/or delete (these options get automatically disabled if Edit all or Edit selected is disabled).

This functionality affects VMS Servers, Profiles and Users tabs

12.4.1.3 Monitoring role

The users with the role Monitoring role have permission to:

12.4.1.3.1 System

- Export logs
- SM Server and VMS server diagnostic
- Licenses
- Watchdog log

12.4.1.3.2 Profiles

Can view the content of the profiles

12.4.1.3.3 Users

Can view the system user groups and users

12.4.1.4 Gateway role

Gateway role enables old Spotter Mobile usage

12.4.1.5 Mirasys Spotter Enterprise role

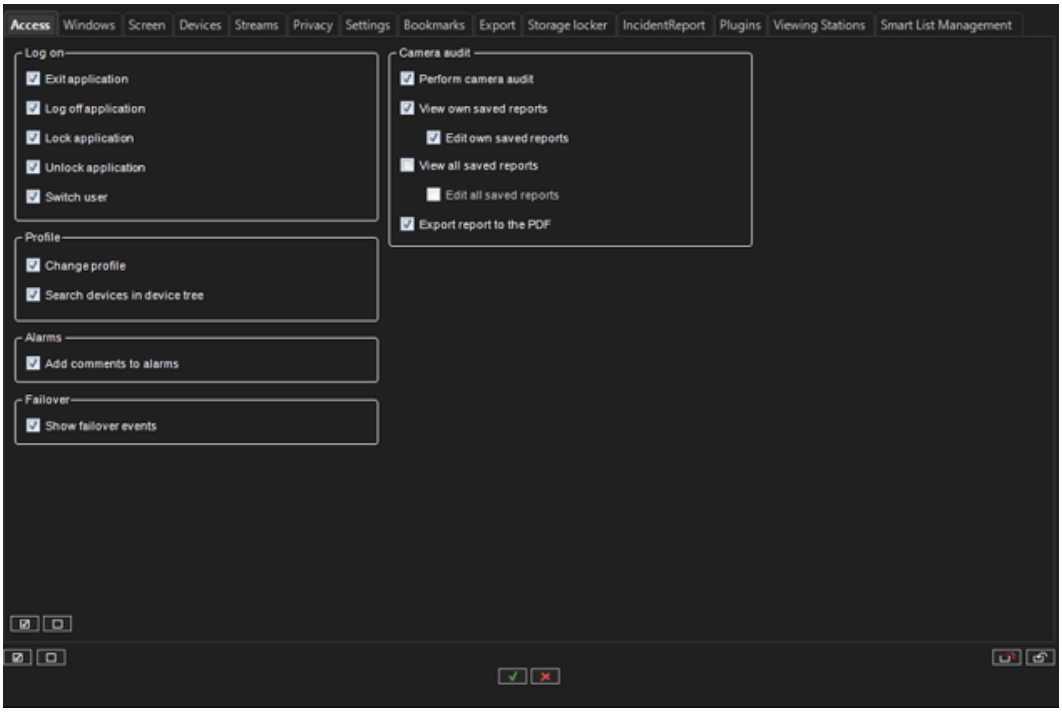
Custom user role properties can be edited by clicking the custom role properties edit button.



The **Spotter** custom roles can be customized with close to a hundred different options (not including plugin-specific adjustments).

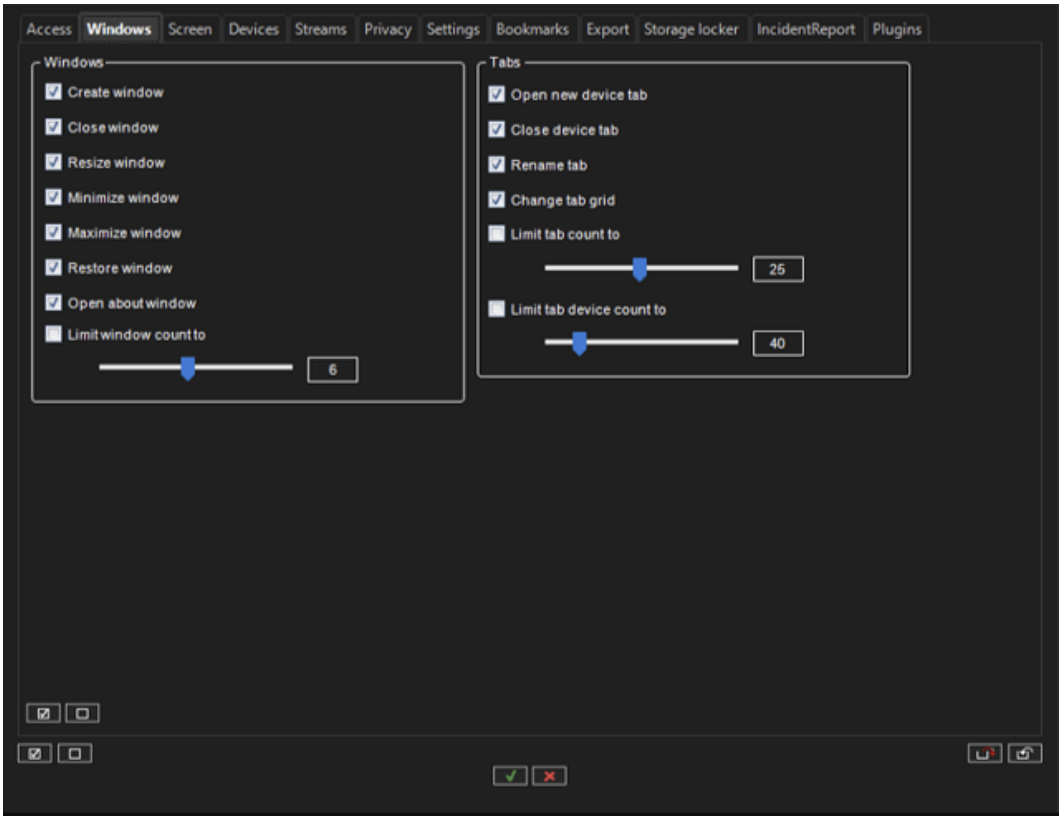
12.4.1.5.1 Access

The Access tab of the role customization contains options for the application access and accessing profiles and alarm commenting.



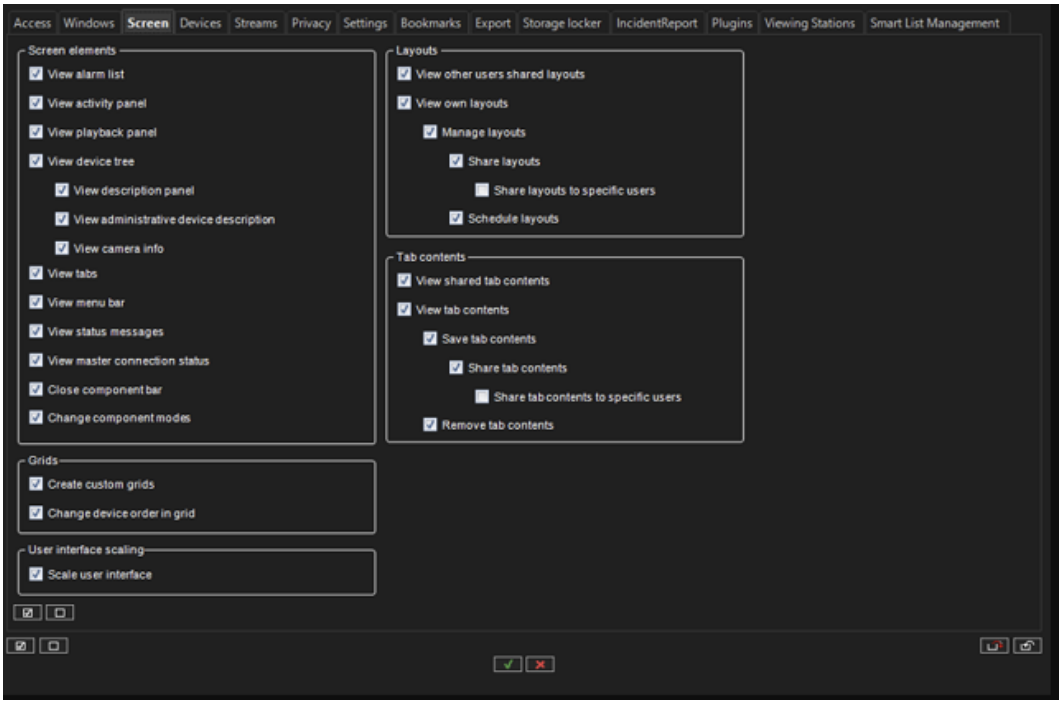
12.4.1.5.2 Windows

The Windows tab contains options for Spotter window management and tab management.



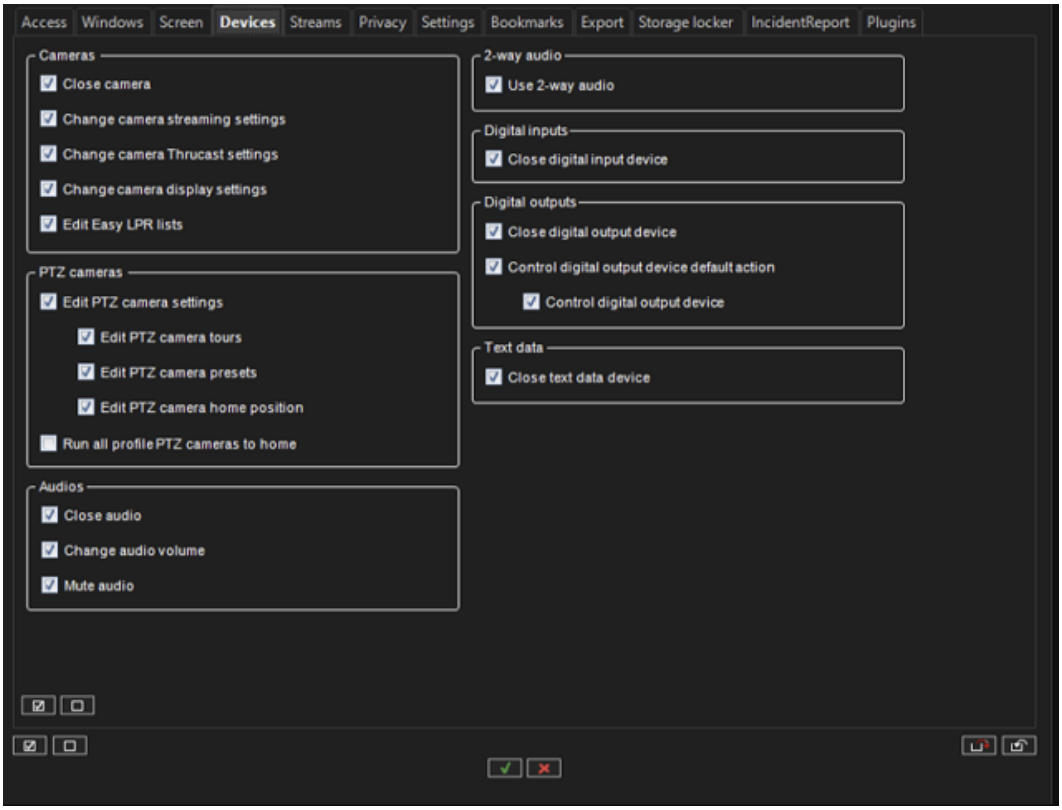
12.4.1.5.3 Screen

The Screen tab contains options for different screen element access and layout access, bookmarks, camera grid and saved camera tabs.



12.4.1.5.4 Devices

The Devices tab contains options for media control.



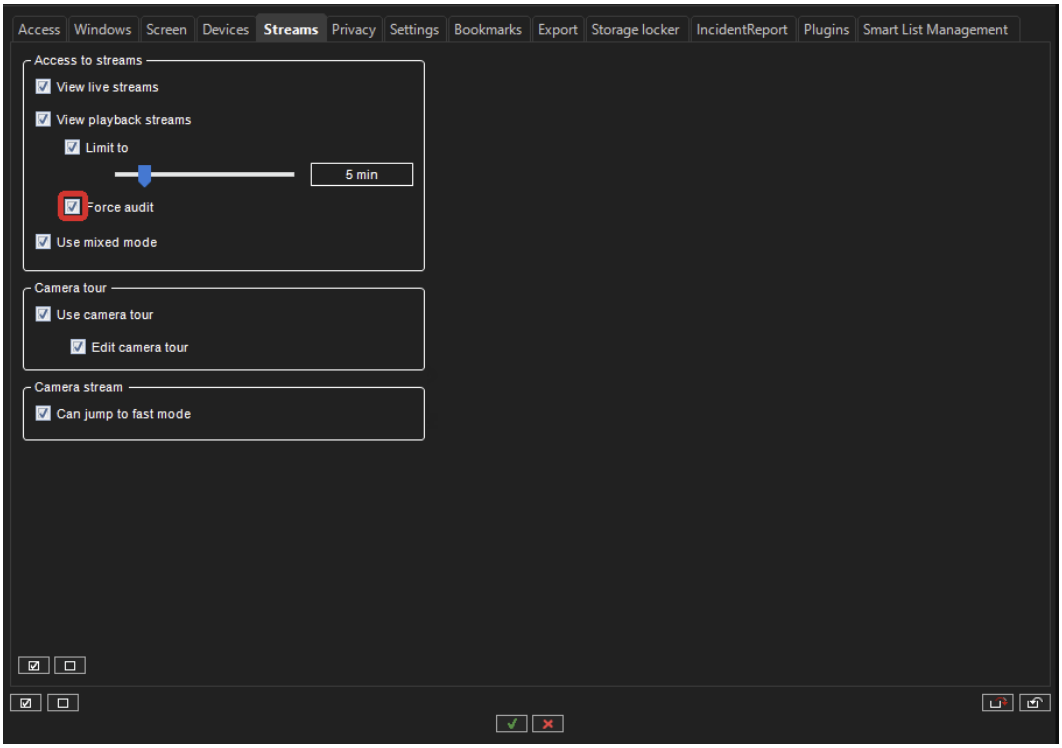
12.4.1.5.5 Streams

The Streams tab contains options for stream access and exporting.

In the Video Wall, the operator can force a user to add a comment before using playback.

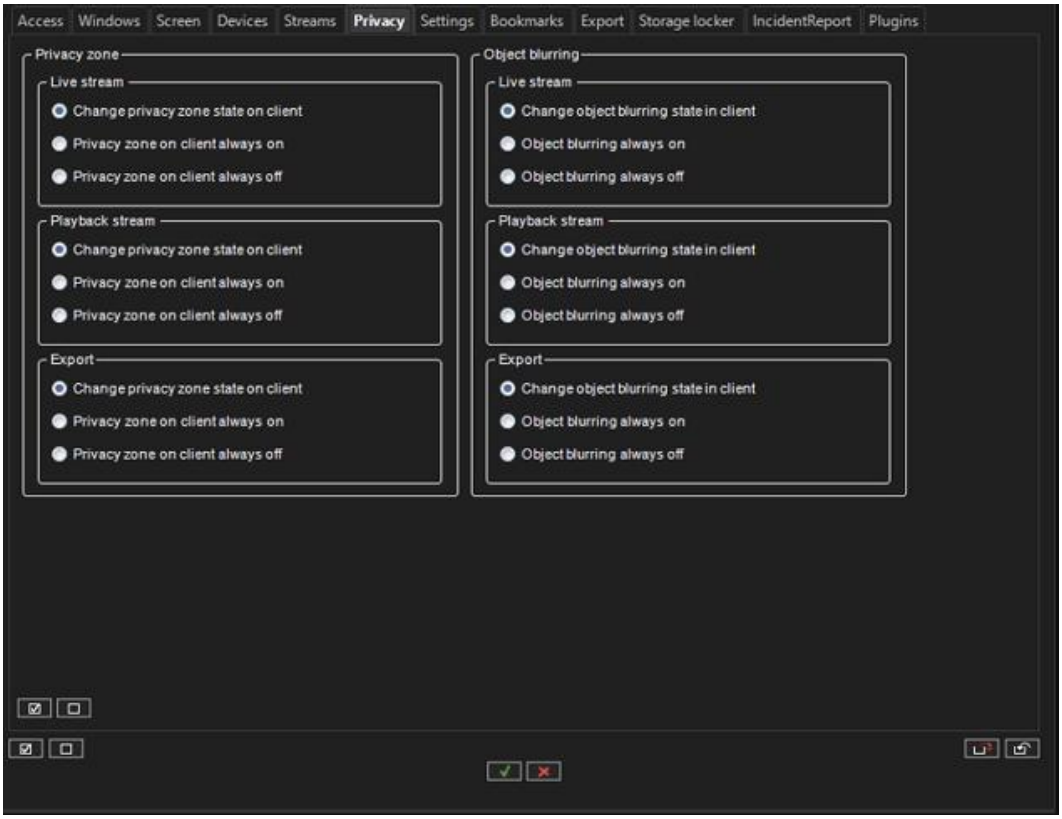
This functionality can be used when the operator requires a reason for using the playback mode before a user can move into playback mode.

The playback comment will be added to the audit log.



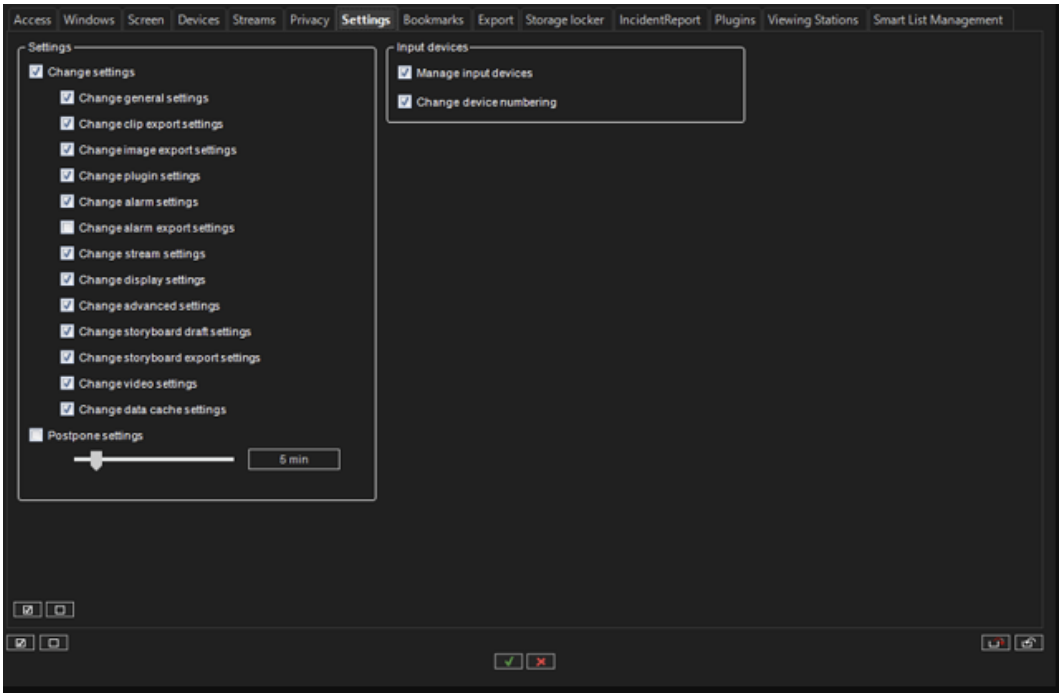
12.4.1.5.6 Privacy

The Privacy tab contains options for privacy.



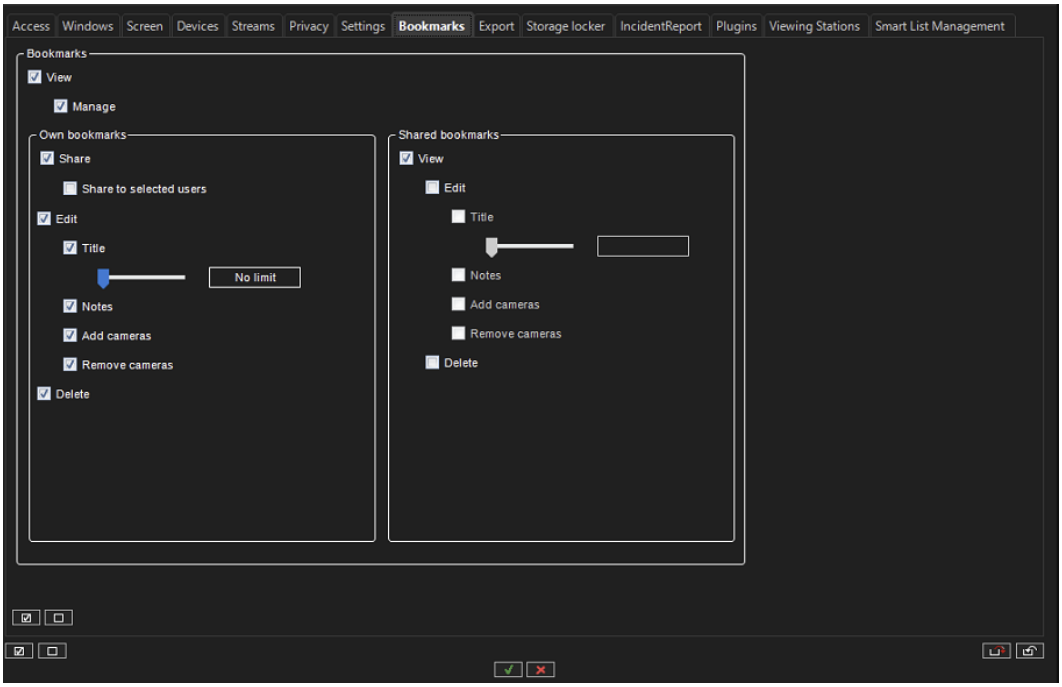
12.4.1.5.7 Settings

The Settings tab contains options for Spotter settings.



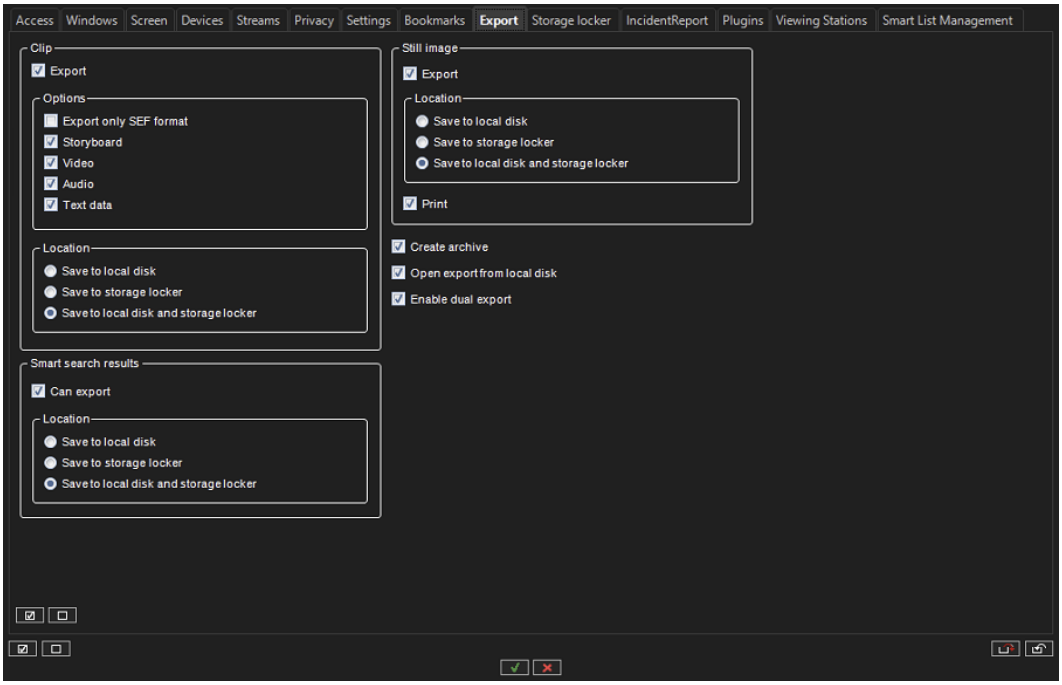
12.4.1.5.8 Bookmarks

The Bookmarks tab contains options for bookmarks.



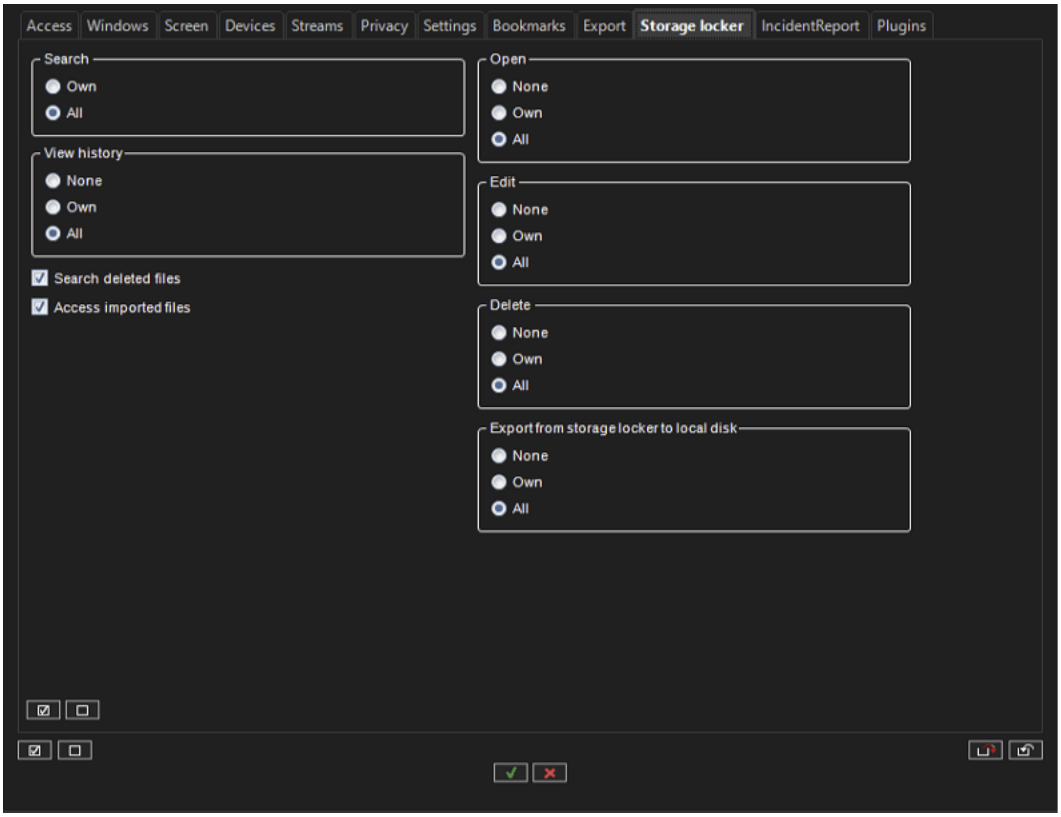
12.4.1.5.9 Export

The Export tab contains options for Export functions.



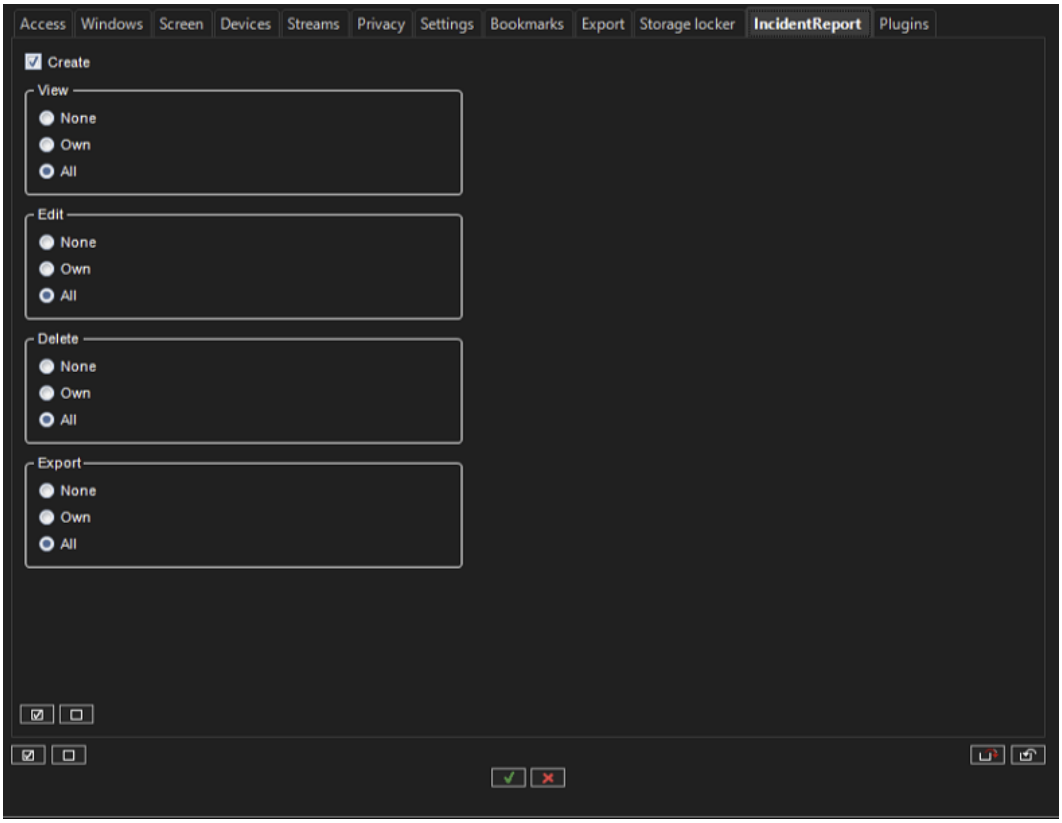
12.4.1.5.10Storage Locker

The Storage Locker tab contains options for the Storage Locker plugin.



12.4.1.5.11Incident Reporting

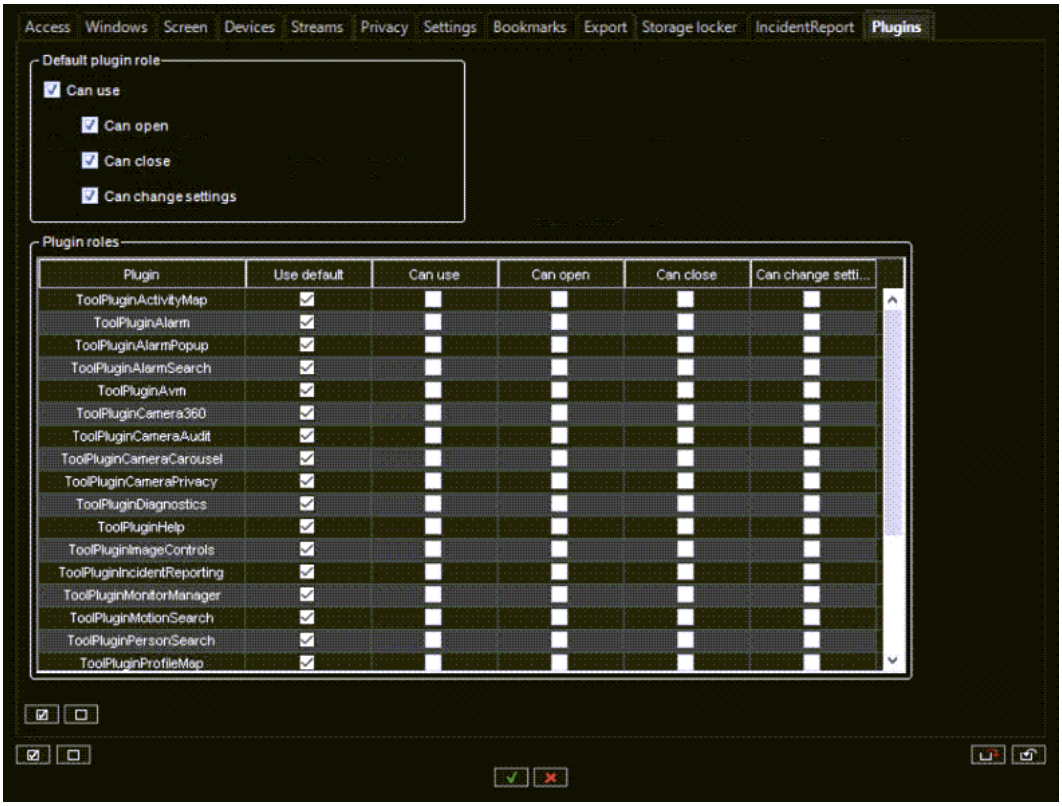
The Incident Reporting tab contains options for the Incident Reporting plugin.



12.4.1.5.12Plugins

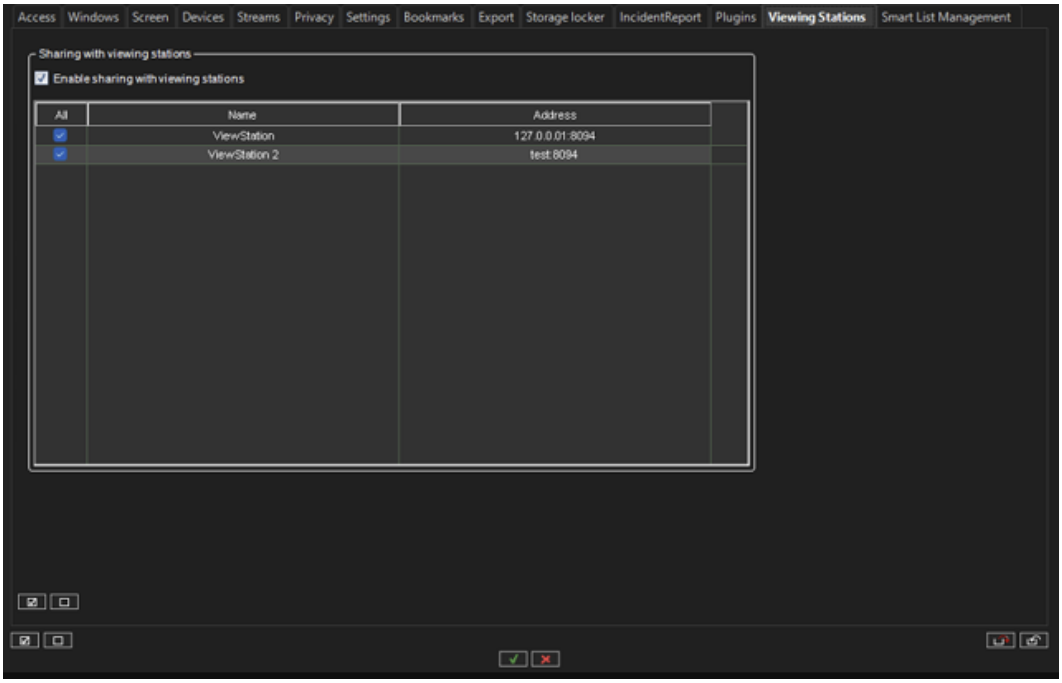
The Plugins tab contains options for Spotter plugins.

Each plugin behaviour can be either default or custom. The default behaviour can be controlled from the ”Default plugin role” controls.



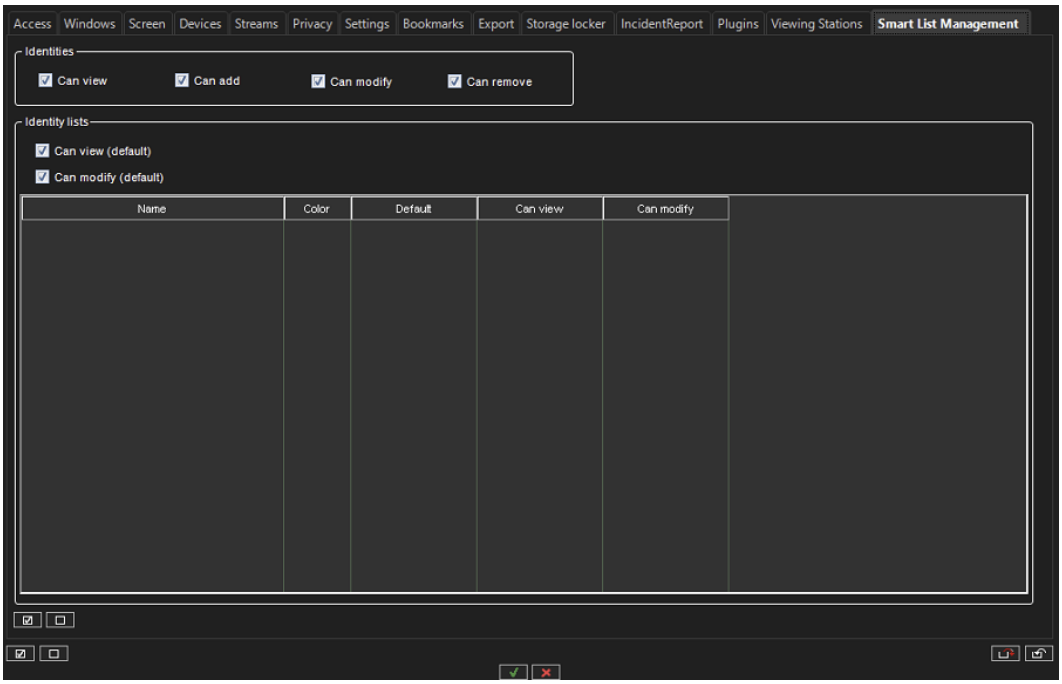
12.4.1.5.13Viewing Stations

The Viewing Stations tab contains options for viewing stations.



12.4.1.5.14Smart List Management

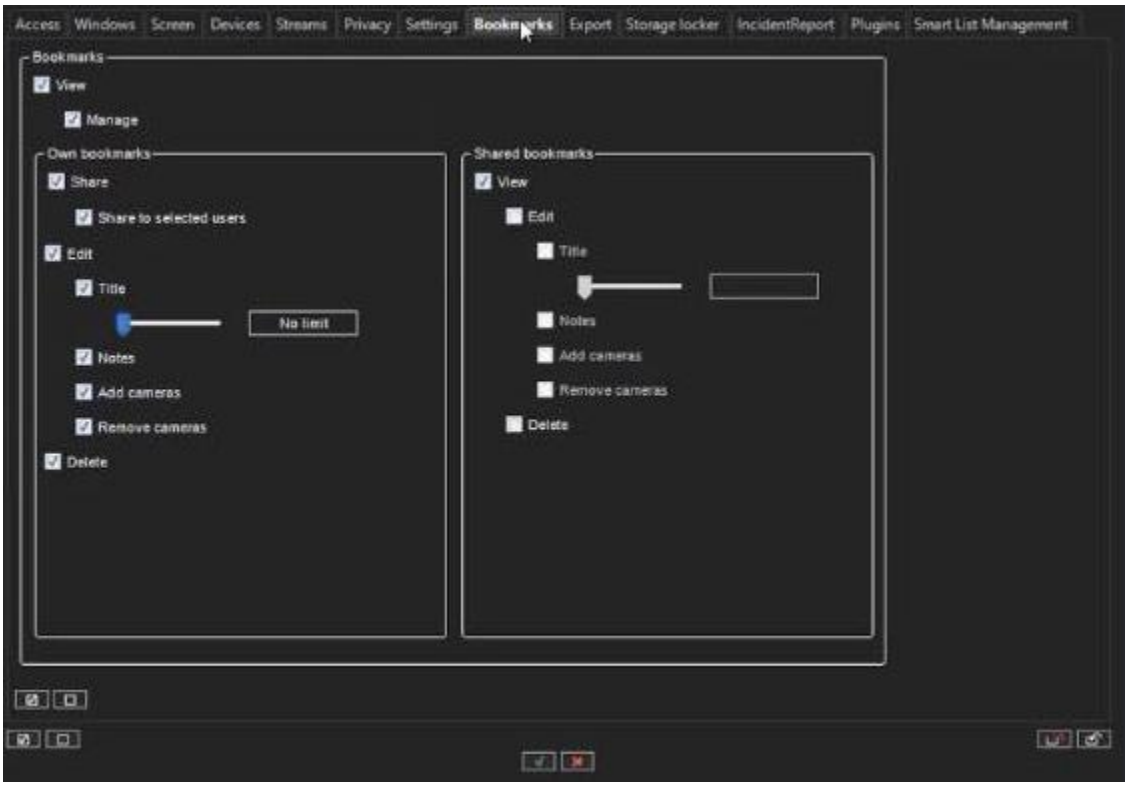
The Smart List Management tab contains options for the Smart List Management plugin.



12.4.1.5.15Sharing with selected users

12.4.1.5.15.1 Share bookmarks with specified users

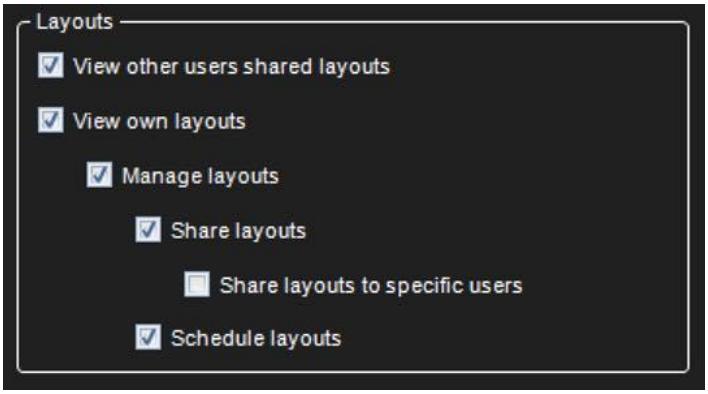
1. In the left-hand side menu, go to the **Users and User groups** tab.
2. Open Edit user group “Administrators” by double-clicking on the Administrotors group in the left-hand side menu.
3. Click the symbol to the right of Mirasys Spotter Enterprise role under **User group roles** to edit Mirasys Spotter Enterprise role properties.
4. Here, you can select to share bookmarks with specified users, under the **Bookmarks** tab by clicking **Share to selected users**.



12.4.1.5.15.2 Share layouts with specified users

1. In the left-hand side menu, go to the **Users and User groups** tab.
2. Open Edit user group “Administrators” by double-clicking on the Administrotors group in the left-hand side menu.
3. Click the symbol to the right of Mirasys Spotter Enterprise role under **User group roles** to edit Mirasys Spotter Enterprise role properties.

4. Here, you can select to tab content, under the **Screen** tab by clicking **Share layouts contents to specific users** under Tab contents.



12.4.1.5.15.3 Share tab content with specified users

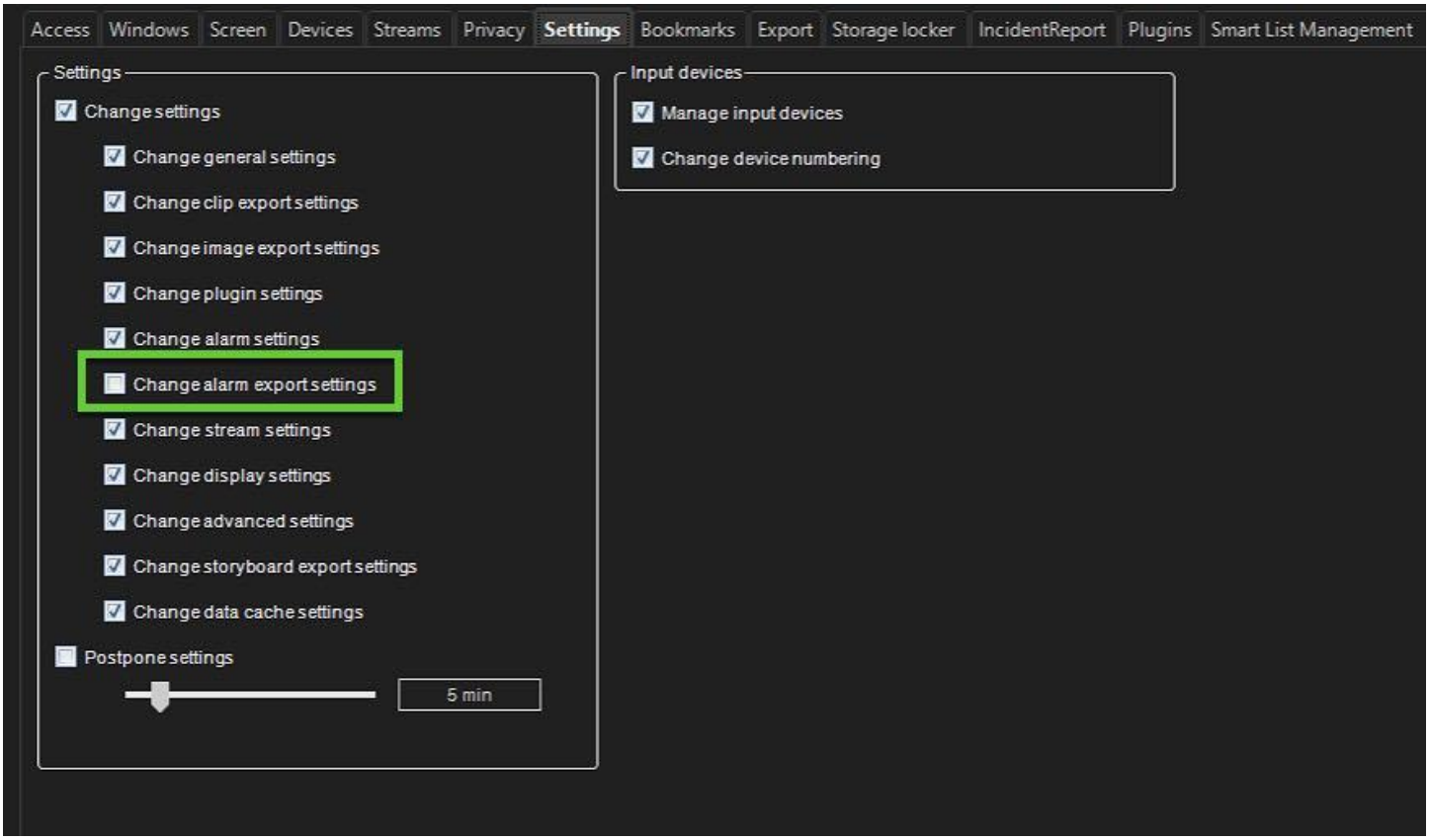
1. In the left-hand side menu, go to the **Users and User groups** tab.
2. Open Edit user group "Administrators" by double-clicking on the Administrotors group in the left-hand side menu.
3. Click the symbol to the right of Mirasys Spotter Enterprise role under **User group roles** to edit Mirasys Spotter Enterprise role properties.
4. Here, you can select to share tab content with selected users, under the **Screen** tab by clicking **Share tab contents to specific users** under Tab contents.



12.4.1.5.16Immediate Alarm Export to a specified folder

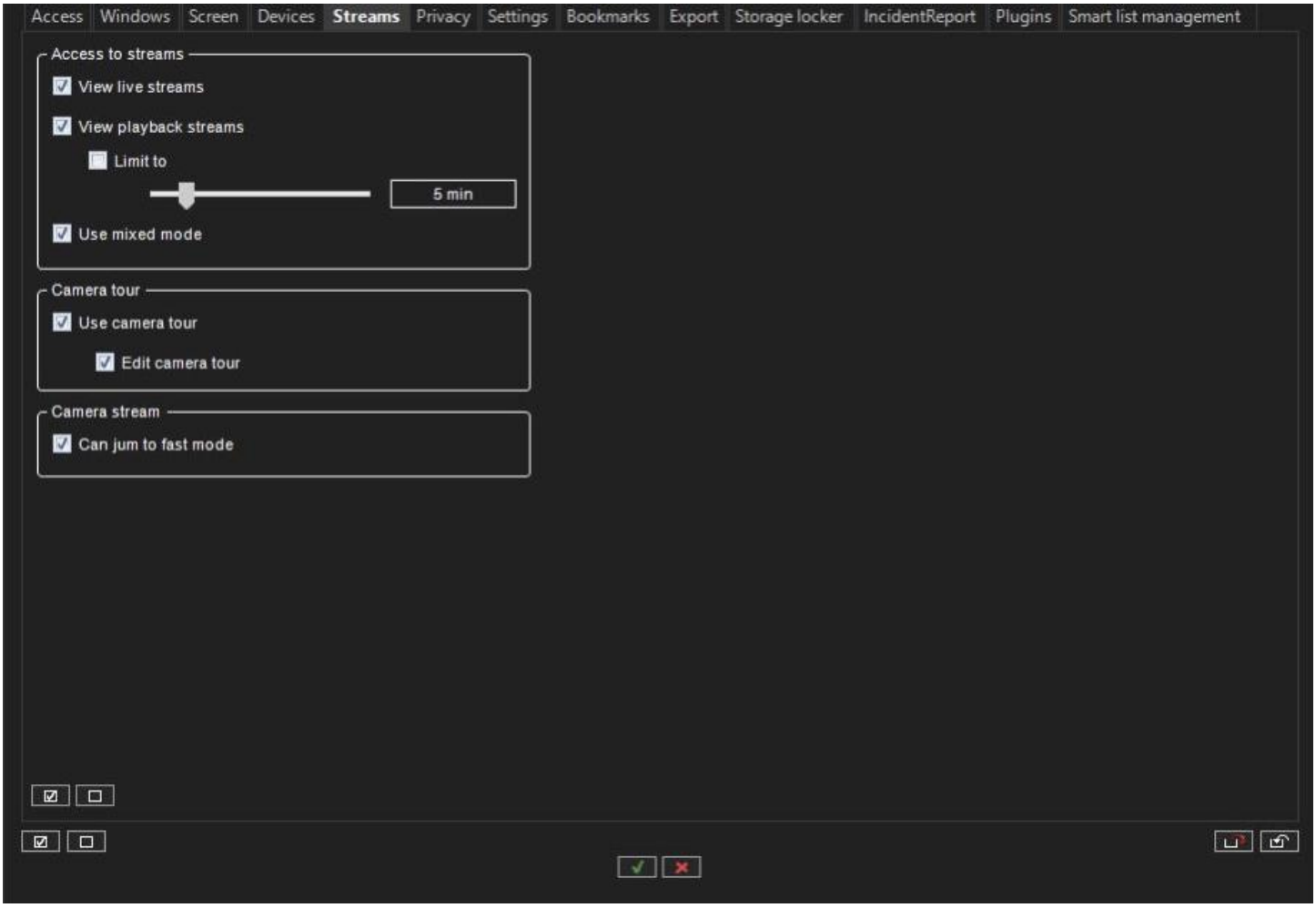
When system administrators enable and configure this feature, it is possible to directly export an alarm to a specific folder in Alarm Search from the Alarms table in Spotter.

1. Click the wrench icon under the User and User groups tab in the left-hand side menu to go to Edit user group, then click the wrench next to Mirasys Spotter Enterprise plus to go to the Spotter role **Settings** tab.
2. Tick the box for **Change alarm export settings** under Change settings.



12.4.1.6 Playback Speed Role

Spotter playback automatic speed adjustment can be enabled or disabled in the Spotter role settings “Streams” tab.



In the Camera streams group, there is a selection for fast playback mode. If selected, with 2x, 4x, and 8x playback speeds, if the playback cannot keep the pace because of too much load, it will jump to fast forward/backward. By default, automatic playback speed adjustment is not selected.

> "Can jump to fast mode" affects to Spotter playback functionality. When it is enabled, playback will change the normal play forward / backward to fast forward / rewind if the playback doesn't keep up to the speed. If this option is not enabled, then the playback will use the play forward / backward speed as the user has set, but the playback speed will be slower if the Spotter machine cannot keep up the playback pace.

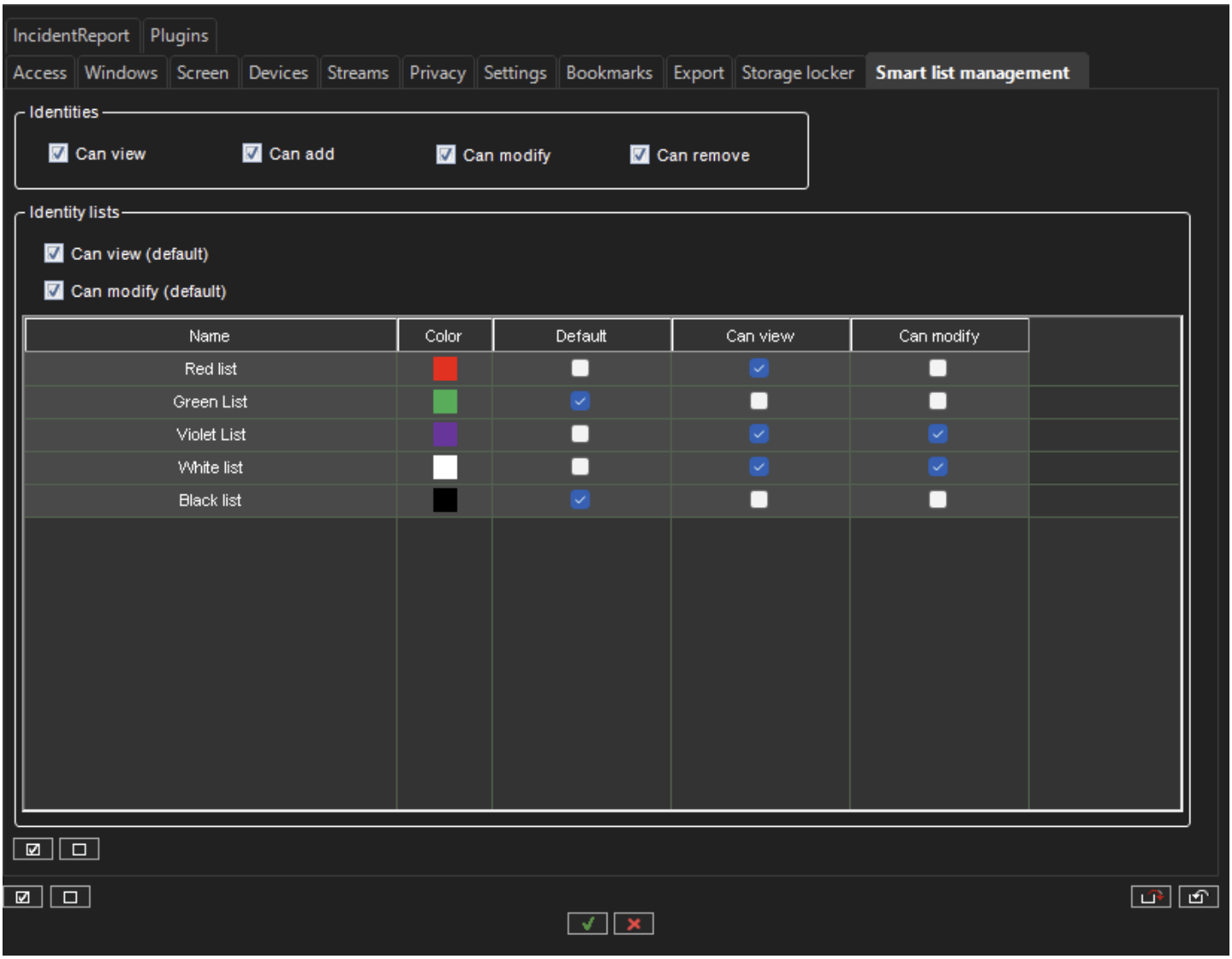
12.4.1.7 Smart List Management role

The Spotter List Management plugin can be enabled on the Spotter user role settings, where it is also possible to limit the permissions to manage identities and identity lists.

12.4.1.7.1 Smart list management properties

The "Smart list management" tab contains role properties related to smart list management functionality:

- Possibility to view, add, modify, and remove identities.
- Possibility to view and modify identity lists (default properties and properties for each list separately).



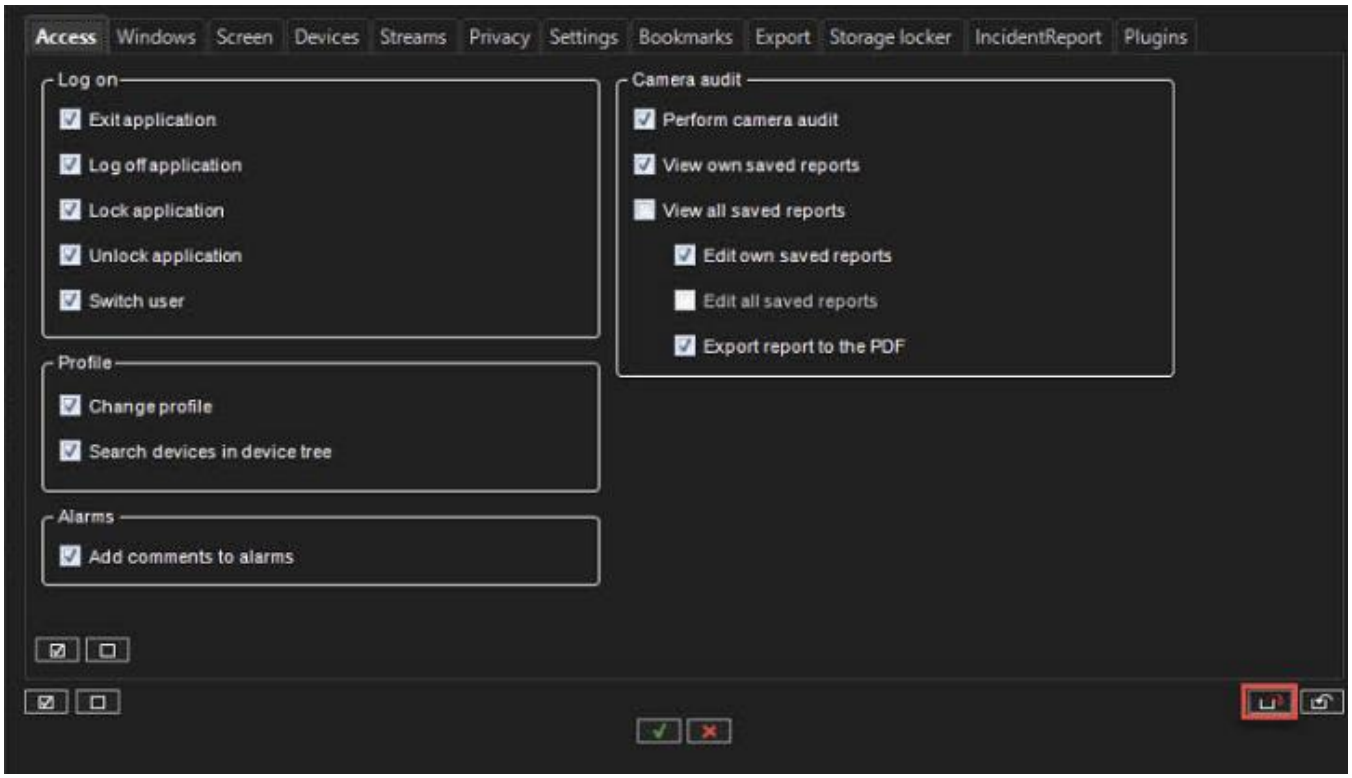
12.4.1.8 Spotter Web role

Spotter Web role enables new Spotter Web and Spotter Mobile usage

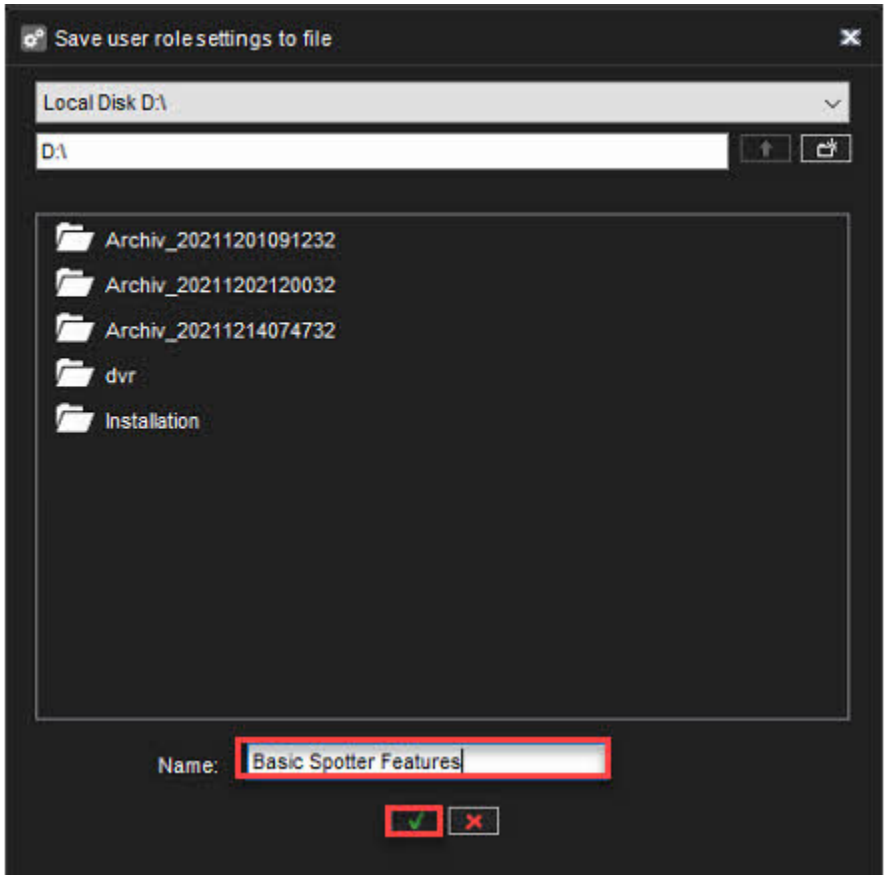
12.4.1.9 Exporting and Importing User Role Settings

12.4.1.9.1 Exporting User role settings

1. Click **Export user role settings to file**

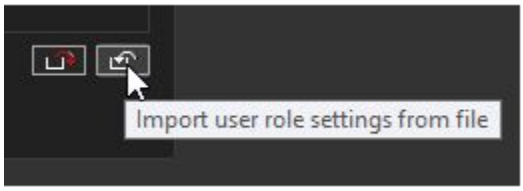


2. Select destination
3. Set the name of the file
4. Click **OK**

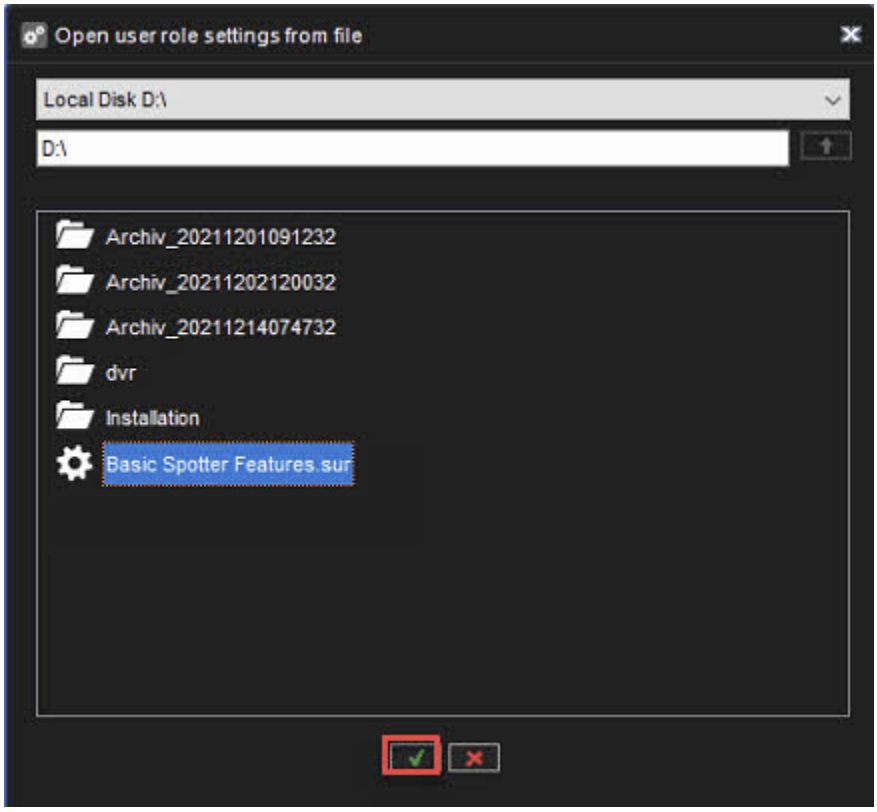


12.4.1.9.2 Importing User role settings

1. Click **Import user role settings from the file**



2. Select file(.sur)
3. Click **OK**



12.4.2 Two-factor authentication

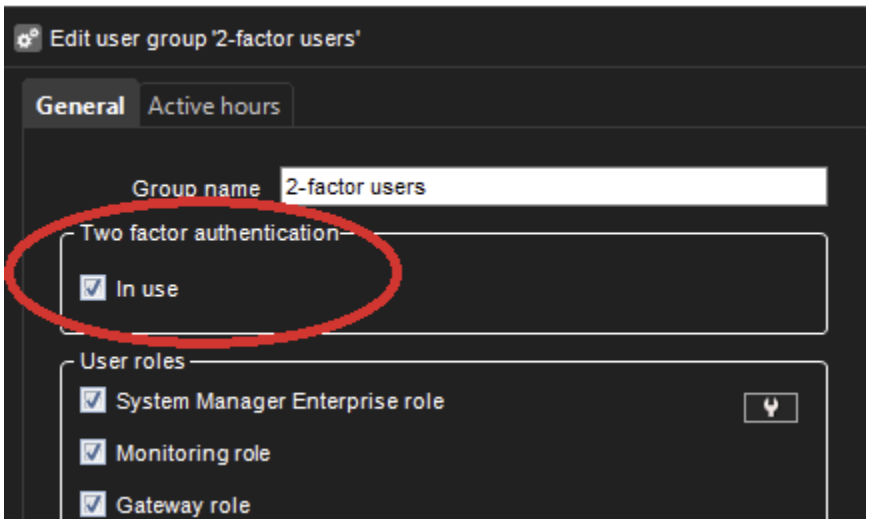
Two-factor authentication is functionality to improve the user's identification by requiring the username and password and a code from an external physical device.

This makes it practically impossible, e.g. certain user groups (e.g. system administrators), to use shared credentials.

(Using shared credentials would make it almost impossible, e.g. to monitor specific user actions from the audit logs later on.)

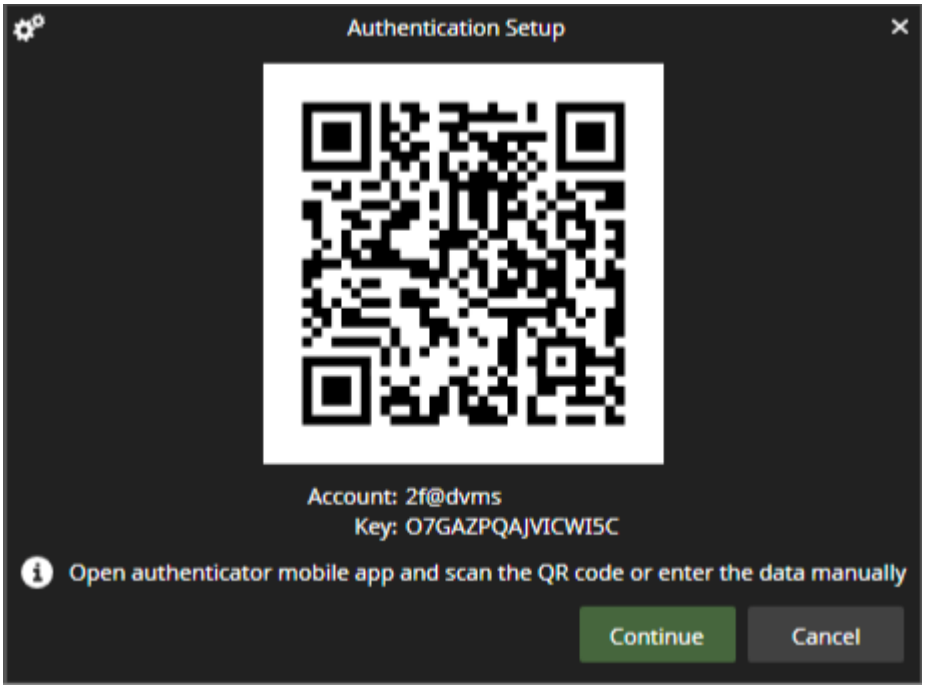
12.4.2.1 Setup:

1. The admin enables the 2-factor authentication for the specific user group.



2. When the user in the group tries to log in for the first time, the user is requested to use or install the 2-factor authentication client (e.g. Authy, Google authenticator, MS Authenticator (available for free)) on his/her mobile device.
3. The VMS and the authentication client are then synchronized with the software with VMS.
4. This happens by transferring the "secret key" generated by the VMS to the authentication software via QR code or directly typing it to the software.

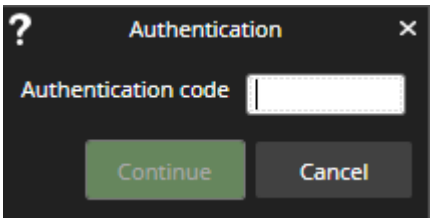
Example below:



1. After that, the authentication client automatically generates new one-time passwords.
    a. (The passwords change periodically and are kept in sync as the VMS clocks and the authentication app have the same time.
    b. Note that this does not require any direct data communication link between the software.)

12.4.2.2 Login:

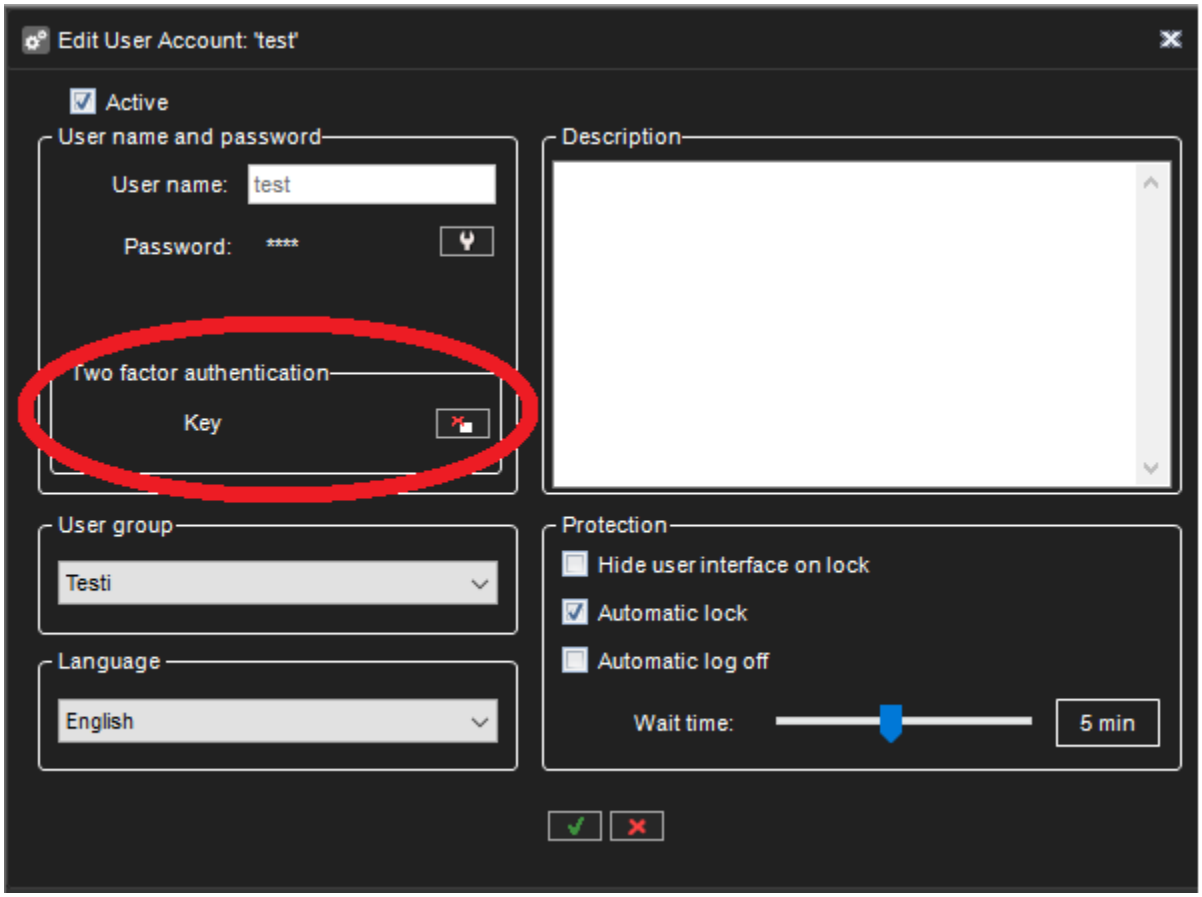
1. The user provides the standard credentials to VMS (username, password)
2. The VMS requests an authentication code from the authentication app for each login.
3. The user provides the one-time password from the authentication app. The user types them to the VMS client.



12.4.2.3 Maintenance:

1. If the user forgets his / her 2-factor secret key, the administrator can then reset the key from the system manager.

2. After the 2-factor secret key reset, the user needs to update the private key next time he/she logs in. (See step 2).



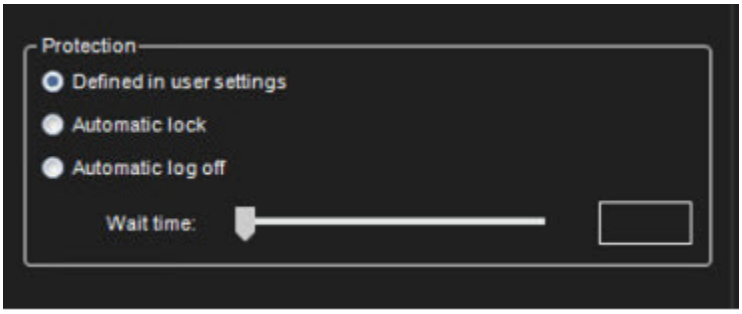
12.4.3 Protection

Protection group box is added in user group / general settings.

As default, "**Defined in user settings**" is set and Automatic lock, Automatic log off are not selected and Wait time settings is disabled.

Only one of the check box selections can be set at the time.

If user group level automatic lock / log off settings are selected, then user level automatic lock / log off settings are not enabled in user account settings

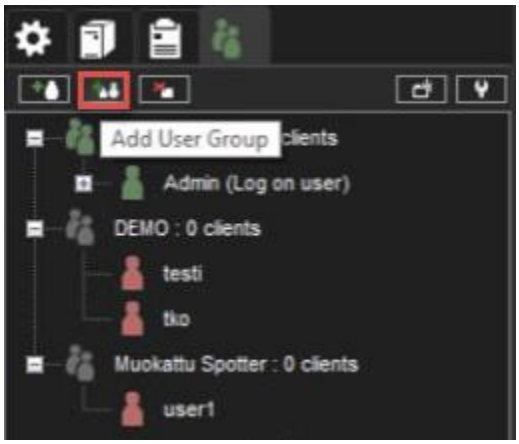


12.4.3.1 Automatic lock and Automatic log off values

- 1-5 min, 10, 15, 20, 30 min, 1-12 hour and 24 hour

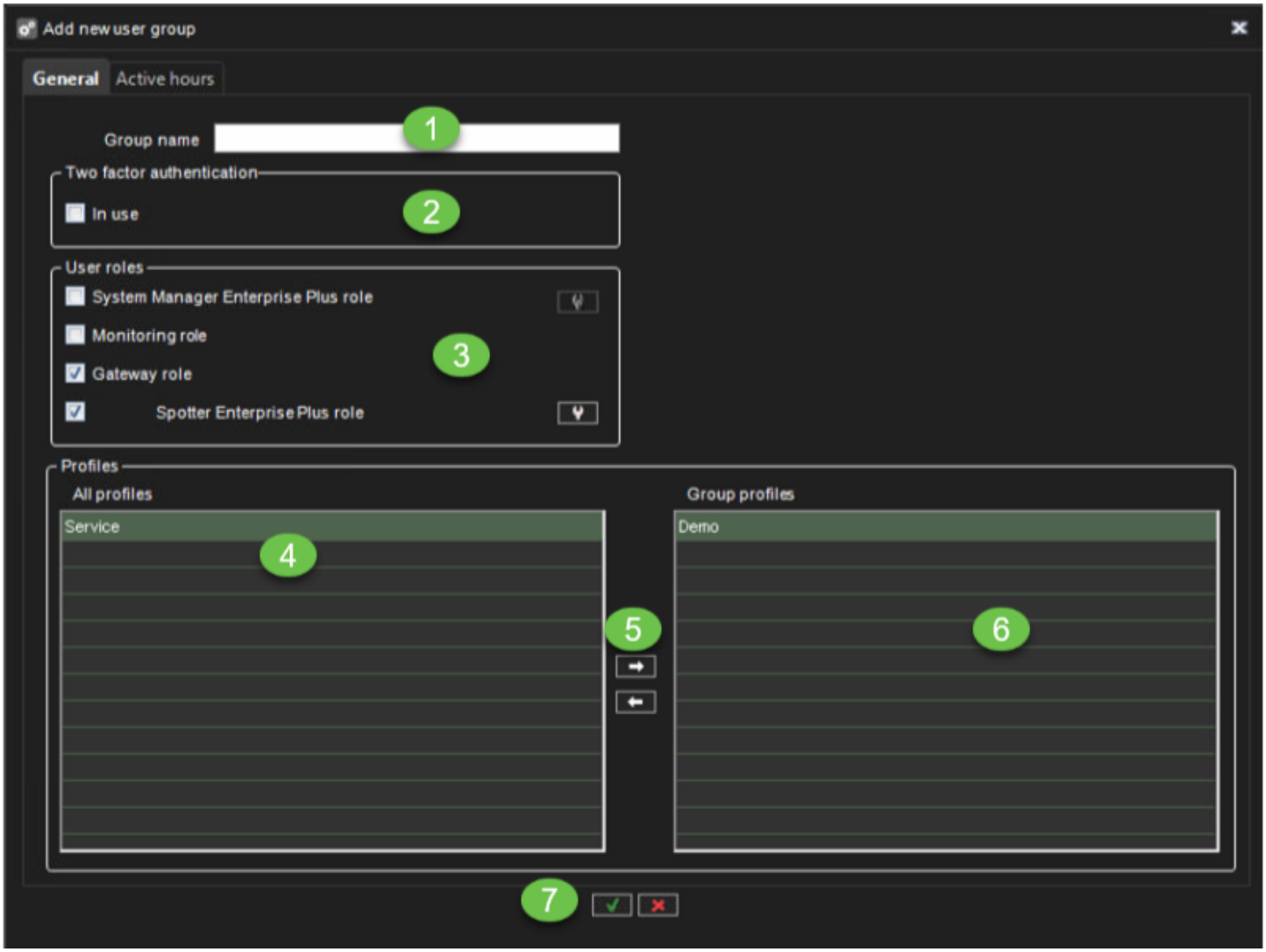
12.4.4 Creating a customer-specific User Group

1. Click **Add User Group**



2. Type a name for the group in the **Group name** box
3. Enable **Two-factor authentication**, if needed
4. Select the **User roles** for the group.
5. Select the **Profile** or **Profiles** you want to assign to the user group.
6. Click the right arrow button or drag the profiles from the left panel to the group profiles box
7. Check that correct profiles is found
8. Click **Ok** to confirm user group creation

Tip: *To select more than one profile at a time, keep the SHIFT, or CTRL key pressed.*



12.4.4.1 Editing a User group

To edit a user group (whether system or domain**-based):**

1. Open the **Users** tab.
2. Click on the user group you want to edit.
3. You can edit the following settings:
    a. Type a name for the group in the **Group name** box.
    b. Select the user roles for the group.
    c. Select the profile or profiles you want to assign to the user group. Click the right arrow button or drag the profiles from the left pane to the right.

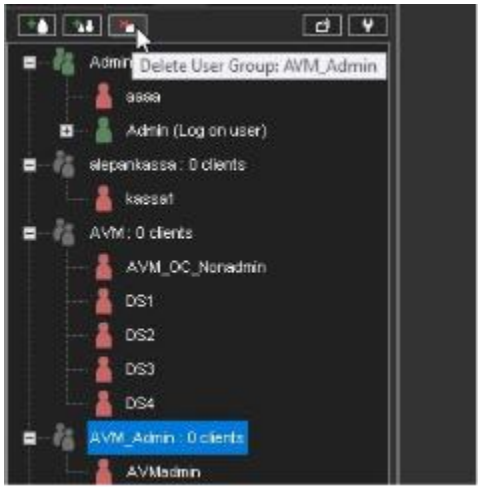
4. Click **OK** to save the changes.

- **Tip:** *To select more than one profile at a time, keep the SHIFT, or CTRL key pressed.*

12.4.4.2 Deleting a user group

To delete a user group (whether system or domain**-based):**

1. Open the **Users** tab.
2. Click on the user group you want to delete. Note that you cannot delete the default **Administrators** group.



3. Click **Delete User Group** in the upper-left corner.

4. Click **OK** to delete the group.

Note: *Domain-based (LDAP) user groups cannot be deleted through System Manager. If deleted, an LDAP group is removed from System Manager, but the domain group is not affected.*

12.4.5 Domain Based User Groups (Active Directory)

12.4.5.1 Domain Based User Groups (LDAP)

The system supports domain-level user rights integration (Microsoft Active Directory, LDAP), enabling users to be synchronized from domain groups.

Domain-based users can log into the VMS system with their domain usernames and passwords.

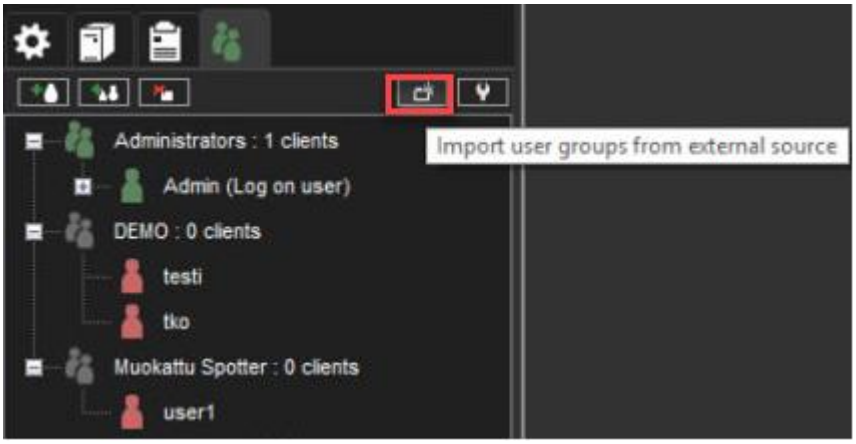
By default, user group rights are synchronized with their parent domain every 30 minutes.

Please contact your system supplier if f you need to change the default interval.

This feature requires a license update.

12.4.5.2 Adding a new domain-based user group to the system

1. Click **Import User Groups from an external source** in the upper-left corner of the **Users** tab
   The Main Server needs to be connected to a domain for the button to be displayed.
   If the server is not connected to a domain, the button is not visible.



1. Type the name of the domain into the **Domain name** dialogue box.
2. Select whether to get all user groups or to search for specific groups.
   If you want to search specific groups by name, you can add a search criterion based on the text string being equal to the group name, contained in the group name, or the group name starting or ending in the text string.

4. Select whether to skip or include open user groups.

5. Select whether to clear or keep previous search results.

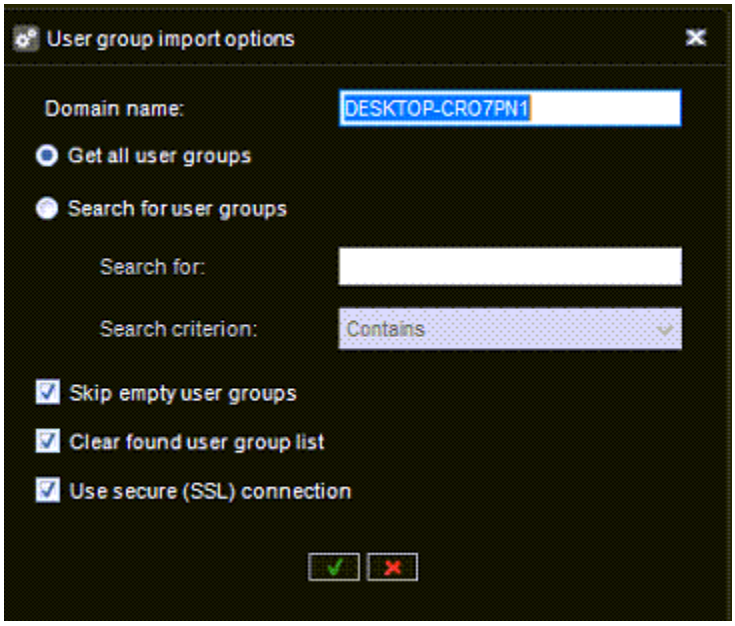
6. Enable **Use secure(SSL) connection**. If needed

7. Click **Ok**.

8. In the **Import user groups** window, select the user groups you wish to import from the domain.

9. Click **Ok** to import the selected groups.

10. Edit the imported user groups to set their user roles as instructed below.



12.4.6 Active hours - User group access schedule

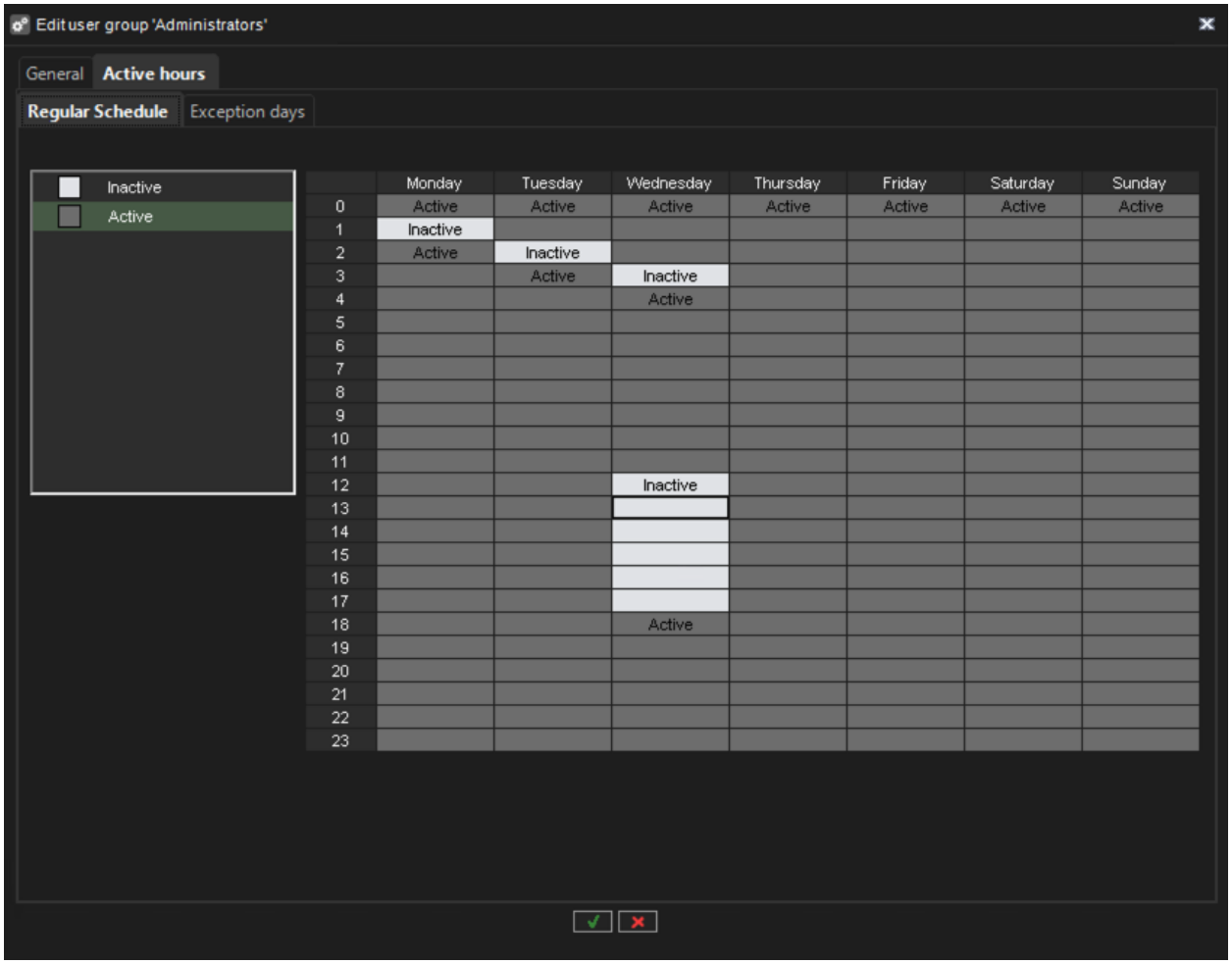
You can set the days and hours a specific user group can access Spotter to control operators' access to it outside of working hours, for example.

Go to **System Manager** > **Users and User Groups** to configure the User group access schedule.

12.4.6.1 Regular Schedule

Use the Regular Schedule tab to set a weekly schedule, controlling when the user group can use Spotter or when it will be prevented.

1. Click on the User group that you want to edit.
2. Click the tab **Active hours**.
3. All hours every day are Active by default.
4. To prevent access during certain hours:
    a. Select **Inactive** to the left of the weekly schedule.
    b. Click the hours the user group should not have access to Spotter (=Inactive).



5. To change an inactive hour back to active, select **Active** to the left of the weekly schedule and click on the hour during which the user group should be able to log in to Spotter.
6. When the Regular Schedule is finalized, click the green checkmark to **Save**.

If an Operator in a user group tries to log in to Spotter during an **Inactive** time, the Operator will not be able to log in, and the message **Unautorized user** will be displayed.

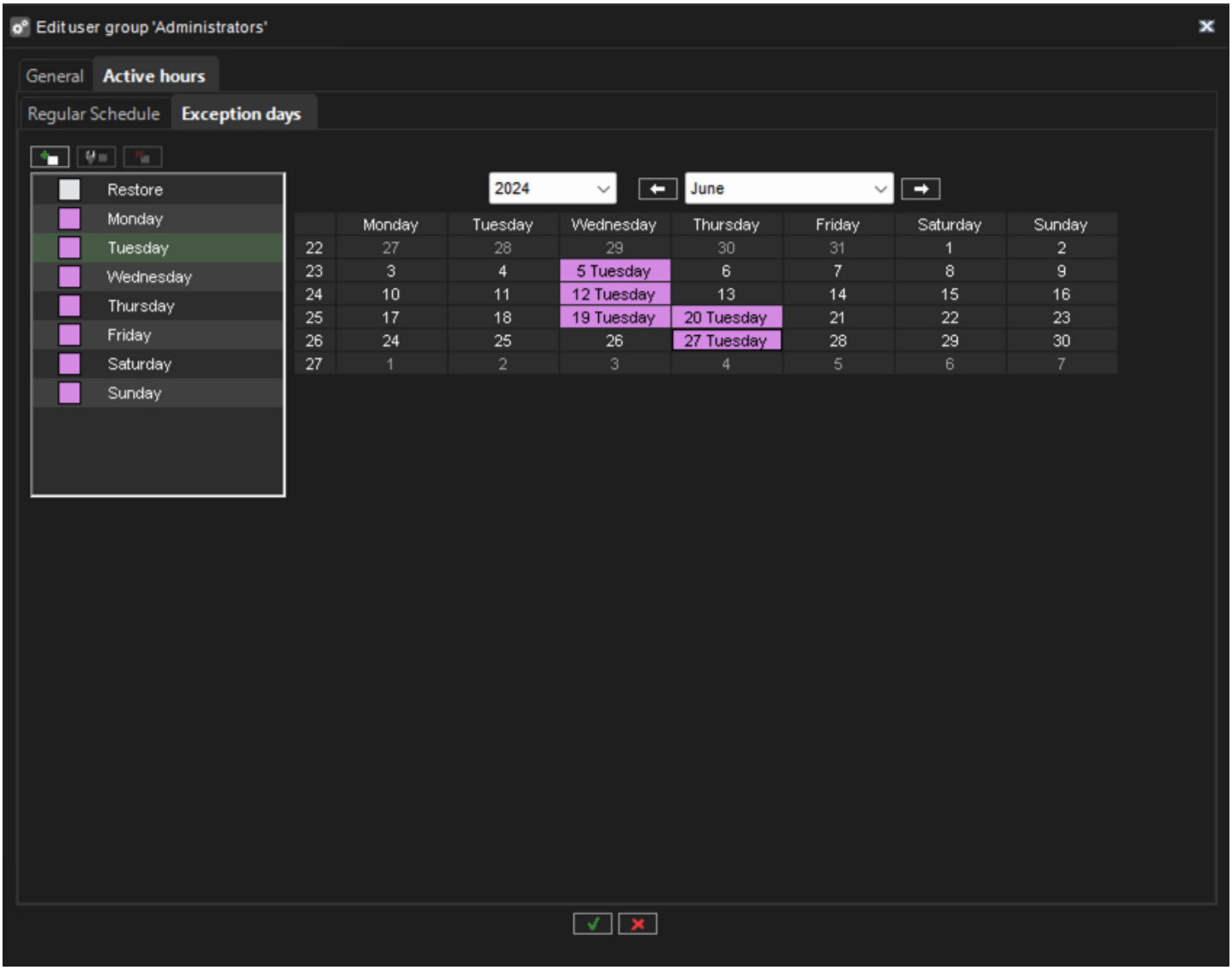


12.4.6.2 Exception days

If you want to use another schedule on a specific date, you can overwrite the regular schedule for that date under the **Exception days** tab

Your Regular Schedule is available for all weekdays to the left of the calendar for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.

1. Select the month and year.
2. Select the day to the right of the schedule to use another day's schedule, then click on the date you want to use another day's schedule.
   For example, the Tuesday schedule below is used for some Wednesdays and Thursdays in July.



1. To remove an exception day, select **Restore** and click the date.
2. Click the green checkmark to **Save**.

12.4.6.2.1 Create a new exception day schedule

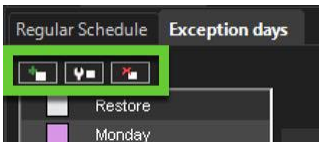
You can also create your exception schedule by clicking the + sign at the top-left of the schedule.

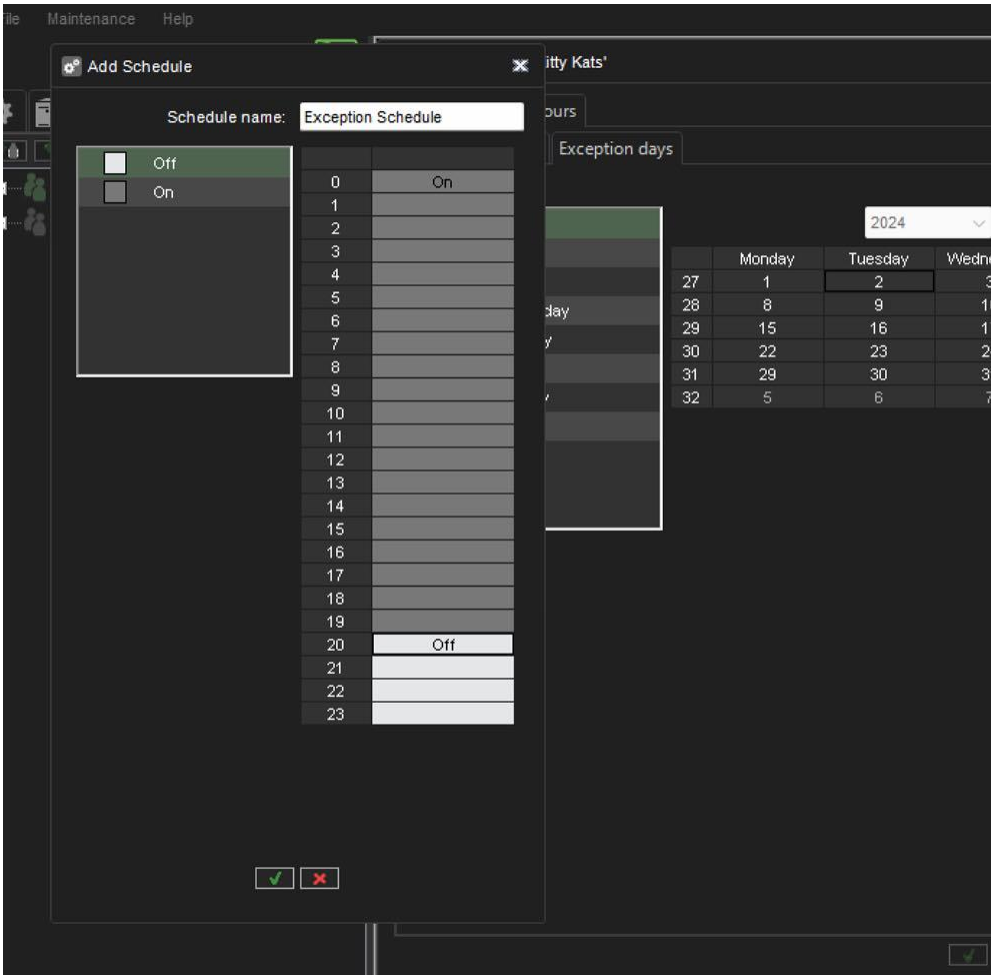
In that exception schedule, you can select which hours there should be an exception to the regular schedule (**On**) or not (**Off**).

1. Select On or Off and click the hours to have the regular schedule not in use or in use.
2. You can name the schedule under the **Schedule name**.
3. **Save** it by clicking the green checkbox.

It is now ready to be used on Exception days.

The exception schedule can be edited and deleted by using the menu:





12.5 CREATING A CUSTOMER-SPECIFIC USER

To add a new user to the system:

1. Open the **Users** tab.
2. Click the name of the user group to which you want to add the user.
    a. Note that you can only add users to the system's native groups, not in domain-based groups.
3. Click **Add User** in the upper-left corner of the Users tab. The Add User dialogue box is shown.
4. Do the following:
    a. Type a name for the account in the **Username** box.
    b. To add a password to the account, click **Change password** and type the password two times.
    c. Type an optional description about the user account.

d. Use the pull-down menu to select the user group into which you want to assign to the user.

e. Select the user interface language for the user.

f. Set protection settings for the programs:

   i. **Hide user interface on lock**

   ii. **Automatic lock**

   iii. **Automatic log-off**

   iv. **Wait time**: if the user does not use the program for the specified time, the program is locked, or the user is logged off.

Note: Users can change their passwords and user interface language in the Spotter program.

12.5.1 Identify users through a user name separate from the user login ID

To improve platform security, users can be identified through a separate user name so as not to display and compromise the user login ID.

The System Administrator can define a public name for users in the System Manager user settings. The public user name should be unique. This is not mandatory, and the field can also be left blank.

As before, the user will use the login user name to log into any application, but if a public user name has been entered for the user, this public user name will be displayed in the client UI.

12.5.2 Adding a public username in the System Manager

1. In the System Manager Desktop Application, go to User Settings and click edit.
2. In the **Public name** field, the system admin can choose to provide a public name for a user:



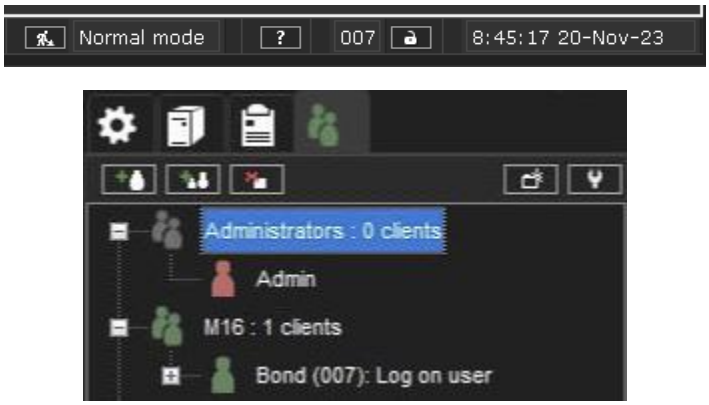
This name is displayed in the System Manager's users list:



It is displayed in the profile settings user list:



And also as logged on user:

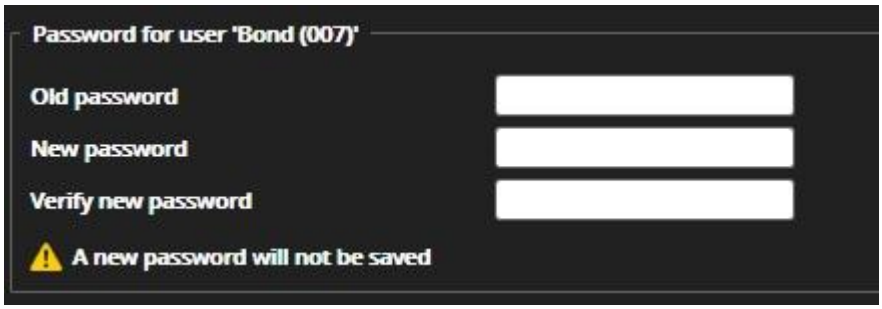


12.5.3 Displaying a public user name to the user in Spotter

If there is a public user name set for a user in System Manager, the public user name is displayed together with the user identity, in switch user:



The users can also view their public user name when changing their password:



12.5.4 Public user name in Spotter web client

The public user name is displayed in Spotter Web in the top right corner if it has been defined in the System Manager.

If the public name has not been defined, the user's login name is shown.

If the user's public name is changed in the System Manager, the Spotter Web user is logged out, and the user needs to log in again. After the login, a new public name is shown on the main screen. If it has been removed in the System Manager, the same process applies, and after login the user's login name is shown.

12.6 User account settings

12.6.1 User account settings contain the following options:

- Account status
- Password
- Two-factor authentication key management, see more from Two-factor authentication
- User group
- Language
- Protection settings

- Hide user interface on lock
- Automatic lock
- Automatic log off

12.6.2 Supported languages

- Arabic
- Chinese
- Czech
- Danish
- Dutch
- Estonian
- Finnish
- French
- German
- Hungarian
- Icelandic
- Italian
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Thai

12.7 Disabling or Activating a User Account

If you want to prevent a user from logging on to the system but want to keep the user account for later use, you can disable the account.

You can activate the account when the user is again permitted to log in to the system.

To disable or activate a user account:

1. On the **Users** tab, select the user account
2. Click **Edit User Account**
3. Do one of the following:

- To disable the account, clear the check box **Active**.
- To activate the account, select the check box **Active**.

4. Click **OK**.

Note: *Domain-based (LDAP) users cannot be deleted or removed with System Manager.*

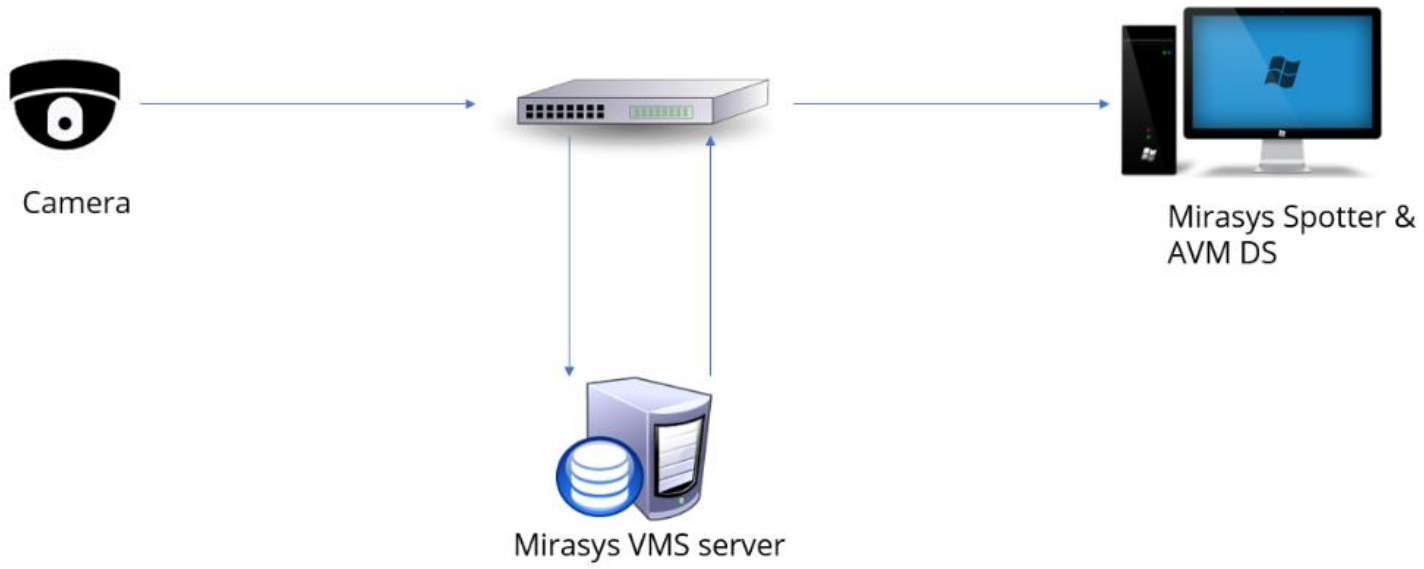
13 THRUCAST STREAMING

ThruCast is the direct camera video streaming feature in Mirasys VMS.

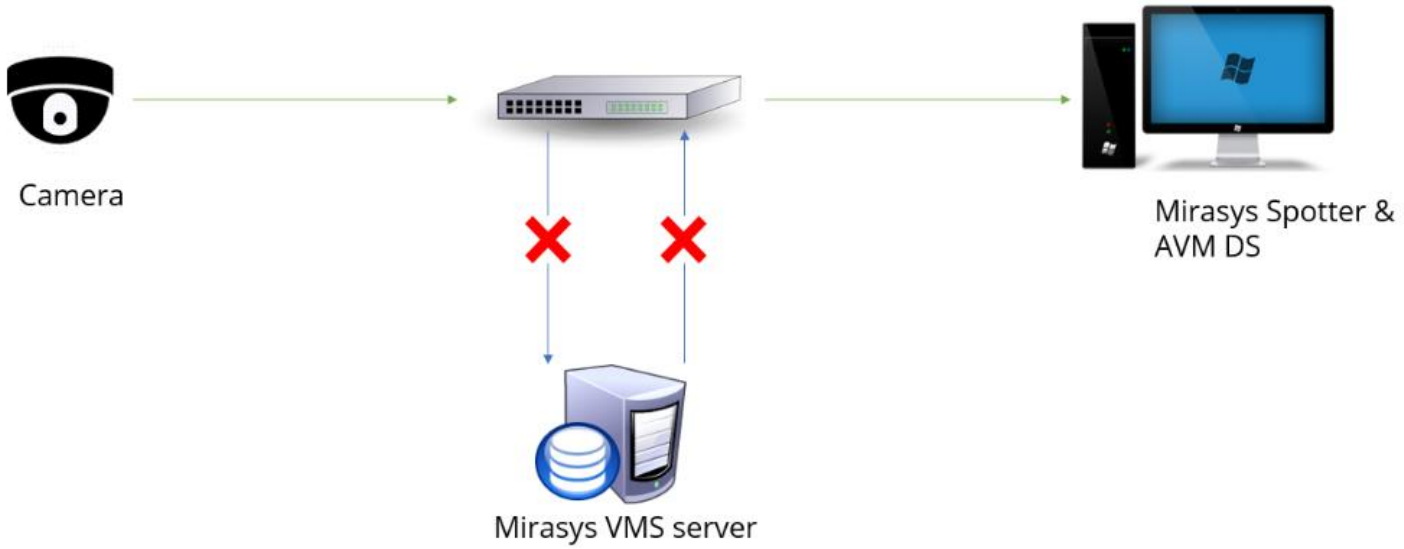
With ThruCast, the video stream comes directly from the camera to the viewing client, the Spotter for Windows application.

In a standard streaming scenario, the stream to the client comes from the VMS Server.

13.1 STREAM FROM THE SERVER TO THE CLIENT



13.2 STREAM FROM THE CAMERA DIRECTLY TO THE CLIENT



It is possible to get the direct stream from the camera to the client when the VMS Server connection is OK. This can be useful if users want to optimize network utilization.

13.3 SUPPORTED CAMERAS

ThruCast requires a separate camera capture driver for the client.

Currently, drivers exist for the following camera manufacturers:

- Acti
- Axis
- Bosch
- Dahua
- Hikvision
- Lilin
- Samsung
- Sony
- Stanley
- ONVIF

Use the ONVIF ThruCast driver for cameras that are not on the supported list.

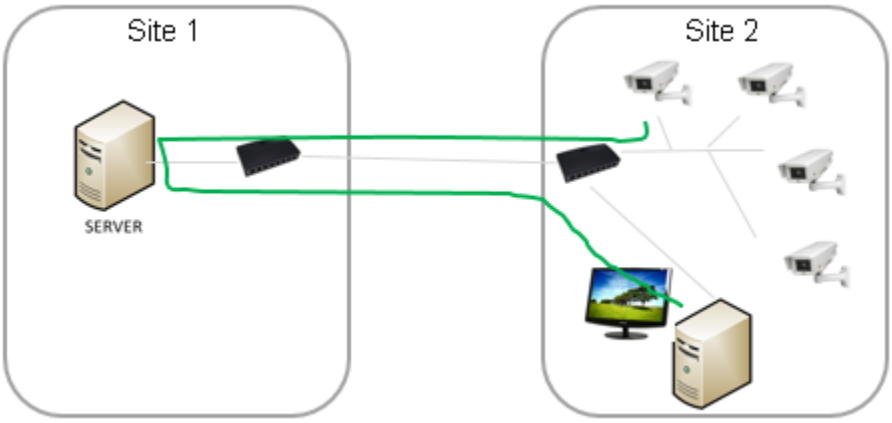
The use of the ONVIF driver requires that the camera is added to the VMS system with the ONVIF driver, not the camera's native driver.

13.4 Network Optimization

ThruCast can be used to reduce network load in specific scenarios.

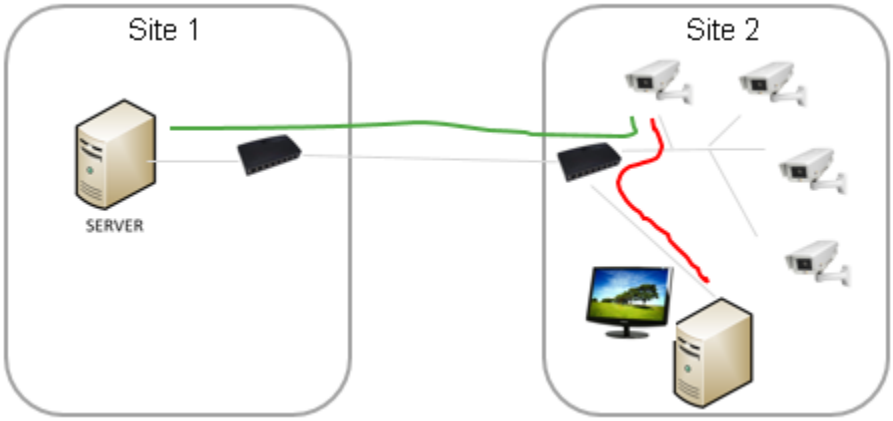
The load reduction mainly occurs when the server is located off-site (remote) and the viewing client is on-site (local to the cameras).

An example scenario 1, we have two sites where the recording is off-site, and the viewing client is on-site. In the following diagram, the viewing is done without ThruCast, and the video goes first to the server and then from the server to the viewing client.



In this solution, the traffic between the two sites is increased.

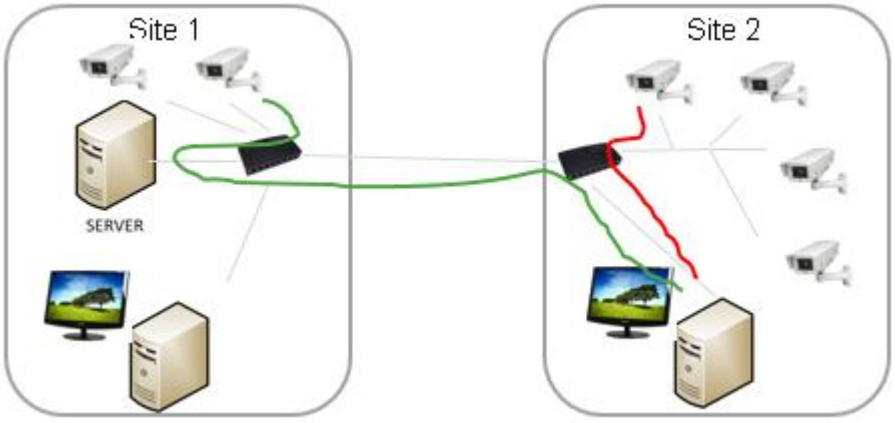
If the stream is consumed directly from the camera with ThruCast, the traffic between the two sites is reduced.



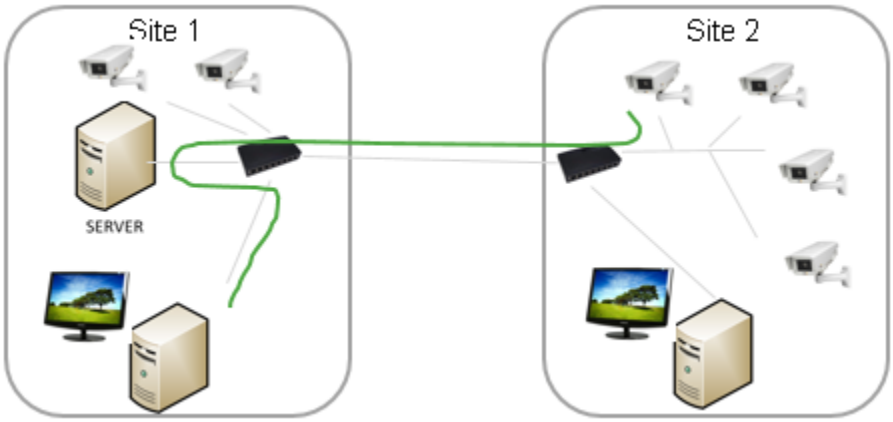
An example scenario 2, there are cameras on two sites and viewing clients on two sites.

For the Site 2 user, the use of ThruCast makes more sense for the on-site cameras.

The user can choose to use ThruCast for all cameras or only for the on-site cameras.



For the Site 1 user, the use of ThruCast only reduces the amount of traffic from the server to the nearest network connection.



Users have complete control over which cameras are using ThruCast and which cameras are viewed typically.

The setting is memorized for each camera and each user and saved to Spotter layouts.

13.5 Multistreaming and ThruCast for Network Optimization and Storage

Since it is also possible to use a different stream for ThruCast than the recording stream, this should be considered when planning the network capacity.

For example, users can choose to view live images with ThruCast at a higher framerate (for example, 25 fps) and always record at a lower framerate (for example, eight fps).

This reduces the storage and network requirements considerably.

13.5.1 Impact of ThruCast on Image Delay

Since the ThruCast stream does not travel to the VMS Server and back, the delay from the camera to the client is slightly smaller, but the difference to the stream received from the server is not large, only some milliseconds.

The difference in the two-stream modes is complicated to observe in real life.

13.5.2 Features Not Supported in ThruCast Streaming

ThruCast does not support PTZ control or Audio

Also, currently, ThruCast supports only live images. Playback (recorded images) is currently always received from the server.

13.5.3 Licenses

ThruCast requires the VMS license to have the ThruCast feature and the ThruCast client driver identifiers used.

These ThruCast driver licenses, and the ThruCast feature, are always enabled in the Mirasys V9 product version.

13.5.4 Multiple Viewers

Since each ThruCast-viewer opens an individual new stream from the camera to the client, users should trial how many streams can reliably be opened from the cameras they are using. In practice, 3-5 streams typically work ok.

13.5.5 Installing Client Drivers

Before using ThruCast, the necessary client drivers need to be installed with the System Manager application if they have not been installed with the original system installation.

The client driver packages are available in the whole setup package from Mirasys. They are named with the ".sdi" filename extension.

These drivers are installed on the System Manager application's first page, "Install client driver."

The new drivers can be added by pressing the "Install new client driver" button and choosing the SDI packages.

After this, click the "OK" button.

After installing the drivers, they still need to be downloaded to the viewing Spotter clients. This is done when Spotter is restarted from the desktop.

After Spotter has downloaded the new drivers, the system is ready for ThruCast use.

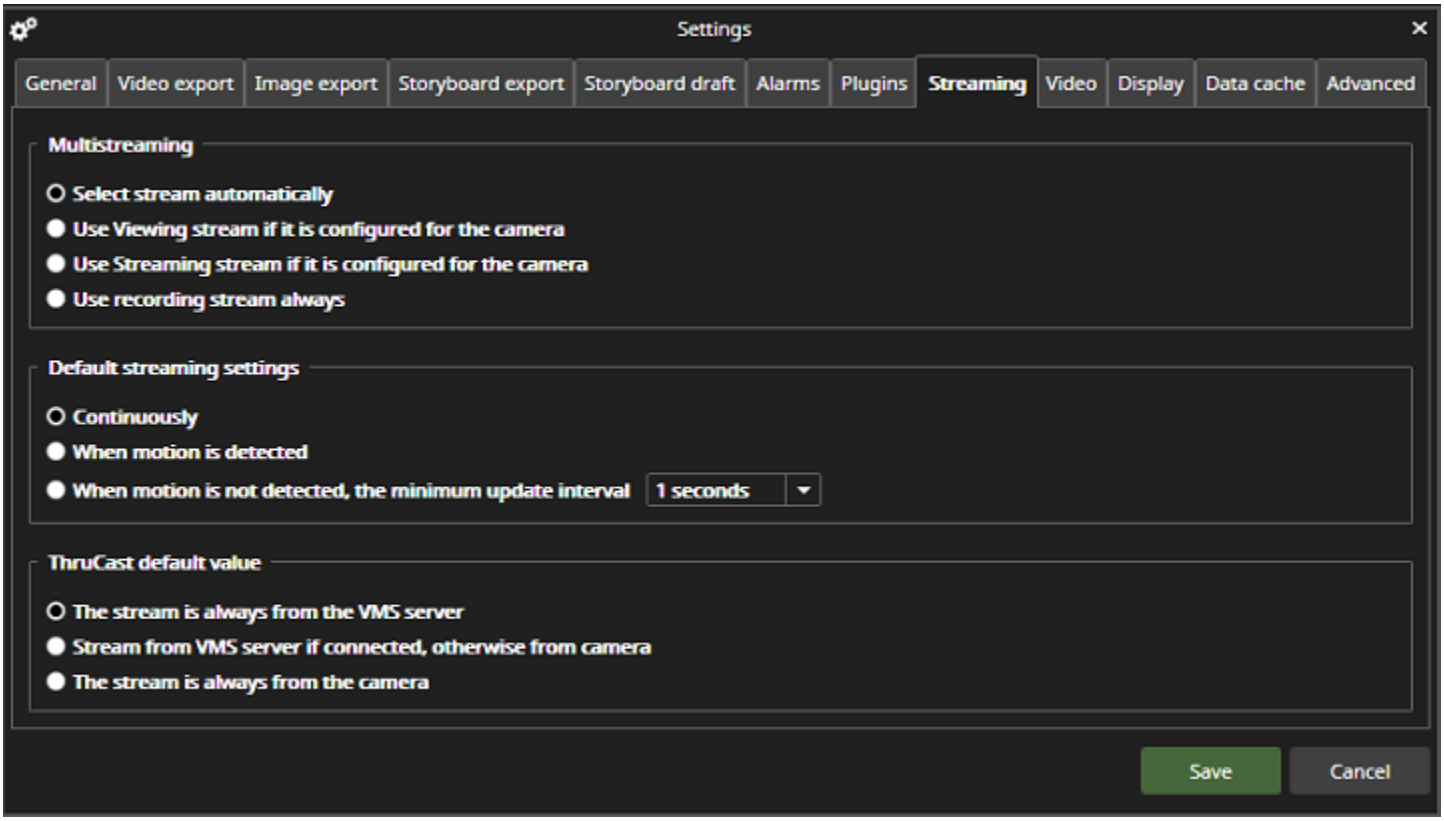
Please note that only those cameras which' client driver was installed will appear as ThruCast enabled.

13.5.6 Configuring multi-streaming

ThruCast can use any stream from the camera, the Recording, Live viewing or Remote streams.

The multi-streaming is enabled and configured typically in System Manager – cameras.

In the Spotter client settings – streaming – multi-streaming, the user can choose which one of the streams is used for viewing. The same setting is used for standard and ThruCast viewing.



13.5.7 ThruCast Default Setting

The default setting for all cameras that have not been used for ThruCast before can be defined in Spotter settings – streaming – ThruCast default value.

The possible values are

- Always stream from the VMS Server
- Stream from the VMS Server normally, but switch to ThruCast if the connection to the server is lost
- Always stream using ThruCast

13.6 Using ThruCast

The user can see the cameras that have ThruCast capability from the camera toolbar – settings.

For those cameras that have ThruCast the setting is available.



For cameras that do not have ThruCast, the lower part of the dialogue is disabled.

The setting is memorized for each camera separately.



When ThruCast is active, there is a small arrow displayed on top of the camera in the device tree.

14 FAILOVER SERVERS

! If you need to failover also the VCA channels, the failover server must contain the correct amount of the activated VCA channels.

Mirasys VMS supports failover video servers as a Mirasys VMS option.
Failover servers are VMS Servers on a passive standby until the system recognizes that one of the active video recording VMS Servers has broken down; at this point, a failover server takes the place of the broken server.
The failed server can be repaired and replaced as a new failover server, while the failover server that took its place can continue operating as an active server.
***Note**: When a failover server takes the place of an active server, any Spotter plugins (such as Grafana or List Management Application) that are not built-in are not included in the switch and must be re-installed manually after a server restore.*

Recording and failover servers should be of a similar hardware setup and share drive letter assignments and version numbers.

14.1 FAILOVER FUNCTIONALITY

When adding a new server into the system, the administrator can select whether the added server is a standard server or failover server.
There can be any number of failover servers (0-n).
If the server is the standard server, the administrator can choose if that particular server will be added to the failover monitoring, i.e., in case of server failure (hardware or software), this server will migrate to the available failover server.
It is important to note that the Main server needs to be installed on hardware separate from those operating with recording licenses or failover licenses.
The minimum hardware setup consists of three servers: one Main Server, one video recording VMS Server, and one standby failover server.

14.1.1 Failover migration will be triggered in the following conditions:

- The Main Server has lost the connection to a VMS Server, and the timeout set by the administrator has been reached
- A VMS Server has informed the Main Server that connection to all the material disks (recording storage) on the server has failed
    - Manual data recovery from server hard drives can be attempted if the disks are still functional
- A server's Watchdog service has informed the Main Server that it cannot initialize the recording service

A recording is continuous after the failover server has taken over to keep the system operational.
The only exception is the timeout time between disconnect and failover trigger. The administrator configures this.
After a failover server has assumed the recording role of a failed server, a system backup will automatically be created to set a new baseline.

14.1.1.1 During the failover restore process and the following system backup:

- Users cannot perform manual backup operations
- Any following broken servers are added to a failover queue

The failover queue is handled after the failover restore has been completed.

14.2 Failover summary since V9.5.0

In V9.5.0 VMS, failover functionality was renewed to work quicker than before. It can be triggered manually. In the same version, failback functionality and material copying from failover server to recorder after failback was also implemented.
Failover log was also added where the user can see all occurred failovers and how those are processing, and the user can also trigger failback and material copying manually.

14.3 Description

Failover in V9.5.0 was changed not to use system backup files. Instead, SMServer will store recorder settings with schedules and motion masks to recorder settings cache and uses these settings when doing the failover.
Recorder settings, schedules and masks are requested from the recorder when SMServer makes connection to the recorder.
As a part of the making failover quicker, recorder startup was also optimized to start as quickly as possible.

There are now also smaller network disconnection detection times added. In earlier version the smallest time was 1min, but now there are options for 10s, 20s, 30s, 40s and 50s.

14.4 Recorder settings cache

- Recorder settings are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderSettingsStore"
- Recorder masks are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderMasksStore"
- Recorder schedules are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderSchedulesStore"

14.5 Failover process

1. When failover is started (triggered manually by user, by network connection lost or by critical recorder failure), SMServer will do following operation
2. Check if there is failover server available that belongs to same failover group as failed recorder and there is connection to the failover server
3. Creates failover log entry about the failover
4. Get settings, masks and schedules of the failed recorder from recorder settings cache

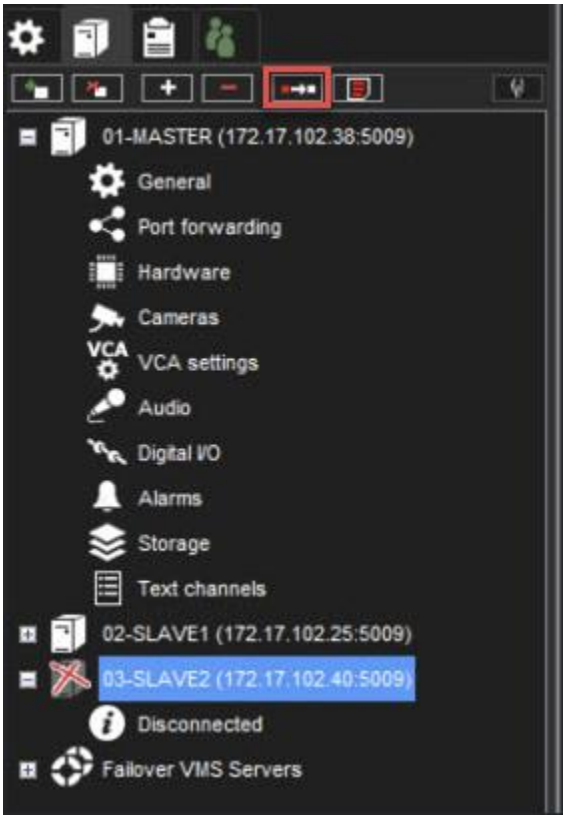
5. Saves failed recorder settings to failover server
6. Makes changes to system data that failover server has taken the tasks of the failed server
7. Makes changes to the system data that failover server is now acting as normal recorder and failed recorder is in broken state
8. Sets failover progress result to failover log
9. Sends system change notification to clients

14.6 MANUAL FAILOVER TRIGGERING

User can trigger manual failover from System Manager UI in recorder settings tab. Manual failover is possible, if

- there is connection to a failover server that belongs to same failover group as the selected recorder
- selected recorder has failover enabled
- User has role that allows to trigger failover manually

1. Select the broken VMS server from the list
2. Click **Start failover from selected VMS server to the failover server**



14.7 MINIMUM REQUIREMENTS

- **Main server installed on separate PC**
    - The license must contain an automatic backup feature
    - The license must contain one or more failover server
- **1 subserver for recording**
- **1 standby failover server**
- The license must contain at least the same amount of video channels as recording subserver
- Same size material HDD and assigned drive letters

14.7.1 IP camera drivers

Please make sure that failover servers contains the same version drivers, which normal recording servers has

14.8 VMS SERVER ROLES

14.8.1 VMS Server role FAILOVER

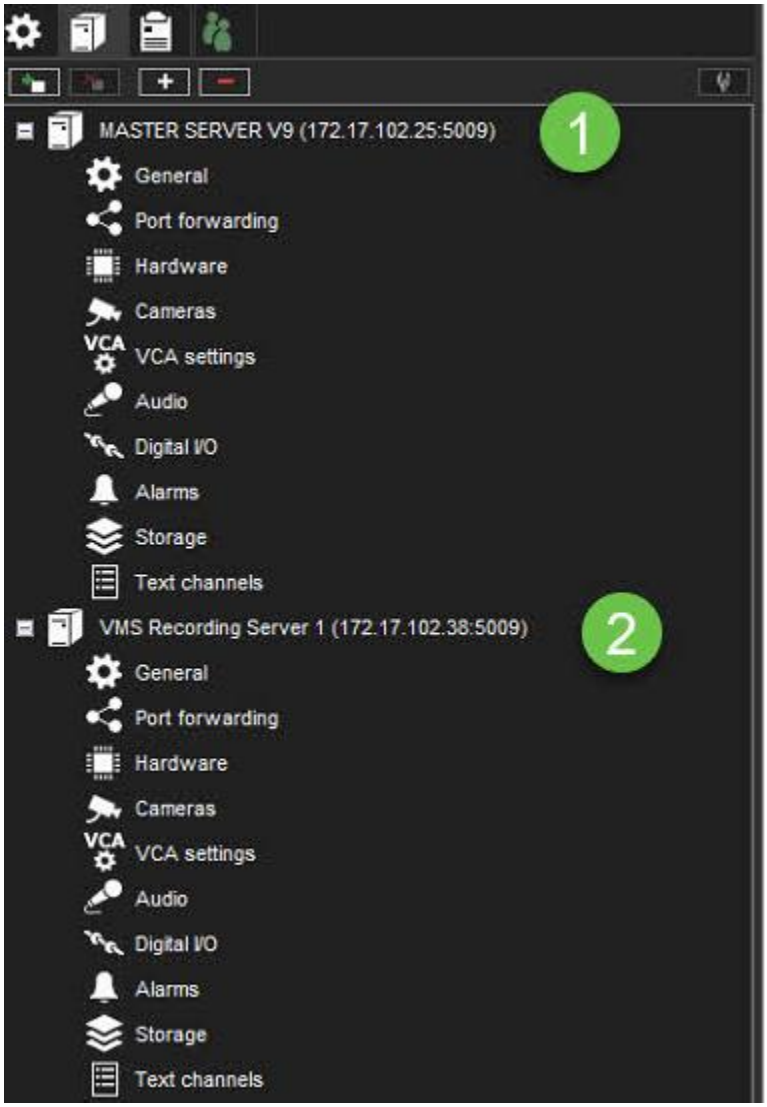
To set a server as a failover server, there has to be a free failover license slot available.
When a server is added as a failover server, the System Manager sets the server to standby mode.
The Failover VMS Servers group shows server connection states and server general settings if the connection is available.

14.8.2 VMS Server role BROKEN

The Broken VMS Servers group displays connection states; the settings on broken servers cannot be changed.
Users can, however, export server logs if there is a connection to a broken server.
To get a broken server that has been replaced by a failover server back into the system, it must first be removed manually and then added again as a new server.

14.9 STARTING POINT

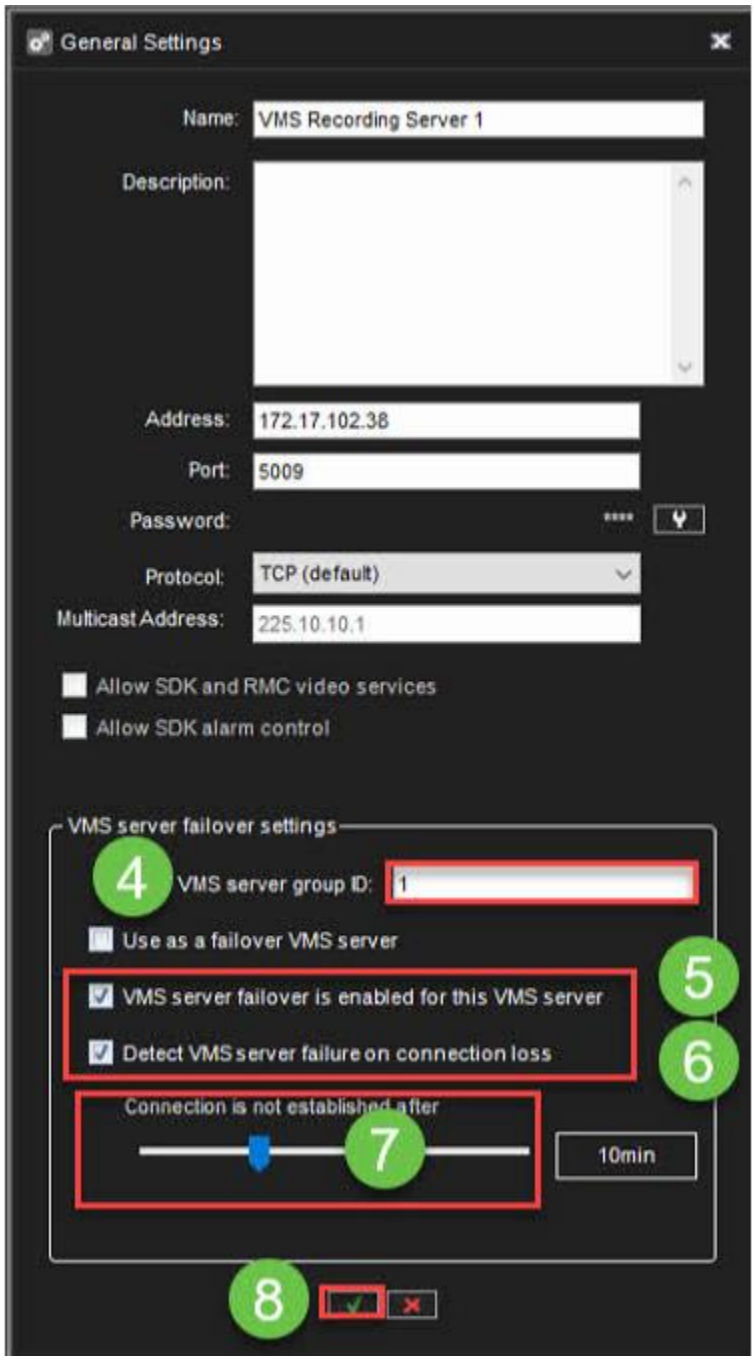
The main server and 1 recording subserver were added to the system



14.9.1 Enabling VMS failover server to the recording server

1. Open the **VMS Servers** tab
2. Select subserver from the list
3. Click **General**
4. Define **VMS server group ID(default 1)**
5. Enable **VMS server failover is enabled for this VMS server**
6. Enable **Detect VMS server failure on connection loss**
7. Define value **Connection is not established an after**

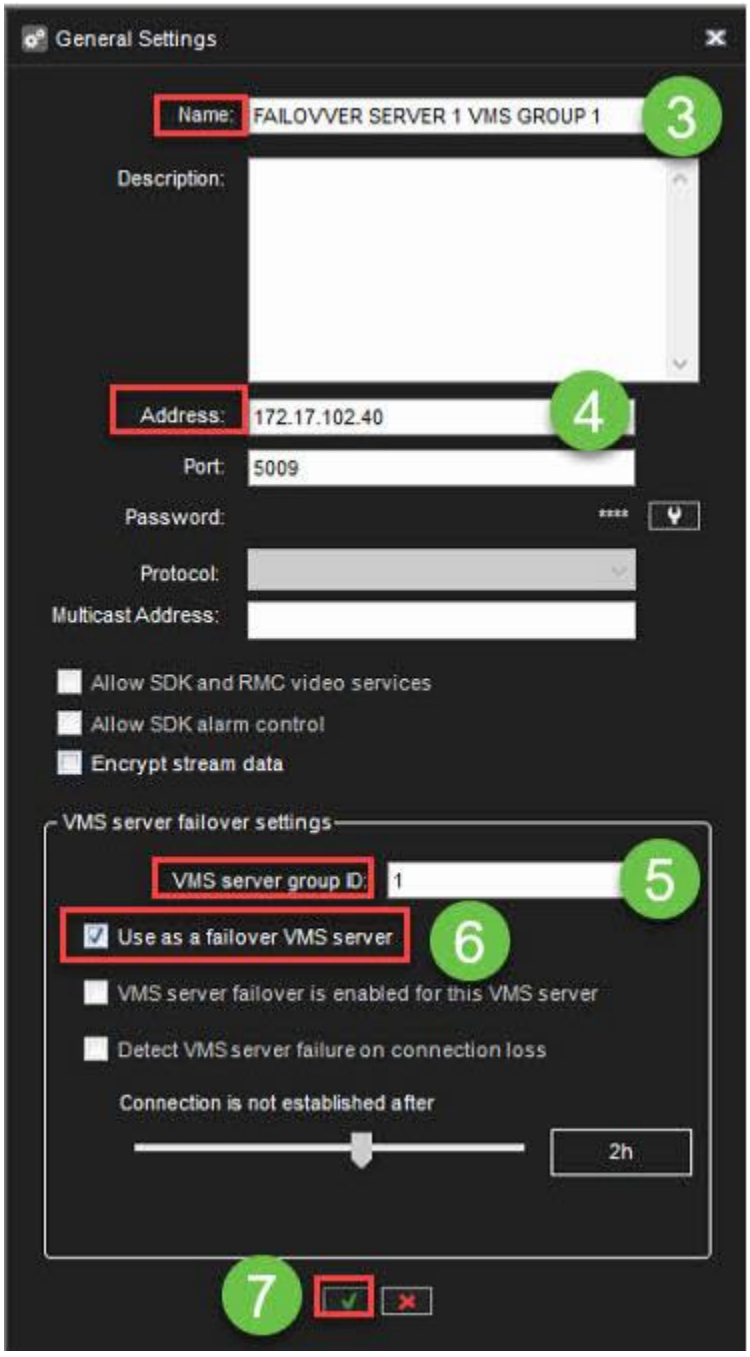
8. Click **OK**



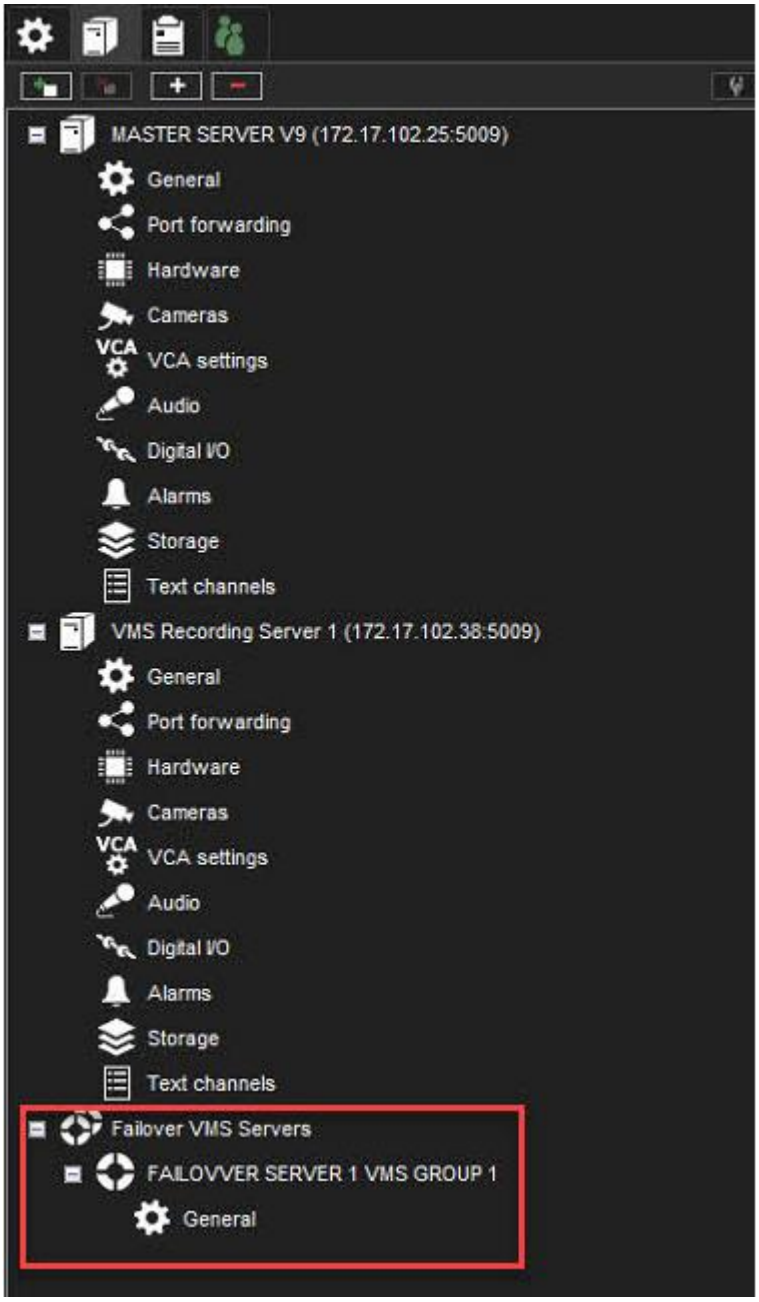
14.9.2 Adding FAILOVER server

1. Open the **VMS Servers** tab

2. Click **Add VMS server**
3. Set the name for the server
4. Set IP address of the server
5. Define the **VMS server group ID**
6. Enable **Use as a failover VMS server**
7. Click **OK**



After the adding, the VMS Server tab shows **Failover VMS Server** line



15 FAILBACK

Supported from V9.5.0

In V9.5.0 failback can be done either automatically or manually and there is no need to use settings backup to revert the failover.

The Failback uses same functionality as failover, but in reverse order by moving server functionality from failover server back to failed server. Manual failback can be triggered from failover log.
Automatic failback will trigger failback when automatic failback is enabled and connection to failed server is restored successfully.

15.1 FAILBACK PROCESS

When failback is triggered (manually or automatically):

1. Check that there is valid failover log entry and the failover state in the log is correct
2. Check that failover server is still acting as normal recorder
3. Check that failed server is still in broken state
4. Check that failover is enabled in the license
5. Check that there is no ongoing failback process running for the failed recorder
6. Update the failover log that failback is started
7. Get failover server recorder settings, configuration files, masks and schedules from recorder settings cache
8. Set failed recorder settings
9. Mark failover server to act as failover server again and mark failed recorder to be in ok state
10. Update the failover log that failback has been performed
11. Send system change notification to clients

15.1.1 Manual failback triggering

Failback can be triggered manually from failover log. Manual failback is possible if

- failover has performed successfully
- failback is not in progress or failback is not performed already
- user has role that allows to trigger failover manually

15.1.2 Automatic failback

Automatic failback can be enabled from server general settings when failover is enabled for the server. Automatic failback will not occur if maintenance mode is on.
Automatic failback is triggered when SMServer service connects successfully to failed server.
Failback functionality will then get all failover log entries from failover log database for the failed server where failover has been done successfully and failback process has not been done successfully and failback process is not ongoing.
If one or more log entries are found, failback process (described above) is processed.
If there are more than one failover log entry that fulfills the automatic failback requirement, newest log entry is

used for failback process.
When the failback process have been successfully done, log entry that was used for failback is updated that failback is done successfully. For other log entries, failback and material copying are marked as done successfully.

15.2 MATERIAL COPYING FROM FAILOVER PERIOD

Material copy is done from failover server to main server, this task is added to server's processing using DVRFailoverService.

DVRFailoverService has those methods:

- **StartDataCopy** - add new material copy task to server processing queue
- **UpdateClientInfo** - update client information for server in case of connection between server and SMServer was lost to communicate with failover server correctly
- **UpdateFailoverTaskState**s - update material copy state in case of connection between server and SMServer was lost
- Server saves material copy task to database and process those tasks one by one. If some task will be failed, server save last task times and state and continue with other tasks.

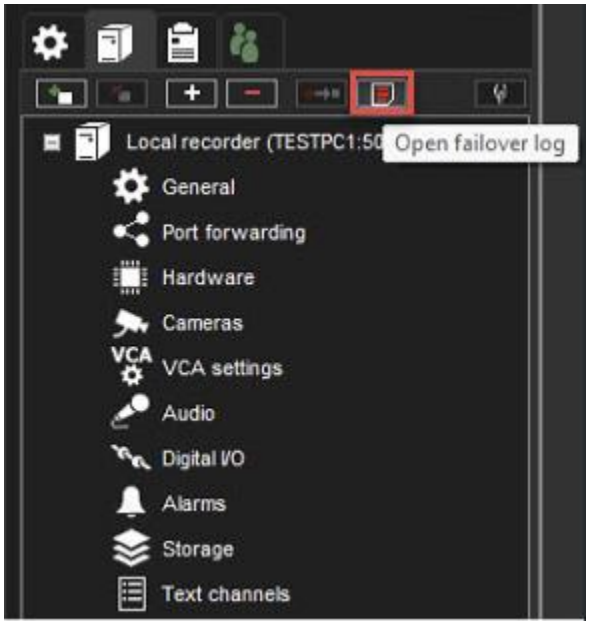
What is copied during material copy for a specified time period (start of failover operation and end of failback operation):

- Audio data for all configured audio channels
- Video data for all configured video channels
- Text data for all configured text channels
- Metadata for all configured video and text data channels
- ANPR data for all configured video channels
- Alarms for all configured alarm id's
- Server process each channel listed above one by one and save last received channel time. If connection between servers will be broken or some error will happen, recorder saves last state of material copy task and continue from last unprocessed channel (and last processed channel time).

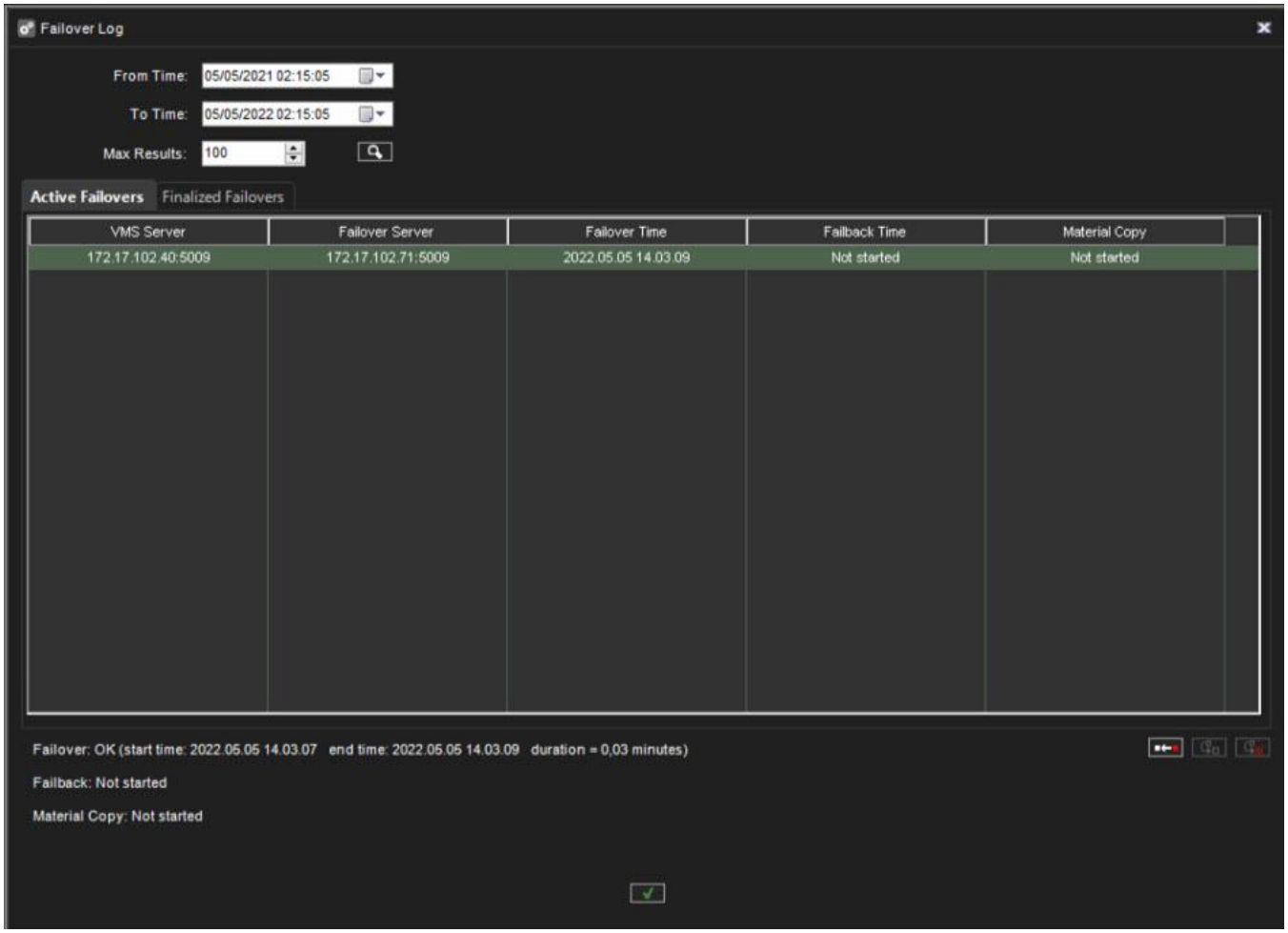
Server use playback functionality for audio, video, text and metadata and ANPR and Alarms search services to get required data for specified time period.
Also, due to Geniune channels security limitations we can't use server as ZpaServer and ZpaClient at the same time, so calllbacks are not working in communication server to server.
So, ANPR and Alarms search services now have additional methods to get required data without using callbacks.

15.3 FAILOVER LOG

1. Click **Open failover log** from the **VMS servers tab**



2. The **Failover log** shows **Active Failovers** and **Finalized Failovers**

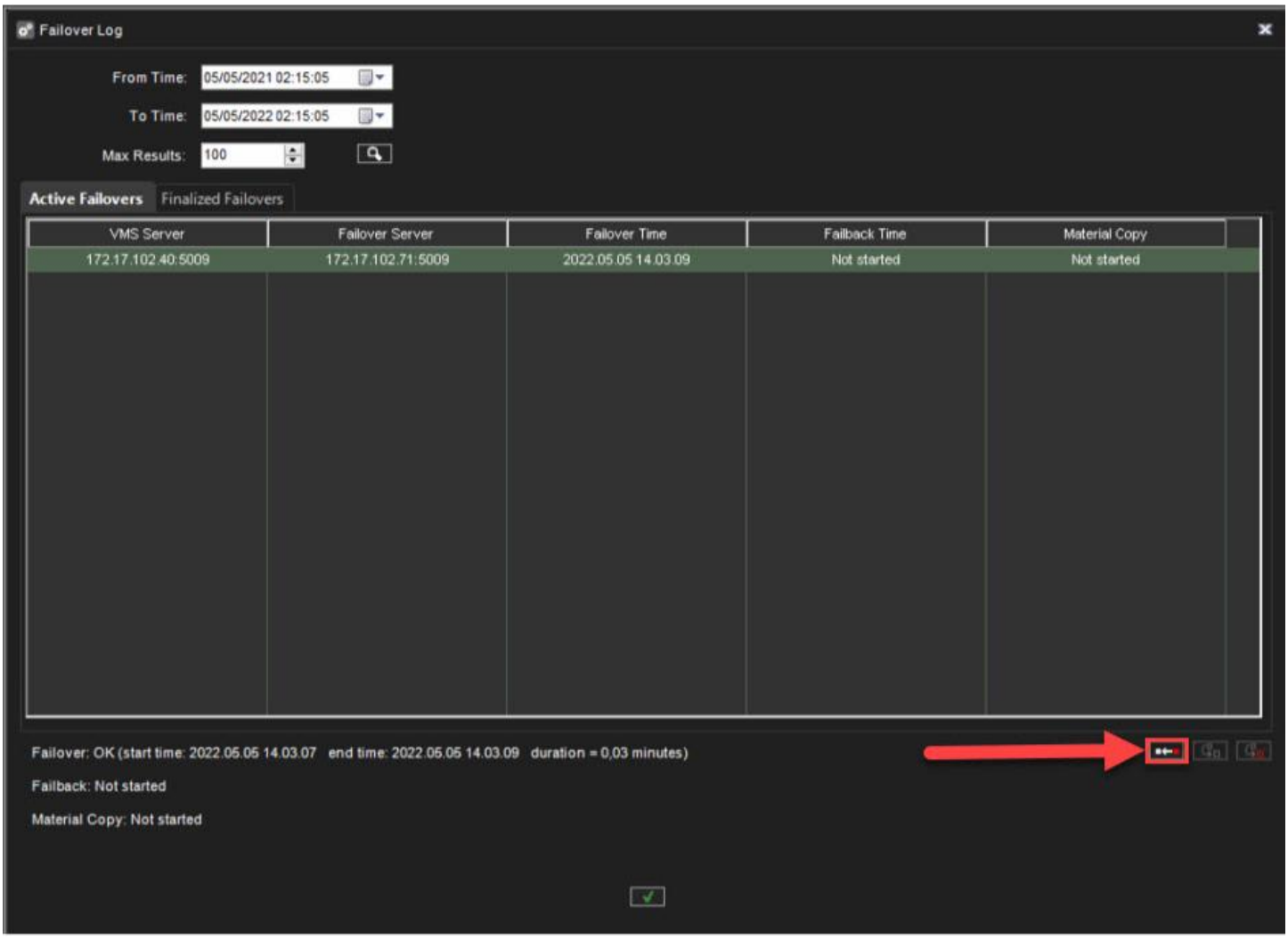


15.3.1 Start Failback for the selected server

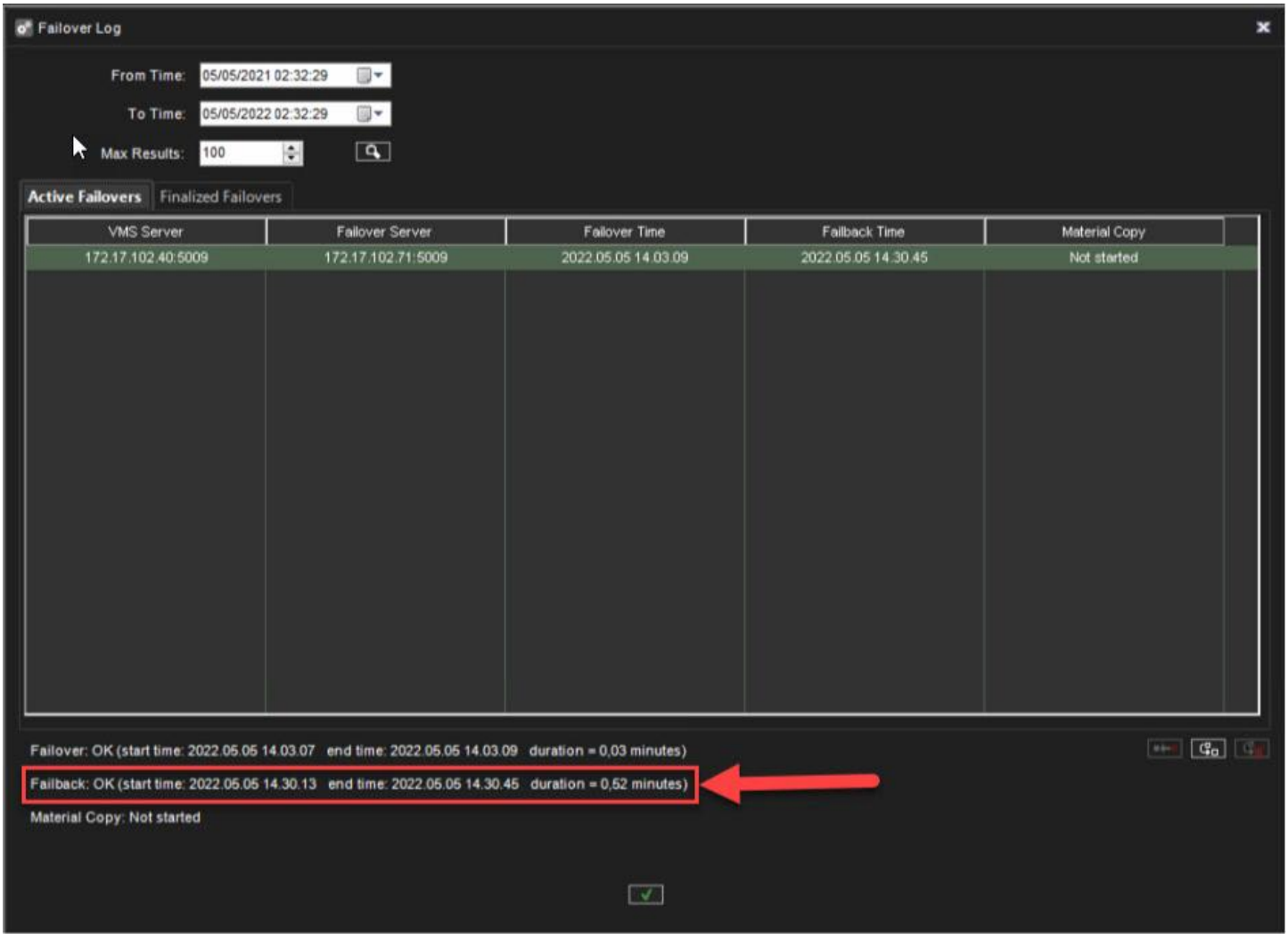
3. Set fixed VMS server to the network with the same IP address

4. Select the server from the list

5. Click **Start failback to the selected server**

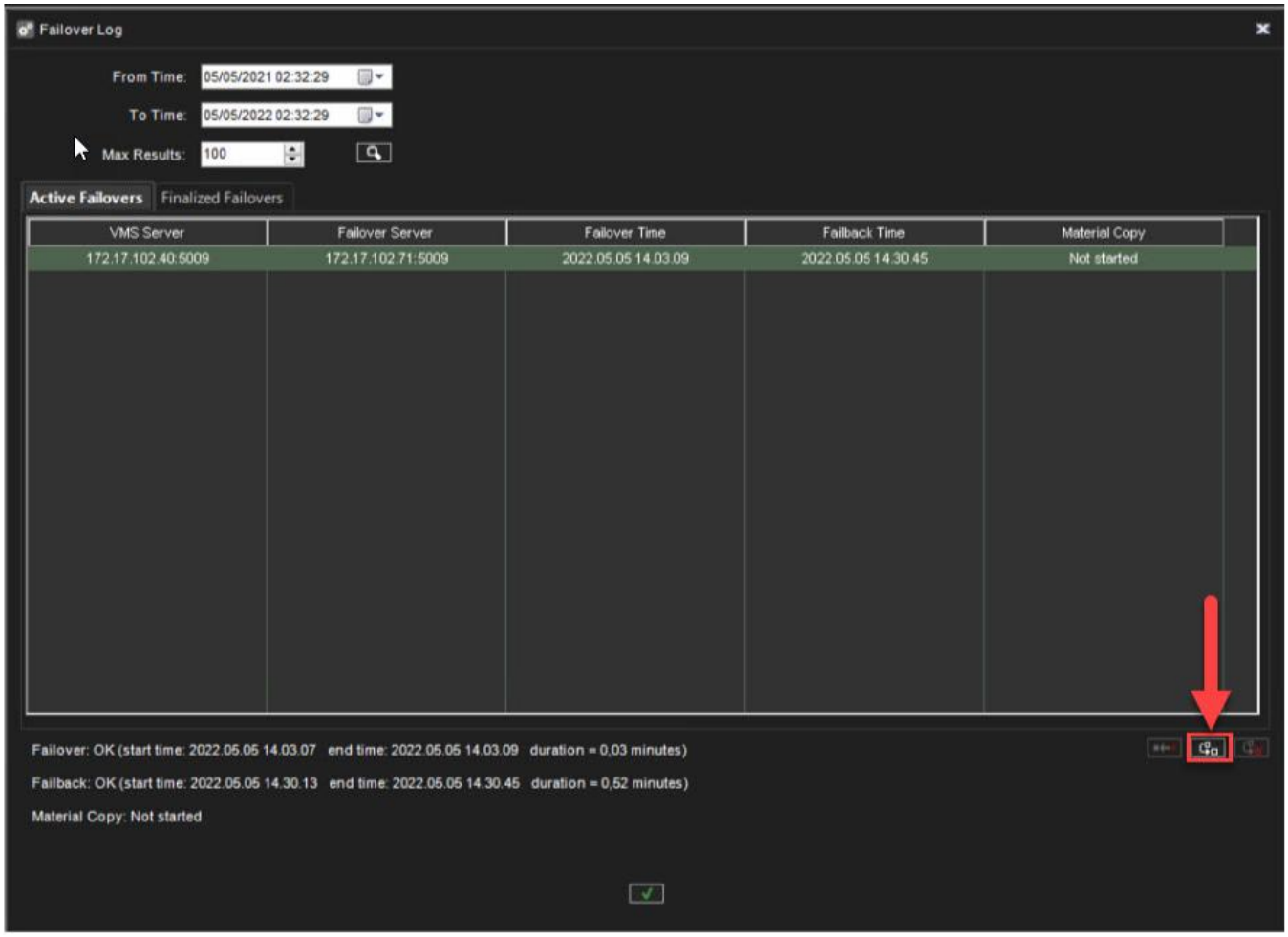


When the failback is successfully done, Failback OK message with the **start time**, **end time** and **duration** is shown



15.3.2 Start material copying to the selected server

1. Select the server from the list
2. Select the first material copy, which has not been finalized from the list
3. Click **Start material copying to the selected server**



15.4 Material copy time after failback – Test results

This page contains information about the VMS server failover material copying test. The test was performed to measure the time it takes to copy the stored data after a failback from the failover server to the VMS server. The test results provide a framework for estimating how much time the material copying takes after a failback.

15.4.1 Test setup

The following VMS servers were used when performing the tests:

- Main VMS server - Real Windows 11 machine with 64 GB RAM
- Failed VMS server - Virtual machine with Windows 11 and 24 GB RAM
- Failover VMS server - Virtual machine with Windows 11 and 24 GB RAM

The failed VMS server used camera emulators to keep the stored data similar in each test scenario. Servers used the dedicated disk (the drive D:\) for the storage, and the disk was cleared before running each test scenario. Used servers were connected to a 1GB network.

15.4.2 Test results

The material copying duration was captured from the VMS server logs (C://Program Files/DVMS/DVR/Logs/DVRl.og.txt).

The following table contains information about the material copying test results containing the following information:

- Duration of failover
- Number of cameras used
- Material size that was copied back to the failed server
- Time in minutes taken for a material copy from failover server to VMS server

Failover Duration	Material Copy									
	1 Camera		5 Cameras		10 Cameras		15 Cameras		20 Cameras	
	GB	Minutes	GB	Minutes	GB	Minutes	GB	Minutes	GB	Minutes
1 Hour	1,4	6	7	13	14	20	22	33	29	40
5 Hours	7	13	35	65	70	130	105	185	140	250
10 Hours	14	26	70	130	140	260	210	390	280	500
15 Hours	22	39	105	195	210	390	315	575	420	750