

Administrator Guide V9 - EN



Table of Contents

1. Mirasys VMS Administrator Guide V9.....	5
1.1. Overview of This Guide.....	6
1.2. Technical Support.....	7
1.3. What is the Mirasys VMS software?.....	8
1.3.1. What does a System Contain?.....	9
1.3.2. VMS Servers.....	10
1.3.3. Master Server.....	11
1.3.4. Client Programs.....	12
1.3.5. Network Requirements.....	13
1.4. OS Compatibility.....	14
1.5. Configuring the System.....	15
1.6. Logging In.....	16
1.6.1. Locking System Manager.....	19
1.7. Management User Interface.....	20
1.8. System.....	21
1.8.1. System settings.....	23
1.8.2. Backup.....	47
1.8.3. Monitoring.....	54
1.8.4. Licenses.....	61
1.8.5. Watchdog.....	68
1.8.6. Add-ins.....	72
1.9. VMS Servers.....	79
1.9.1. General.....	81
1.9.2. Port Forwarding.....	85
1.9.3. Hardware.....	90
1.9.4. Adding and Removing VMS Servers.....	110
1.9.5. Cameras.....	113
1.9.6. VCA settings.....	140



Administrator Guide V9 - EN

1.9.7. Audio.....	141
1.9.8. Digital I/O.....	151
1.9.9. Alarms.....	170
1.9.10. Storage.....	184
1.9.11. Text Channels.....	192
1.10. Profiles.....	195
1.10.1. Creating a customer-specific profile.....	197
1.11. Users.....	207
1.11.1. User group.....	209
1.11.2. Creating a customer-specific user.....	243
1.11.3. User account settings.....	244
1.11.4. Disabling or Activating a User Account.....	245
1.12. TruCast.....	246
1.12.1. Supported Cameras.....	248
1.12.2. Network Optimization.....	249
1.12.3. Multistreaming and TruCast for Network Optimization and Storage.....	252
1.12.4. Using TruCast.....	255
1.13. Failover Servers.....	257
1.13.1. Minimum requirements.....	259
1.13.2. FAILOVER trigger conditions.....	260
1.13.3. FAILOVER process.....	261
1.13.4. FAILOVER MINIMUM SCENARIO.....	262
1.13.5. FAILOVER SCENARIO 2.....	263
1.13.6. FAILOVER SCENARIO 3.....	264
1.13.7. VMS Server roles.....	265
1.13.8. Building Failover system.....	266
1.13.9. Restoring the fixed server to the system.....	270
1.14. Easy LPR.....	271
1.14.1. Configuration process.....	272

Administrator Guide V9 - EN

1.14.2. Licensing.....273
1.14.3. Enabling Easy LPR..... 274
1.14.4. Creating an alarm from Easy LPR event..... 276

MIRASYS
DEEP VISION DATA COMPANY



Administrator Guide V9 - EN

1. Mirasys VMS Administrator Guide V9



Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

-

info@mirasys.com

-

www.mirasys.com

1.1. 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.

1.2. Technical Support

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

1.3. 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.

1.3.1. What does a System Contain?

The Mirasys system consists of these components:

- 1-150 VMS Servers
 - **Master 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
 - Mirasys Spotter Mobile

1.3.2. VMS Servers

The VMS servers record video and audio from multiple cameras and audio channels and write the data to a storage device.

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.

A server is a computer with storage, the Windows operating system, and the installed VMS software with required drivers.

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)

1.3.3. Master Server

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

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

All other VMS Servers connect to it, and all client applications communicate through the Master Server.

If the system contains only one server, then that server is the Master Server.

If there is more than one server, the Master Server can be set freely.

It is recommended that the Master Server is a dedicated server for this purpose alone in a more extensive system.

NOTE: Master Servers must have *SQL Server Express 2014* or other *Microsoft SQL Server 2014* installed.

The Master Server does these things:

- 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.

1.3.4. 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

1.3.5. Network Requirements

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

1.4. OS Compatibility

Mirasys VMS V9 supports the following operating systems:

Operating System	Server with analogue camera support via capture cards	Server with only IP cameras or connected video servers (encoders)	Gateway server	System Manager application	Spotter application
Windows 10	-	X	X	X	X
Windows 11	-	X	X	X	X
Windows Server 2016	-	X	X	X	X
Windows Server 2019	-	X	X	X	X

NOTES:

Make sure that the “Desktop Experience” feature is activated for Windows server operating systems.

1.5. 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.

Note: *Install the client programs on each computer used to access the system over a network.*

A separate "Spotter only" installer is provided.

Note: *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.

1.6. Logging In

This section describes how to log in and log off from System Manager.

Only system administrators or users with monitoring rights are allowed to log in to System Manager.

Default username and password

Username: Admin

Password: 0308

The default username and password should not be used even in closed networks.

Please ensure that the default username and password are not in use after the system has been installed.

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 Master Server address configured, the System Manager login screen is shown.

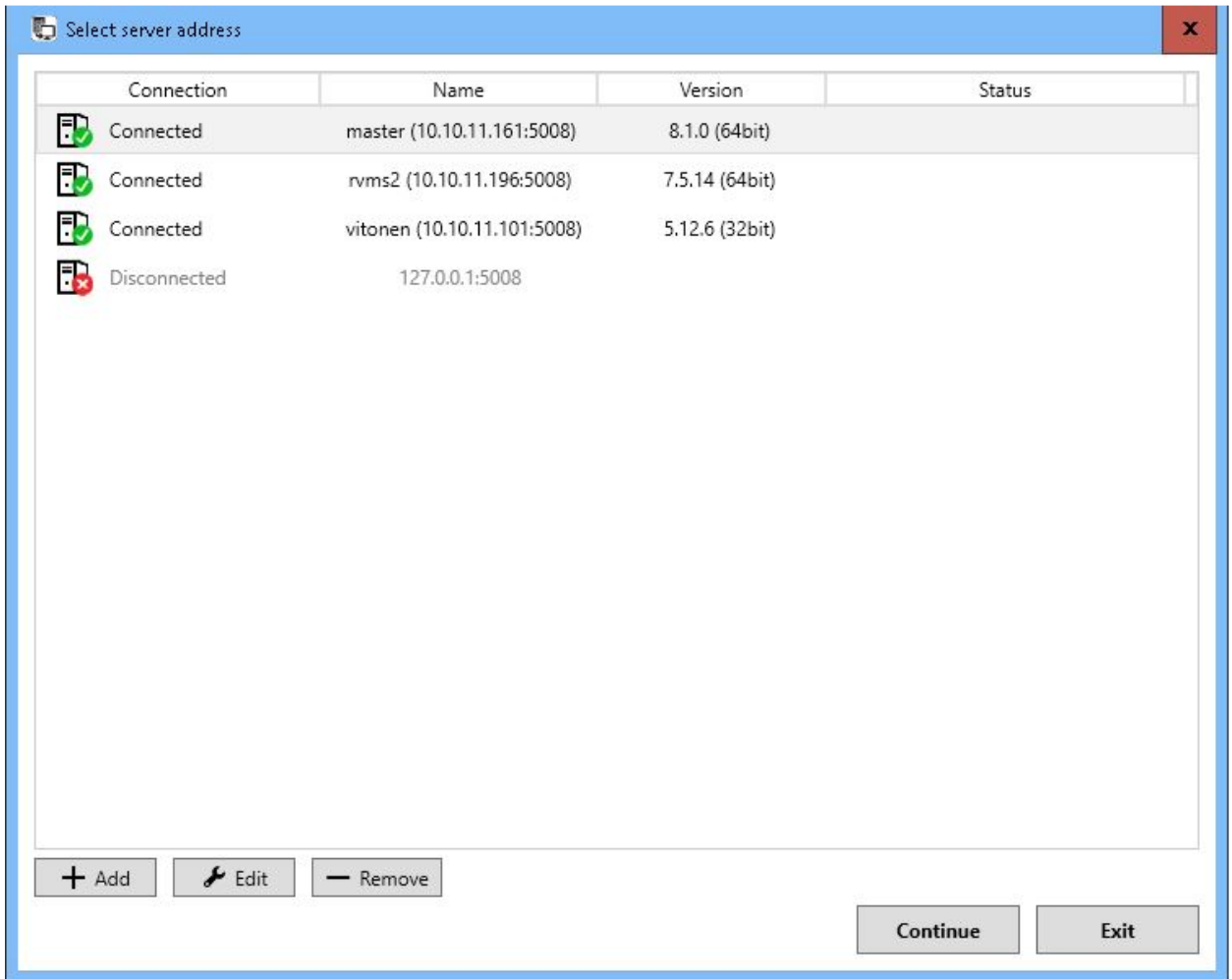
In systems with multiple masters, addresses configured, or if the user presses the "Delete" key in the initial startup phase, the site selection screen is shown.

The user can add, remove or edit Master Server addresses, or choose a server to log on on this screen.

After selecting a server and pressing the "Continue" button, a user is taken to the login screen.



Administrator Guide V9 - EN



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



Administrator Guide V9 - EN



Note: *The username and password are case sensitive.*

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

After the program starts, the user interface is shown. To **log off** or to **change 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.

Note: 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 Master Server, exit from the current Master and choose another Master Server from the site selection screen.

1.6.1. 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.

Note: *The password is case sensitive.*

1.7. Management User Interface

The System Manager User interface

The System Manager User Interface contains these elements:

Menu bar.

- File
- Log Off
- Lock Program
- Import
- Export

Maintenance

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

Help

About

to see information about the program version.

and then **Help Topics** to use the online guide.



Administrator Guide V9 - EN

1.8. 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

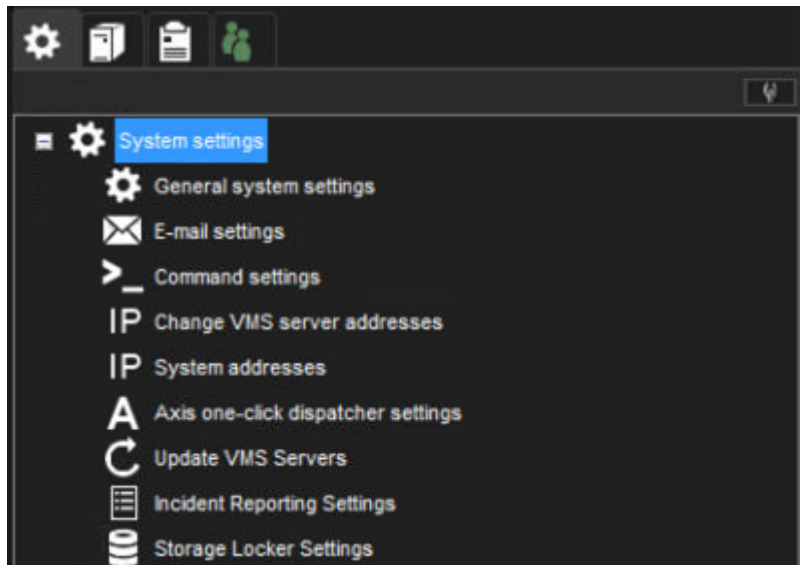
Administrator Guide V9 - EN

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



1.8.1. System settings

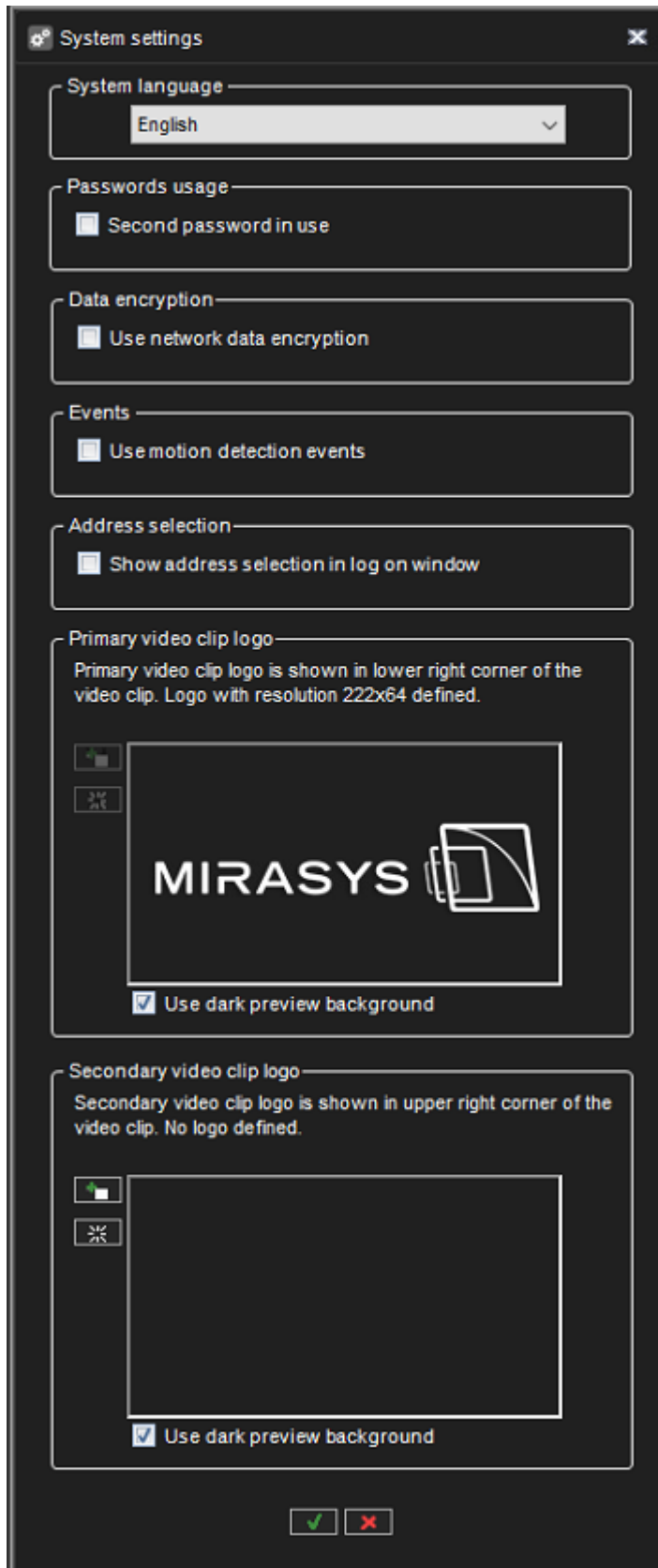


Administrator Guide V9 - EN

1.8.1.1. General System Settings



Administrator Guide V9 - EN



In this section, you can control:

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

-

info@mirasys.com

-

www.mirasys.com

Administrator Guide V9 - EN

- System language
- The password usage

It is possible to configure the system to require two separate passwords from all users.

This is done by activating the “Second password in use” option in 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 that no single person can review videos alone.

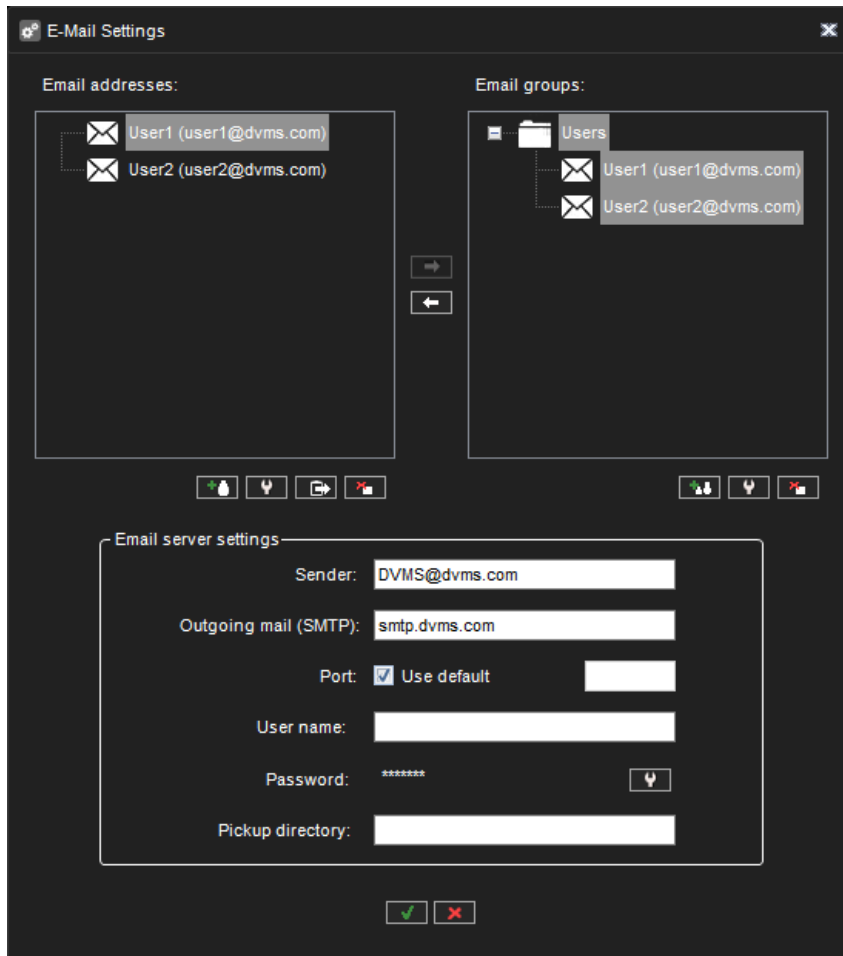
If one password is known to one person and the other password is known to another person, both persons must be present when reviewing videos.

- Data encryption
- Events(the setting for sending motion information to clients)
- 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)



Administrator Guide V9 - EN

1.8.1.2. 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.

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.

Administrator Guide V9 - EN


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.


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**.


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**.


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

Other available actions:

Editing email names, addresses, group names and removing persons from groups is possible with the edit  buttons.

Persons can be removed from groups with the arrow 

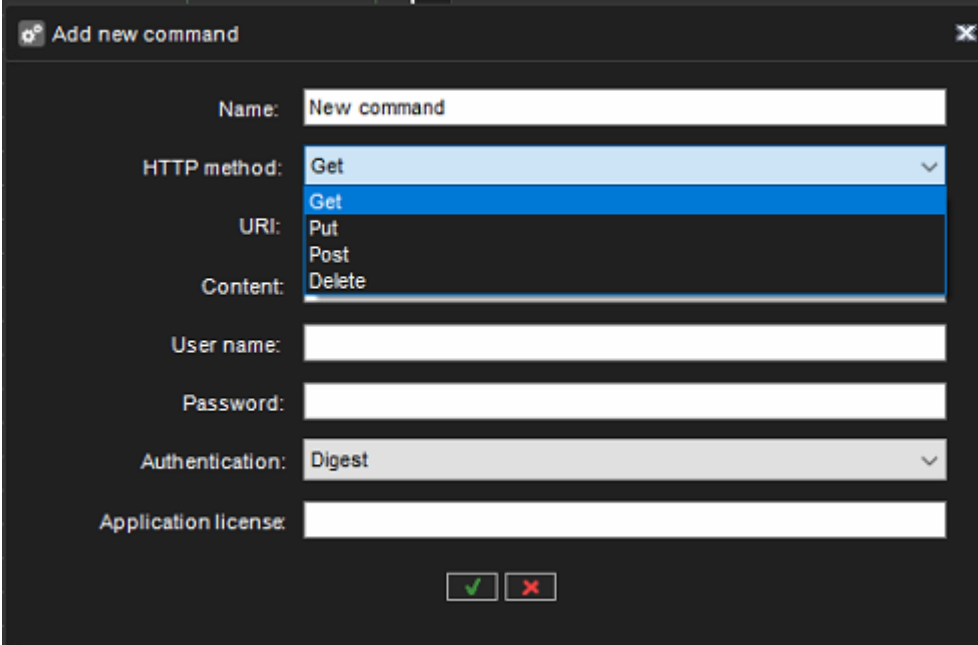
Persons and groups can be removed with the  button.

Test email can be sent with  a button to a selected email address using the settings defined in the email settings dialogue.

Administrator Guide V9 - EN

1.8.1.3. Command Settings

Command settings are used for HTTP command sending



Add new command [Close]

Name:

HTTP method: (dropdown menu open showing: Get, Put, Post, Delete)

URI:

Content:

User name:

Password:

Authentication: (dropdown menu)

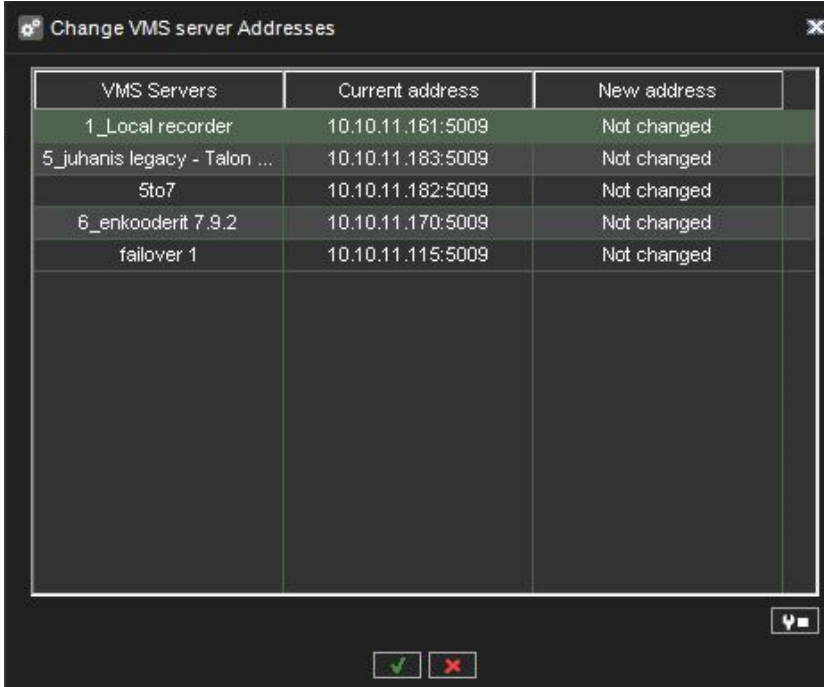
Application license:

[Checkmark] [X]

Administrator Guide V9 - EN


1.8.1.4. Change VMS Server Addresses

If the IP address or DNS name of a server changes, you can define the new address/name through the **Change VMS Server addresses** tool.



VMS Servers	Current address	New address
1_Local recorder	10.10.11.161:5009	Not changed
5_juhanis legacy - Talon ...	10.10.11.183:5009	Not changed
5to7	10.10.11.182:5009	Not changed
6_enkooderit 7.9.2	10.10.11.170:5009	Not changed
failover 1	10.10.11.115:5009	Not changed

To change a server's IP address or DNS name:

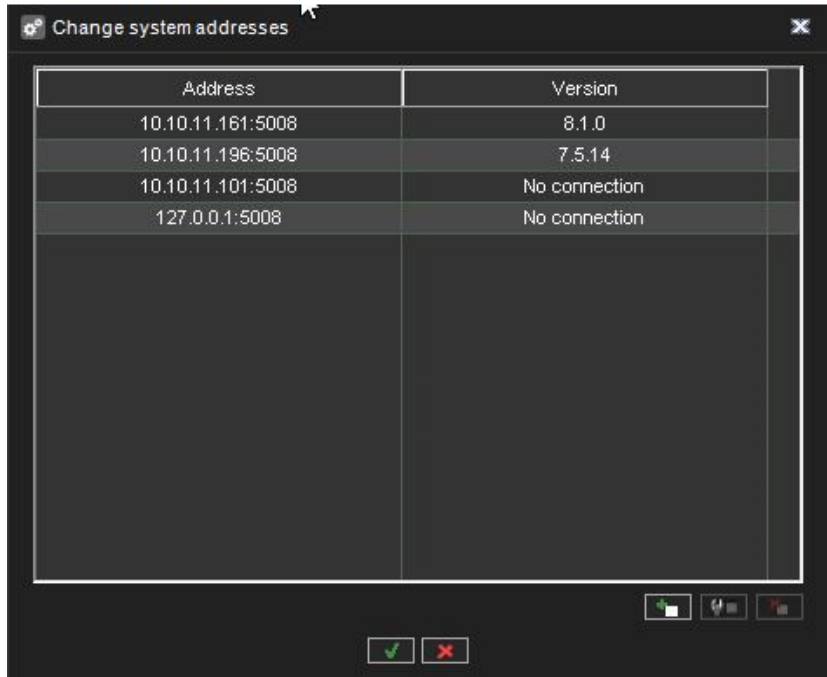
1. On the **System** tab, open **Change VMS Server addresses**.
2. Click on the name of the server with the changed IP address.
3. Click **Change VMS Server address** .
4. Type the new IP address or DNS name of the server into the **New VMS Server address** field.
5. Click **OK**.

Administrator Guide V9 - EN

1.8.1.5. System Addresses

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

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




You can define multiple Master 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 Master Server addresses provided they have a compatible username and password for the Master Server.

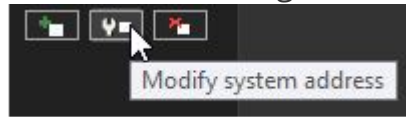
To add a Master Server address:

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**.

To edit a Master Server address:


Administrator Guide V9 - EN

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



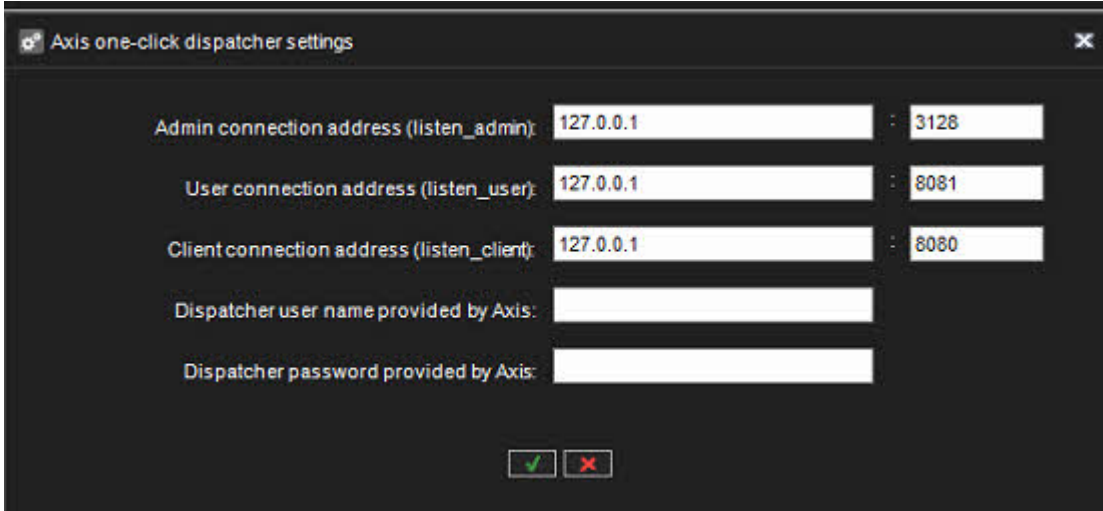
3. Click **Modify system address**.
4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

To remove a Master Server address:

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

Administrator Guide V9 - EN

1.8.1.6. Axis one-click dispatcher settings



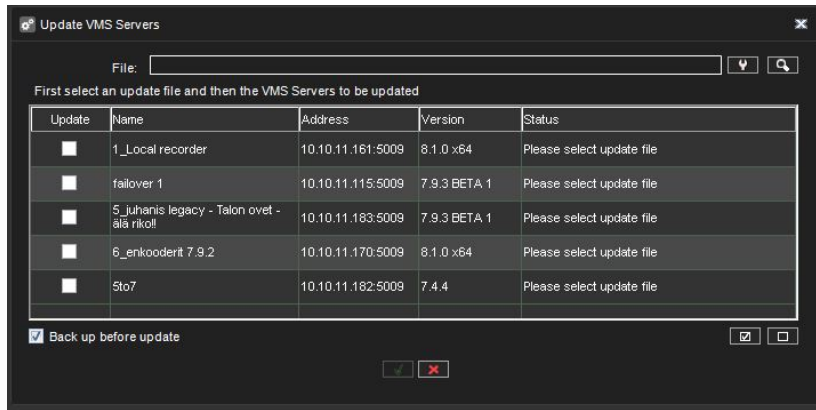
Axis one-click dispatcher settings


Admin connection address (listen_admin):	127.0.0.1	:	3128
User connection address (listen_user):	127.0.0.1	:	8081
Client connection address (listen_client):	127.0.0.1	:	8080
Dispatcher user name provided by Axis:			
Dispatcher password provided by Axis:			

Administrator Guide V9 - EN

1.8.1.7. Update VMS Servers

It is possible to update the local server and all connected VMS Servers remotely via the **Update VMS Servers** -option



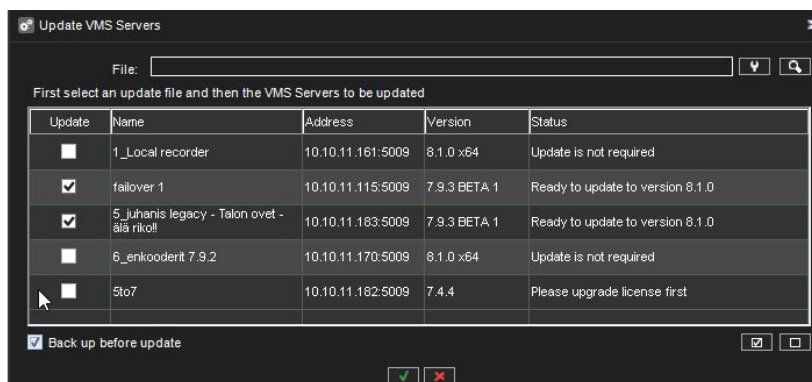
To update servers, first, select the installation file with the  button.


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.

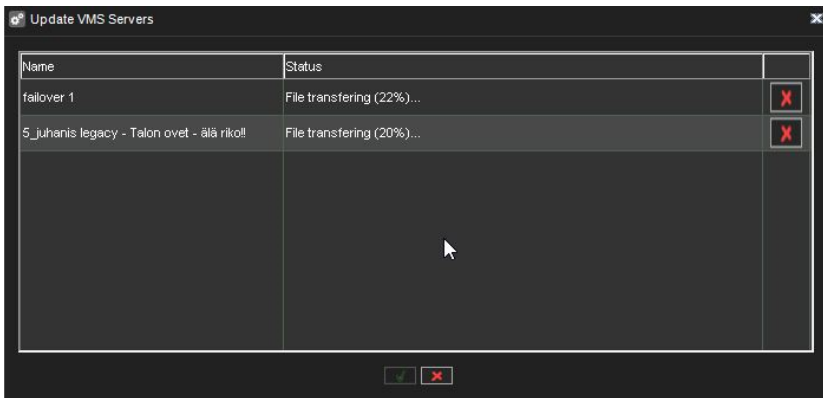
Next, choose which servers you want to update and if you want to perform a backup before updating.



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



Administrator Guide V9 - EN



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 Master 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.

Administrator Guide V9 - EN

1.8.1.8. 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.

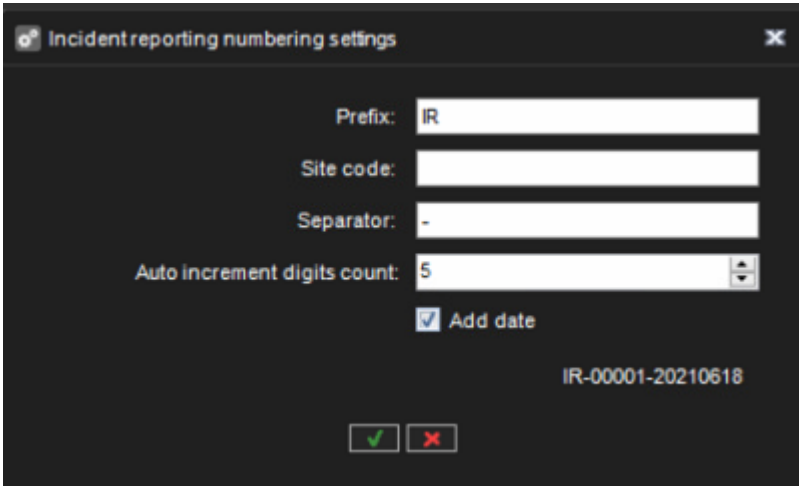
Company information

- Company name
- Company address
- Company logo

Reporting numbering

Incident Reporting numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



The screenshot shows a dialog box titled "Incident reporting numbering settings". It contains the following fields and controls:

- Prefix: IR
- Site code: (empty)
- Separator: -
- Auto increment digits count: 5 (with a spinner control)
- Add date
- Example: IR-00001-20210618
- Buttons: [✓] [✗]

Daily log numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



Administrator Guide V9 - EN

Daily log numbering settings

Prefix: DL

Site code:

Separator: -

Auto increment digits count: 5

Add date

DL-00001-20210618

OK Cancel

Fields info

- Department
- Site
- Location
- Sublocation
- Incident level
- Incident type
- Incident status
- Category



Administrator Guide V9 - EN

Incident Reporting Settings

Company information

Company name:

Company address:

Company logo:

Report numbering

Incident Reporting numbering:

Daily log numbering:

Fields info

Department:

Site:

Location:

Sublocation:

Incident level:

Incident type:

Incident status:

Category:



Administrator Guide V9 - EN

1.8.1.8.1. Add values


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

Incident Reporting settings

Company information

Company name: Mirasys Oy

Company address: Vaisalantie 2-6

Company logo: 

Report numbering

Incident reporting numbering: IR-00001-20211229

Daily log numbering: DL-00001-20211229

Fields info

Department: Tuotanto;Markkinointi;Tuotetuki;Myynti

Site: Espoo;Helsinki;Vantaa;Tukholma;Oslo

Location: Suomi;Ruotsi;Norja

Sublocation: Pitäjänmäki;Pasila;Herttoniemi

Incident level: Pieni;Suuri;Kriittinen

Incident type: Laite;Henkilöstö;Ohjelmisto;Tiedonkulku

Incident status: Uusi;Avoin;Käsittelyssä;Suljettu

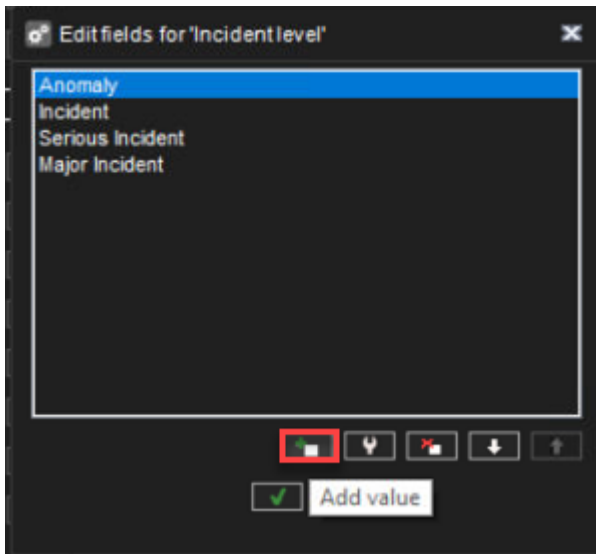
Category: Erittäin tärkeä;Tärkeä;Ei tärkeä

✓ ✗

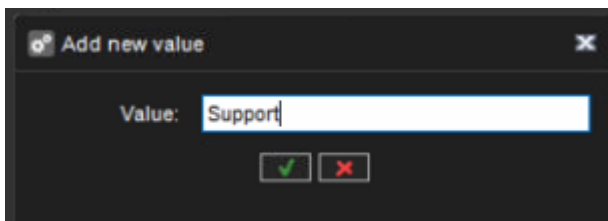
2. Click **Add value**



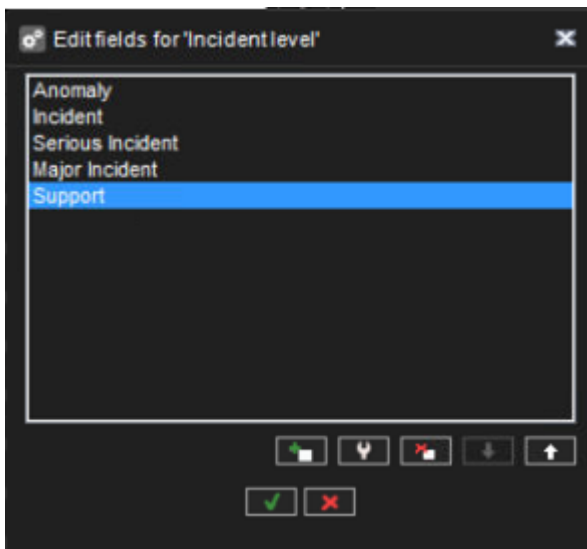
Administrator Guide V9 - EN



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



New added value can be seen in the list





Administrator Guide V9 - EN

1.8.1.8.2. Edit values

1. Click icon **Update values**

Incident Reporting settings

Company information

Company name: Mirasys Oy

Company address: Vaisalantie 2-6

Company logo: 

Report numbering

Incident reporting numbering: IR-00001-20210601

Daily log numbering: DL-00001-20210601

Fields info

Department: R&D;Finance;Production;Support

Site: Espoo;Helsinki

Location: Finland

Sublocation:

Incident level: Anomaly;Incident;Serious Incident;Major Incident

Incident type: Investigation;Communication;Administration;Documentation

Incident status: New;Open;In Progress;Closed

Category: Hardware;Person;Environment

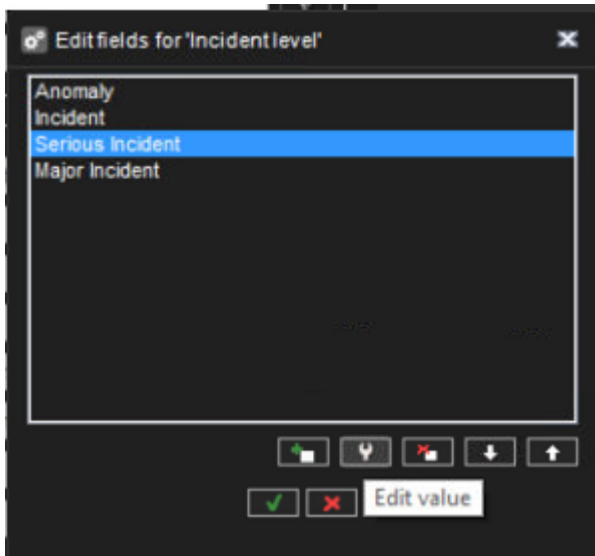
Update level values

✓ ✗

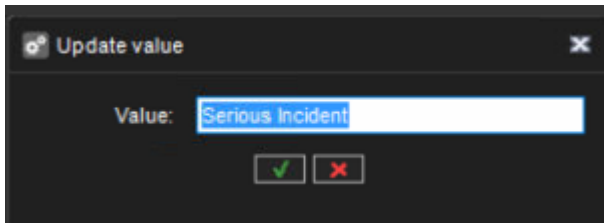
2. Select a value from the list and click **Edit value**



Administrator Guide V9 - EN



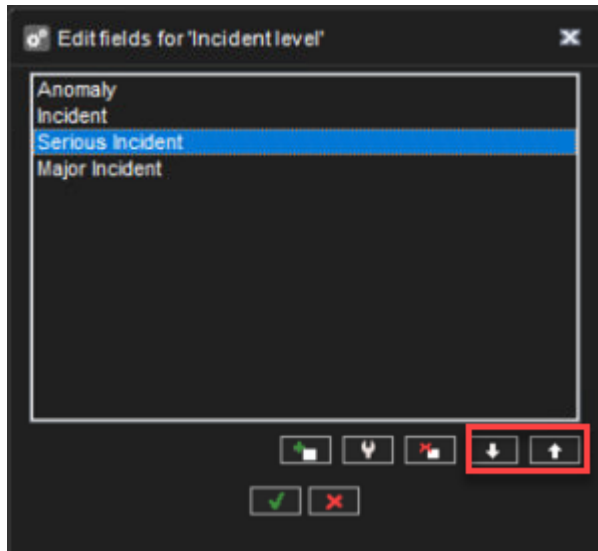
3. Enter a new value name and click **OK**

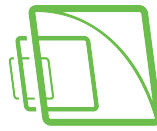


Administrator Guide V9 - EN

1.8.1.8.3. 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





Administrator Guide V9 - EN

1.8.1.9. Storage Locker Settings

Storage Locker Settings contains the following values:

File path:

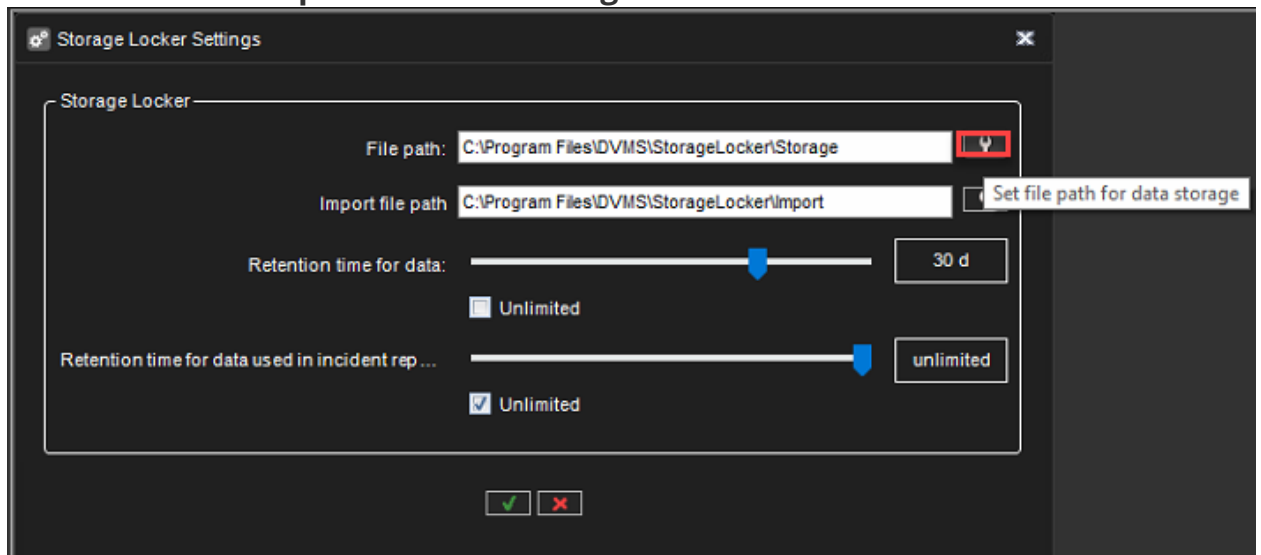
Defines the location of the Storage Locker.

As default location Storage Locker is located in the master server.

Changing the file path

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

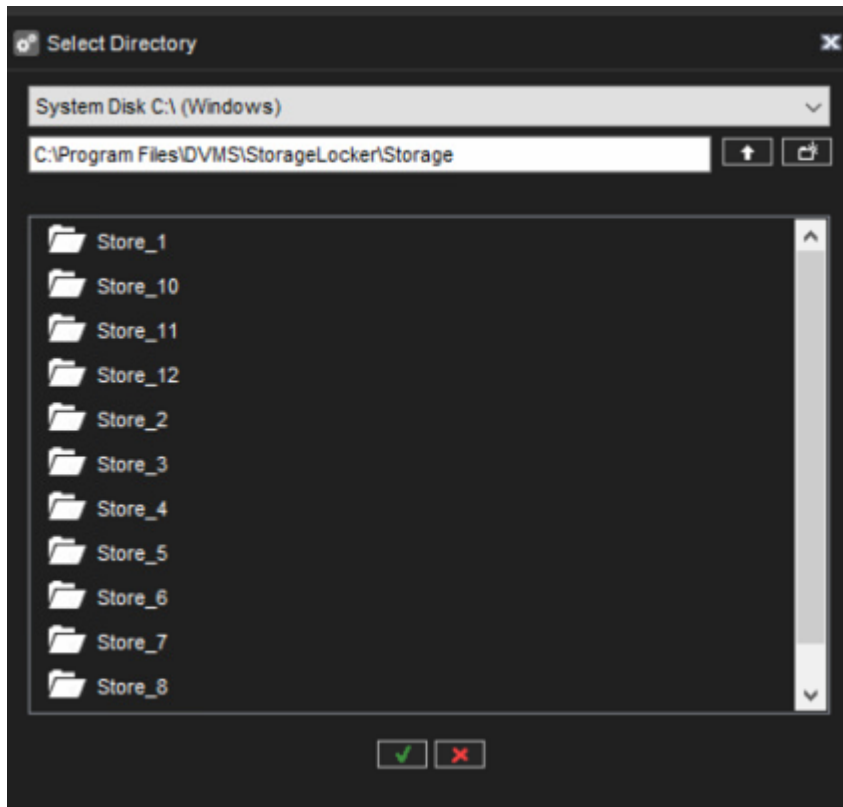
1. Click **Set file path for data storage**



2. Select a new location and click **OK**



Administrator Guide V9 - EN



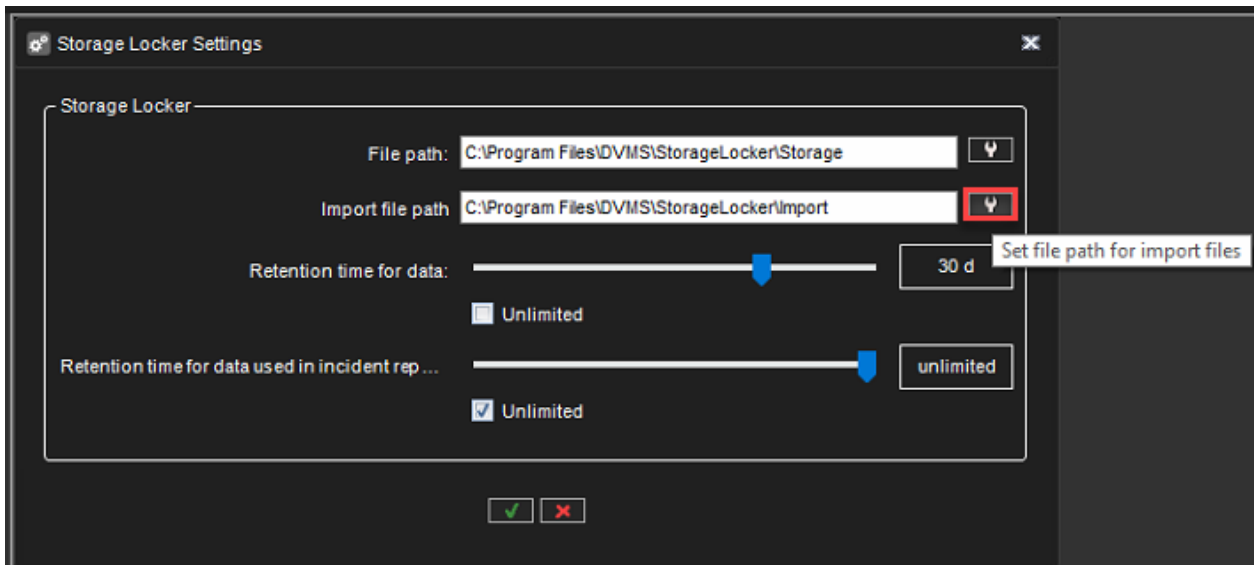
Import file path:

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 to 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 own folder, files added to existing folders is not supported (those files will not be processed)



Administrator Guide V9 - EN

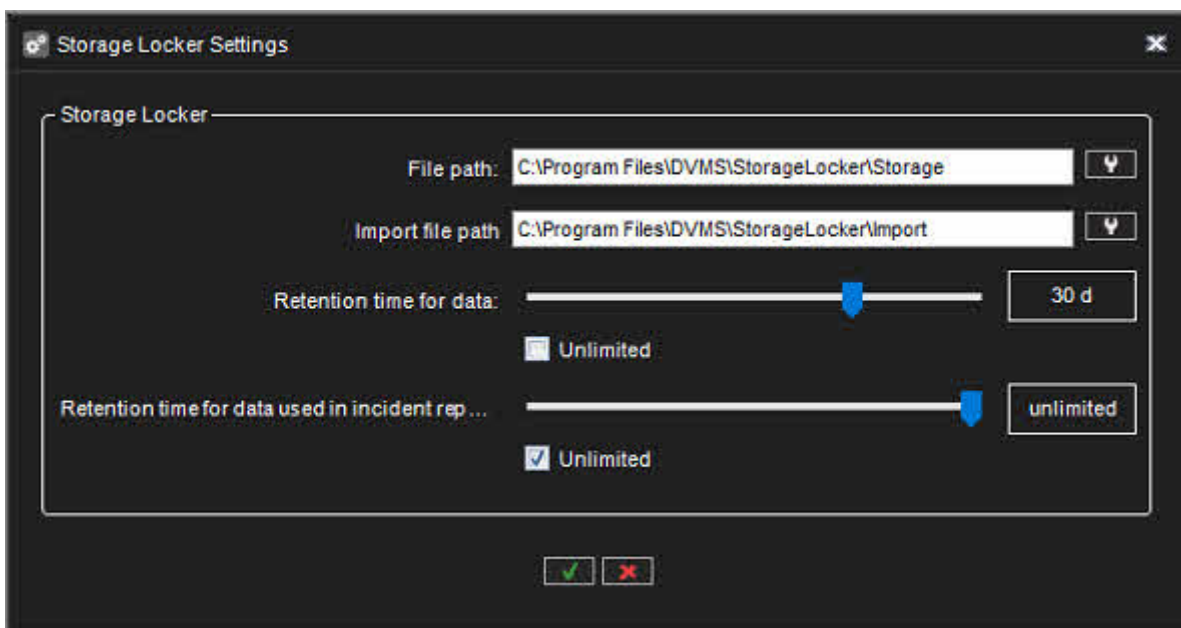


The retention time for data

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

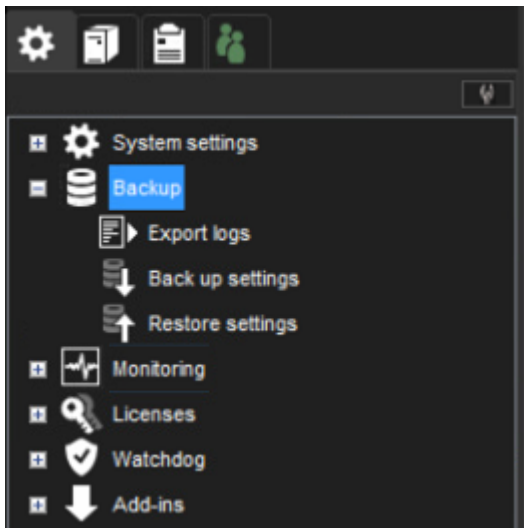
The retention time for data used in the incident reports

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





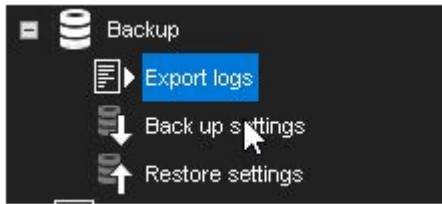
1.8.2. Backup





Administrator Guide V9 - EN

1.8.2.1. Export logs



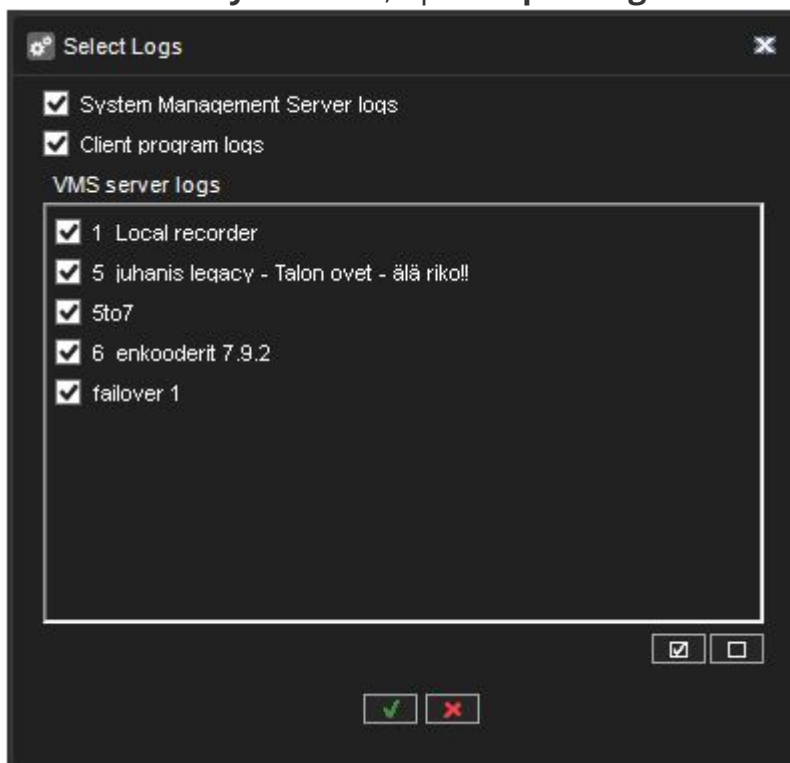
If there are problems with the system, you can export log files and send them to the system supplier.

You can save the log files to a hard disk, floppy disk, or another removable or non-removable device.

Log files are saved to a compressed (zipped) file.

To export log files:

1. On the **System** tab, open **Export logs**.



2. Select the logs to export and click **OK**.

If there are problems with a server, select that server's logs. In addition, select the System Management Server and client program logs.

- b. Note that the client logs are from the machine where you are accessing the system manager application.

Administrator Guide V9 - EN

3. Select the storage device and the folder where you want to save the log files.
To create a new folder, click the **New folder** button.
4. Type a name for the ZIP file and click **OK**. The system exports the files to a ZIP file. Send the ZIP file to the system supplier.

Administrator Guide V9 - EN

1.8.2.2. 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.

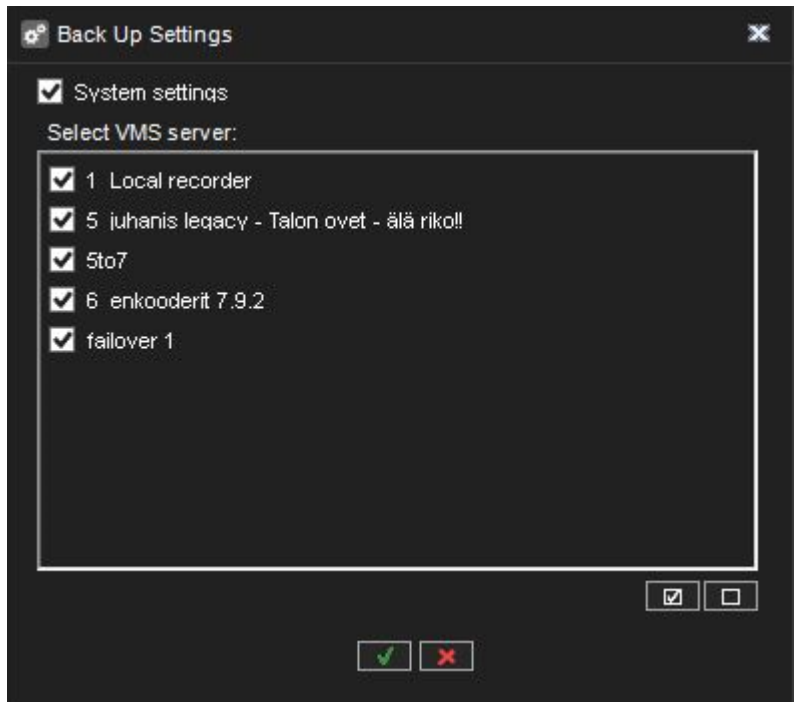
Backup files have the file extension “.vbk”.

To backup settings:

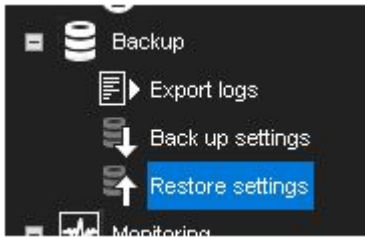
1. On the **System** tab, open **Backup settings**. The **Backup settings** dialogue box is shown.
2. Select the system and server-specific settings that you want to back up and click **OK**.
1. Select the storage device and the folder where you want to save the backup file. To create a new folder, click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



Administrator Guide V9 - EN



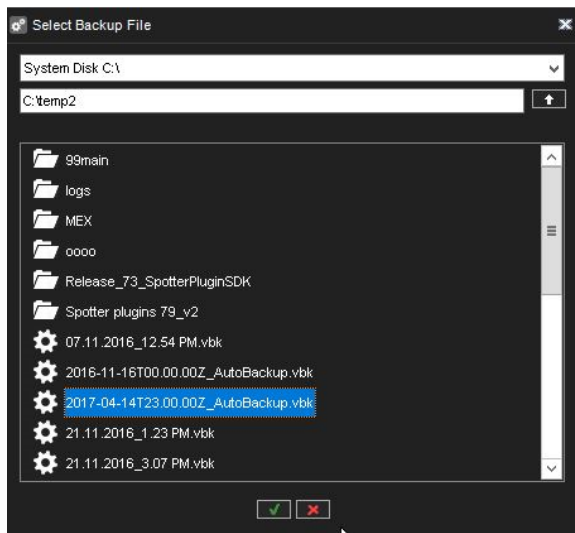
1.8.2.3. Restore settings



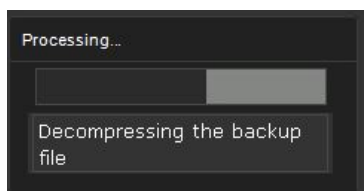
If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs.

To restore settings:

1. On the **System** tab, open **Restore settings**. The Select backup file dialogue box is shown.



2. Find and select the backup file (.vbk) and click **OK**. The system decompresses the file and then shows the **Restore settings** dialogue box.
 - b. The dialogue box also shows a description of the settings.



Administrator Guide V9 - EN

Restore settings

Name: 2017-04-14T23.00.00Z_AutoBackup.vbk

Description: Automatic backup on 2:00

Select	Component
<input checked="" type="checkbox"/>	System settings
<input checked="" type="checkbox"/>	1_Local recorder
<input checked="" type="checkbox"/>	2_slave1
<input checked="" type="checkbox"/>	3_vanha-failover1
<input checked="" type="checkbox"/>	5_juhanis legacy - Talon ovet - älä rikoi!
<input checked="" type="checkbox"/>	6_enkooderit 7.9.2
<input checked="" type="checkbox"/>	7_enkooderit_r-vms2 7.5
<input checked="" type="checkbox"/>	Sto7

Do automatic settings backup after successful settings restore

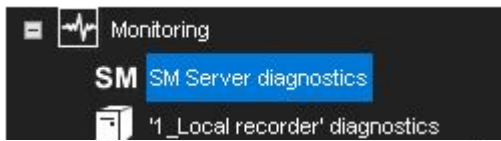
3. Select the system and server-specific settings that you want to restore and click **Start Restore**. The settings are restored.
4. Click **OK** to accept the new settings or **Start the restore process again** to return to the **Restore settings** dialogue.

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

1.8.3. Monitoring

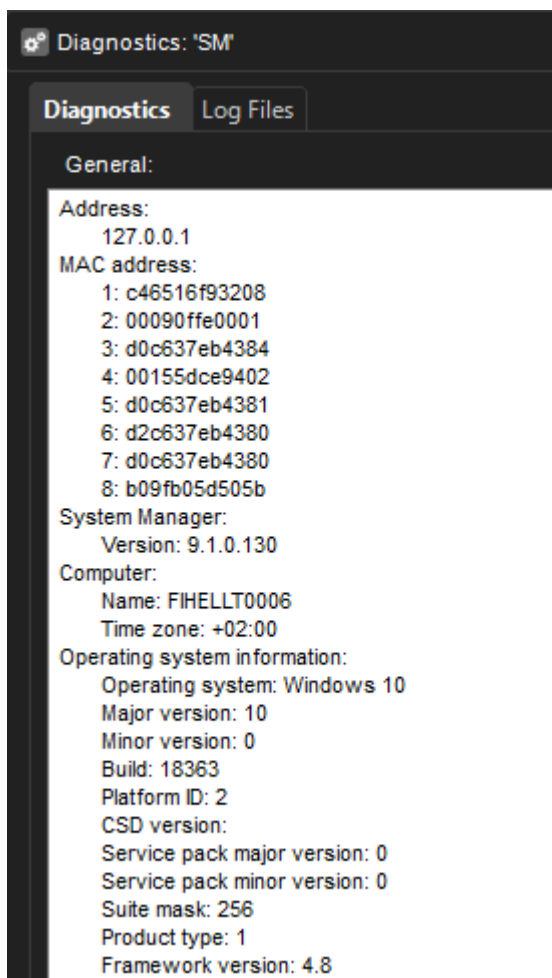
Administrator Guide V9 - EN

1.8.3.1. SM Server Diagnostics



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

General



In SMServer Diagnostics, you can examine this information:

- SM Server version
- Computer name and time zone
- Operating system information
- Major version
- Minor version

Administrator Guide V9 - EN

- Build
- Platform ID
- CSD version
- Service pack major version
- Service pack minor version
- Suite mask
- Product type
- Framework version

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.

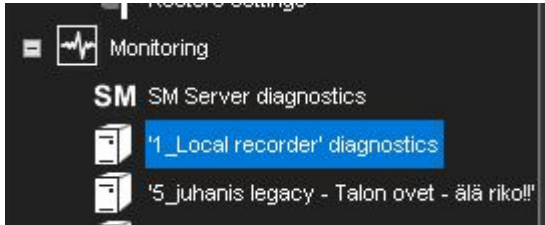
The contents are shown in the **Contents of the selected log file**.



Administrator Guide V9 - EN

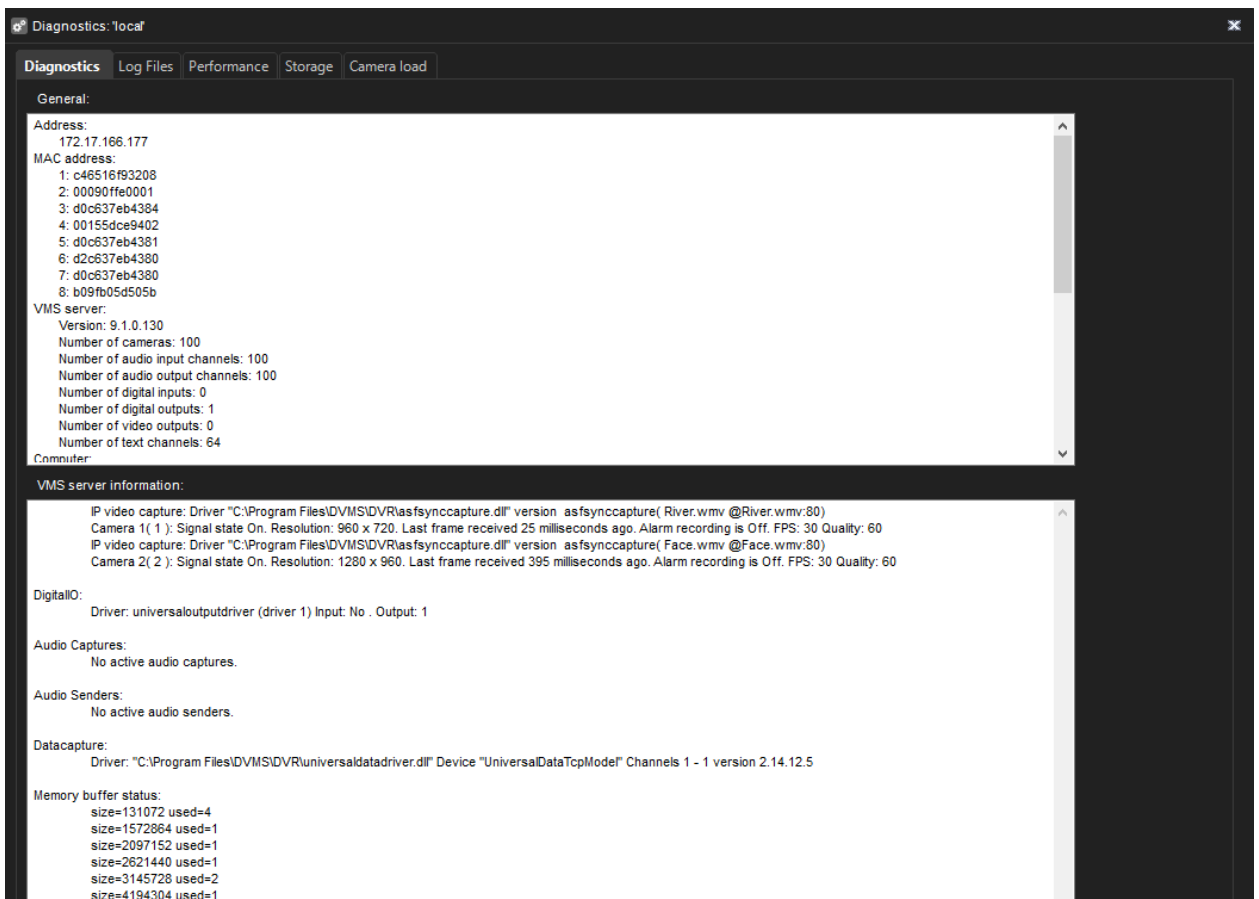
1.8.3.2. Server Diagnostics

Server Diagnostics



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

Diagnostics



The **Diagnostics** tab shows this information:

- Information about the server:
- Software version
- Model

Administrator Guide V9 - EN

- 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.

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**.

Performance

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

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

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.

General

Total 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.

Administrator Guide V9 - EN

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.

Disks

Total 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.

Cameras

Oldest 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.

Administrator Guide V9 - EN

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.

1.8.4. Licenses



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.



Administrator Guide V9 - EN

License Information



System Manager Enterprise 9.2.0 DEVELOPMENT

Demo license

This software is protected by copyright laws and international treaties. Unauthorized modification, reproduction, disassembly or distribution of this software.

Copyright © Mirasys Ltd. 2005 - 2021. All rights reserved.

License details

- TCPXML SMeEventProvider
 - Version: 9.*.*
- Metadata Enrichment UDP
 - Version: 9.*.*
- TCP Watchdog health provider
 - Version: 9.*.*
- MFTHEVC H.265 decoder
 - Version: 9.*.*
- UHDCode H.265 decoder
 - Version: 9.*.*
- Maximum SMServer connections in VMS server 10
- 20 Video channels
- Unlimited storage time
- 40 Audio channels
- 64 Text channels
- 20 VCA channels
- Archiving
- Multi streaming
- Blurring mask editing
- Can use camera motion detection
- Can use network storage
- Can use alarm recording
- Supports multiple servers login on clients
- Missing features
 - Automatic settings backup
 - SDK and RMC video services

License management

<input type="checkbox"/> Import license from clipboard	<input type="checkbox"/> Export license to clipboard
<input type="checkbox"/> Import license from file	<input type="checkbox"/> Export license to file
<input type="checkbox"/> Export MAC to clipboard	<input type="checkbox"/> Export VCA Core HW GUID to clipboard

MAC:



Administrator Guide V9 - EN

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300 - **info@mirasys.com** - **www.mirasys.com**

Administrator Guide V9 - EN


1.8.4.1. License details

License details show all supported features of the license.



Administrator Guide V9 - EN

License Information



System Manager Enterprise 9.2.0 DEVELOPMENT

Demo license

This software is protected by copyright laws and international treaties. Unauthorized modification, reproduction, disassembly or distribution of this software.

Copyright © Mirasys Ltd. 2005 - 2021. All rights reserved.

License details

- TCPXML SMeventProvider
 - Version: 9.*.*
- Metadata Enrichment UDP
 - Version: 9.*.*
- TCP Watchdog health provider
 - Version: 9.*.*
- MFTEVC H.265 decoder
 - Version: 9.*.*
- UHDCode H.265 decoder
 - Version: 9.*.*
- Maximum SMServer connections in VMS server 10
- 20 Video channels
- Unlimited storage time
- 40 Audio channels
- 64 Text channels
- 20 VCA channels
- Archiving
- Multi streaming
- Blurring mask editing
- Can use camera motion detection
- Can use network storage
- Can use alarm recording
- Supports multiple servers login on clients
- Missing features
 - Automatic settings backup
 - SDK and RMC video services

License management

<input type="checkbox"/> Import license from clipboard	<input type="checkbox"/> Export license to clipboard
<input type="checkbox"/> Import license from file	<input type="checkbox"/> Export license to file
<input type="checkbox"/> Export MAC to clipboard	<input type="checkbox"/> Export VCA Core HW GUID to clipboard

MAC:



Administrator Guide V9 - EN

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300 - **info@mirasys.com** - **www.mirasys.com**

1.8.4.2. License Management

To import a license key:

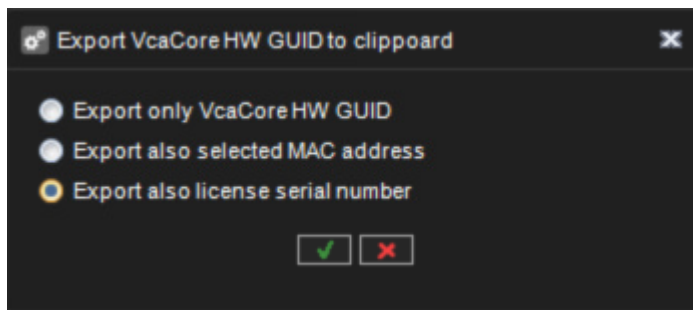
1. Click **Import license from the file**.
2. Browse to the license file location
4. Click **OK**. The new license is updated immediately.

To export a license key:

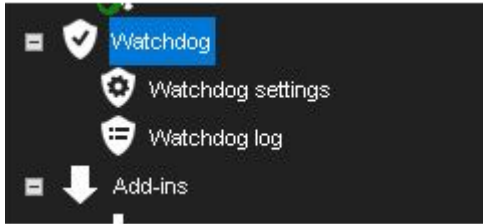
1. Click **Export license key to file** to create a text file for the license or **Export license key to the clipboard** to copy the key to the clipboard.
2. If exporting the license to a file, set the destination folder and the name of the file.
3. Click **OK**.

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**



1.8.5. 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.

Administrator Guide V9 - EN

1.8.5.1. 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.

To add or remove events on the notification list:

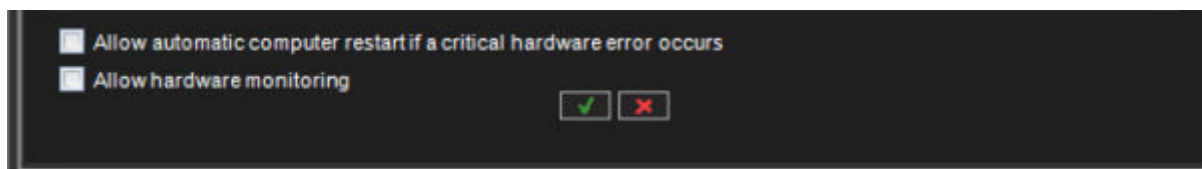
1. On the **System** tab, select **Watchdog settings**.
2. Mark the **Send mail** checkbox for each event type for which a notification e-mail should be sent.
3. Click **OK**.

Automatic restart

Select the check box. **Allow automatic computer restart if a critical hardware error occurs** to restart the computer when serious hardware errors occur automatically.

The computer will not be restarted more than once a day.

Select **Allow hardware monitoring**.if needed



Digital output notifications

In addition to e-mail notifications, notifications can be performed through digital outputs.

Administrator Guide V9 - EN

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**.

Administrator Guide V9 - EN

1.8.5.2. 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.

Additional Watchdog Delivery Methods

The Watchdog functionality includes three new protocols: TCP, SMS (requires an external SMS module), and customizable e-mail form.

Each new protocol has its driver:

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

- WDEventProviderSMS.xml
- 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.

1.8.6. Add-ins



Administrator Guide V9 - EN

1.8.6.1. 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.

However, if necessary, new drivers and plugins can be installed manually.

To install a new driver, you need a device-specific driver installation package.

The driver installation package is a compressed (zipped) folder that contains 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 usually installs the files only if they do not exist on the servers or if the files in the installation package are newer than the files on the servers.

However, you can force the system to install any driver version if necessary.

Note: *If you want to update an already existing camera driver, remove the camera from the system before updating the driver.*

After removing the camera, install the driver file, after which you can reinstall the camera.

After installing a new driver, you need to configure the devices that use the driver.

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.



Administrator Guide V9 - EN



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.

Notes:

- 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.

Administrator Guide V9 - EN

1.8.6.2. Installing Metadata Drivers

It is possible to update and install new metadata drivers using the **Install metadata drivers** -option in the **System** tab.

Administrator Guide V9 - EN

1.8.6.3. Installing Client Drivers

TruCast (direct streaming from camera to Spotter client) requires a different type of camera driver.

These are called (Managed) TruCast Client drivers.

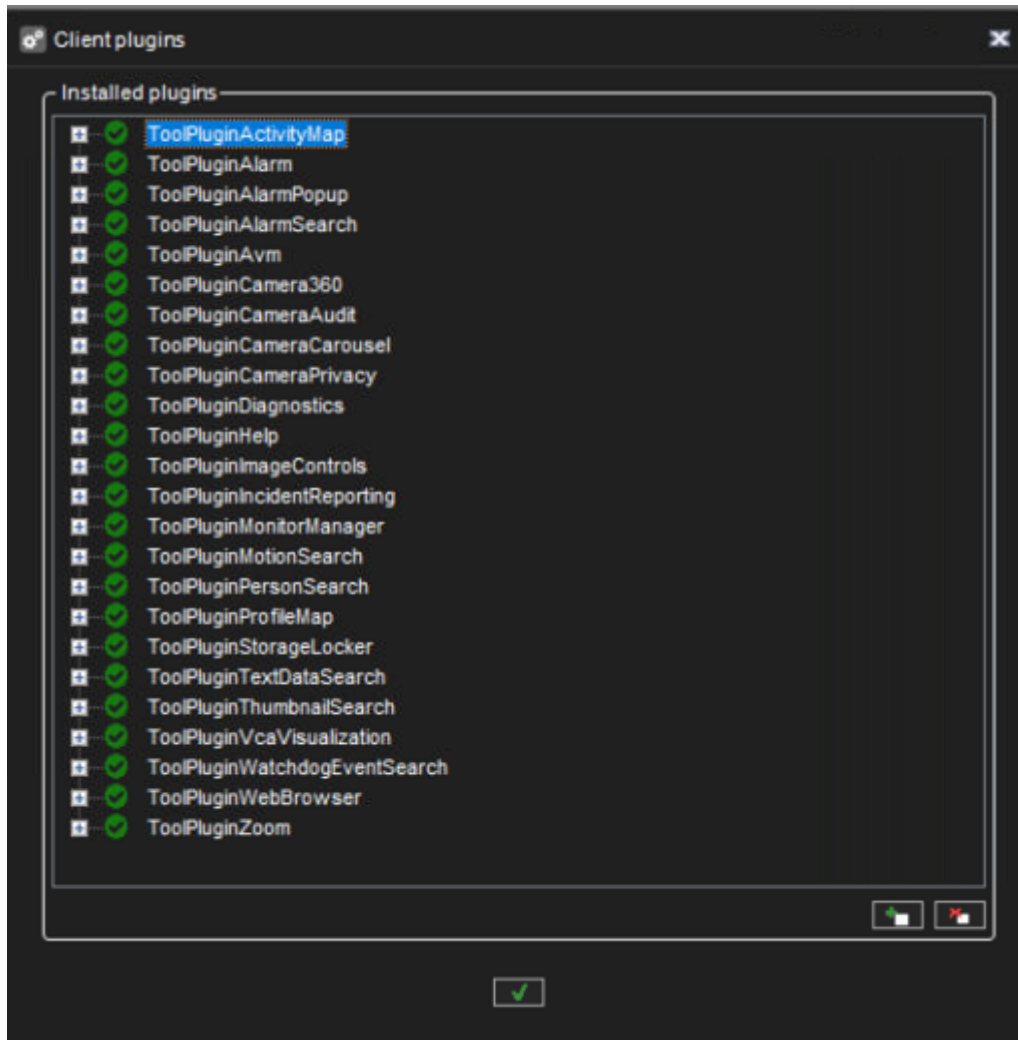
The client camera drivers are installed similarly as spotter plugins and metadata drivers, using the **Install client driver** option in the system manager.



Administrator Guide V9 - EN

1.8.6.4. Install client plugin

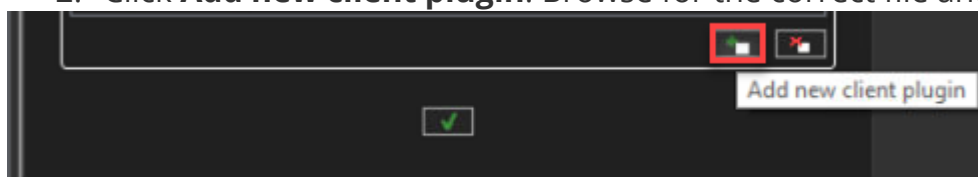
Client plugins for user interfaces such as Spotter can be installed through System Manager.



Plugin installation can be opened from the system tab under Add-ins.

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.



3. Find and select the plugin package (.zip file) and click **OK**. The **Install Plugin** dialogue box is shown.

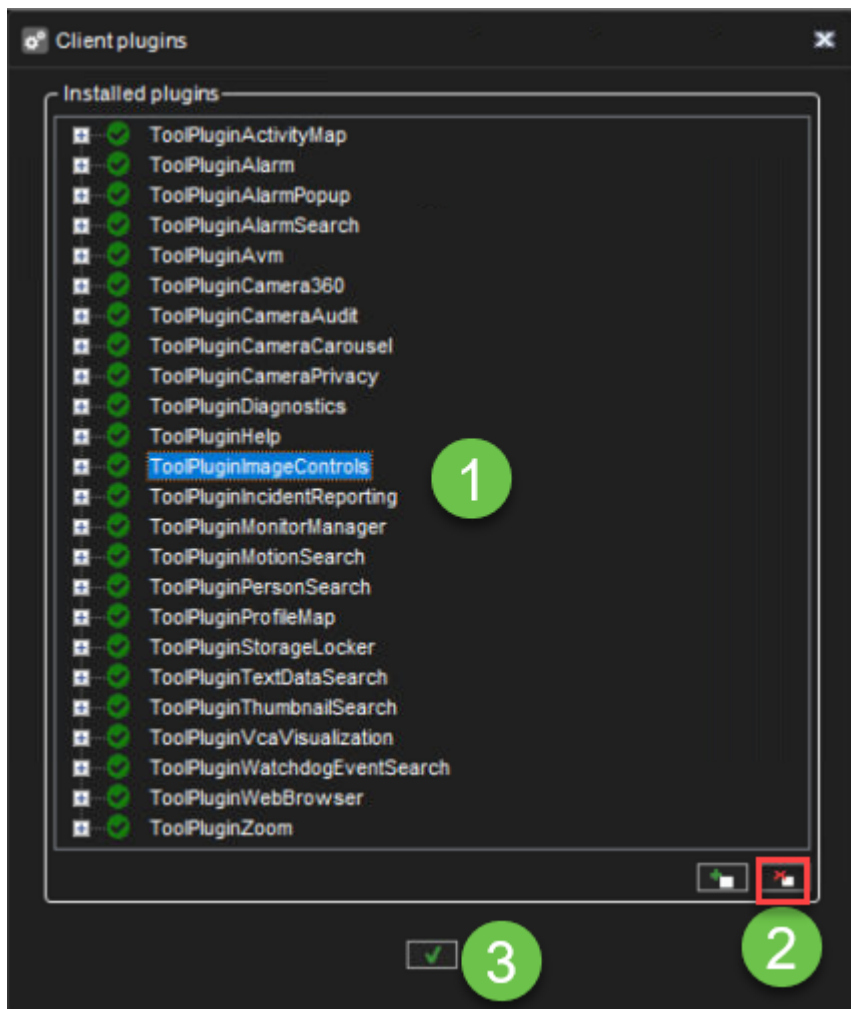
Administrator Guide V9 - EN

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 **Ok**

To remove a client plugin:










Open the **Install client plugin**

1. Select plugin from the list
2. Click **Remove client plugin**
3. Click **Ok**




1.9. 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.

Administrator Guide V9 - EN

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.



Administrator Guide V9 - EN

1.9.1. General

- VMS server name
- Description
- Password
- Protocol
- Multicast Address
- VMS server failover settings

General Settings

Name: MASTER SERVER V9

Description:

Address: 172.17.102.25

Port: 5009

Password: ****

Protocol: TCP (default)

Multicast Address: 225.10.10.1

Allow SDK and RMC video services

Allow SDK alarm control

VMS server failover settings

VMS server group ID: 1

Use as a failover VMS server

VMS server failover is enabled for this VMS server

Detect VMS server failure on connection loss

Connection is not established after

10min

OK Cancel

Multicast address

Administrator Guide V9 - EN

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.

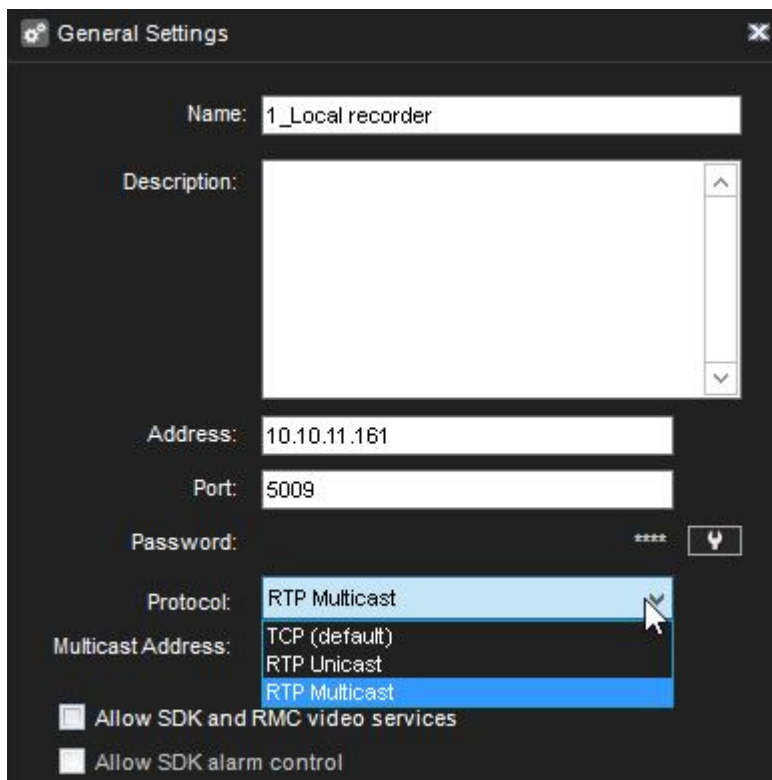
When using multi-casting, the stream for each video channel is sent to the LAN only once.

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.

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

- info@mirasys.com

- www.mirasys.com

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.

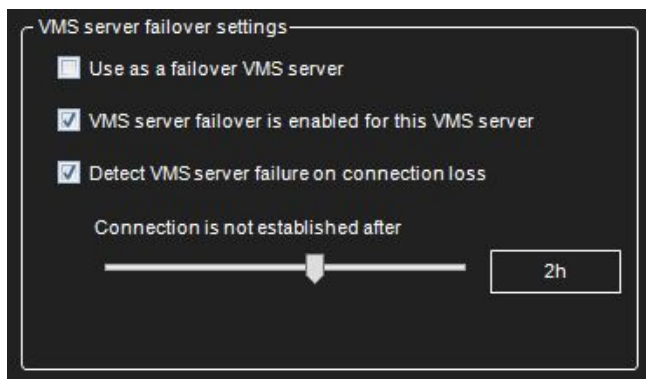
When in standby mode, failover servers appear under a separate folder in the *VMS Server* list.

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.

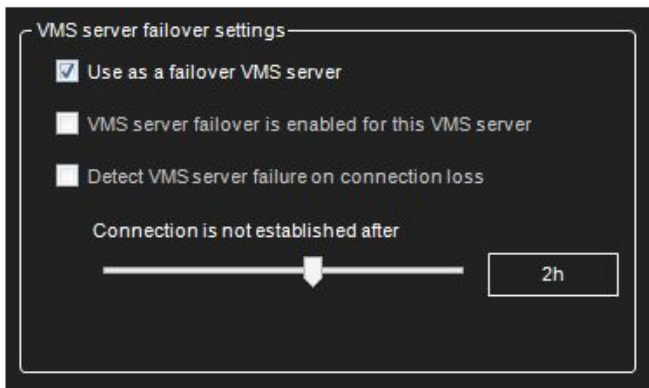
The failover transition is done if all material disks are broken or the server is inaccessible for longer than a defined period.



For example, under failover protection, if inaccessible for longer than 2 hours, the failover switch would happen.



Administrator Guide V9 - EN



1.9.2. Port Forwarding

The basic idea with port forwarding is that it can access one or more VMS Servers or Master 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."

Administrator Guide V9 - EN

1.9.2.1. 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...**)

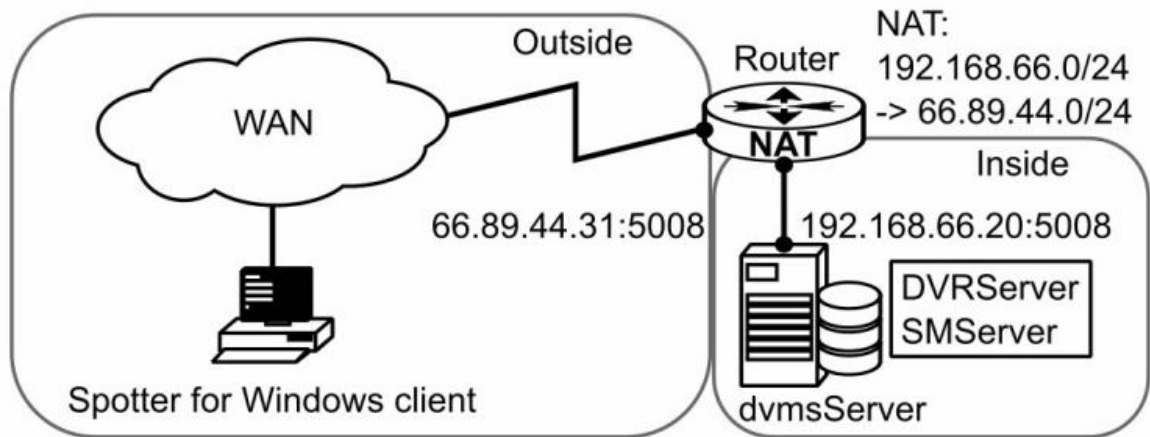
When connecting to a Master Server, the port is typically 5008. When adding new servers to the master, the port is typically 5009. If there are more than one server on-site, then the ports are 5009 +4, 5009 + 8 etc.



Administrator Guide V9 - EN

1.9.2.2. Single Server Behind Router

Scenario 1: Using a system with a single server behind a router/firewall



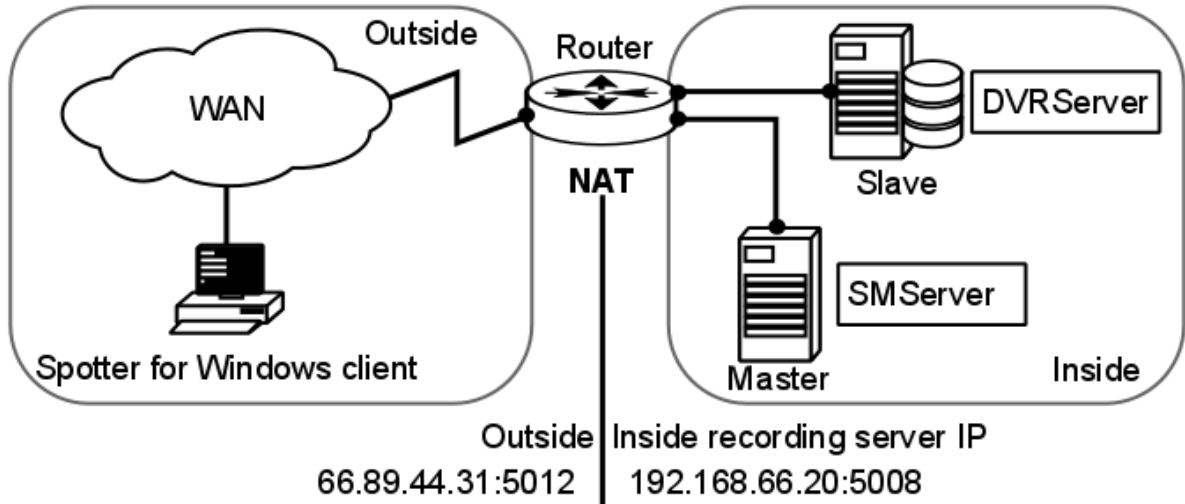
If the user is accessing a single server from the WAN, he needs to connect to the VMS Server with the outside IP address that the router has translated.

The user can check the port forwarding what the port in use is, but it is highly likely port 5008.

Administrator Guide V9 - EN

1.9.2.3. 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 Master 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.

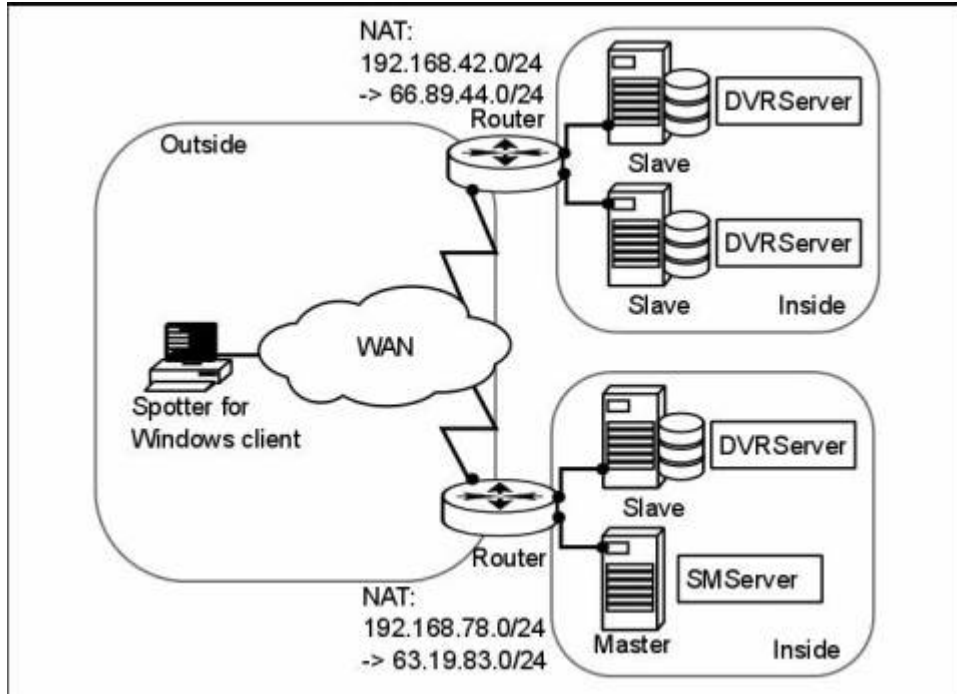
If the added server is a single, standalone server, the port is most likely 5009.

If multiple servers are on the same site, they most likely get the ports starting with **5009, 5013, 5017, 5021...**

Administrator Guide V9 - EN

1.9.2.4. 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 Master Server from the other site.

1.9.3. 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 timezone and time is the same as the VMS server



Administrator Guide V9 - EN

Hardware Settings

Video | Audio

No.	Name	Model	Settings
1	AXIS P1455-LE	AXIS P1455-LE Network Camera	http://172.17.100.84
2	XND-6081V	Samsung Techwin XND-6081V	http://172.17.100.26
3	XND-9082R	Hanwha WiseNet XNV-9082R	http://172.17.100.79
4	FLEXIDOME IP 5000i IR	Bosch FLEXIDOME IP 5000i IR	http://172.17.100.25
5	AXIS P5665-E	AXIS P5665-E PTZ Dome Network Came...	http://172.17.100.88

Device settings

Edge storage

Edge storage fetching for offline period

Camera in passive mode

Name:

Resolution:

Record rate:

Navigation icons: A+, +, -, A-, Search, Filter, Refresh

Buttons: [OK] [Cancel]

Administrator Guide V9 - EN

1.9.3.1. 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 when 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).

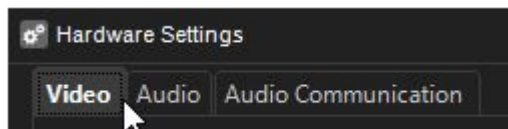
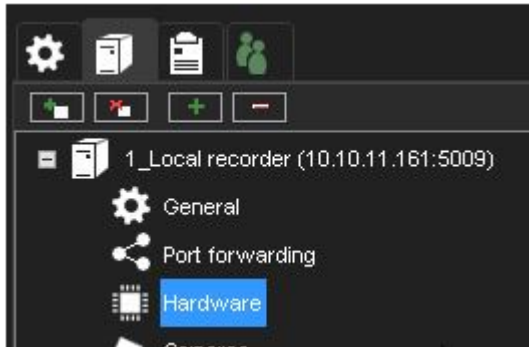
Administrator Guide V9 - EN

The system will not store last used options for modifying cases because the options will be available for adding cameras only

Administrator Guide V9 - EN

1.9.3.1.1. Add device

IP cameras or analogue video servers (encoders) can be managed through the **Video** tab of **Hardware settings**.



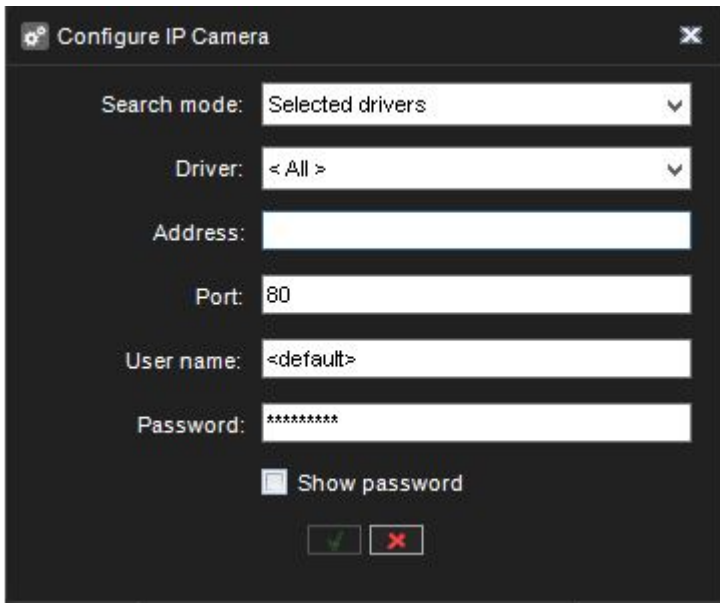
To add a new IP camera when the IP address is known:

1. On the **Video** tab, click **Add device**



2. Type the IP address or DNS name of the camera or video server.
 - o Change the port number if needed. Usually, port 80 is used.
3. Type the username and password for the camera.
4. Click **OK**.

Administrator Guide V9 - EN



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.

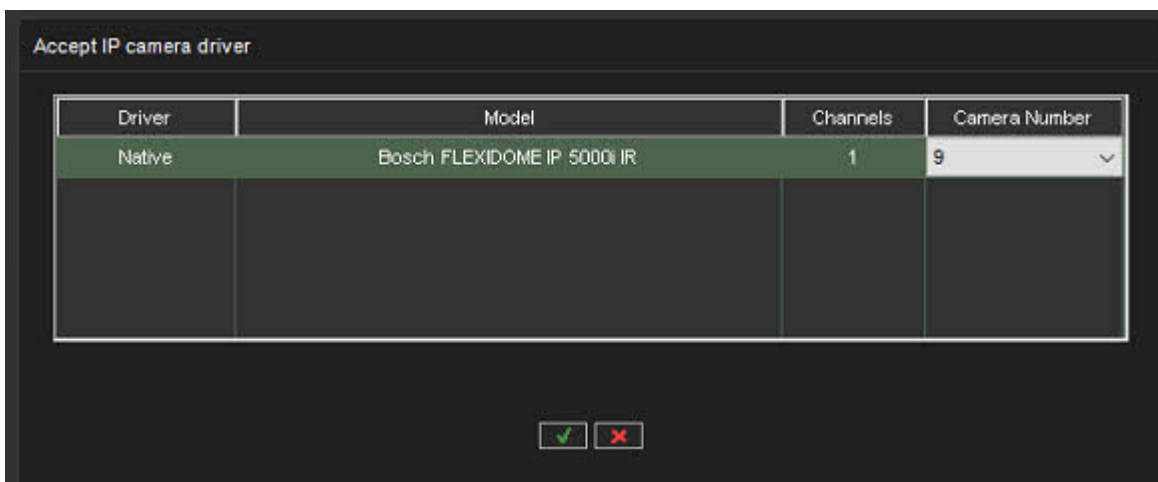
5. Select a driver from the list.

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**

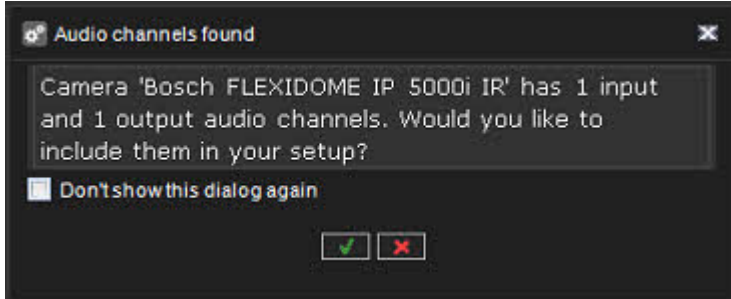


Driver	Model	Channels	Camera Number
Native	Bosch FLEXIDOME IP 5000i IR	1	9

Administrator Guide V9 - EN

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



Administrator Guide V9 - EN

Hardware Settings

Video Audio

No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision IDS-2CD7A26G0P-IZHSY	http://172.17.100.83
2	EASY LPR IN	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117
3	Axis P5665-E	AXIS P5665-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:

Resolution: 3072x1728

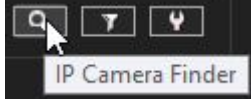
Record rate: 30 / s

Navigation icons: Home, A+, +, -, Search, T, Y, Check, X

Administrator Guide V9 - EN

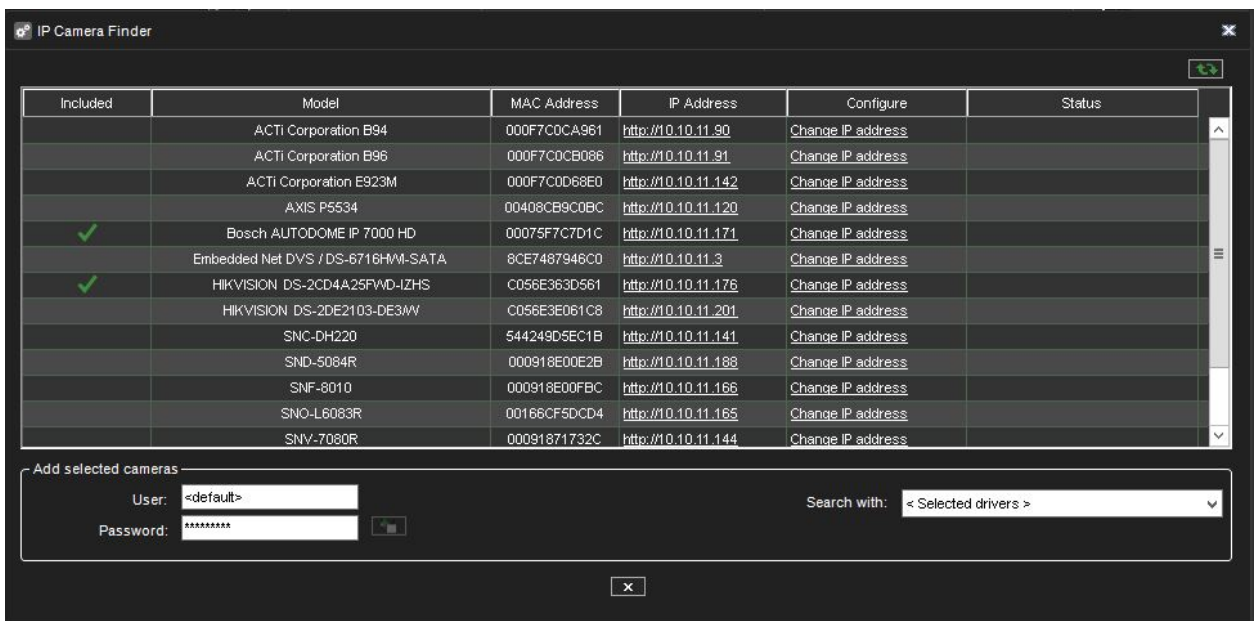
1.9.3.1.2. IP Camera Finder

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.

Administrator Guide V9 - EN

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:





Administrator Guide V9 - EN

1.9.3.1.3. 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**

The screenshot shows the 'Video' tab in the Mirasys interface. A table lists various IP cameras. The fourth row, 'RD sisäänkäynti', is highlighted with a red border. Below the table, the 'Device settings' panel is visible, showing fields for Name, Resolution, and Record rate. The 'Name' field contains 'RD sisäänkäynti', 'Resolution' is set to '1920x1080', and 'Record rate' is '25 / s'. A red box highlights the 'Edit IP Camera' button at the bottom right of the settings panel.

No.	Name	Model	Settings
1	RD takaseinä	Hanwha WiseNet QND-6012R	http://172.19.100.106
2	Lobby	Hanwha WiseNet LND-6070R	http://172.19.100.120
3	Office Corridor	Hanwha WiseNet GND-8080R	http://172.19.100.107
4	RD sisäänkäynti	Hanwha WiseNet LND-6010R	http://172.19.100.105
5	Aula	Hanwha WiseNet XND-6010	http://172.17.100.74
6	Office side	Hanwha WiseNet XND-L6080R	http://172.17.100.77
7	Katunäkymä	Street Walk Video.wmv	http://Street Walk Video.wmv
8	Testing room	Bosch FLEXIDOME IP 5000i IR	http://172.17.100.25
9	HIKVISION DS-2DF6223-...	Hikvision DS-2DF6223-AEL	http://172.19.100.101

Device settings

Edge storage

Edge storage fetching for offline period

Camera in passive mode

Name:

Resolution:

Record rate:

1. Do needed modifications
2. Click Ok to confirm changes



Administrator Guide V9 - EN

Configure IP Camera [X]

Search mode: Currently active drivers [v]

Driver: WisenetIPCapture [v]

Address: 172.19.100.105

Port: 80

User name: admin

Password: [masked]

Show password

[✓] [✗]

Administrator Guide V9 - EN

1.9.3.1.4. 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

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**.

Administrator Guide V9 - EN

The screenshot shows the 'Hardware Settings' window with the 'Video' tab selected. A table lists two camera devices. The second device, a Dahua ITC215-PW6M-P..., is selected. Below the table, the 'Used camera licenses' are shown as 2/10. The 'Device settings' panel for the selected camera includes checkboxes for 'Edge storage', 'Edge storage fetching for offline period', and 'Camera in passive mode'. It also features input fields for 'Name' (DAHUA ITC215-PW6M-PW6M), 'Resolution' (1920x1080), and 'Record rate' (25 / s). At the bottom, there are navigation icons and a 'Remove Selected Device' button.

No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision IDS-2CD7A26G0P-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:

Resolution: 1920x1080

Record rate: 25 / s

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**

Administrator Guide V9 - EN

The screenshot shows the 'Hardware Settings' window with the 'Video' tab selected. A table lists video channels, with 'Kamera 6' highlighted. Below the table, the 'Device settings' for 'Kamera 6' are shown, including checkboxes for 'Edge storage', 'Edge storage fetching for offline period', and 'Camera in passive mode'. Sliders for 'Resolution' (set to 2560x1920) and 'Record rate' (set to 5/s) are also visible. A red box highlights the minus sign icon in the bottom toolbar, and a tooltip indicates 'Remove video channel from the selected device'.

No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision IDS-2CD7A26G0P-IZHSY	http://172.17.100.83
2	EASY LPR IN	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117
3	Axis P5665-E	AXIS P5665-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

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**



Administrator Guide V9 - EN

Hardware Settings

Video Audio

No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision IDS-2CD7A26G0P-IZHSY	http://172.17.100.83
2	EASY LPR IN	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117
3	Axis P5665-E	AXIS P5665-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	Harwha WiseNet SPE-420	http://172.18.100.109
7	Kamera 7	Harwha WiseNet SPE-420	http://172.18.100.109
8	Kamera 8	Harwha 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

Administrator Guide V9 - EN

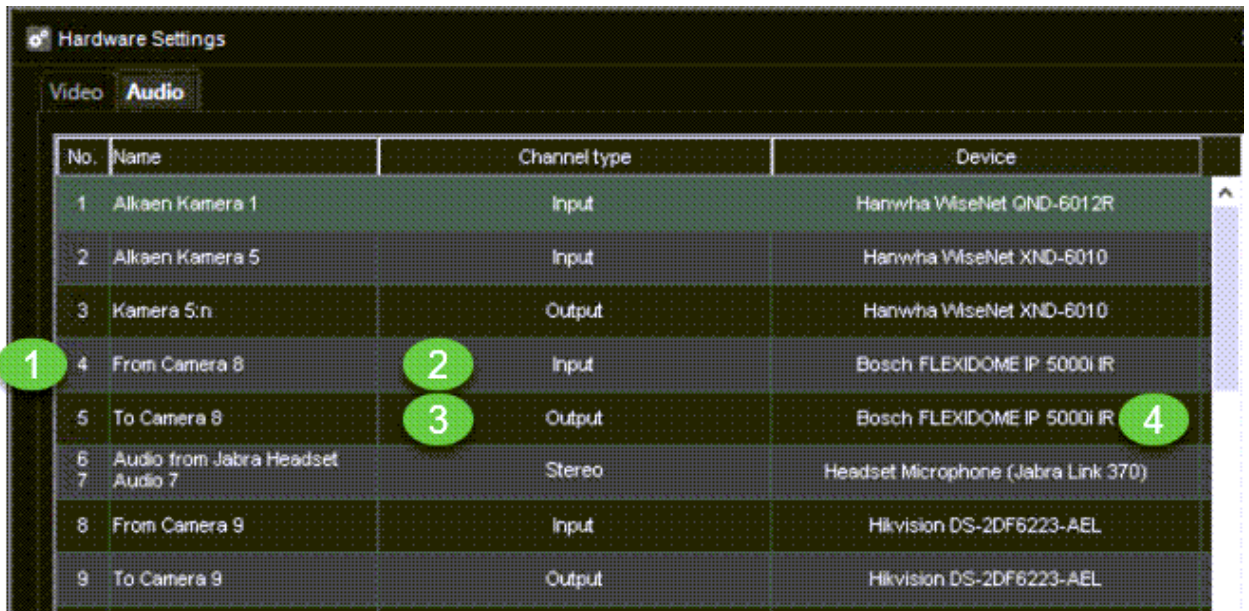
1.9.3.2. Audio

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.

Information shown:

1. Camera hardware ID
2. Channel type(Input)
3. Channel type(Output)
4. Device model



No.	Name	Channel type	Device
1	Alkaen Kamera 1	Input	Hanwha WiseNet QND-6012R
2	Alkaen Kamera 5	Input	Hanwha WiseNet XND-6010
3	Kamera 5:n	Output	Hanwha WiseNet XND-6010
4	From Camera 8	Input	Bosch FLEXIDOME IP 5000i IR
5	To Camera 8	Output	Bosch FLEXIDOME IP 5000i IR
6	Audio from Jabra Headset	Stereo	Headset Microphone (Jabra Link 370)
7	Audio 7		
8	From Camera 9	Input	Hikvision DS-2DF6223-AEL
9	To Camera 9	Output	Hikvision DS-2DF6223-AEL



Administrator Guide V9 - EN

1.9.3.3. Device Settings

Edge Storage

The Edge storage functionality enables uninterrupted recording during network blackouts. In practice, in-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.

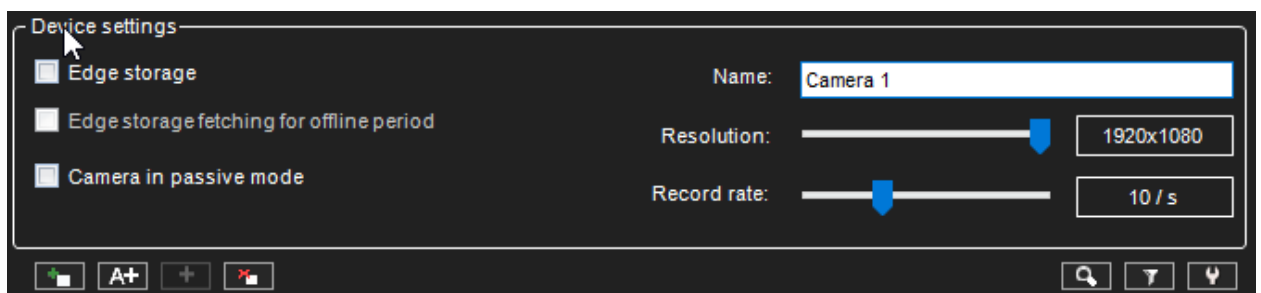
Edge storage fetching for offline period

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.

Camera information

Camera name, resolution and record rate can be set directly from the **Video** tab



1.9.4. 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 Master 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.


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.*



Administrator Guide V9 - EN

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.

Connection status:

If the connection to the server is lost, the System Manager application will automatically try to connect to the server.

NOTE:

When you have added Mirasys VMS as a slave server, please do the following actions:

1. Change Admin user password using a slave server System Manager

Administrator Guide V9 - EN

2. Disable SMServer service from the slave server

1.9.5. Cameras

After the camera has been added to the server, the camera settings can be configured from the **Cameras** page.



Camera Settings contain settings for:

- General
- Motion Detection
- VCA features
- Privacy
- Scheduler



Administrator Guide V9 - EN

1.9.5.1. Camera Settings

Camera Settings

General Motion Detection VCA features Privacy Scheduler

Settings

No.	In Use	Name	Quality	Resolution	Rate	Camera Driver Information	Load
1	✓	HIKVISION IDS-2CD7A26	60%	1920x1080	15 / s	Chipcapture_H.264	30,0%
2	✓	EASY LPR IN	60%	1920x1080	25 / s	Dahuacapture_H.264	100,0%
3	✓	Axis P5665-E	60%	1920x1080	15 / s	Newaxiscapture_H.264	30,0%
4	✓	EASY LPR OUT	60%	1920x1080	15 / s	Newaxiscapture_H.264	30,0%
7	✓	Kamera 7	60%	2560x1920	5 / s	Wisenetcapture_H.264	41,7%
8	✓	Kamera 8	60%	2560x1920	5 / s	Wisenetcapture_H.264	

General Streams Advanced

Name: HIKVISION IDS-2CD7A26

In use
 360 camera

Control Mode: Active

Transport Type: RTP over UDP

Decompression codecs:

H.264: CoreAVC SW / HW

H.265: Intel SW / HW

Description Administrative Description

Reference image

Frame rate optimization

Local use 50% Remote use 50%

Total load: 19,38%

✓ ✗

Administrator Guide V9 - EN

1.9.5.1.1. General settings

Name

The name of the camera. The system suggests names of the type *Camera 1*, *Camera 2*, and so on.

In Use

Clear this check box if no camera is connected to the camera input or if you want to disable the camera.

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)

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.

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.

Decompression codecs.

Codecs are used for encoding and decoding video data

Description.

Here you can type a description of the camera shown to all users in the Spotter program.

Administrative Description.

Here you can type a description of the camera. The description will be shown in the Spotter program to only system administrators.

Reference 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.

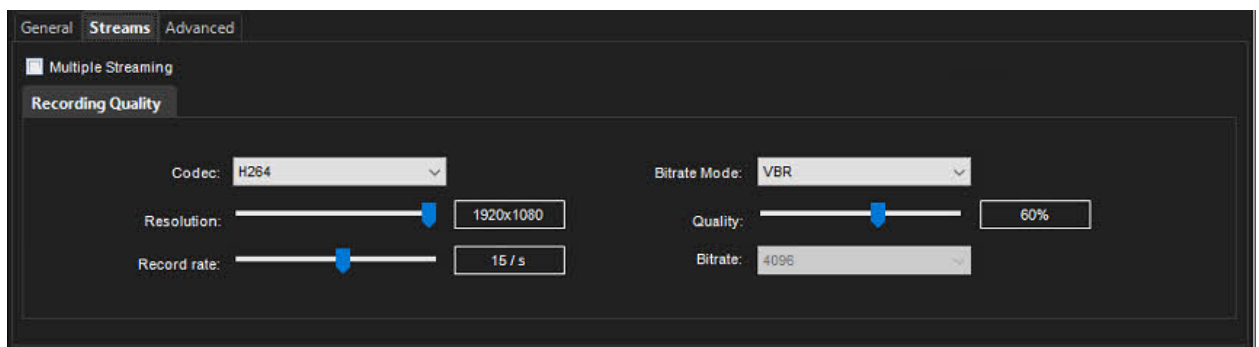
To change the current reference image, click the **Capture image** button. To delete a reference image, click the **Delete image** button.



1.9.5.1.2. Streams

By default, Mirasys VMS receives recording quality stream from the camera.

Mirasys VMS server send recording stream by default to the Mirasys Spotter



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.

Bitrate mode.

This setting controls if the Variable bit rate (VBRMax) or Constant bit rate (CBR) is used.

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

Administrator Guide V9 - EN

lower also decreases the quality of the images.

50% is usually sufficient. For wireless and low bandwidth connections, select 0%.

Resolution

For automatically configured IP cameras, the exact image resolutions supported by the camera model are displayed.

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)



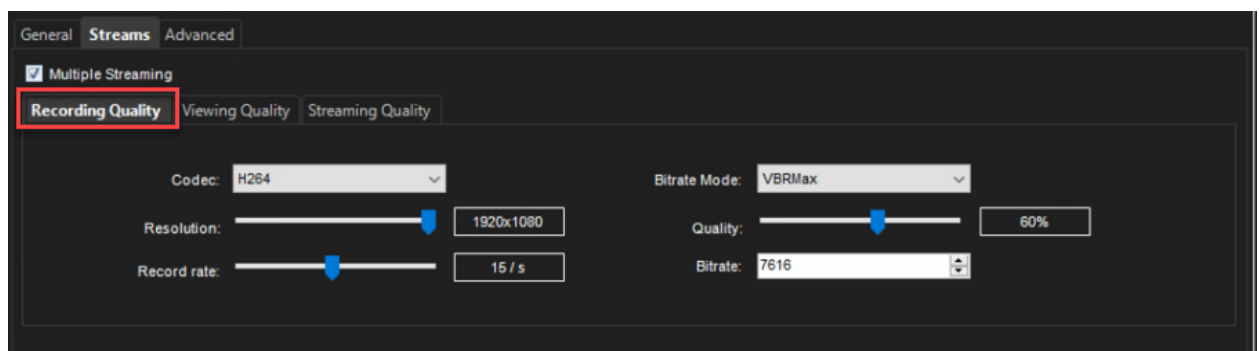
Administrator Guide V9 - EN

1.9.5.1.2.1. Multi-Streaming

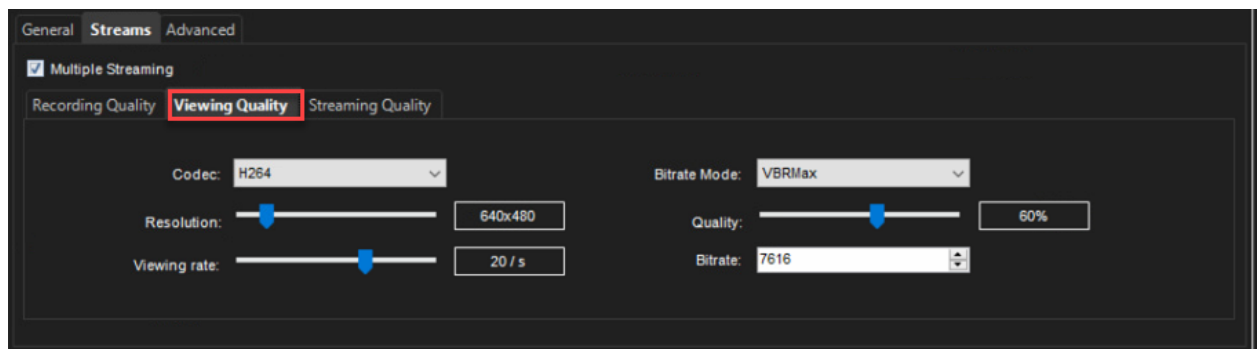
Multi-streaming enables separate feeds from a single camera. The feature allows for separate streams to be used for recording and viewing. The feature is available only if the camera and driver support it.

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

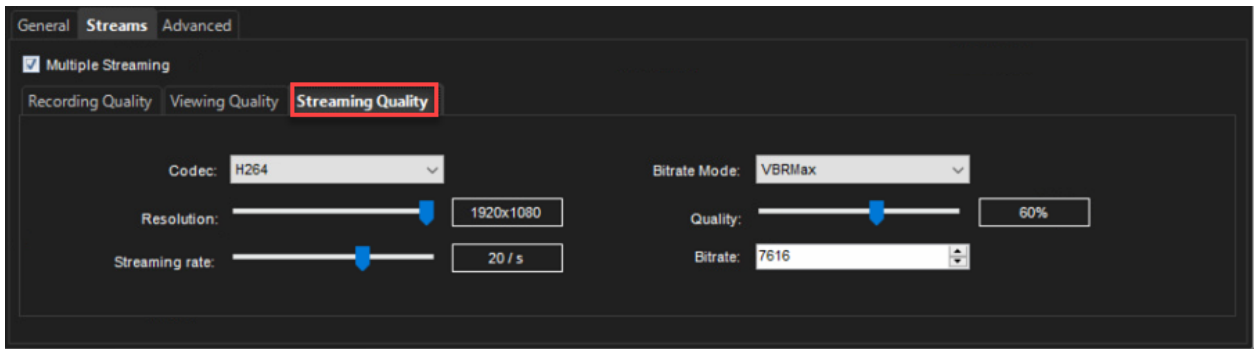


Viewing Quality



Streaming Quality

Administrator Guide V9 - EN



Administrator Guide V9 - EN

1.9.5.1.3. Advanced

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.

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



Administrator Guide V9 - EN

General Streams **Advanced**

RTP Packet Size 1400

RTSP session logging

GOV Length Automatic

Custom GOV Length 20

Manage privacy masks by the driver

Network Interface <Default>

Multicast address: Recording stream 236.19.100.106

Multicast port: Recording stream 40010

Multicast address: Viewing stream 236.19.100.106

Multicast port: Viewing stream 40020

Multicast address: Streaming stream 236.19.100.106

Multicast port: Streaming stream 40030

Multicast TTL 1

Enable Time Synchronization feature

Administrator Guide V9 - EN

1.9.5.1.4. Frame rate optimization

The slider is intended to estimate load when using the server both as a recording server and a client workstation.

The default assumption for local/remote use is 50%.

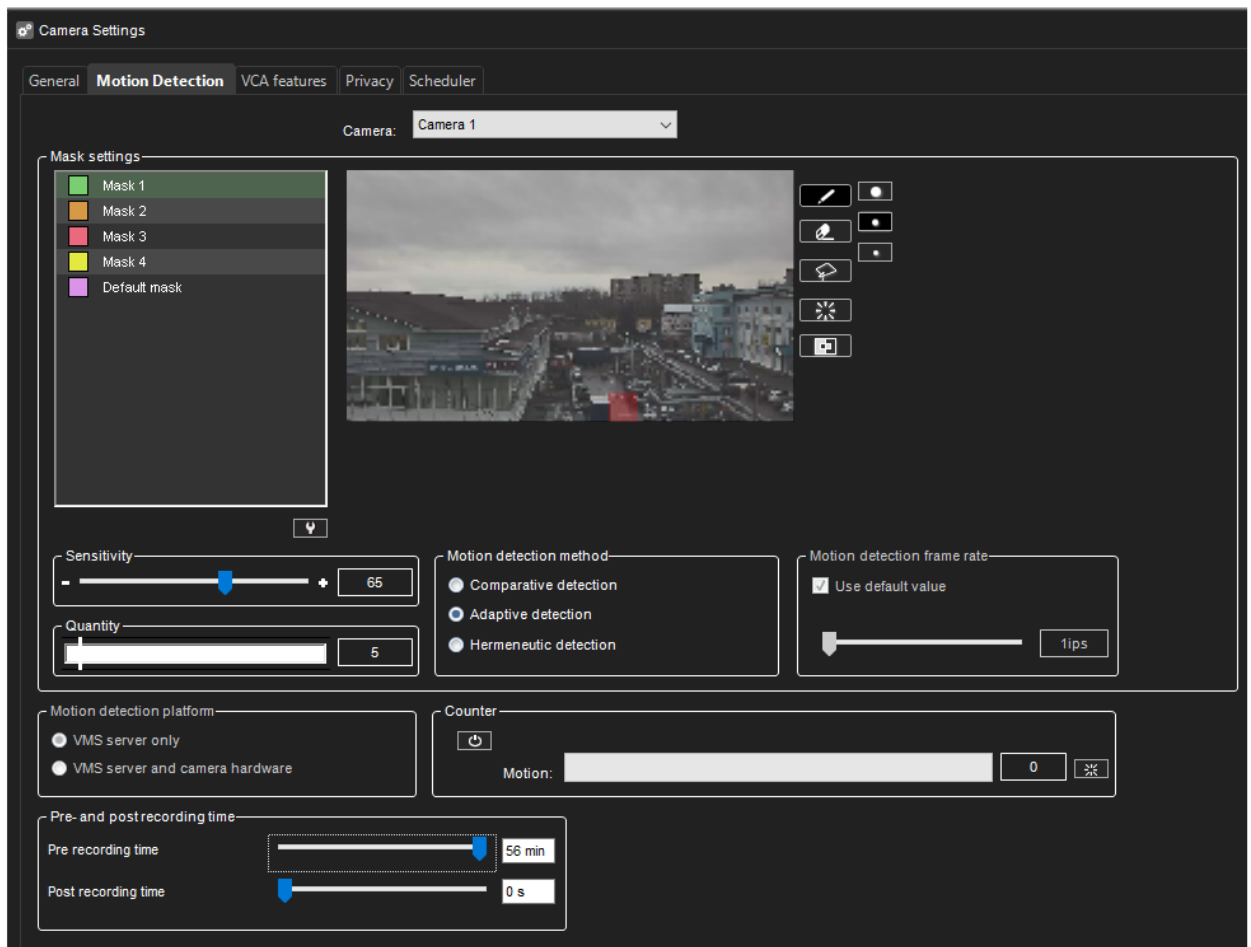
If this limits the number of cameras or use of desired camera settings, the slider can be dragged towards 100% to add all desired cameras with desired settings.

However, care should be taken not to overload the server in such a situation.

After specifying whether frame rates should be optimized for local or remote viewing, click **Optimize**.

The system sets the record rates to the highest possible values.

1.9.5.2. Motion Detection



Sensitivity and quantity

The system detects motion when:

- Pixels change more than the set limit (**Sensitivity**).
- The specified number of pixels change (**Quantity**).

If there is a lot of background noise in the image, for example, changes in lighting conditions, decrease the sensitivity by dragging the slider to the left or increase the quantity limit by dragging the slider to the right.

Motion detection methods

Comparative detection

Administrator Guide V9 - EN

Compares an image to the image before it. If the differences exceed the set limits, the system detects motion.

You can use comparative motion detection in most conditions.

However, if there is a lot of movement in the background, for example, rain, moving leaves, or changes in light levels, use adaptive motion detection.

Adaptive detection

Compares each image to a background image. The system learns the background image and the movement that belongs there automatically.

Thus, the system does not interpret, for example, moving leaves as motion.

In addition, if more than half of the pixels in an image change, the system concludes that the lighting conditions have changed.

As a result, it resets the reference image and starts learning it again.

Hermeneutic detection

Is a sophisticated motion detection system for challenging weather conditions (e.g. heavy rain, “noisy” background image, etc.) and situations in which external video content analytics (VCA) tools are used.

It should be noted that hermeneutic detection requires more processing resources than the other detection methods.

Motion detection frame rate

Defines 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.

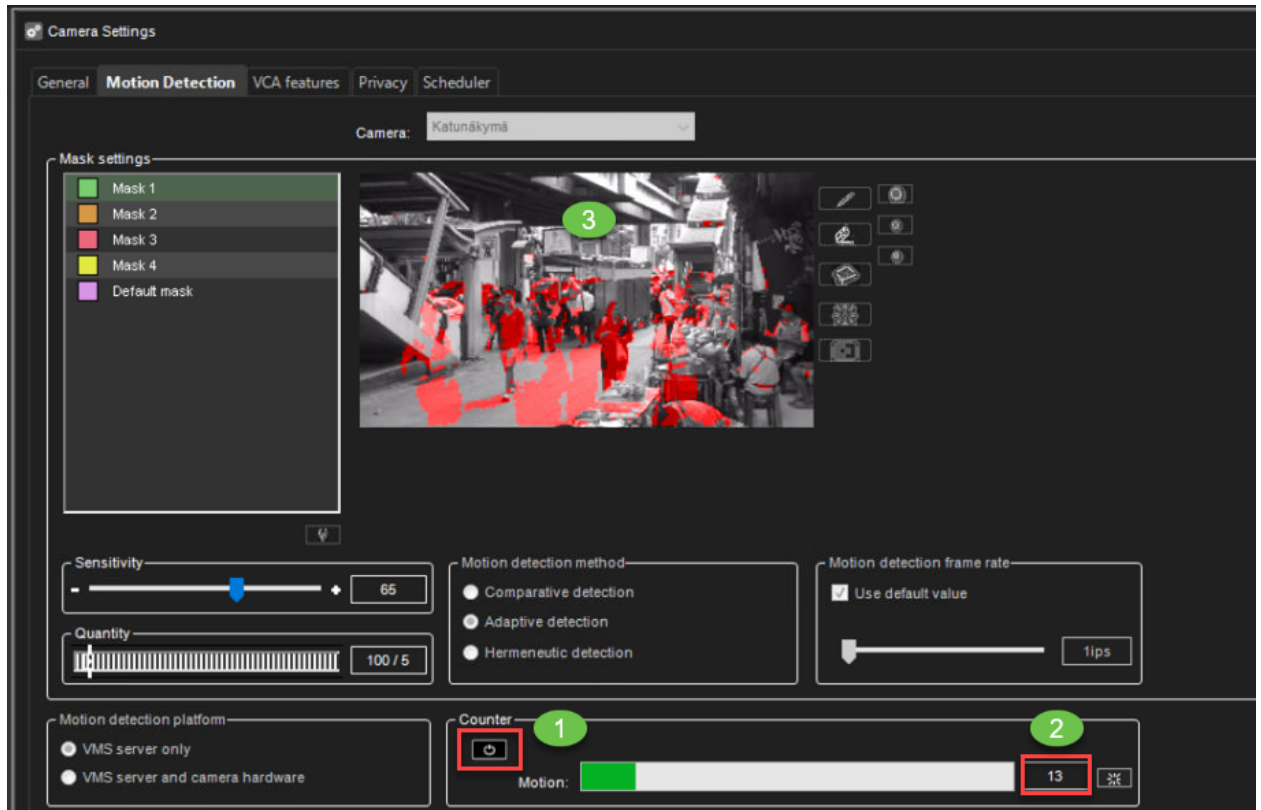
Counter

1. Enable **Counter**



Administrator Guide V9 - EN

2. Check the motion values
3. The camera image shows which area of the camera image causes motion detection recording



Pre- and Post- recording time

Motion pre-and post-recording is used to have recorded material before and after the motion.

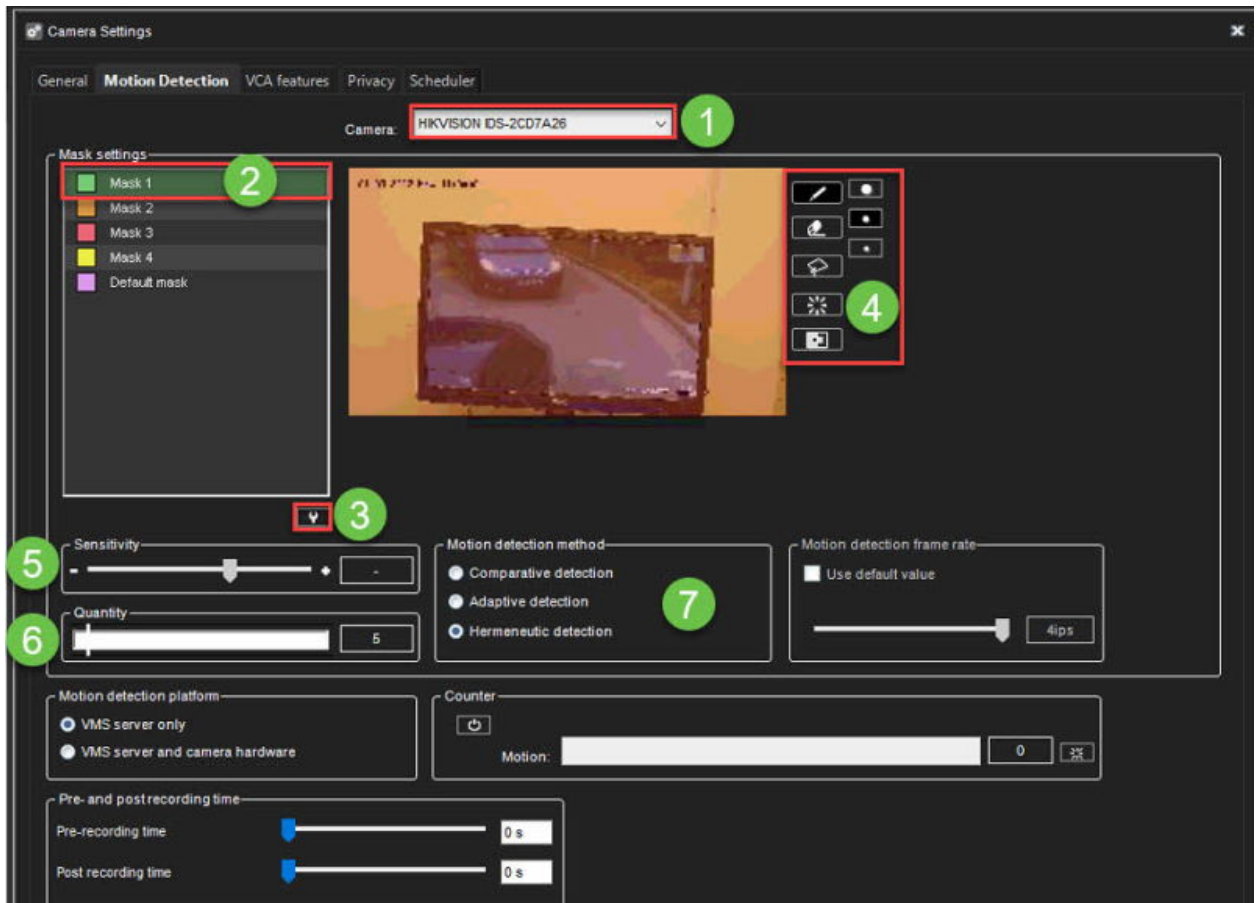
Each mask can be configured separately.

Values are from 0s to 60 minutes.

Administrator Guide V9 - EN

1.9.5.2.1. Editing a mask

1. In the **Motion Detection** tab, select the camera from the camera list.
2. Click the mask that you want to edit.
3. To change the mask's name, click **Change Mask Name** and type a new name for the mask.



4. With the drawing tools presented in the following table, paint the areas red where you want the system to detect movement and remove the red from areas where you want to ignore the movement.
5. Set the detection sensitivity.
6. Set the minimum quantity of movement.
7. Select the motion detection method: comparative, adaptive, or hermeneutic motion detection.







Detected motion is shown in red in the image, and the counter increments each time motion is detected.

Drawing Tools:

Tool	Name	Description
------	------	-------------



Administrator Guide V9 - EN

	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).

Administrator Guide V9 - EN

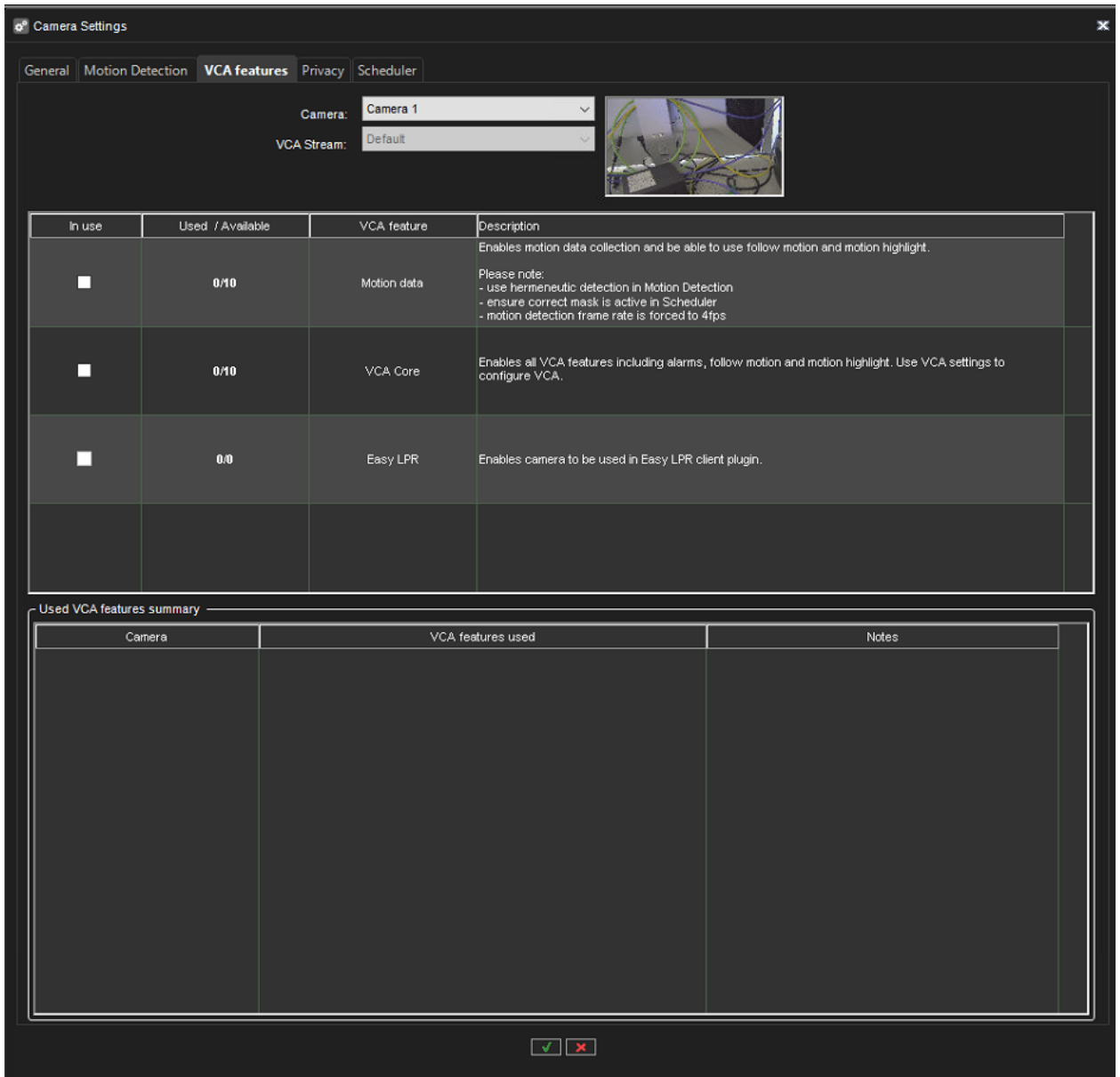
1.9.5.3. VCA features

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 image)



Camera Settings

General Motion Detection **VCA features** Privacy Scheduler

Camera: Camera 1
VCA Stream: Default

In use	Used / Available	VCA feature	Description
<input type="checkbox"/>	0/10	Motion data	Enables motion data collection and be able to use follow motion and motion highlight. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps
<input type="checkbox"/>	0/10	VCA Core	Enables all VCA features including alarms, follow motion and motion highlight. Use VCA settings to configure VCA.
<input type="checkbox"/>	0/0	Easy LPR	Enables camera to be used in Easy LPR client plugin.

Used VCA features summary

Camera	VCA features used	Notes

✓ ✗

Administrator Guide V9 - EN

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.

Administrator Guide V9 - EN

1.9.5.4. 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.

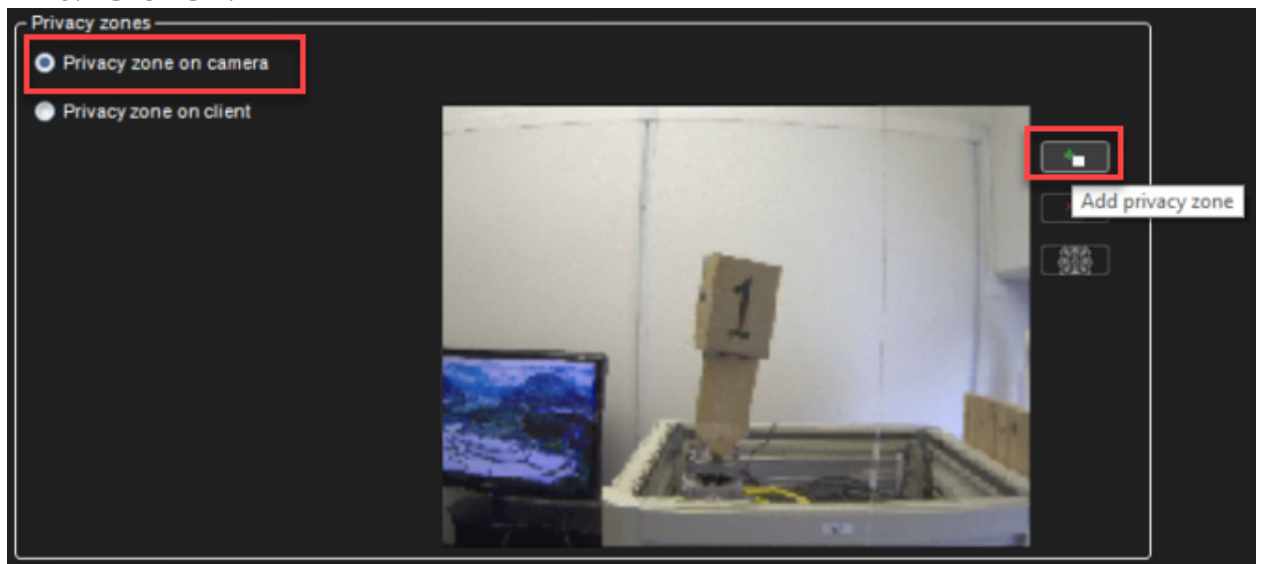
(I.e. if the camera does not have, e.g. the facial blurring defined, this camera shall not have the faces blurred – even if the user group of the end-user would have permission level set to view only unblurred materials.

This also applies when exporting the materials.

1.9.5.4.1. Privacy zone on the camera

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**.



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**.

Administrator Guide V9 - EN

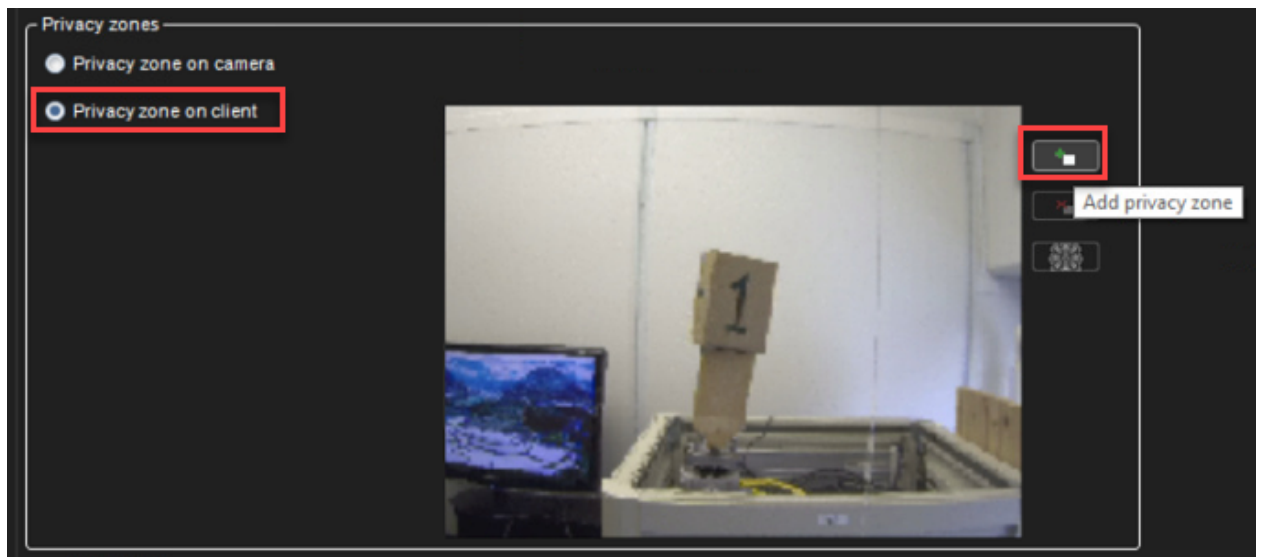
1.9.5.4.2. Privacy zone on the client

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.

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**.



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**.

Administrator Guide V9 - EN

1.9.5.4.3. 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.

Blur Faces

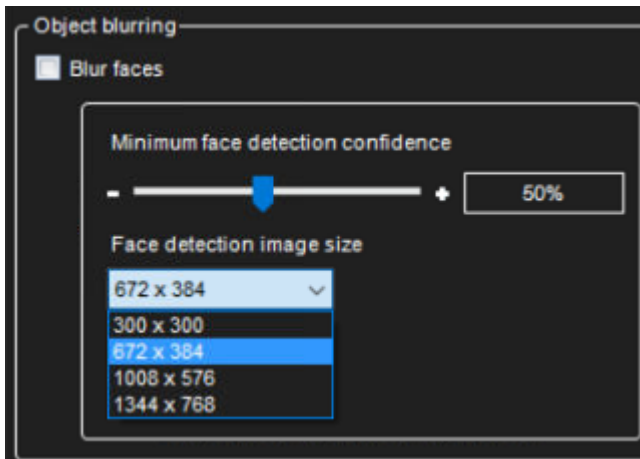
Minimum face detection confidence

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



Blur Moving objects

Motion detection sensitivity

How sensitively pixel in the image is detected as motion pixel

Background image detection history length

How quickly stationary objects are detected as background

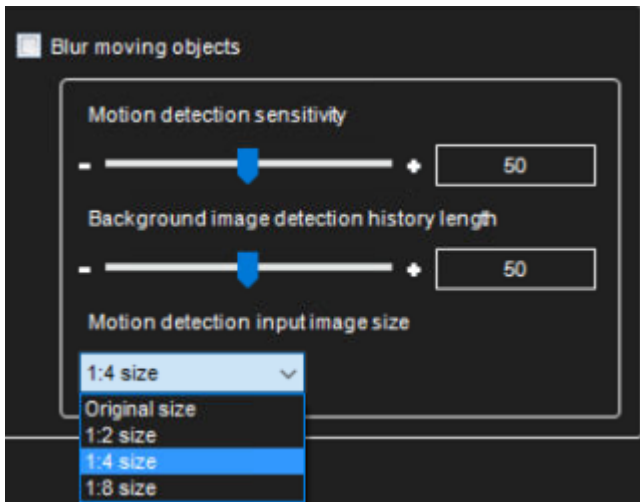
Motion detection input image size

The smaller size is quicker to process but outputs the worse results.

- Original size
- 1:2 size
- 1:4 size
- 1:8 size



Administrator Guide V9 - EN

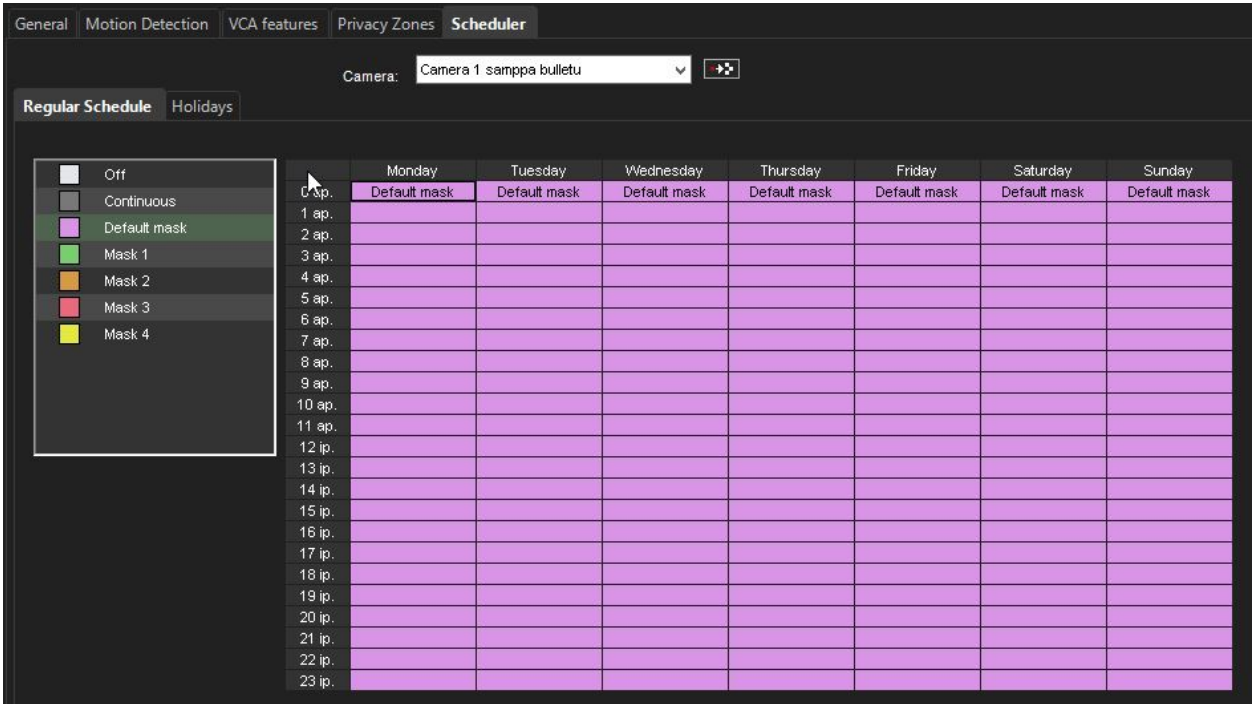


Administrator Guide V9 - EN

1.9.5.5. Scheduler

Scheduler defines which mask is used on each camera and what is active days and hours for the mask.

By default, video is recorded when the system detects motion in the default mask. The default mask is active 24/7.



	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
0 ap.	Default mask	Default mask	Default mask	Default mask	Default mask	Default mask	Default mask
1 ap.							
2 ap.							
3 ap.							
4 ap.							
5 ap.							
6 ap.							
7 ap.							
8 ap.							
9 ap.							
10 ap.							
11 ap.							
12 ip.							
13 ip.							
14 ip.							
15 ip.							
16 ip.							
17 ip.							
18 ip.							
19 ip.							
20 ip.							
21 ip.							
22 ip.							
23 ip.							

However, you can set different options for each hour of the week. For example, use different motion detection masks during the day and the night.

First, set the regular weekly schedule on the **Regular Schedule** tab and then, if necessary, set holiday schedules on the **Holidays** tab.

To change the schedule, click on the mask you want to activate, and then click on the scheduled hour where you want it to be used.

Tip: To change more than one hour at the same time, drag with the mouse.

You can also 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).

Administrator Guide V9 - EN

These options are available:

- **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.

To copy the current schedule for all cameras:

You can copy the currently selected recording schedule for all cameras in the system.



1. Click **Copy Schedule**
2. When asked for confirmation, click **OK**.

An exception days settings allow you to set holidays to the calendar.

To set an exception day schedule:

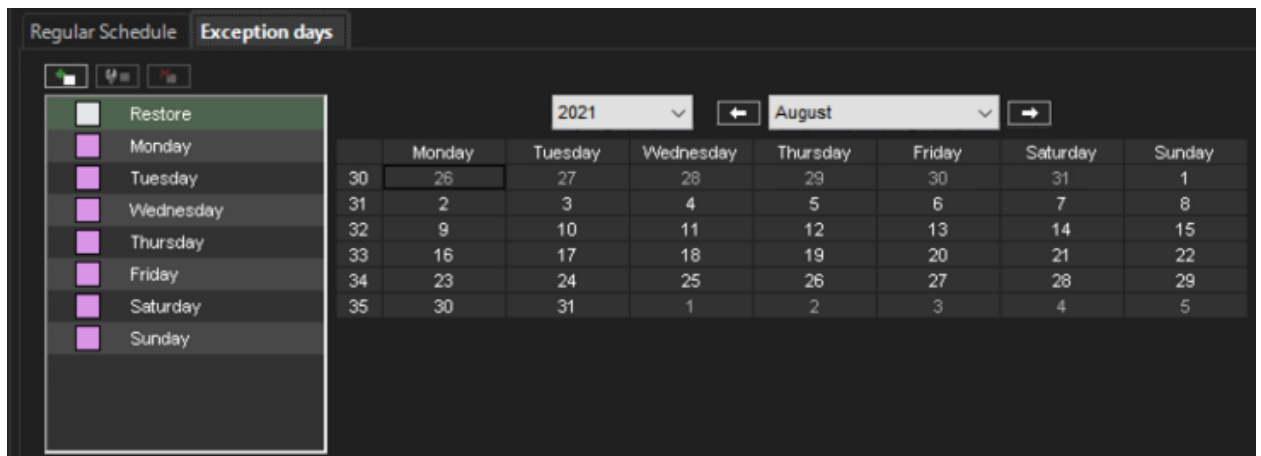
You can use different recording schedules for holidays.

You can apply a daily schedule from the **Regular Schedule** or use an **Exception days** schedule.

1. On the **Exceptions days** tab, select the year and month.
2. Click the schedule that you want to apply from the left panel and then click the holiday in the calendar.

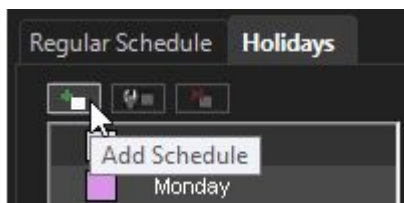


Administrator Guide V9 - EN



To add a custom schedule:

Click **Add Schedule**



1. Type a name for the schedule.
2. Click the mask you want to apply and then click the hours you want to apply the mask to.
3. Click **OK**.

To edit a custom schedule:

1. Select the schedule and click **Edit Schedule**.
2. Edit the schedule and click **OK**.

To delete a custom schedule:

- Select the schedule from the left pane and click **Delete Schedule**.

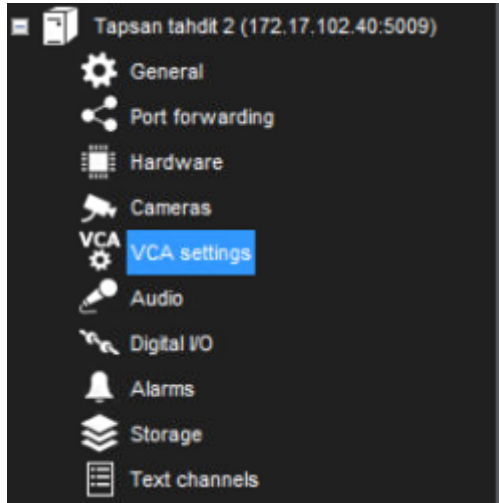
To restore the original schedule:

Click **Restore** and then click the day that you want to restore.



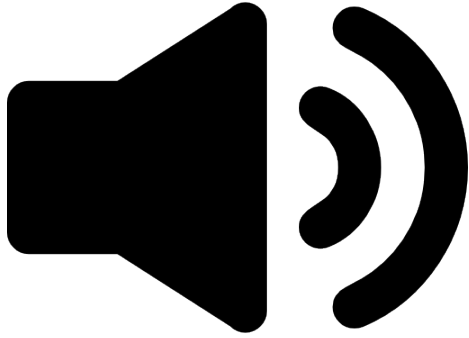
Administrator Guide V9 - EN

1.9.6. VCA settings





1.9.7. Audio



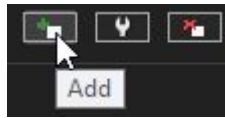
Administrator Guide V9 - EN

1.9.7.1. Adding, Editing and Removing Audio Devices

The system supports three basic types of audio components: one-way analogue 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.
7. 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.


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**.

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.

Administrator Guide V9 - EN

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.

Administrator Guide V9 - EN

1.9.7.2. Audio Settings

The system supports three basic types of audio components:

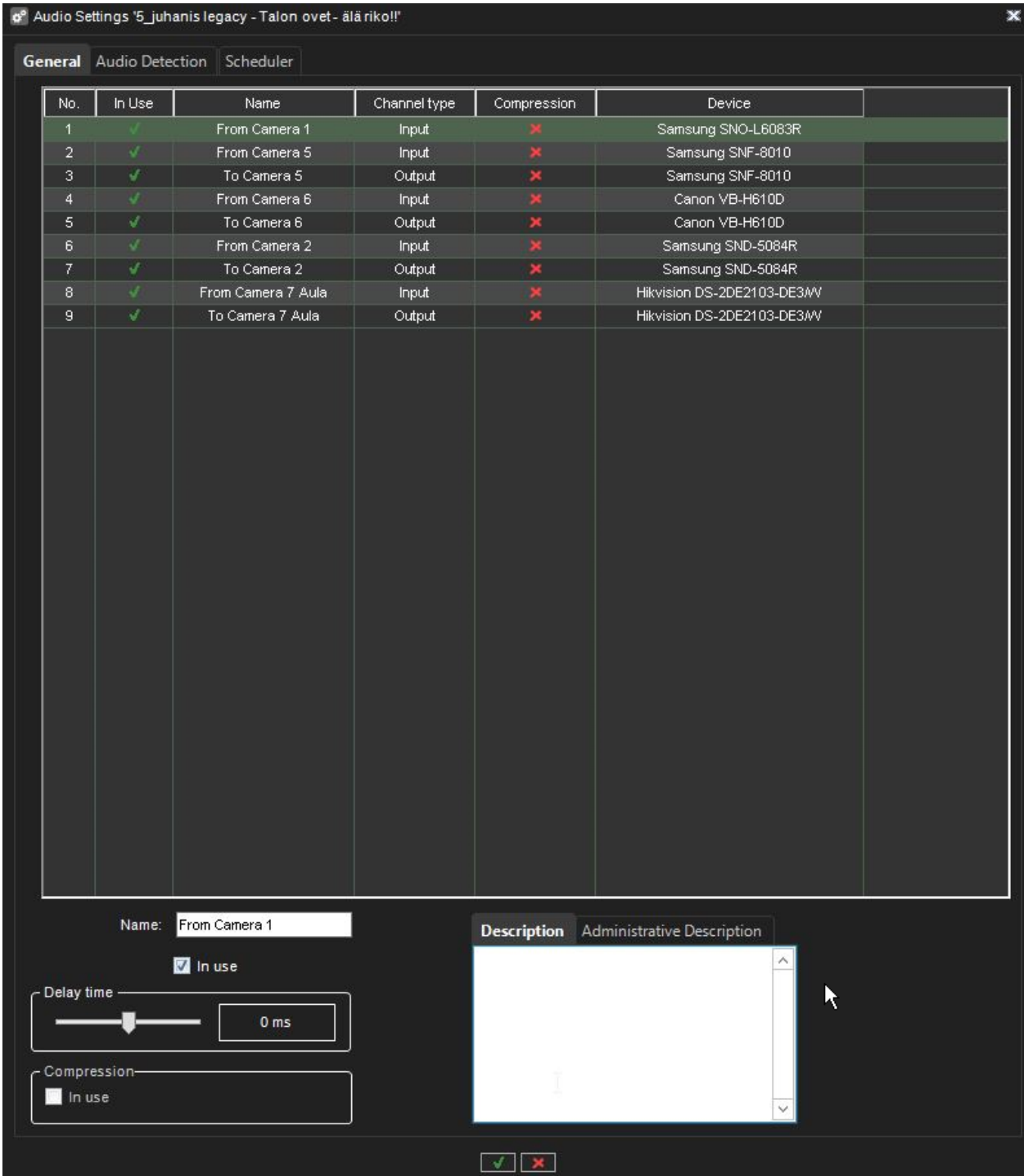
- **One-way analogue and IP audio channels:** These include mainly camera-based and separate microphones.
- **Two-way IP audio channels:** Two-way IP audio channels require an IP camera with an audio input and output channel.
 - Two-way IP audio channels are used for communication between the camera 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.

Administrator Guide V9 - EN

1.9.7.3. General Settings



Administrator Guide V9 - EN



Audio Settings '5_juhanis legacy - Talon ovet - älä rikoi!'

General Audio Detection Scheduler

No.	In Use	Name	Channel type	Compression	Device
1	✓	From Camera 1	Input	✗	Samsung SNO-L6083R
2	✓	From Camera 5	Input	✗	Samsung SNF-8010
3	✓	To Camera 5	Output	✗	Samsung SNF-8010
4	✓	From Camera 6	Input	✗	Canon VB-H610D
5	✓	To Camera 6	Output	✗	Canon VB-H610D
6	✓	From Camera 2	Input	✗	Samsung SND-5084R
7	✓	To Camera 2	Output	✗	Samsung SND-5084R
8	✓	From Camera 7 Aula	Input	✗	Hikvision DS-2DE2103-DE3W
9	✓	To Camera 7 Aula	Output	✗	Hikvision DS-2DE2103-DE3W

Name:

In use

Delay time: 0 ms

Compression: In use

Description Administrative Description

✓ ✗

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.

Administrator Guide V9 - EN

- **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**.

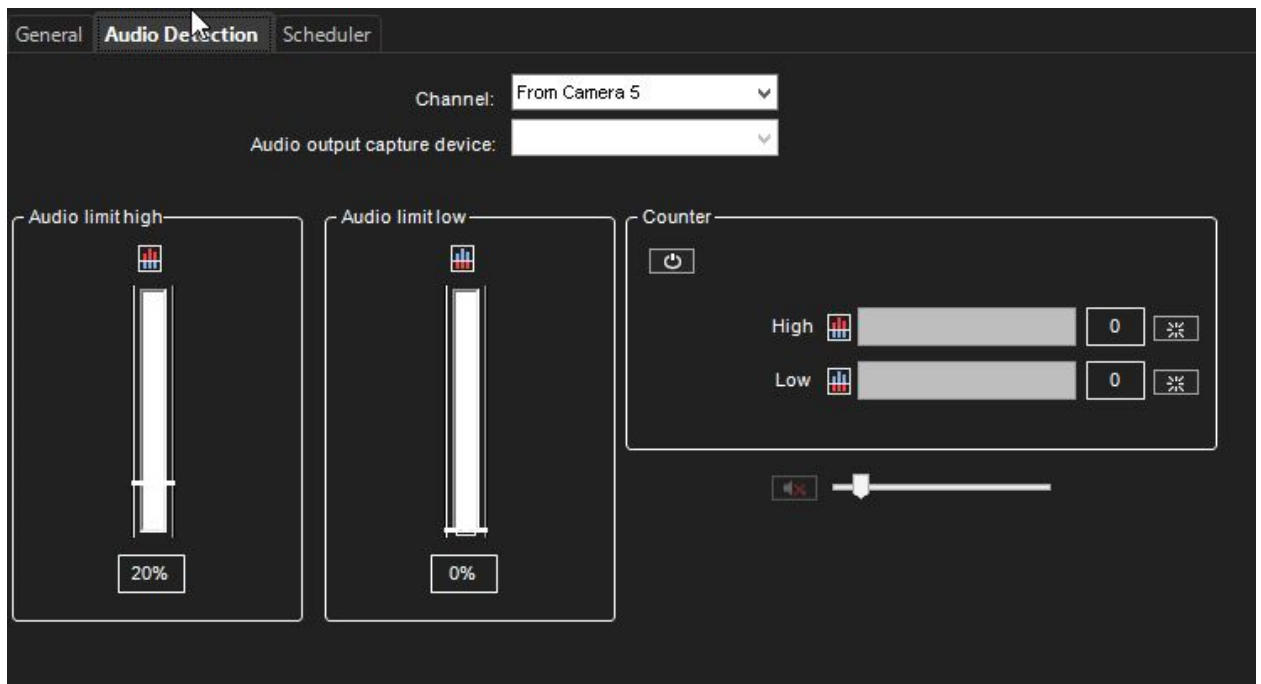
To change general settings:

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.



Administrator Guide V9 - EN

1.9.7.4. 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.

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

- info@mirasys.com

- www.mirasys.com

Administrator Guide V9 - EN

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.

Administrator Guide V9 - EN

1.9.7.5. Scheduler (Audio)

By default, audio is recorded when the detected level of audio exceeds the default detection limit (**Audio limit high**).

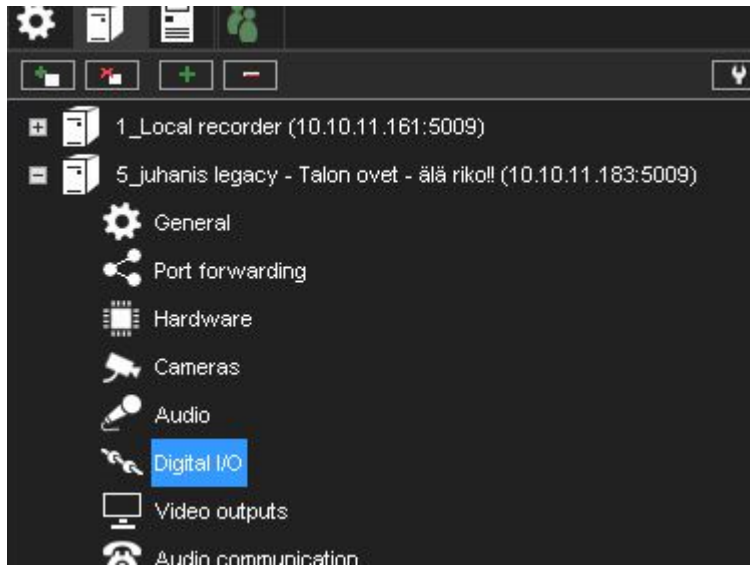
Similarly, to the video scheduler, it is possible to control the audio recording with the following options both for regular weeks and holidays.

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.



1.9.8. Digital I/O



Administrator Guide V9 - EN

1.9.8.1. Digital I/O Settings

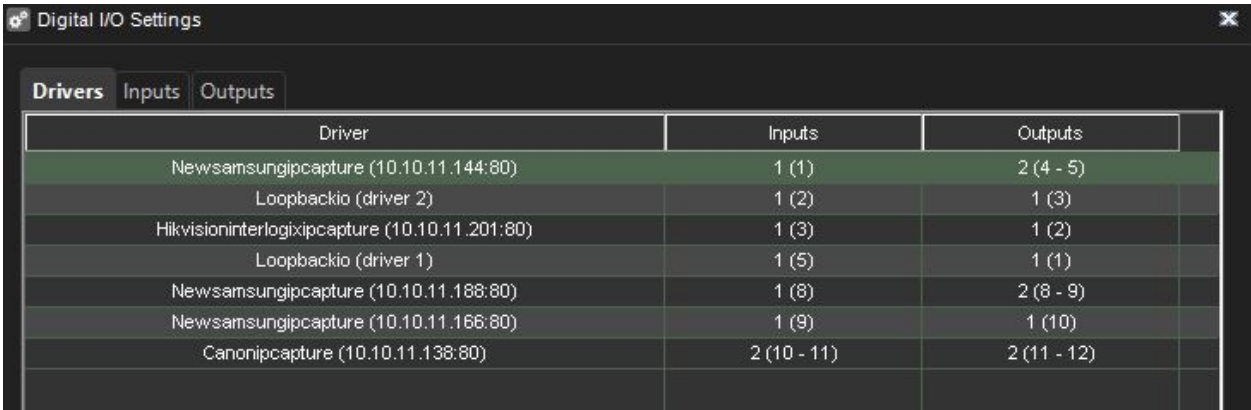
In **Digital I/O** settings, you can add digital input and output devices and configure the input and output settings.

These sections describe how to set up digital I/O devices.

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.

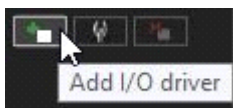
Once an I/O device driver has been added to the system, the device can be configured and taken into use through the **Drivers** tab.



Driver	Inputs	Outputs
Newsamsungipcapture (10.10.11.144:80)	1 (1)	2 (4 - 5)
Loopbackio (driver 2)	1 (2)	1 (3)
Hikvisioninterlogixipcapture (10.10.11.201:80)	1 (3)	1 (2)
Loopbackio (driver 1)	1 (5)	1 (1)
Newsamsungipcapture (10.10.11.188:80)	1 (8)	2 (8 - 9)
Newsamsungipcapture (10.10.11.166:80)	1 (9)	1 (10)
Canonipcapture (10.10.11.138:80)	2 (10 - 11)	2 (11 - 12)

To take an I/O device driver into use:

1. If necessary, install the device driver package.
2. Open the **VMS Servers** tab.



4. Select the correct server and open the **Digital I/O** page from the menu.
3. Click **Add I/O driver** in the lower right corner of the screen.
4. Select the driver from the **Model** drop-down menu.
5. Configure the device settings in the **Properties** list.
6. 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.

Administrator Guide V9 - EN

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:

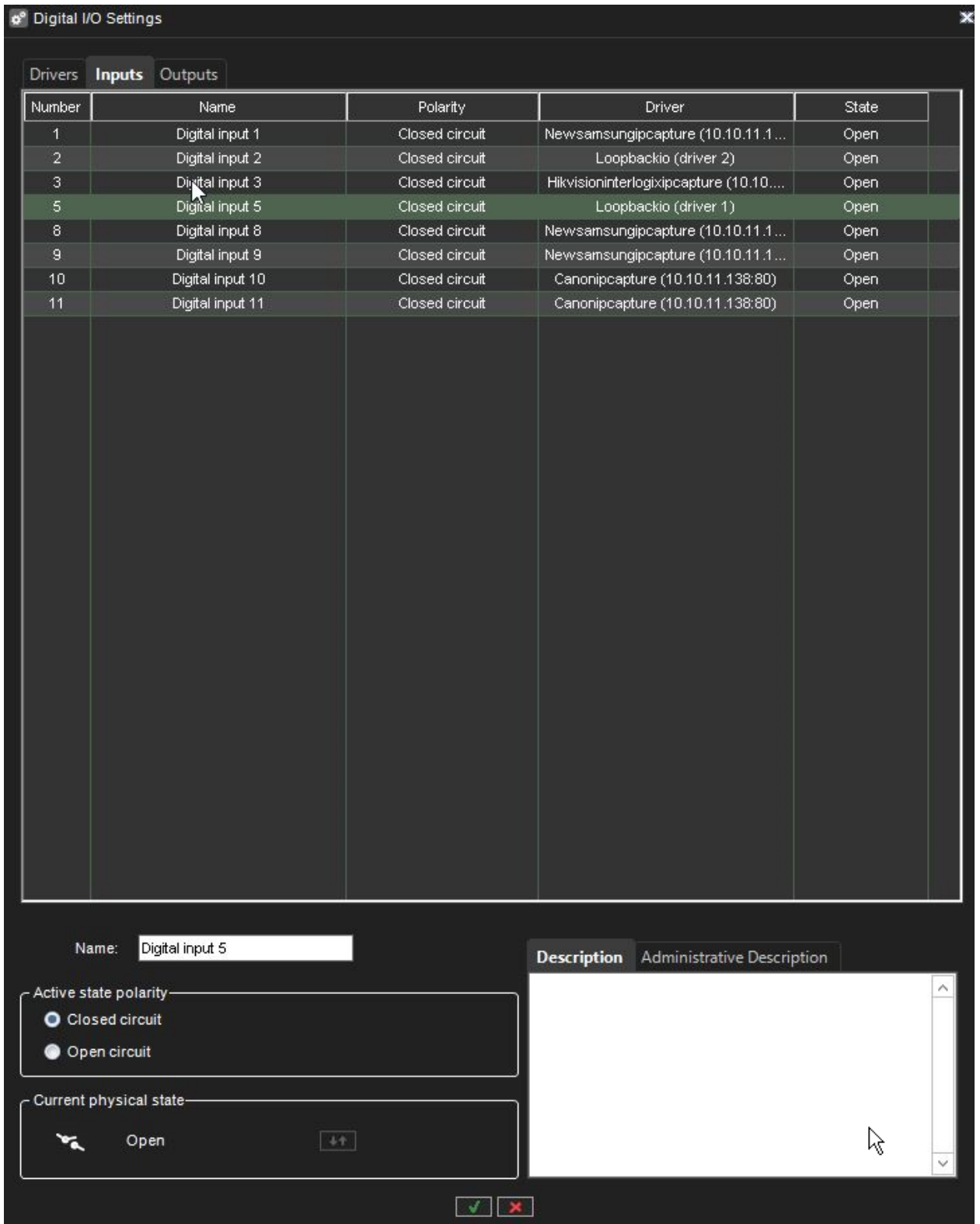
1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Click on the I/O device driver you want to delete.
4. Click **Delete I/O driver** in the lower right corner of the screen.
5. Click **Ok** to confirm the deletion.

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.

Administrator Guide V9 - EN



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:

Active state polarity

Closed circuit

Open circuit

Current physical state

 Open

Description Administrative Description

Name. To rename an input, select the input and then type a new name for the input in **Name**.

Administrator Guide V9 - EN

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.

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.

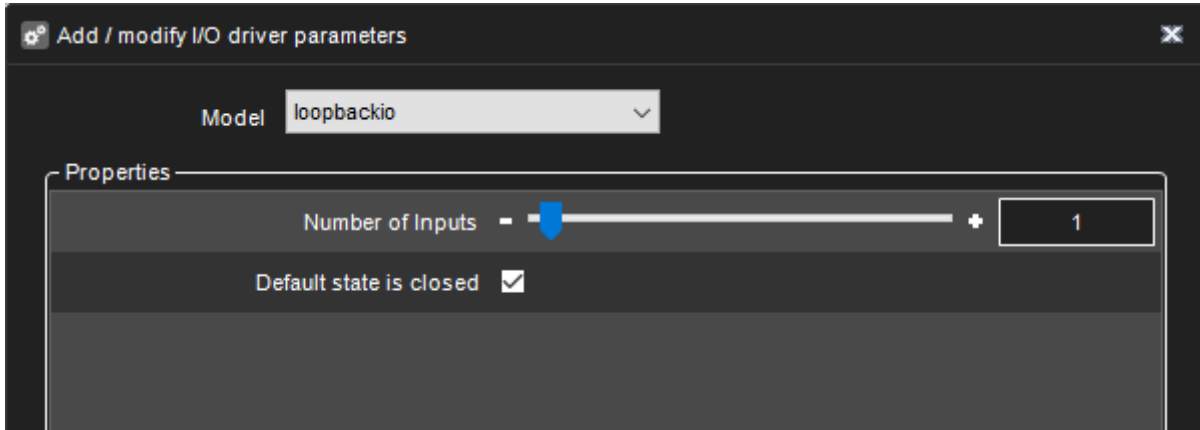
To test a digital output, click the **Change State (Toggle)** button.

Administrator Guide V9 - EN

1.9.8.2. 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.



Administrator Guide V9 - EN

1.9.8.3. 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.

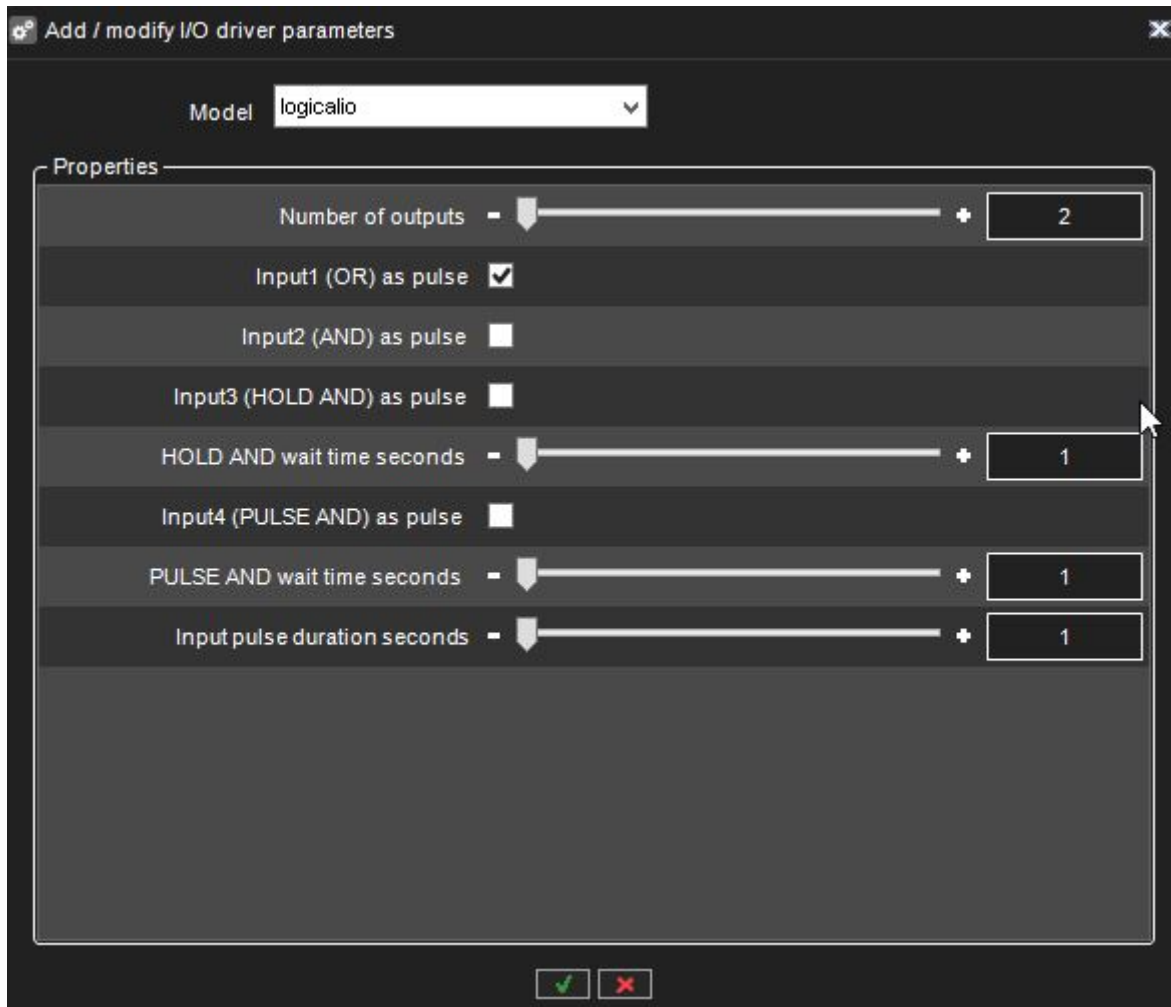
A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

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.



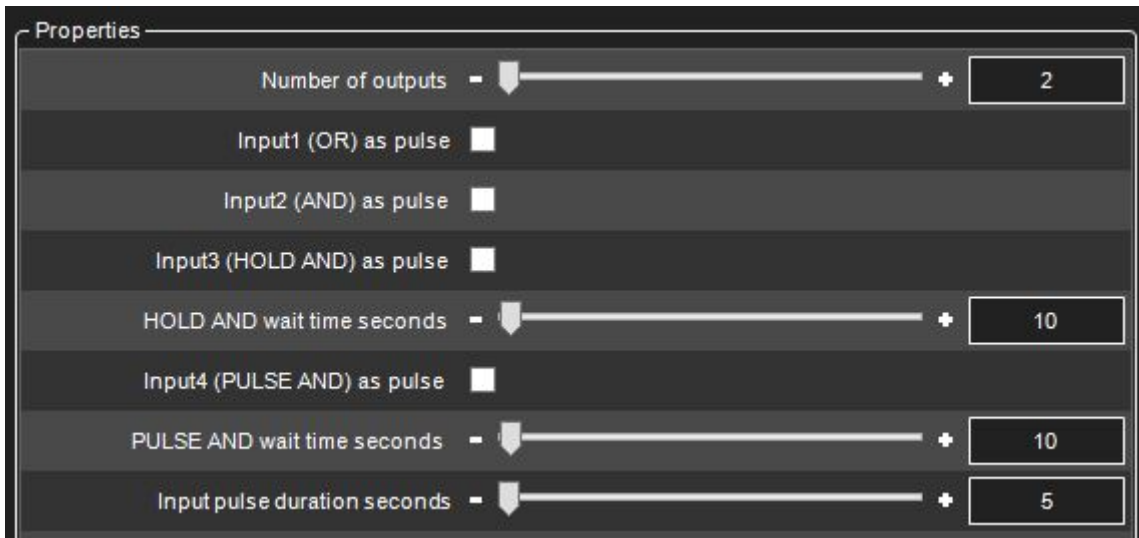
Administrator Guide V9 - EN



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:

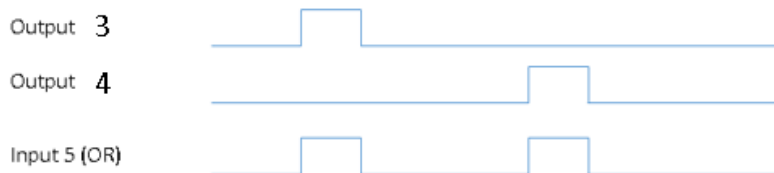


The example has 2 outputs that are the operands. These can be seen in the IO list as outputs 3 and 4.

The automatically created 4 inputs are seen in the list as inputs 5,6,7 and 8.

“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.



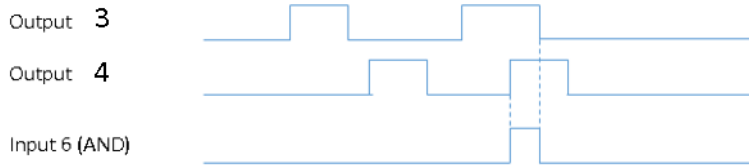
In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, input 5 will be turned on as a result.

Input will remain on as long as any of the outputs remains on. (Unless pulse mode is selected, see below for details)

“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.

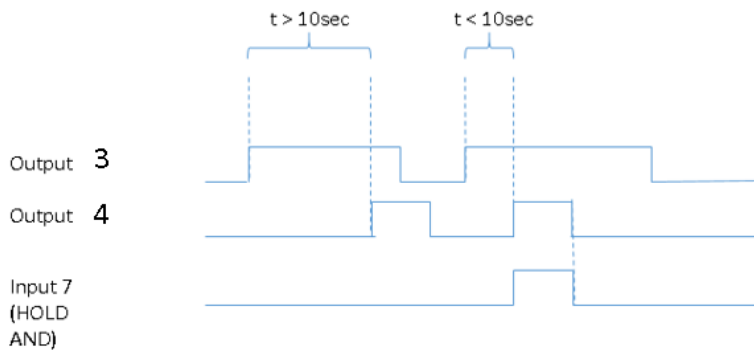
Administrator Guide V9 - EN



Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details)

“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.

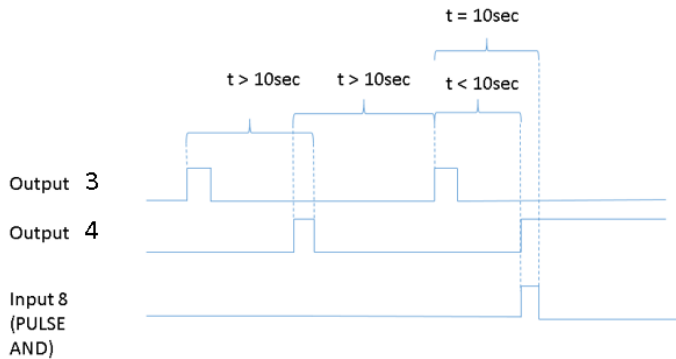
Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details)

“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.

Administrator Guide V9 - EN

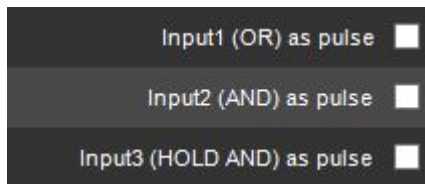


Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

In our example, when 10 seconds have elapsed from output 3 activation, input 8 will be turned off.

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.

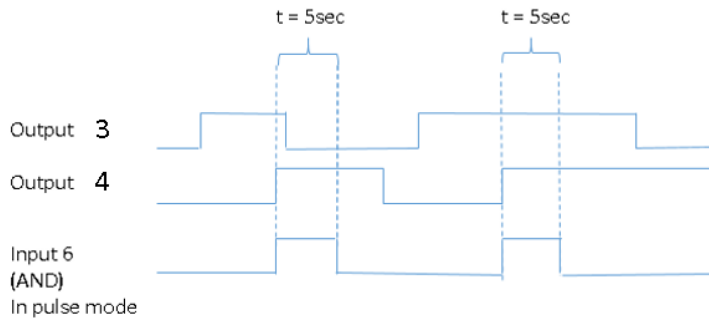
If in our example, we would set the AND input to be in pulse mode like this:



It would mean behaviour like this:



Administrator Guide V9 - EN



Administrator Guide V9 - EN

1.9.8.4. 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.

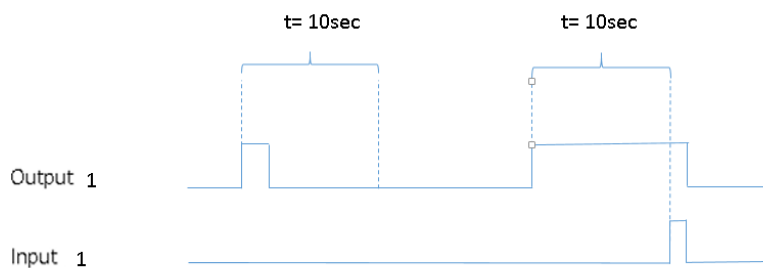
A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

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.

Expected Trigger Mode (Type 2)

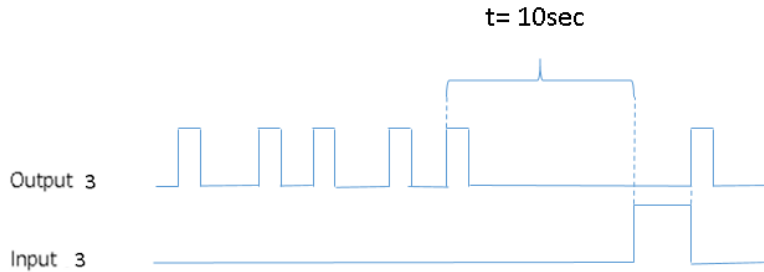
Secondly, it is possible to trigger an alarm if an expected pulse is not received inside the defined time.

For example, the time is 10 seconds, and we expect the regular operation to get pulses from output 3 every 2-3 seconds.



Administrator Guide V9 - EN

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.



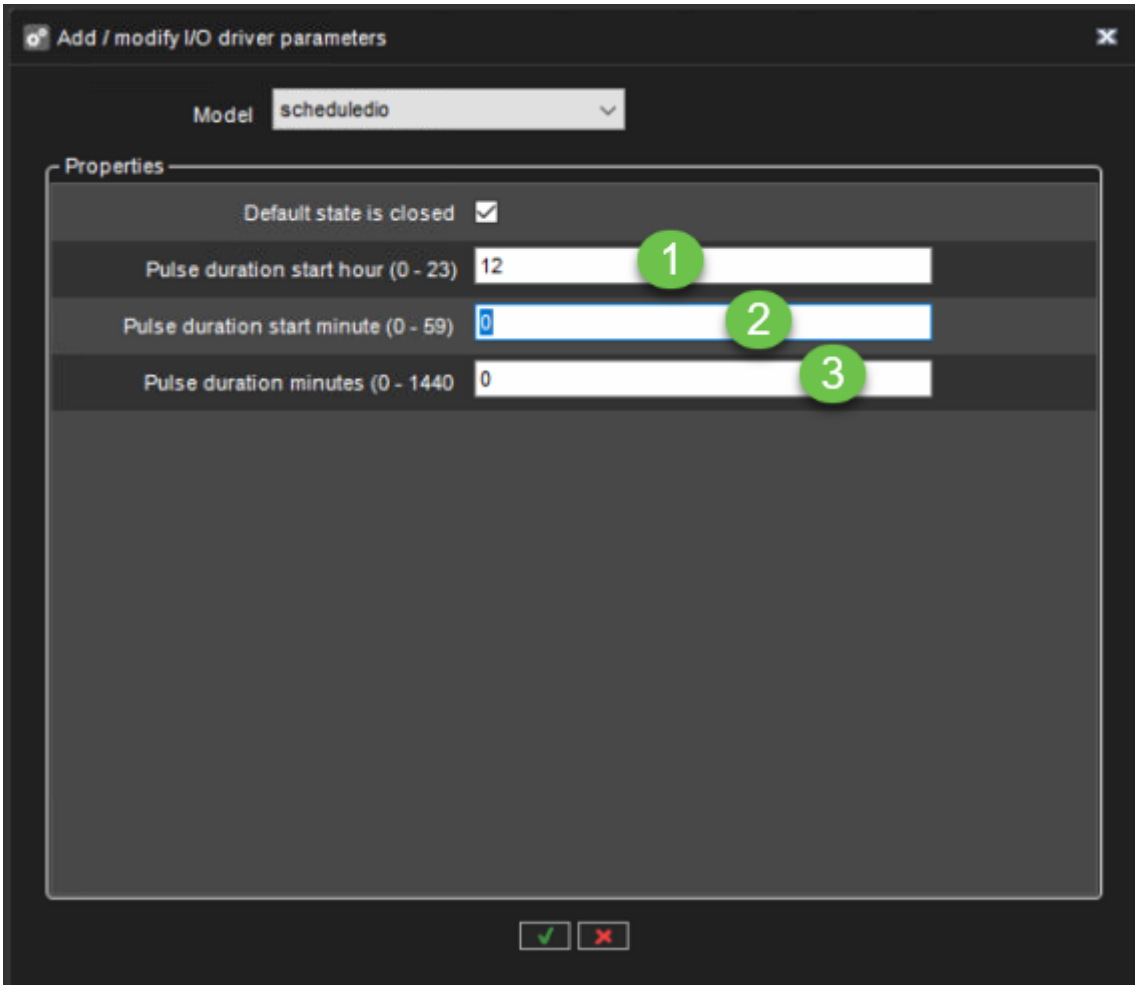
When creating a new Countdown I/O, the last input-output pair is of this type.

1.9.8.5. Scheduled IO

With the Scheduled IO is possible to create a schedule for any digital output, which are 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



Add / modify I/O driver parameters

Model **scheduledio**

Properties

Default state is closed

Pulse duration start hour (0 - 23) 1

Pulse duration start minute (0 - 59) 2

Pulse duration minutes (0 - 1440) 3



Administrator Guide V9 - EN

Digital I/O Settings

Drivers **Inputs** Outputs

Number	Name	Polarity	Driver	State
1	Digital input 1	Closed circuit	Wfsenetipcapture (172.19.100.106:...	Open
2	Digital input 2	Closed circuit	Wfsenetipcapture (172.19.100.107:...	Open
3	Digital input 3	Closed circuit	Wfsenetipcapture (172.17.100.74:80)	Open
4	Digital input 4	Closed circuit	Newboschcapture (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	Logiciallo (driver 1)	Open
8	LOGICAL INPUT AND	Closed circuit	Logiciallo (driver 1)	Open
9	LOGICAL INPUT BOTH ON 30s	Closed circuit	Logiciallo (driver 1)	Open
10	LOGICAL INPUT BOTH ON INSIDE 10s	Closed circuit	Logiciallo (driver 1)	Open
11	Digital input 11	Closed circuit	Ehipcapture (172.19.100.101:80)	Open
12	Digital input 12	Closed circuit	Ehipcapture (172.19.100.101:80)	Open
13	Digital input 13	Closed circuit	Ehipcapture (172.19.100.101:80)	Open
14	Digital input 14	Closed circuit	Ehipcapture (172.19.100.101:80)	Open
15	Digital input 15	Closed circuit	Ehipcapture (172.19.100.101:80)	Open
16	Digital input 16	Closed circuit	Ehipcapture (172.19.100.101:80)	Open
17	Digital input 17	Closed circuit	Ehipcapture (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 INPUT	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:

Active state polarity

Closed circuit

Open circuit

Current physical state

Closed

Description Administrative Description



1.9.8.6. HTTP IO

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



Administrator Guide V9 - EN

o Add / modify I/O driver parameters ✕

Model

Properties

HTTP Method (Opened)	<input type="text" value="GET"/>	<input type="button" value="Test"/>
URI (Opened)	<input type="text" value="http://"/>	<input type="button" value="Test"/>
Content (Opened)	<input type="text"/>	
User (Opened)	<input type="text" value="admin"/>	
Password (Opened)	<input type="password" value="....."/>	
Add Application Code (Opened)	<input type="checkbox"/>	
HTTP Method (Closed)	<input type="text" value="GET"/>	
URI (Closed)	<input type="text" value="http://"/>	<input type="button" value="Test"/>
Content (Closed)	<input type="text"/>	
User (Closed)	<input type="text" value="admin"/>	
Password (Closed)	<input type="password" value="....."/>	
Add Application Code (Closed)	<input type="checkbox"/>	

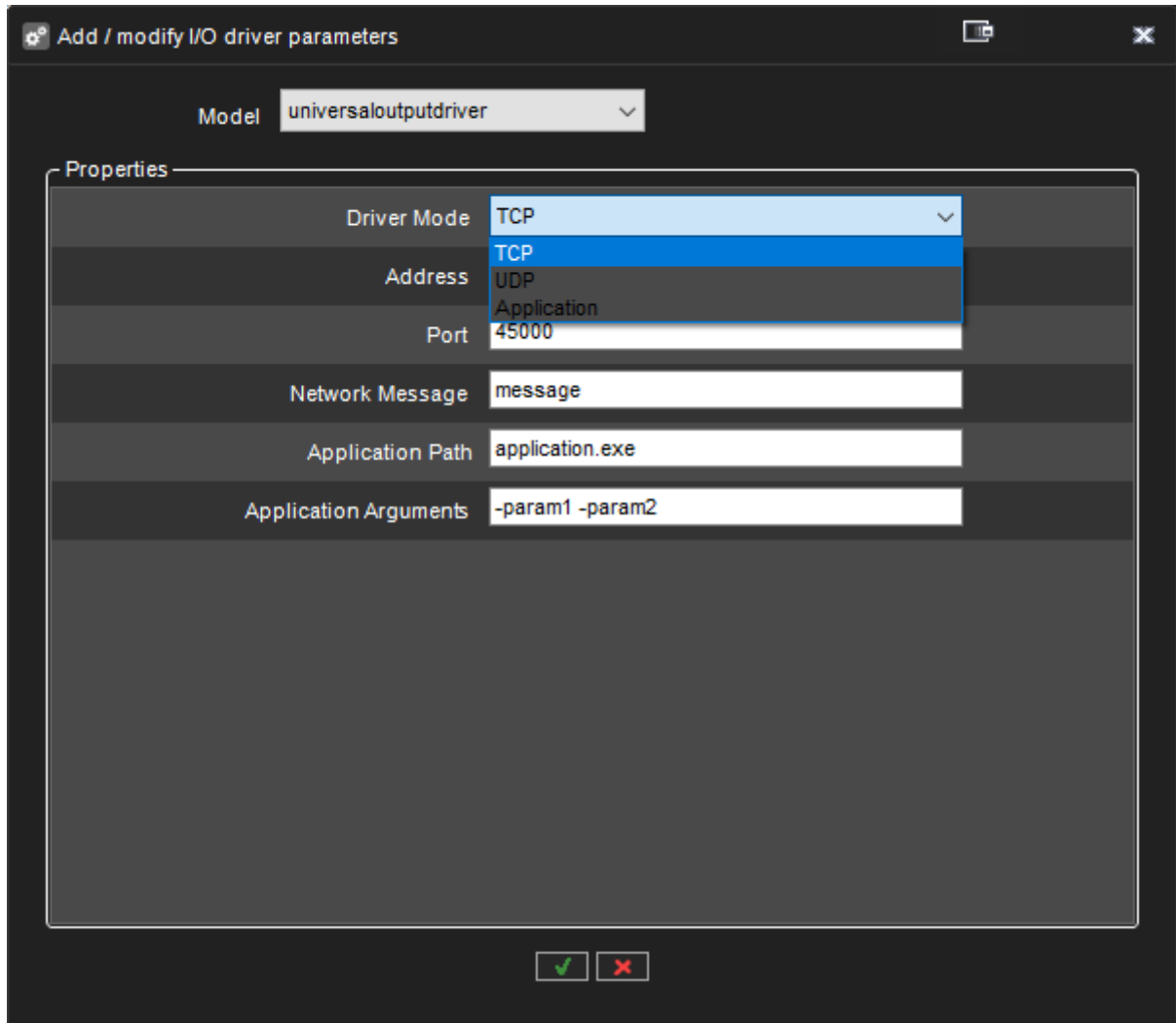


Administrator Guide V9 - EN

1.9.8.7. UniversalOutputDriver

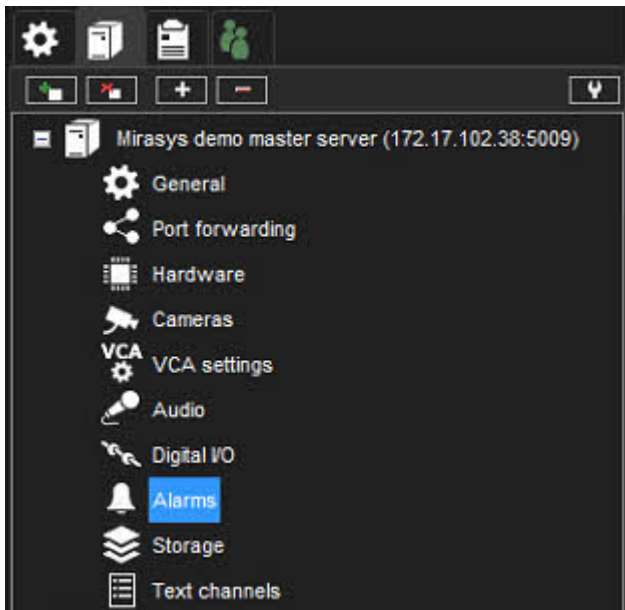
This driver enables you to send data to 3rd party systems or start applications on the server or remote systems.

Please see additional documentation for this driver from our extranet or contact support.





1.9.9. Alarms



Alarm Settings

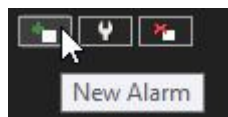
The alarm management tools enable the creation of server-specific alarms based on various triggers based on motion, sound level or specific text data triggers.

In addition, the triggers can include custom-made third-party triggers.

Alarms can be created, edited and deleted through the **Alarms** screen in the **VMS Servers** tab.

Adding a New Alarm

General



1. Click **New Alarm** at the lower-left corner of the **Alarms** screen.
2. Type the name of the new alarm in the **Name** field.
3. Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.

Administrator Guide V9 - EN

4. 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.
5. 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.
6. **Alarm highlight colour** allows administrators to define a custom colour for each alarm separately.
7. In the **View Alarms in Profiles** menu, select the profiles in which the alarm will be used. *Note: Alarms can also be added to profiles through the **Profiles** tab.*



Administrator Guide V9 - EN

The screenshot shows the 'Alarm Configuration' window with the following elements:

- 2**: Alarm name input field.
- 3**: Description text area.
- 4**: Priority selection (High, Normal, Low).
- 5**: Option 'The alarm is active until it is acknowledged'.
- 6**: Alarm highlight color selection (Use default color, Use custom color).
- 7**: Visible checkbox for the 'Mirasys AVM' profile in the 'View alarm in profiles' table.

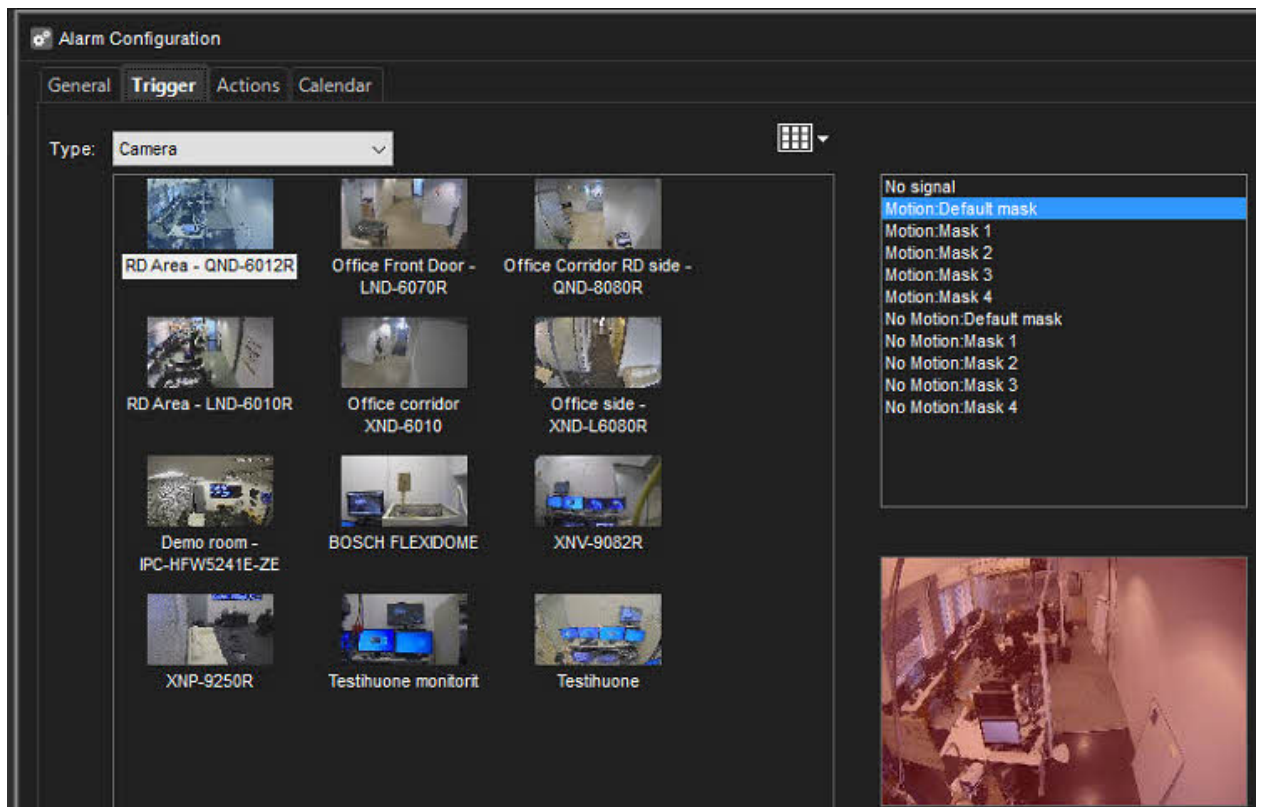
Visible	Profiles
<input type="checkbox"/>	Service
<input type="checkbox"/>	Demo
<input checked="" type="checkbox"/>	Mirasys AVM
<input type="checkbox"/>	Koulutus
<input type="checkbox"/>	BODYCAM

Trigger

- Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.



Administrator Guide V9 - EN



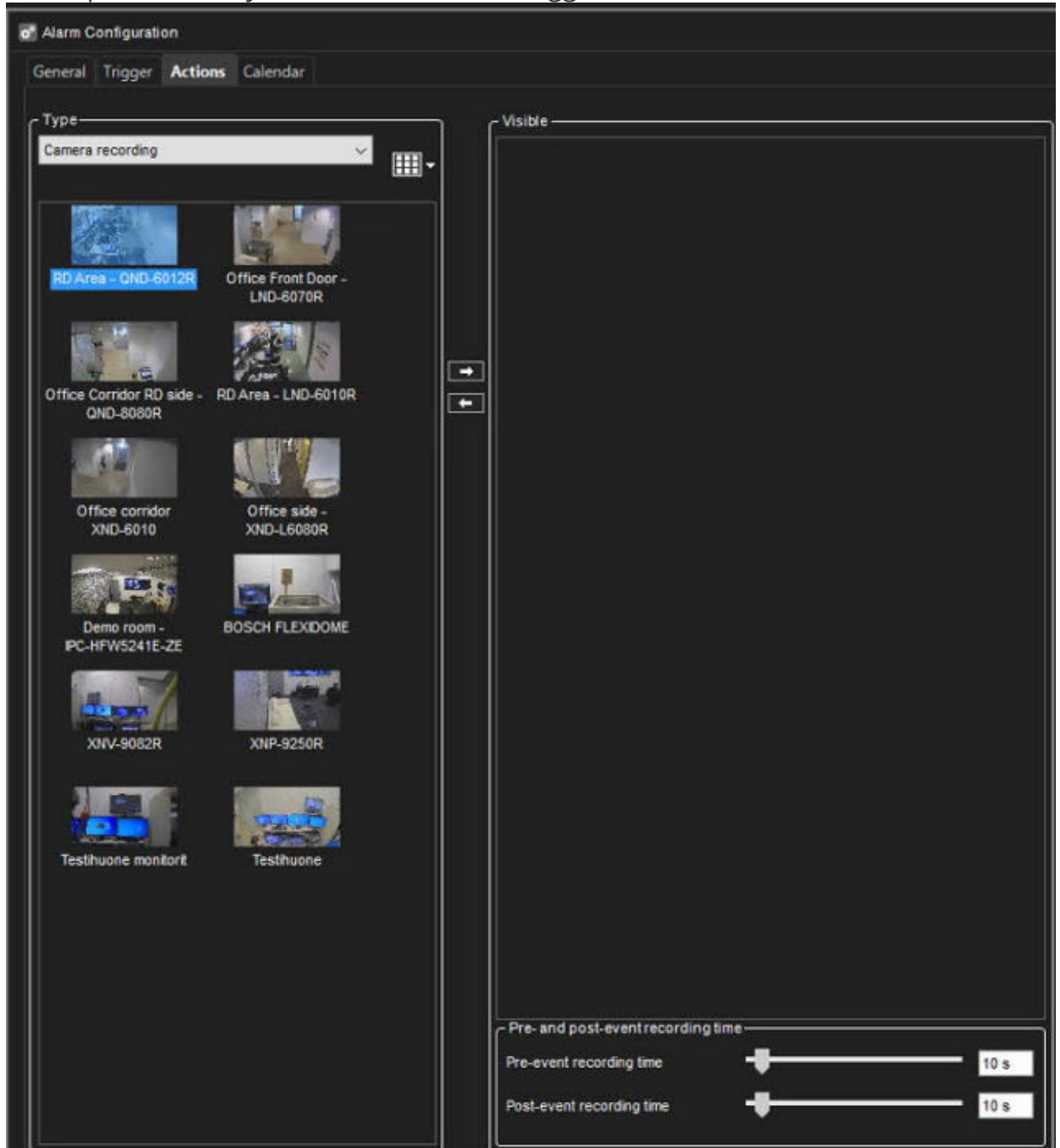
9. Select the trigger type from the **Type** drop-down menu.
 - i. Camera
 - j. Audio
 - k. Metadata
 - l. Text data
 - m. Digital input
10. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.
11. Select the triggering condition from the condition list on the right side of the screen.
 - i. For camera-based triggers, you can select the mask used in motion detection to trigger the alarm.
 - j. For audio-based triggers, you can set the alarm to trigger based on a high or low audio level.
 - k. 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.
 - l. For digital input-based triggers, the alarm is triggered based on the change of the input's polarity.



Administrator Guide V9 - EN

Actions

12. Open the **Actions** tab. The **Actions** tab is used to define the actions performed by the alarm when it is triggered.



13. Select the action type from the **Type** drop-down menu. The action type defines the basic functionality of the alarm.

Action Types and Settings

Administrator Guide V9 - EN

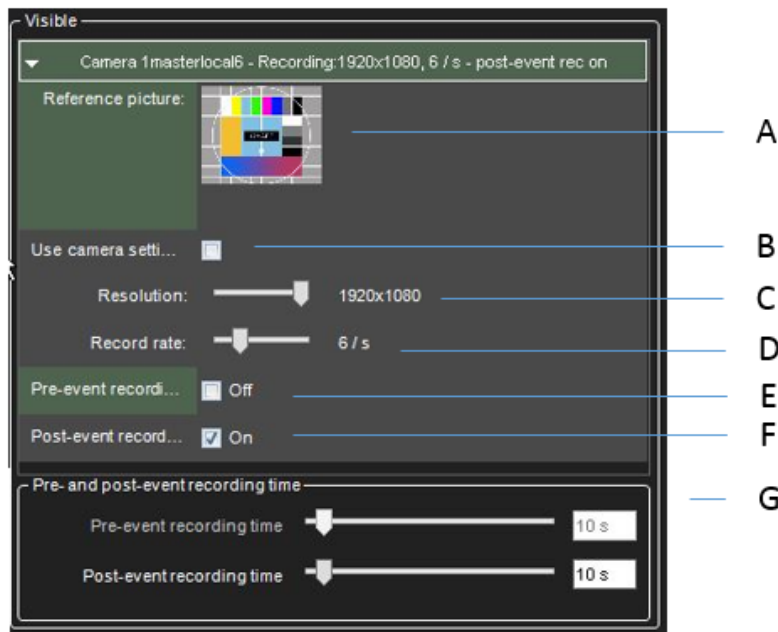
The list below contains the default action types and their parameters. Some of the action types listed above may not be available on all systems.

Note: In addition to the default actions, the system may include alarm actions installed through third-party modules.

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.



The action includes the following fields and parameters:

A) Reference picture. This static field contains the reference picture (image) of the camera.

B) Use camera settings. The alarm recording will be performed using the camera-specific resolution and record rate setting by marking this checkbox.

C) Resolution. Use the slider to change an IP camera's resolution during alarm recording. The slider is active only for IP cameras.

Administrator Guide V9 - EN

D) 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.

E) 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.

F) 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.

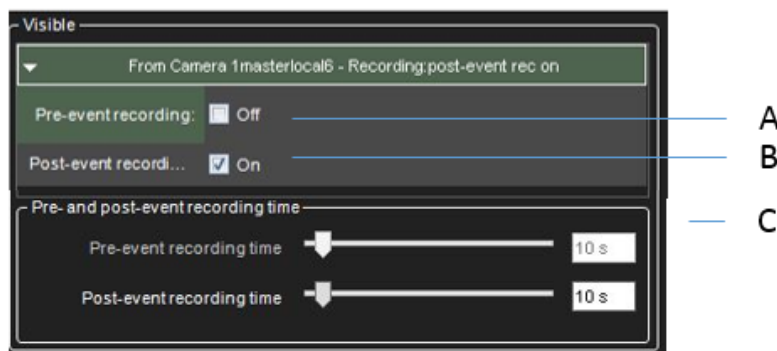
G) Pre- & post-event recording duration. These sliders can be used to set the pre- and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

Note 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.

Audio 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:



Administrator Guide V9 - EN

A) 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.

B) 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.

C) 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.

***Note:** 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.*

Digital output

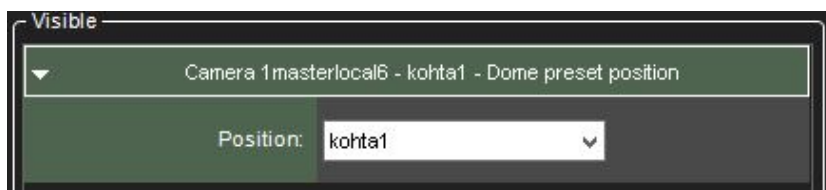
The **digital output** is the default action for digital I/O devices. When an alarm that contains this action type is triggered, the I/O device is activated.

***Note:** Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

PTZ (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 fields and parameters:

Administrator Guide V9 - EN

- **Position.** Use the drop-down menu to select the preset position to which the PTZ camera will move during the alarm.

Note: Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

PTZ (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 fields and parameters:

- **Program.** Use the drop-down menu to select the PTZ camera tour, starting when the alarm is triggered.

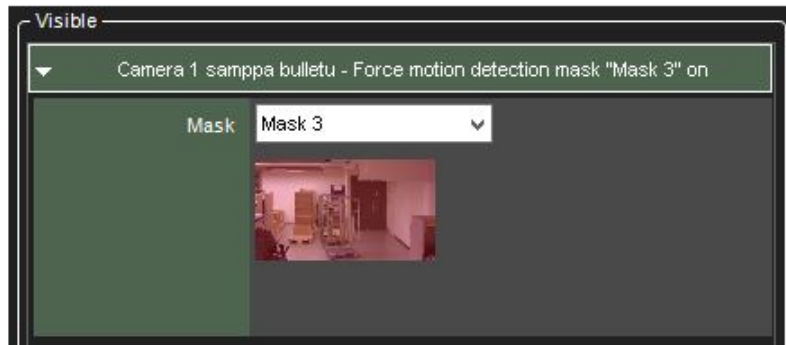
Note: Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

Set 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.



Administrator Guide V9 - EN



The action includes the following fields and parameters:

- **Mask.** Use the drop-down menu to select the motion detection mask that will be used during the alarm.

Note: Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.

Send 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



Administrator Guide V9 - EN

Visible

Send e-mail

To: 1 addresses, 1 groups

Format: Send in shortformat (max. 160 characters)

Message:

Attachments: Attach images ⓘ

From camera: Camera 2 support - sivu ovi

Limit image size to: Small

Maximum images: 3

Time before alarm: 1s

Time after alarm: 1s

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.

Note:

- 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 fields and parameters:

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).

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.

Note:



Administrator Guide V9 - EN

- 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.

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.

Calendar

14. Define that when the alarm is active

15. Click **OK**

Alarm Configuration

General Trigger Actions **Calendar**

Regular Schedule Exception days

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
0 ap.	On	On	On	On	On	On	On
1 ap.							
2 ap.							
3 ap.							
4 ap.							
5 ap.							
6 ap.							
7 ap.							
8 ap.							
9 ap.							
10 ap.							
11 ap.							
12 ip.							
13 ip.							
14 ip.							
15 ip.							
16 ip.							
17 ip.							
18 ip.							
19 ip.							
20 ip.							
21 ip.							
22 ip.							
23 ip.							

Holiday Schedules


Administrator Guide V9 - EN

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.


To set 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.


To create 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.

To edit 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.

To delete 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.

To restore the original schedule:

Administrator Guide V9 - EN

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.

Deleting an Alarm

To delete 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. The alarm is deleted from the system.

1.9.10. 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.

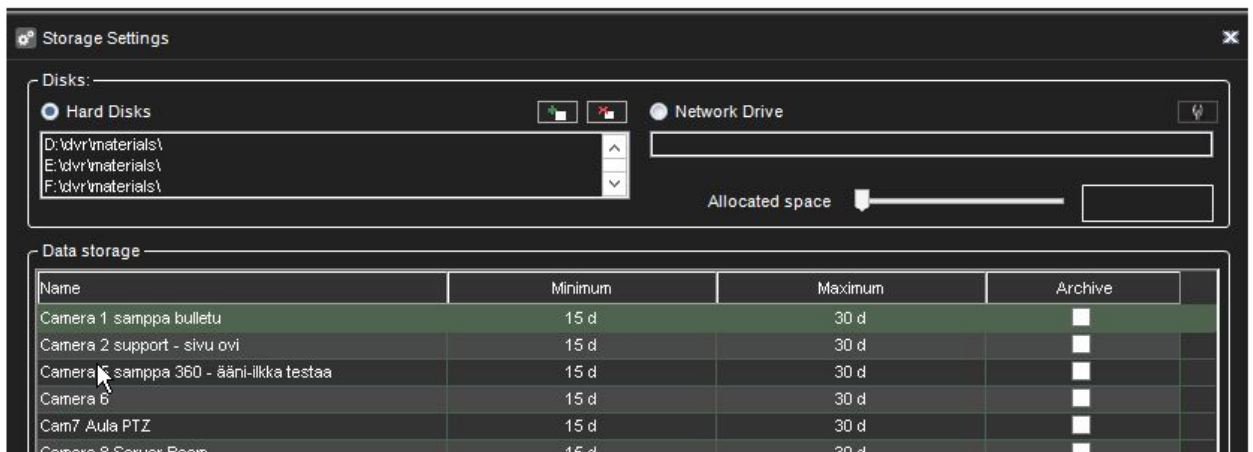
The storage settings are also used to configure the automatic archiving functionality, enabling the creation of backup copies of the server-specific video, audio, and text data daily or weekly.

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.

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.


Administrator Guide V9 - EN

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.


To add a hard disk:

1. Install the new disk.
2. In **Storage Settings**, click **Add Disk** . The Add Disk dialogue box is shown.
 - a. The **Minimum free space on the new disk box** shows how much free space the new disk must-have.
3. Select the disk from the list and click **OK**.

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.

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.

Video, audio and text data storage settings

Minimum

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

- info@mirasys.com

- www.mirasys.com

Administrator Guide V9 - EN

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.

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.*

Alarm limits

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.

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.

Log entries

This value specifies how many alarm events will be kept in the alarm log at the most.

Administrator Guide V9 - EN

The system examines the number of log entries hourly and deletes the oldest entries if they are exceeded.

% 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.

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**

Administrator Guide V9 - EN

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.

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.

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



Administrator Guide V9 - EN

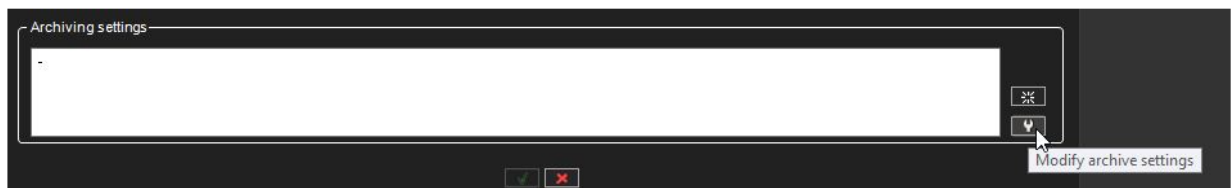
remove.

Note: *Selecting a device group (folder) also selects its contents.*

2. Mark the **Archive** checkbox.

Name	Minimum	Maximum	Archive
Camera 1 samppa bulletu	15 d	30 d	<input type="checkbox"/>
Camera 2 support - sivu ovi	15 d	30 d	<input type="checkbox"/>
Camera 5 samppa 360 - ääni-ilkka testaa	15 d	30 d	<input type="checkbox"/>
Camera 6	15 d	30 d	<input checked="" type="checkbox"/>
Cam7 Aula PTZ	15 d	30 d	<input type="checkbox"/>
Camera 8 Server Room	15 d	30 d	<input type="checkbox"/>
From Camera 1	15 d	30 d	<input type="checkbox"/>
From Camera 5	15 d	30 d	<input checked="" type="checkbox"/>
To Camera 5	15 d	30 d	<input type="checkbox"/>
From Camera 6	15 d	30 d	<input type="checkbox"/>

3. Click **Modify archive settings**





Administrator Guide V9 - EN

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

Data archiving settings

Archive password
Password:

Archiving start time
 Every day
 Once a week
 Archiving weekday: Sunday
 Archiving time: 0.00

Archiving directory
 VMS server directory

 Network directory

Archived period
 Previous day 0.00 Current day 0.00

 Starting from: Previous day 0.00 → Ending to: Current day 0.00 = Archive length: 1 d 0 h

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.

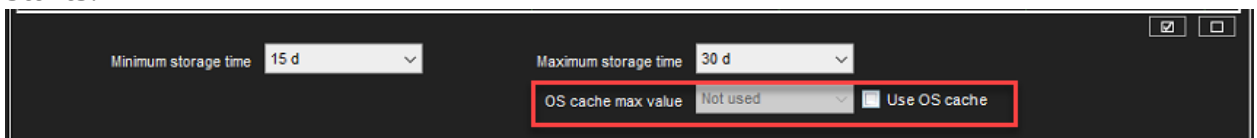
The last one helps to deal with unstable load to HDD and caching most used parts of data.

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.



1.9.11. Text Channels

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.

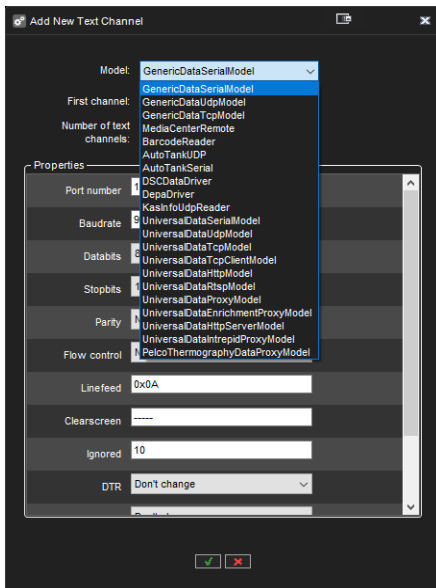
An additional document for UniversalData drivers can be downloaded from our extranet or contact support. This driver opens endless possibilities for integration to 3rd party systems.

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.




Administrator Guide V9 - EN




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.


To edit text channels:

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 a general description and an administrative description 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.
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.

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.

1.10. Profiles

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 Master 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.

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.

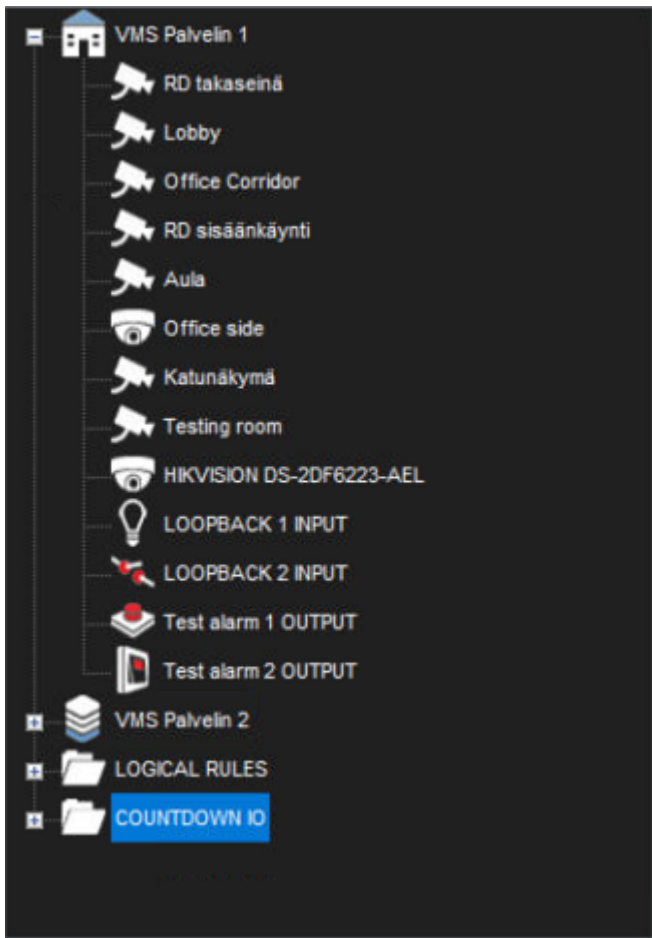
A *profile* sets a user's rights in the system. Each user can have 1 to 5 profiles that contain these *devices*:

- 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

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.



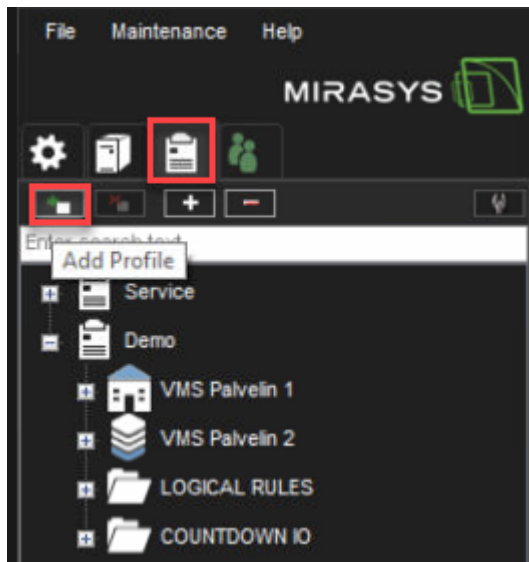
Administrator Guide V9 - EN



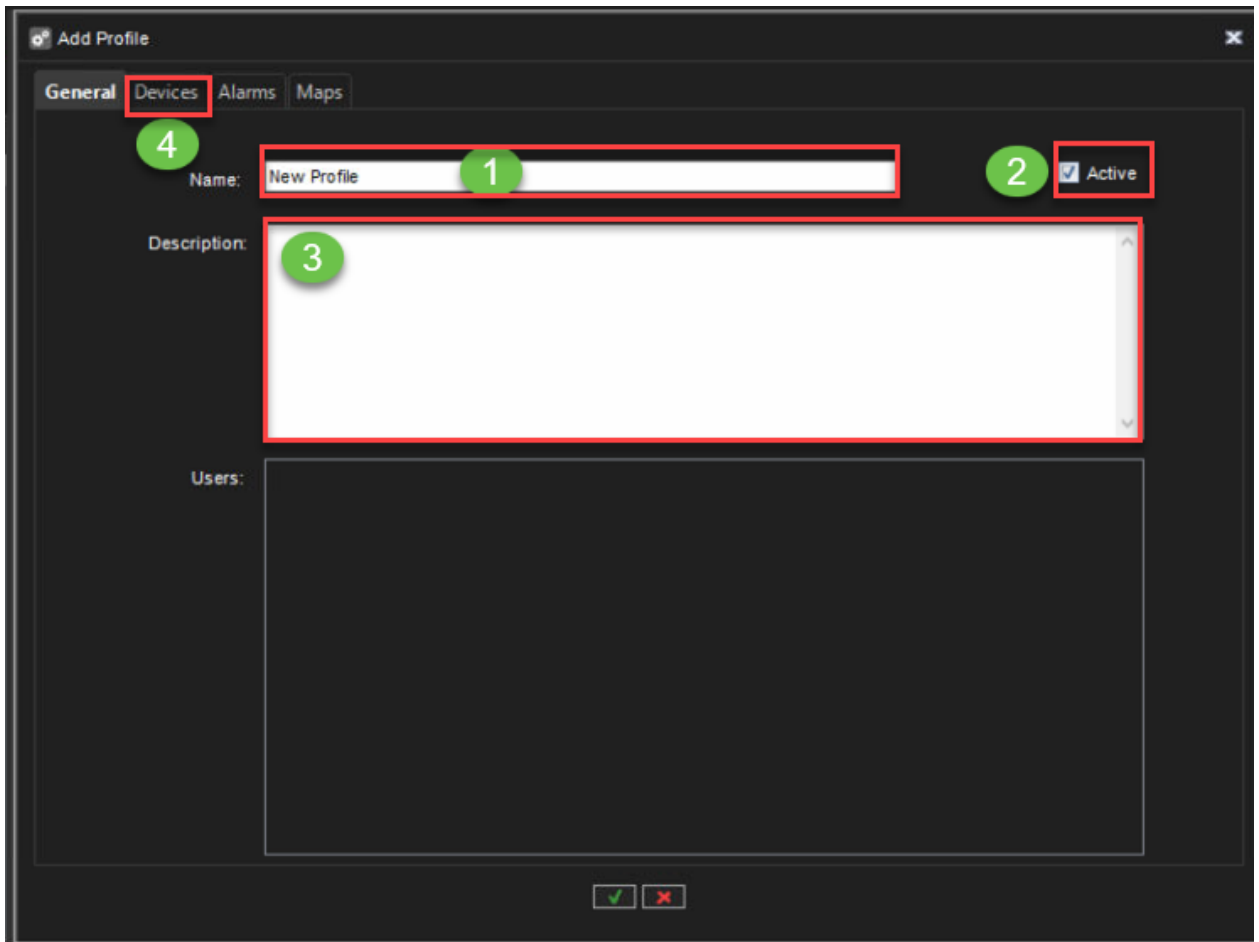
1.10.1. Creating a customer-specific profile

To add 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 System Manager
4. Open **Devices**

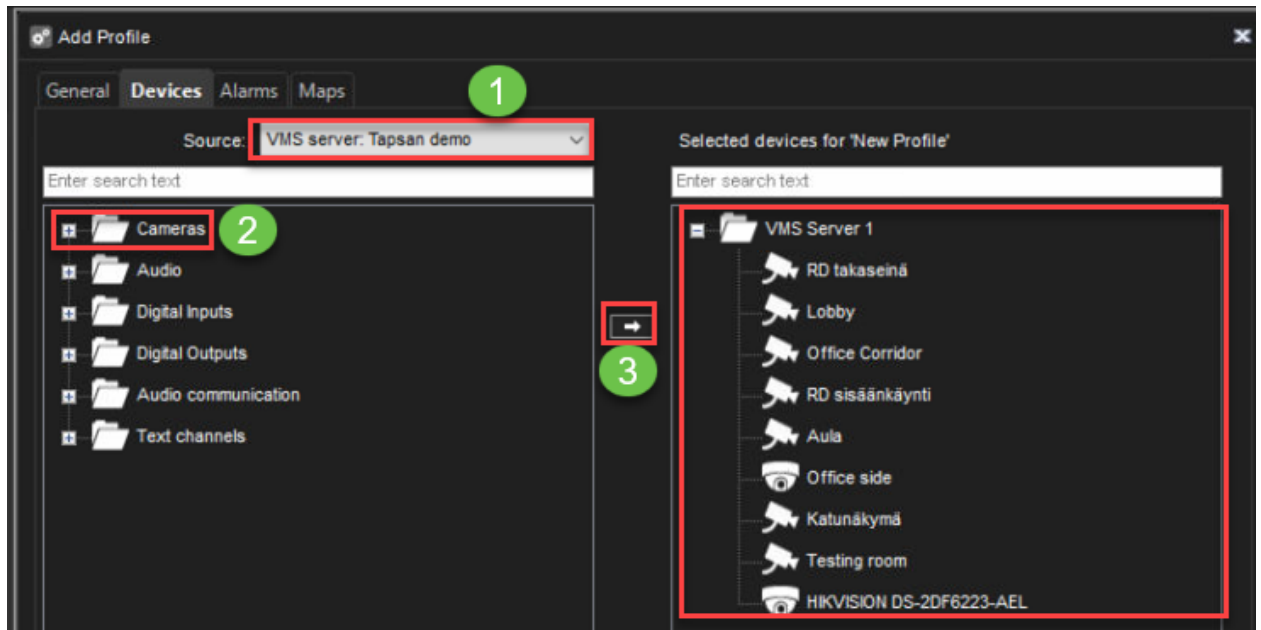


Devices

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**



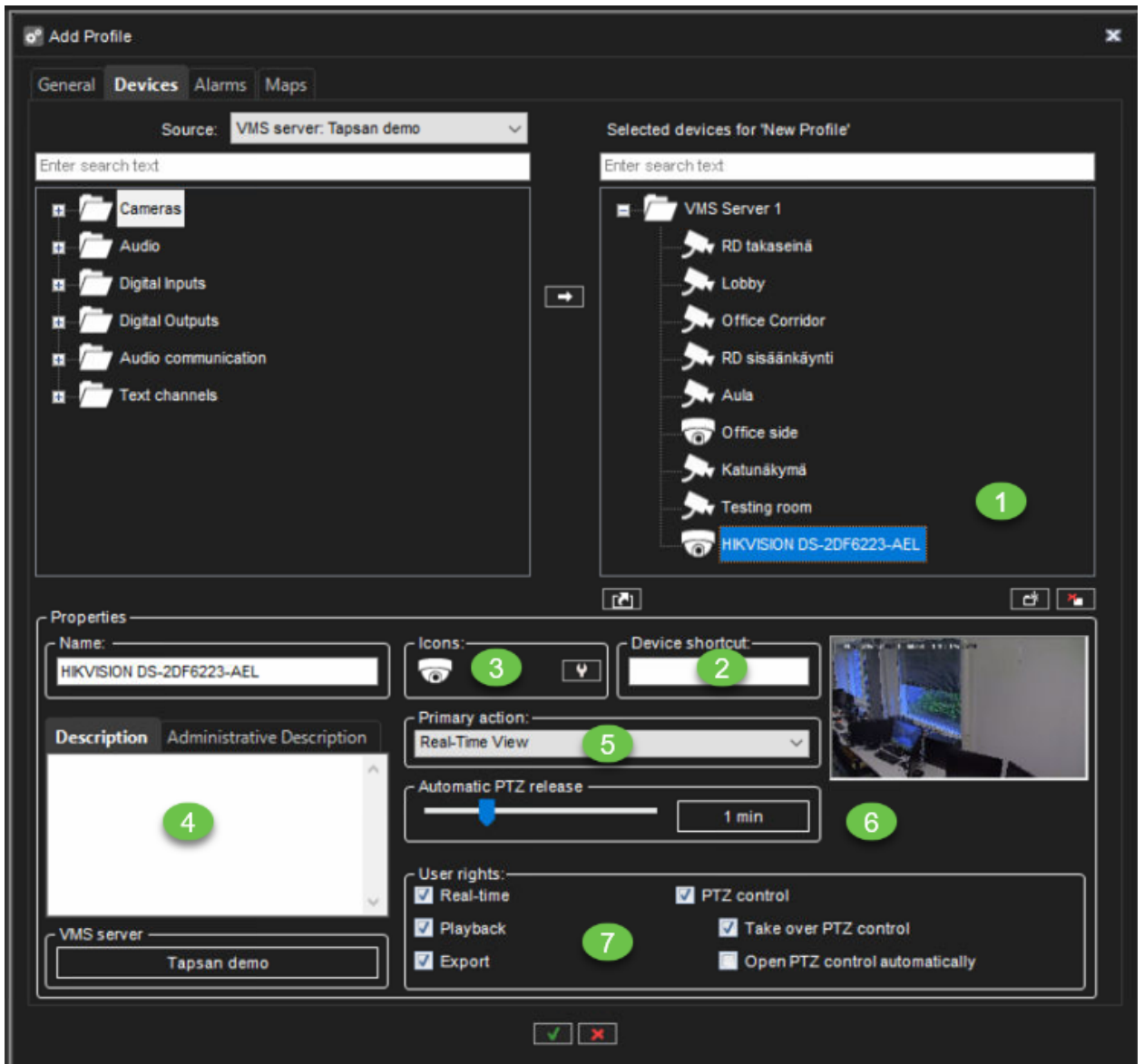
Administrator Guide V9 - EN



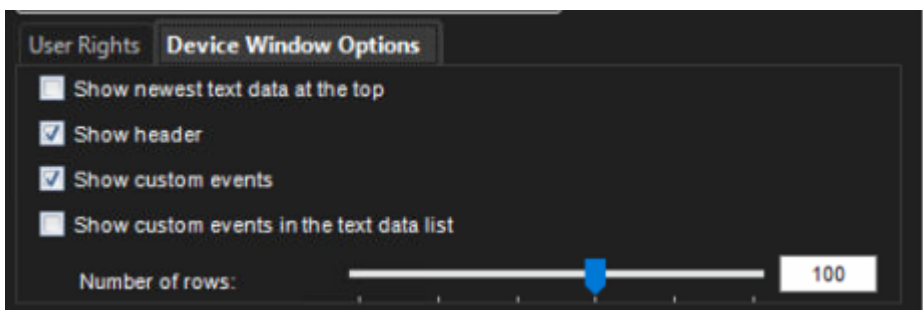
Selected Device Properties

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

Administrator Guide V9 - EN



Text channel Device Window Options



In Device Window Options, you can select how text data is shown to users. These options are available:

Administrator Guide V9 - EN

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.

Show header

Select to show identification data specified by the text data capture driver.

Show custom events

Select to show custom events specified by the text data capture driver.

Show custom events in the text data list

Select to show custom events in the text data list (instead of the custom event list).

The number of rows

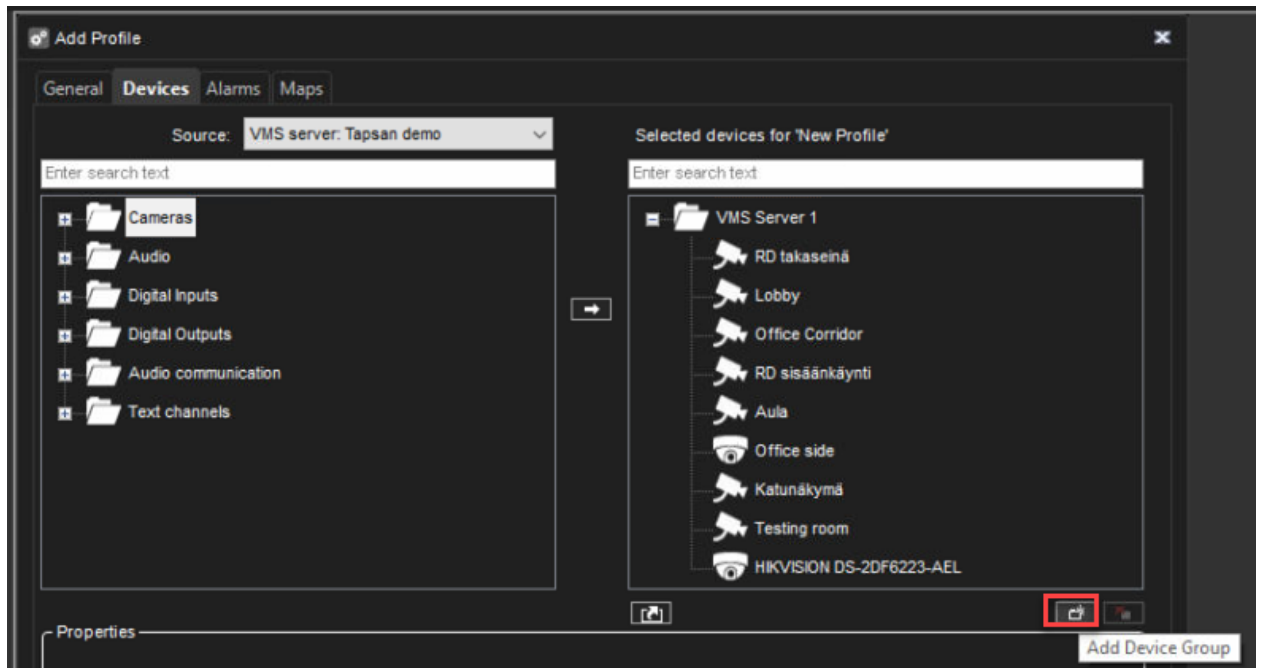
Specify the number of rows that are shown in the text data list at the most.

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.

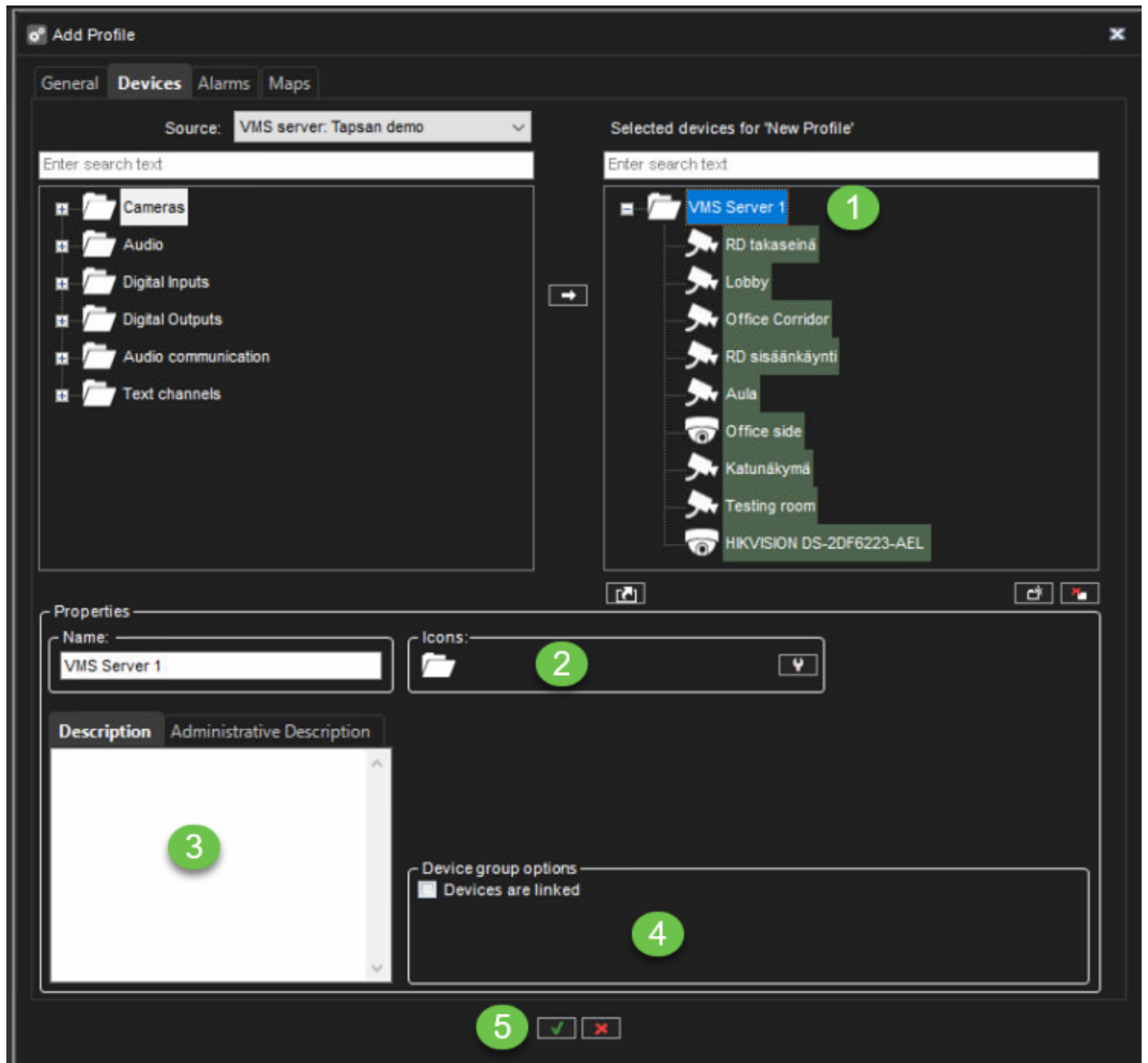


Administrator Guide V9 - EN



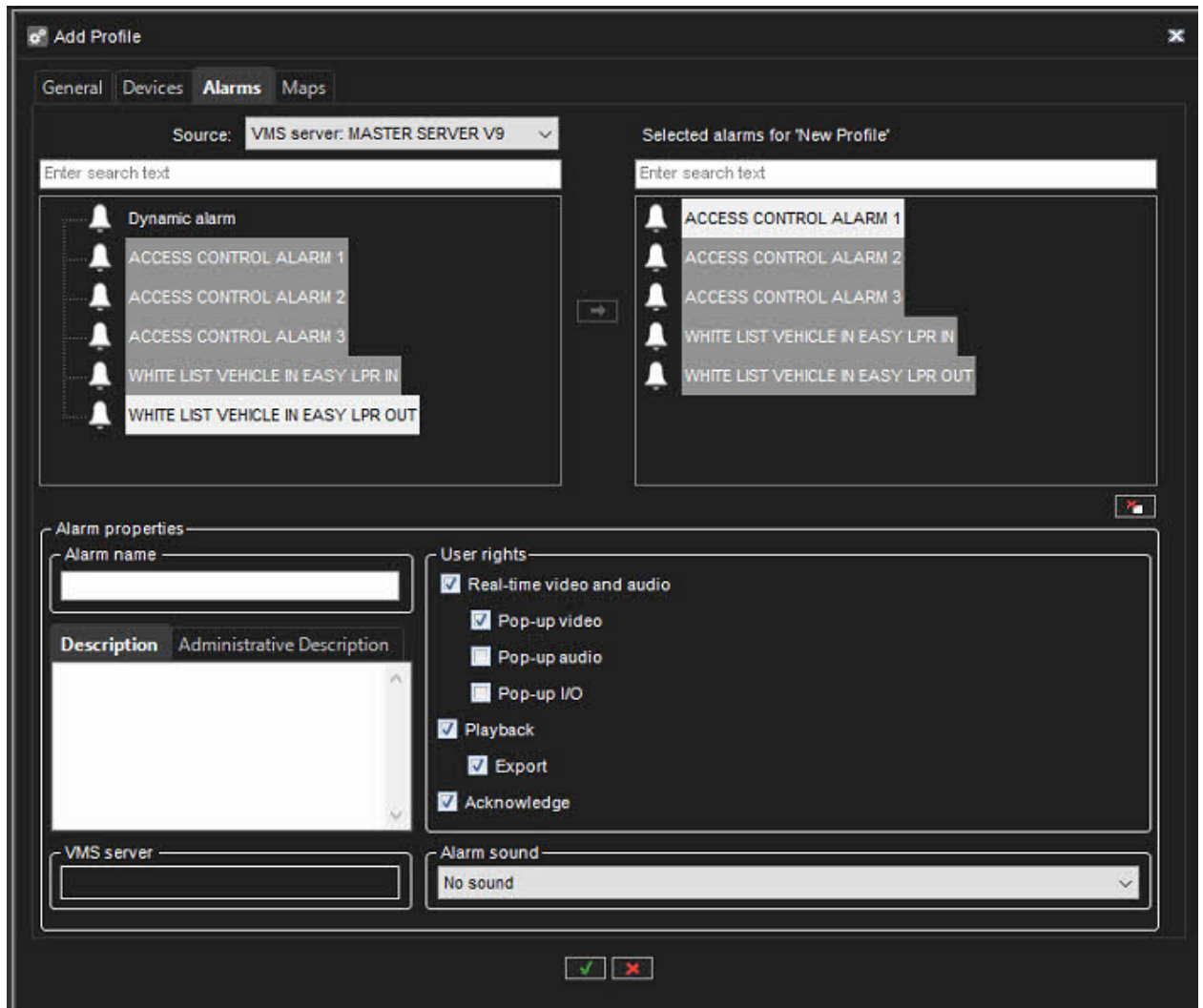
Note: A new device group is always added under the selected device group. To add a device group to the top level, make sure that none of the existing device groups is selected.

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).



Alarms

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.

To add 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.*

To edit profile-specific alarm user rights:



Administrator Guide V9 - EN

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.

Maps

Adding Maps to Profiles

To add a map:

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.
 - a. 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. Select the devices and device groups you want to add to the map from the left pane and click the **Add to Map** arrow.
 - a. 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.

Administrator Guide V9 - EN

- b. Users can move to a lower level map by double-clicking the subgroup icon.

Tip: To select more than one device 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. For cameras, you can select the direction that the camera icon points to.
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. If you need to fit several device icons in a small space, you can use placemarks.
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.

To remove a site map:

- Display the map that you want to remove and click **Remove Map**

To remove an icon from the map:

- Select the icon and click **Remove**

1.11. Users

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.

Logging Users Off

If you have administrative rights, you can log a user off from the Spotter program.

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.

Monitoring Users

The **Users** tab shows if users are logged on to the system:

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

-




info@mirasys.com

-

www.mirasys.com



Administrator Guide V9 - EN

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.

1.11.1. 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.



Administrator Guide V9 - EN

1.11.1.1. User Roles

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

General Active hours

Group name TEST1

Two factor authentication

In use

User roles

- System Manager Enterprise role
- Monitoring role
- Gateway role
- Mirasys Spotter Enterprise role
- Spotter Web role

Profiles

All profiles

Service

Group profiles

v9.4

→

←

✓ ✗



Administrator Guide V9 - EN

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300 - **info@mirasys.com** - **www.mirasys.com**



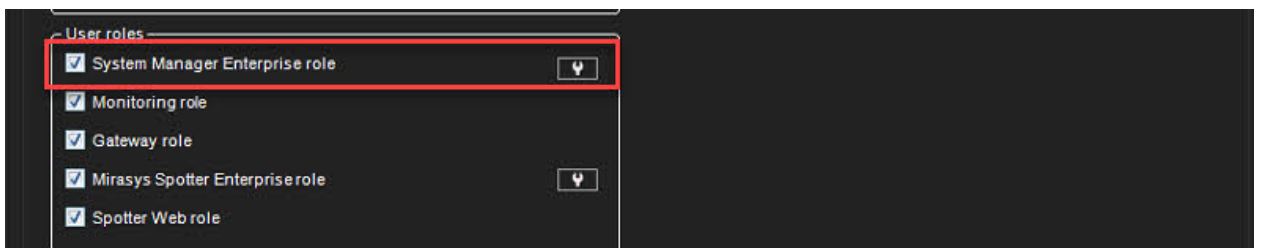
Administrator Guide V9 - EN

1.11.1.1.1. System Manager Enterprise role


It is possible to set explicit permissions for the system manager for different user groups.

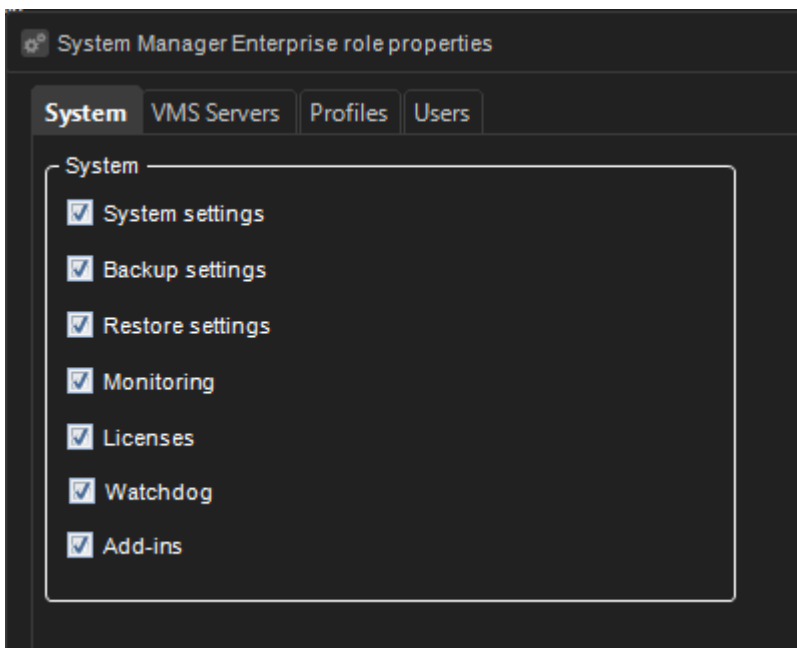
This allows, for instance, implementing functionality for allowing different user groups for hardware maintenance and user administration, which is helpful for large scale systems.

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.




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

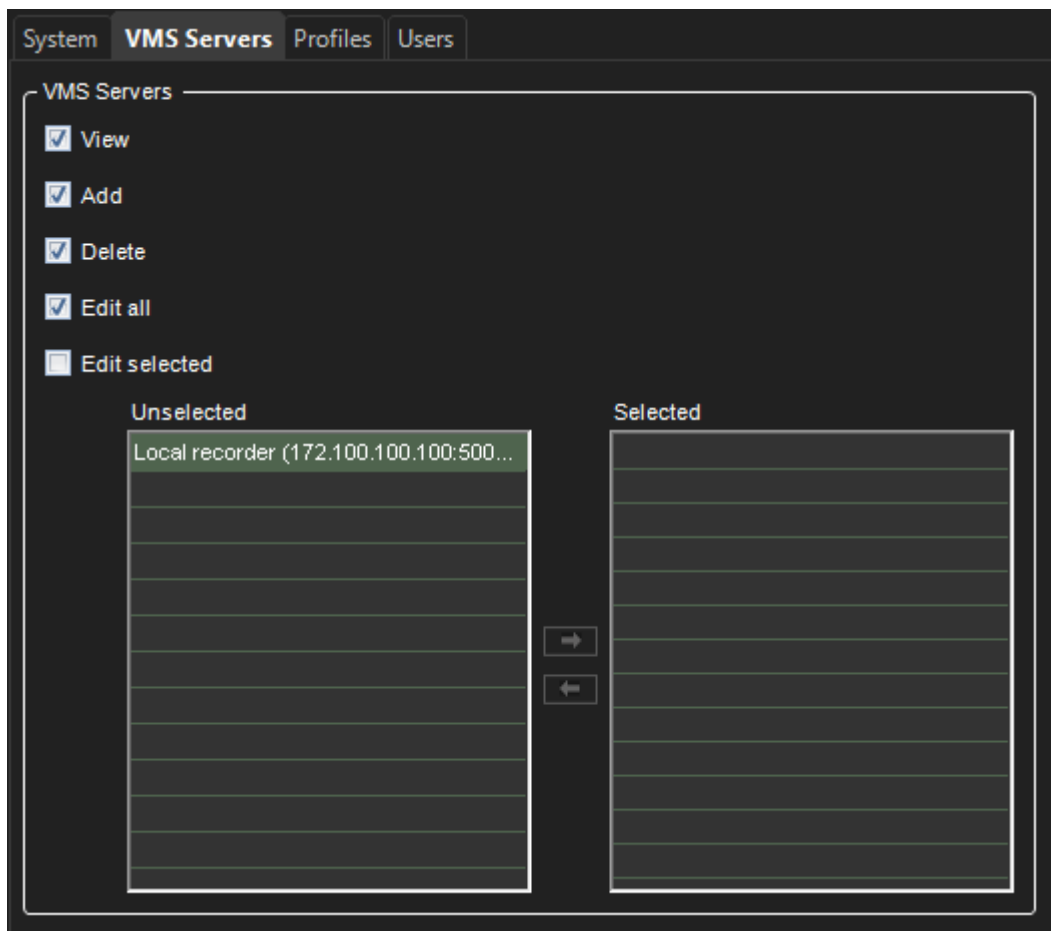




VMS Servers

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.)



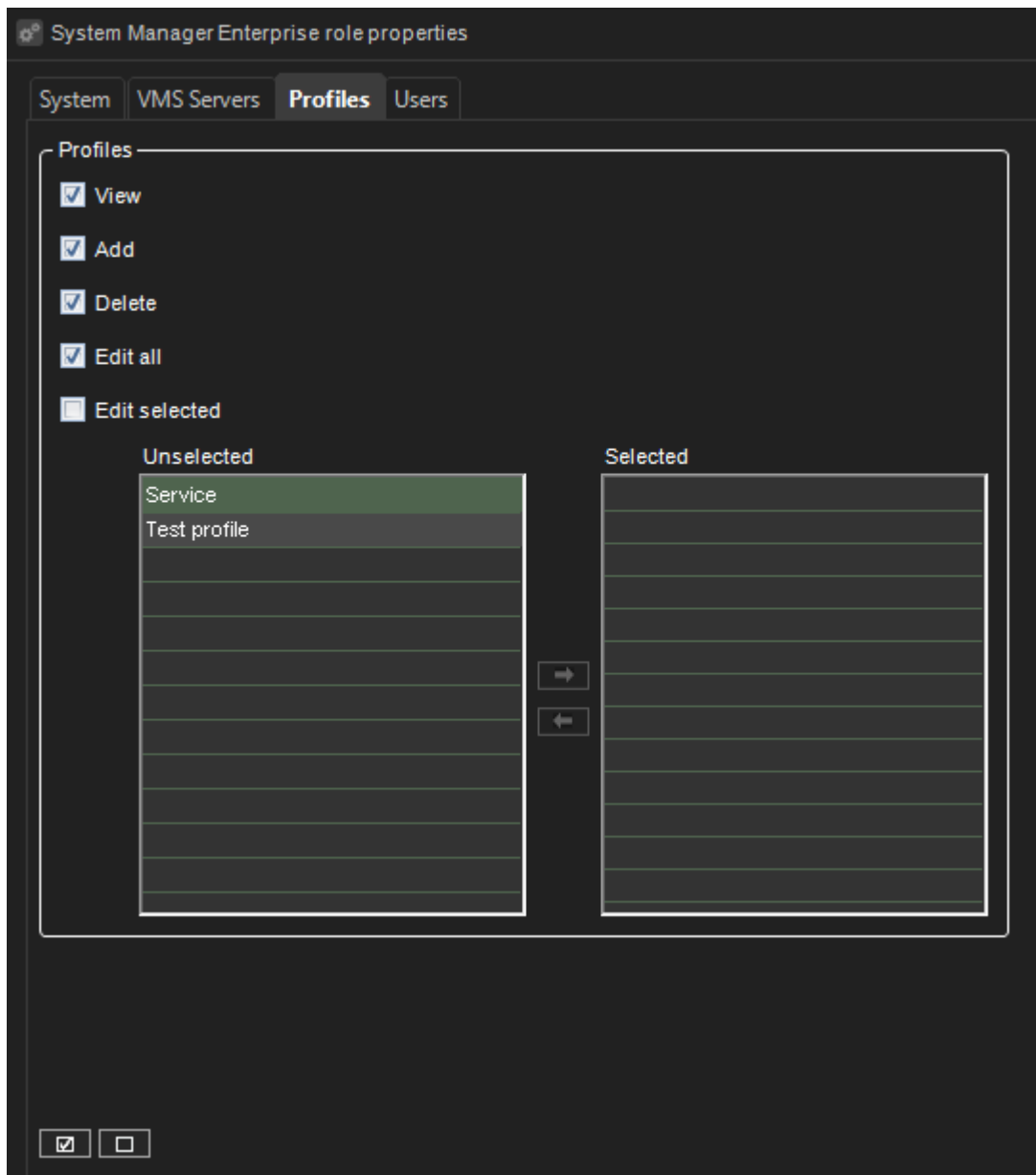
Profiles

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).



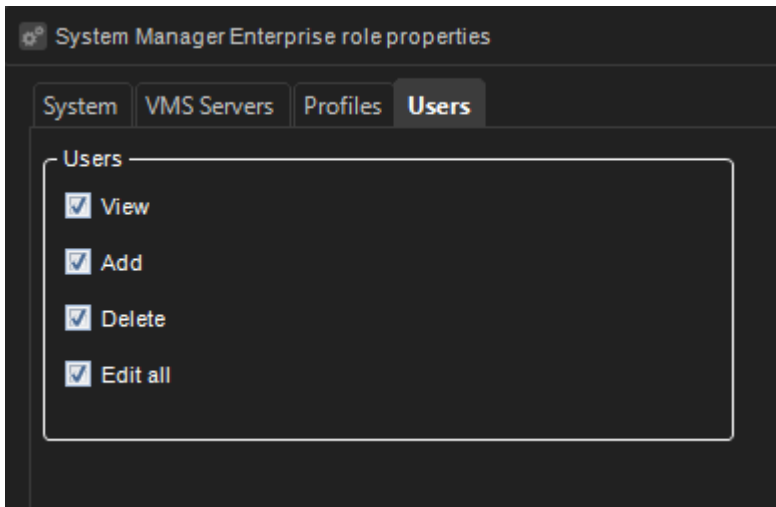
Administrator Guide V9 - EN



Users

The user tab/permissions that can be set for the user group:

Administrator Guide V9 - EN



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

Administrator Guide V9 - EN

1.11.1.1.2. Monitoring role

The users with the role Monitoring role have permission to:

System

- Export logs
- SM Server and VMS server diagnostic
- Licenses
- Watchdog log

Profiles

Can view the content of the profiles

Users

Can view the system user groups and users

Administrator Guide V9 - EN

1.11.1.1.3. Gateway role

Gateway role enables old Spotter Mobile usage

Administrator Guide V9 - EN

1.11.1.1.4. Mirasys Spotter Enterprise role

Custom user role properties can be edited by clicking the custom role properties edit button.



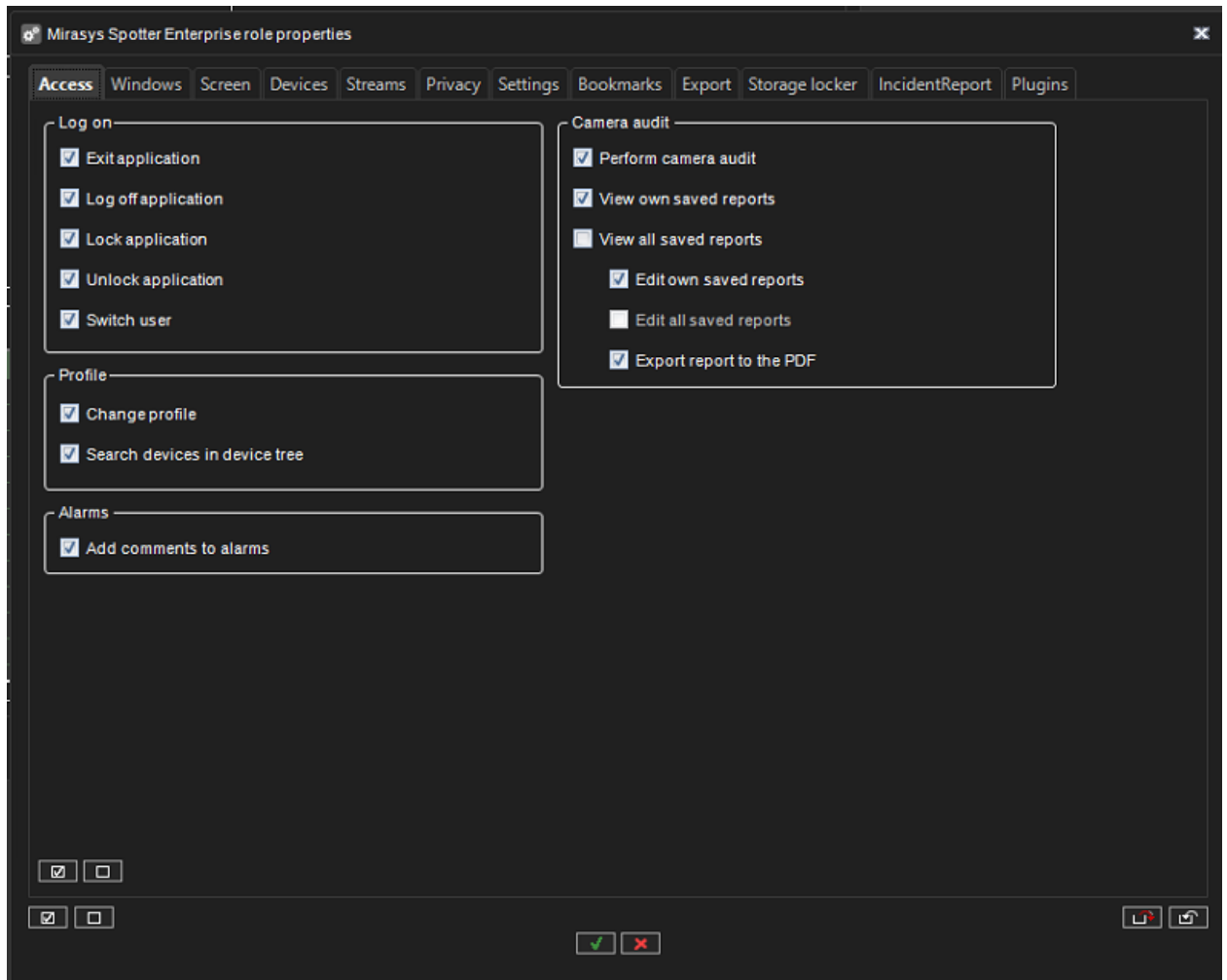
The **Spotter** custom roles can be customized with close to a hundred different options (not including plugin-specific adjustments).

Access

The Access tab of the role customization contains options for the application access and accessing profiles and alarm commenting.



Administrator Guide V9 - EN

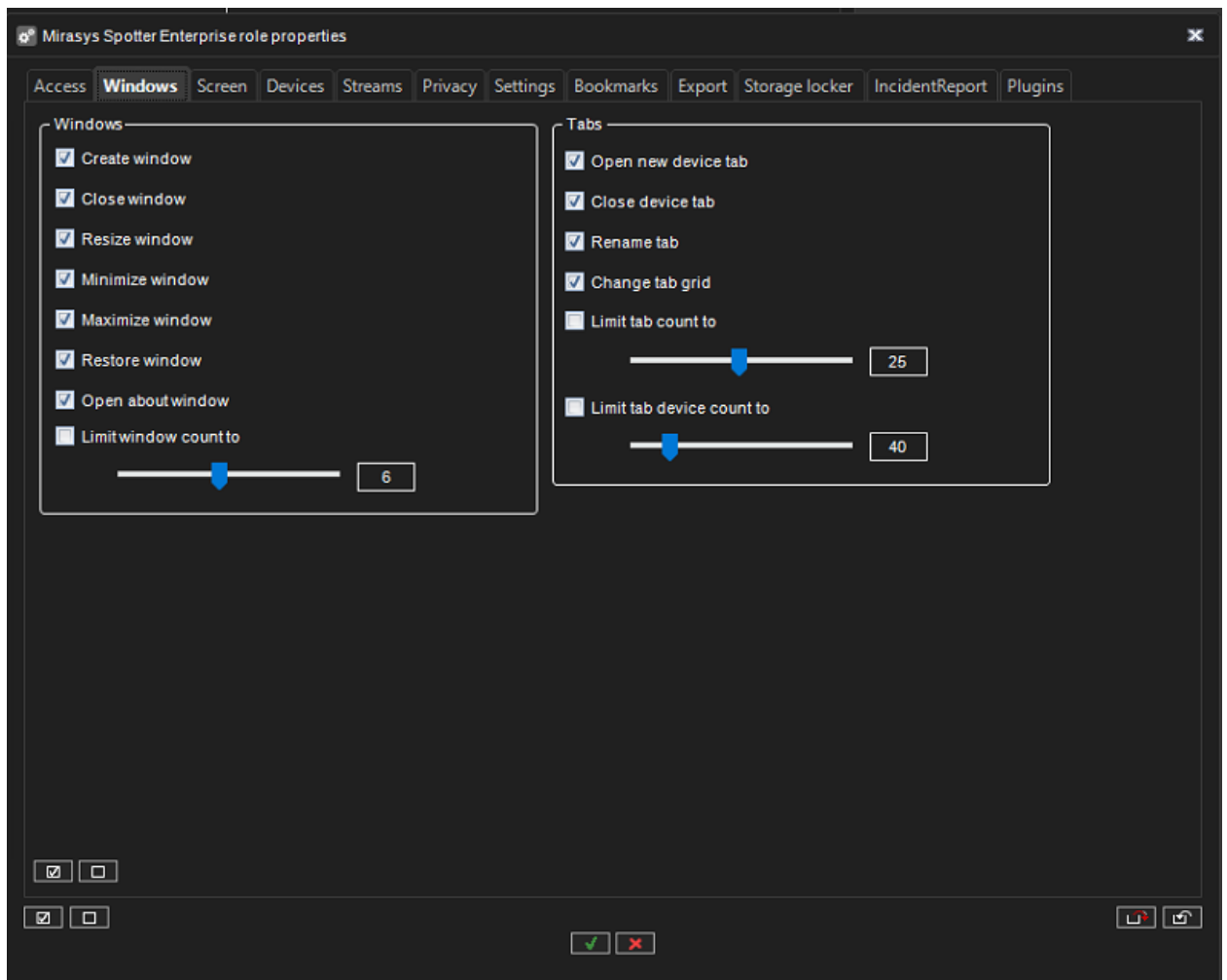


Windows

The Windows tab contains options for Spotter window management and tab management.



Administrator Guide V9 - EN

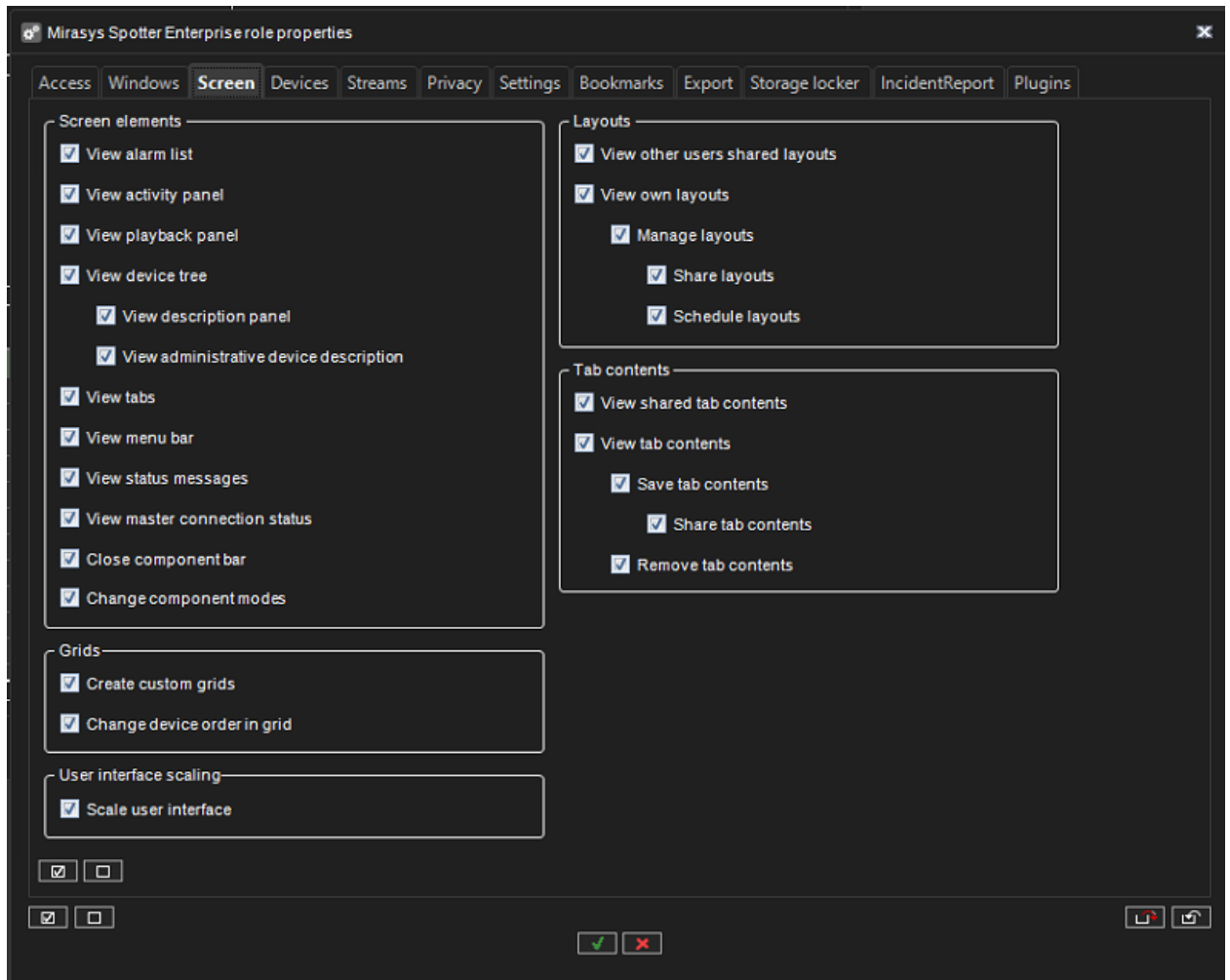


Screen

The Screen tab contains options for different screen element access and layout access, bookmarks, camera grid and saved camera tabs.



Administrator Guide V9 - EN

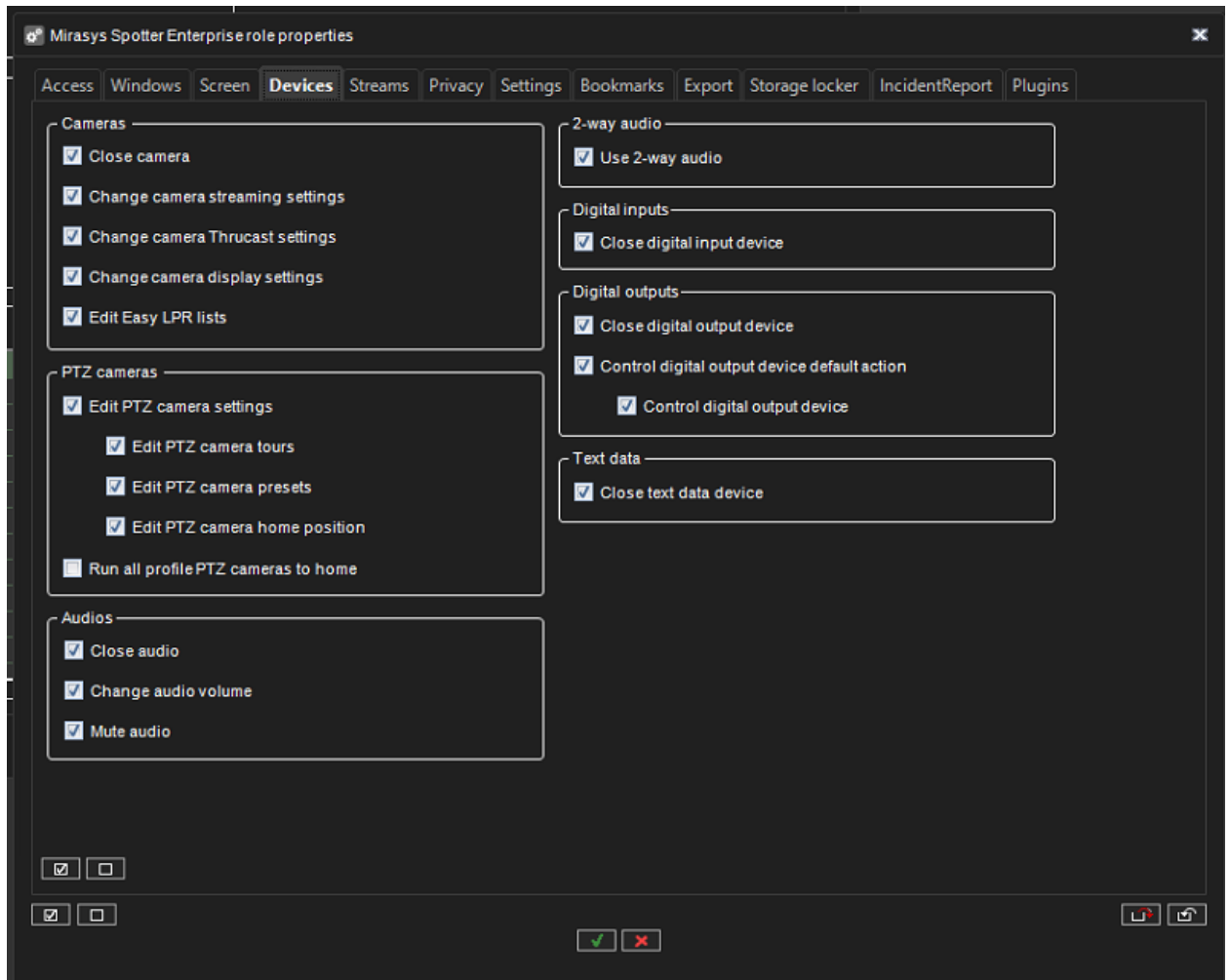


Devices

The Devices tab contains options for media control.



Administrator Guide V9 - EN

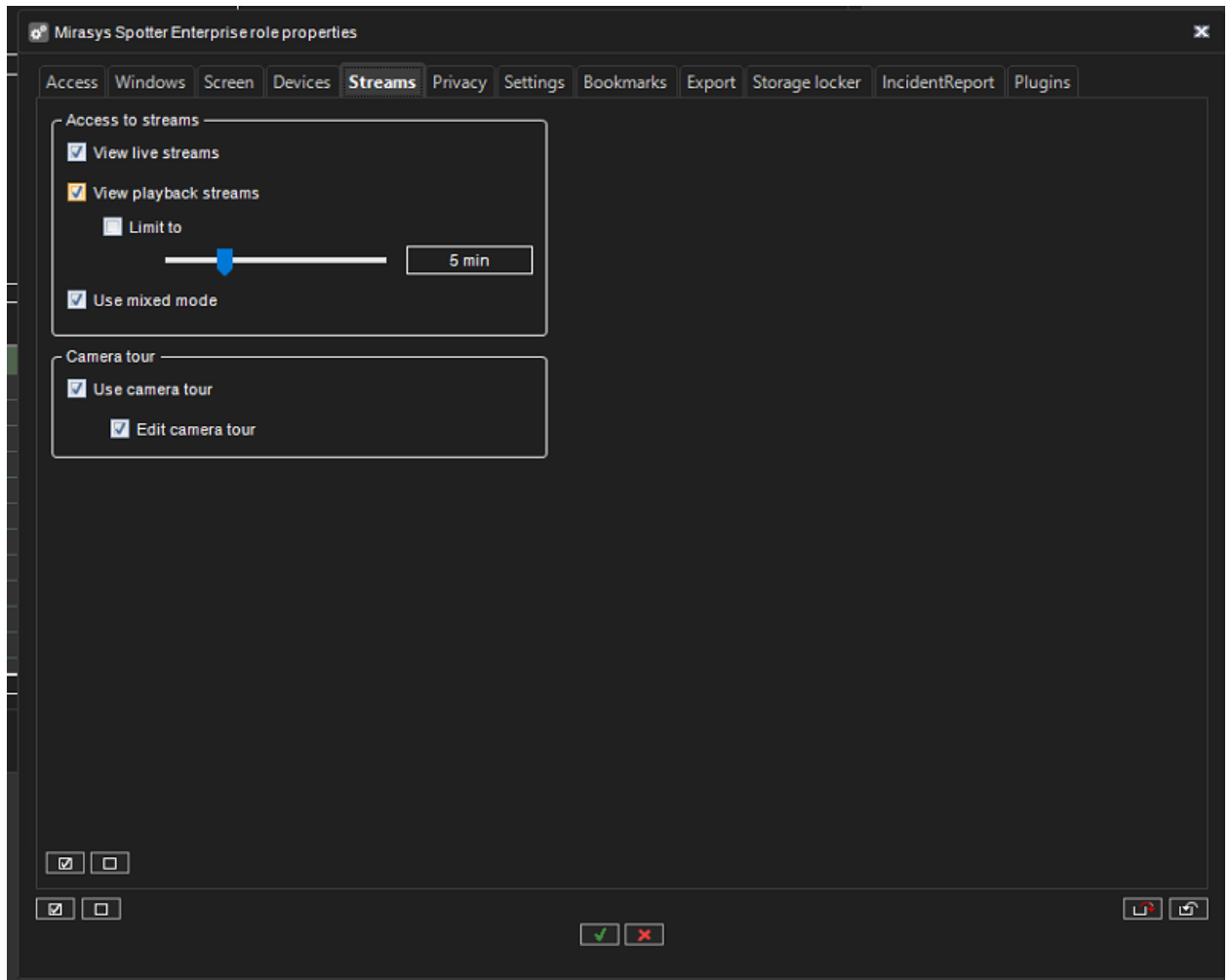


Streams

The Streams tab contains options for stream access and exporting.



Administrator Guide V9 - EN

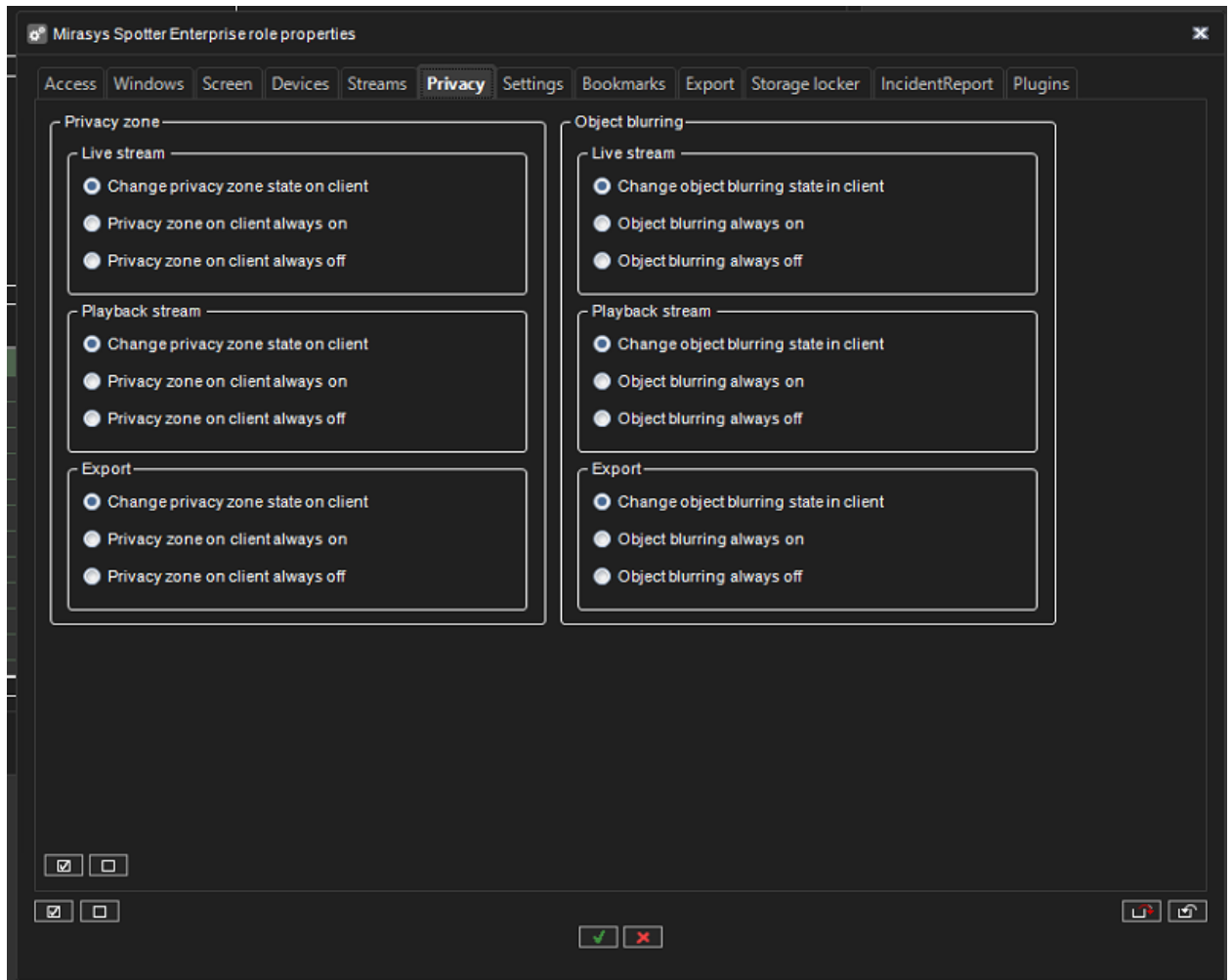


Privacy

The Privacy tab contains options for privacy.



Administrator Guide V9 - EN

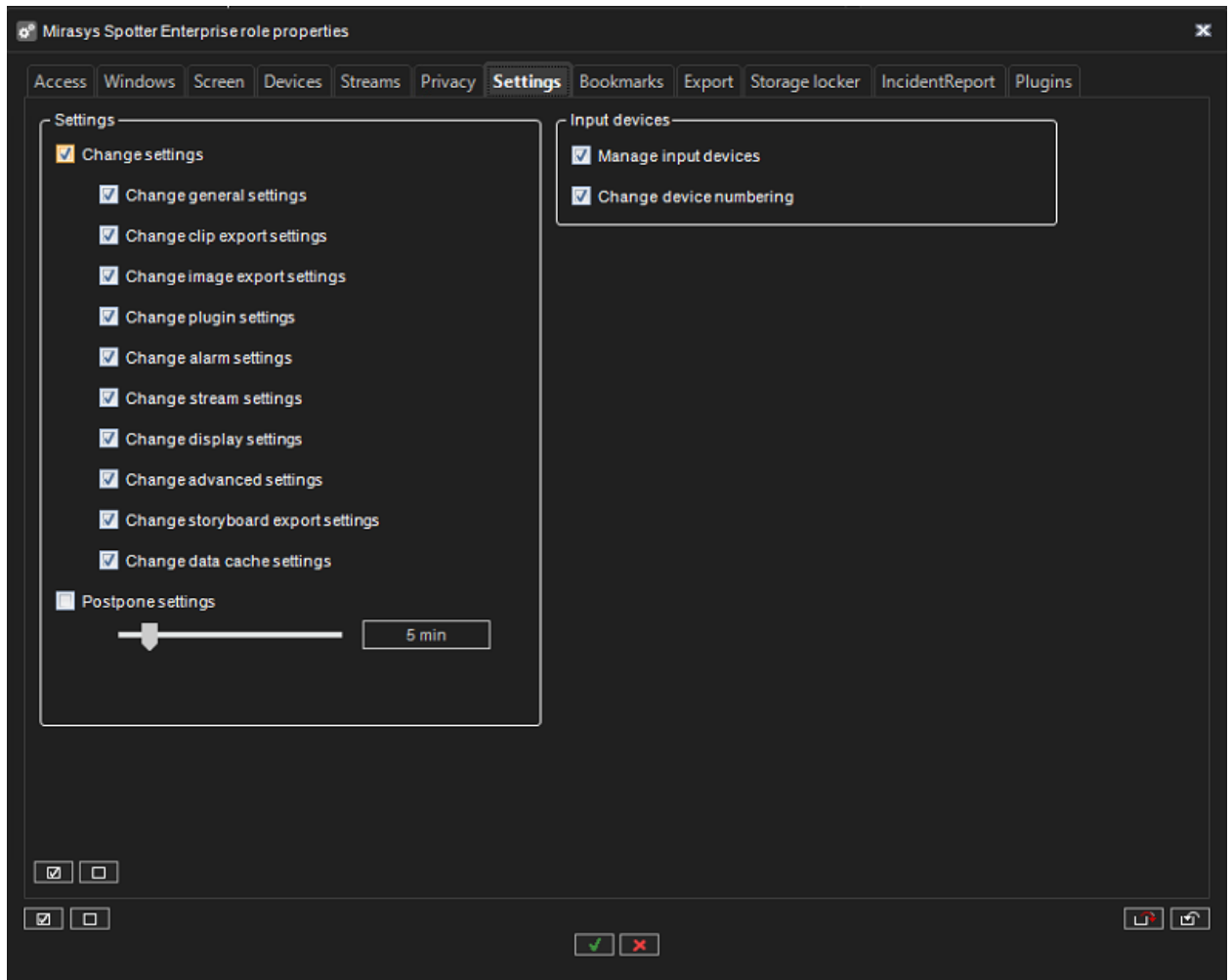


Settings

The Settings tab contains options for Spotter settings.



Administrator Guide V9 - EN

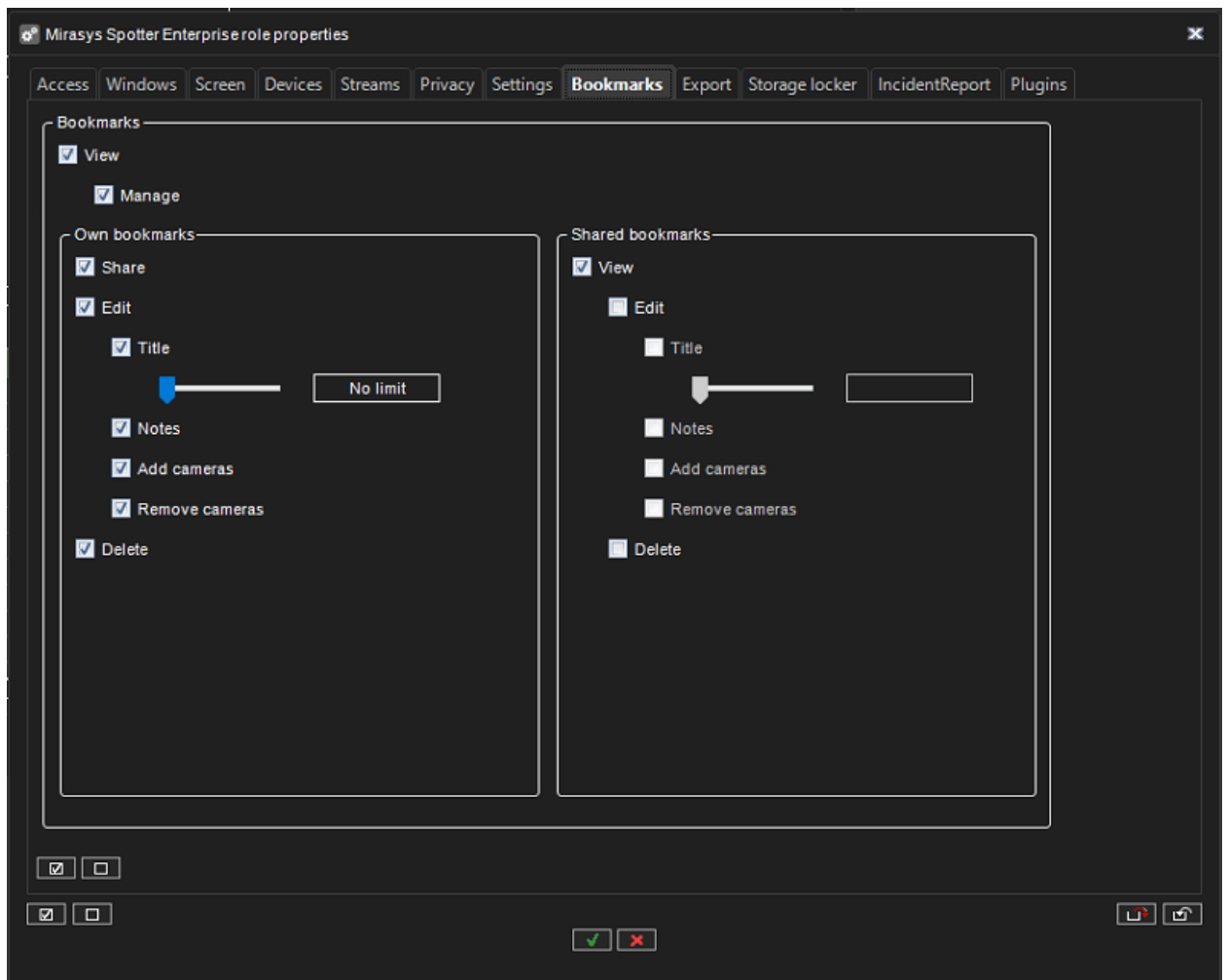


Bookmarks

The Bookmarks tab contains options for bookmarks



Administrator Guide V9 - EN

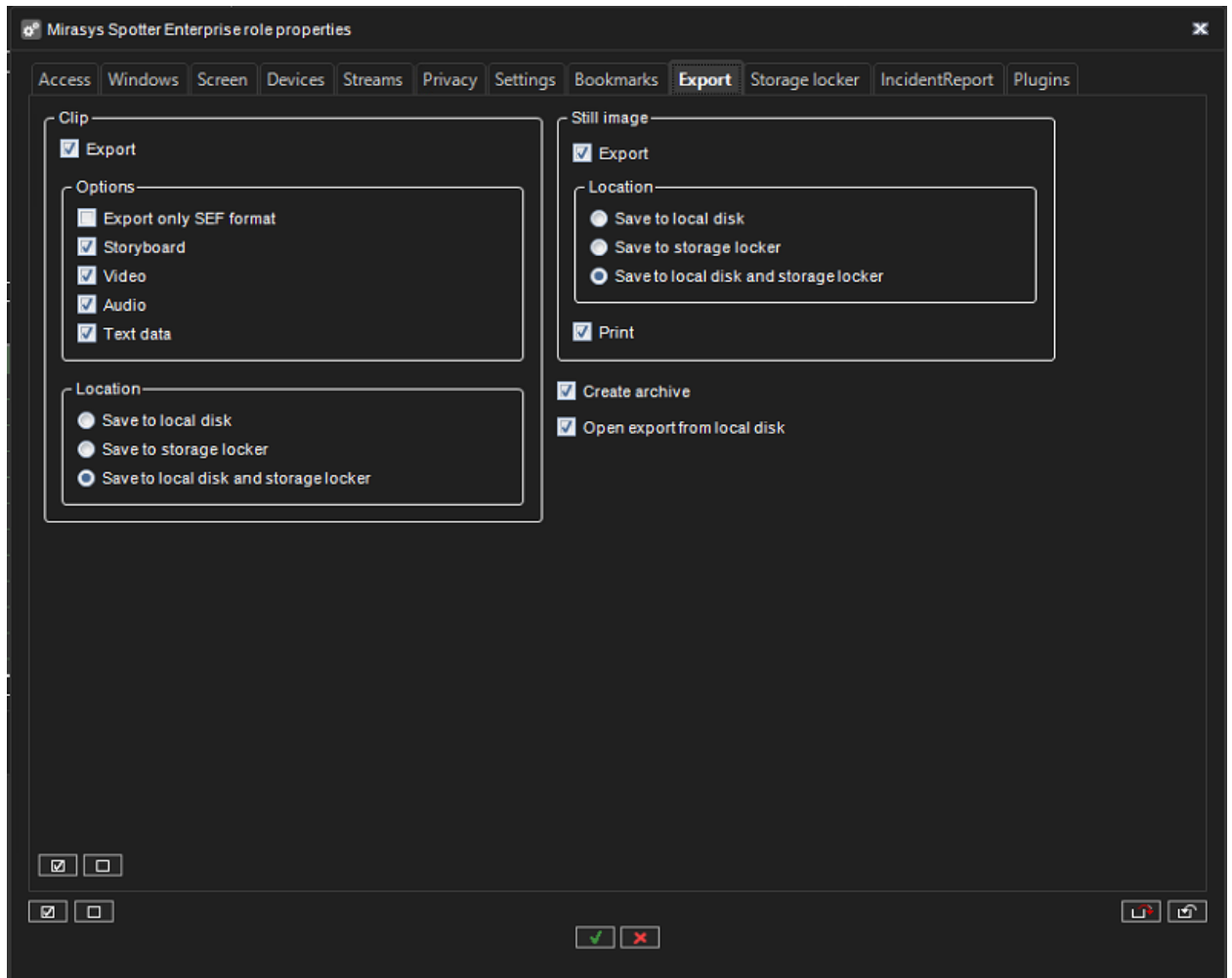


Export

The Export tab contains options for Export functions



Administrator Guide V9 - EN

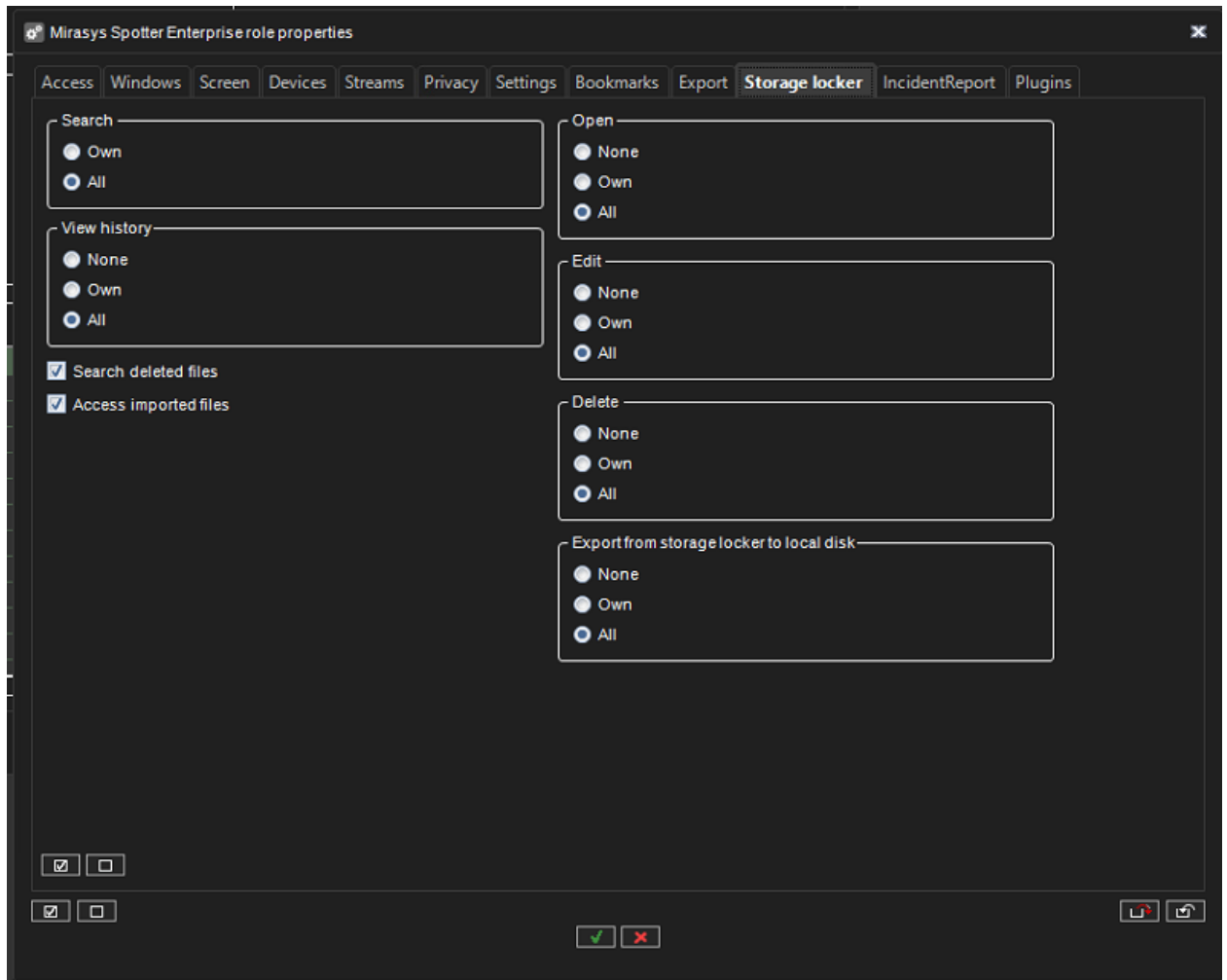


Storage Locker

The Storage Locker tab contains options for the Storage Locker plugin.



Administrator Guide V9 - EN

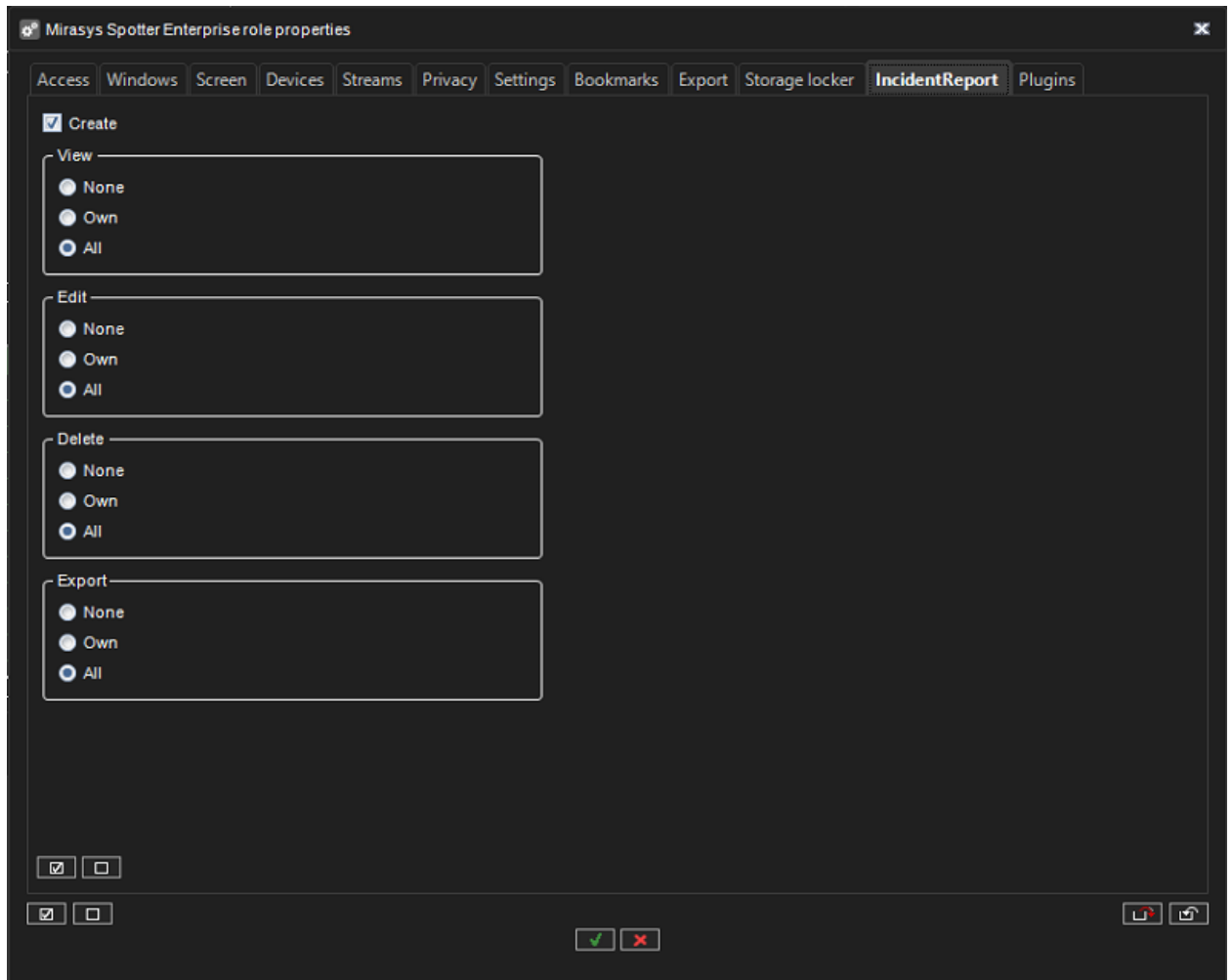


Incident Reporting

The Incident Reporting tab contains options for the Incident Reporting plugin



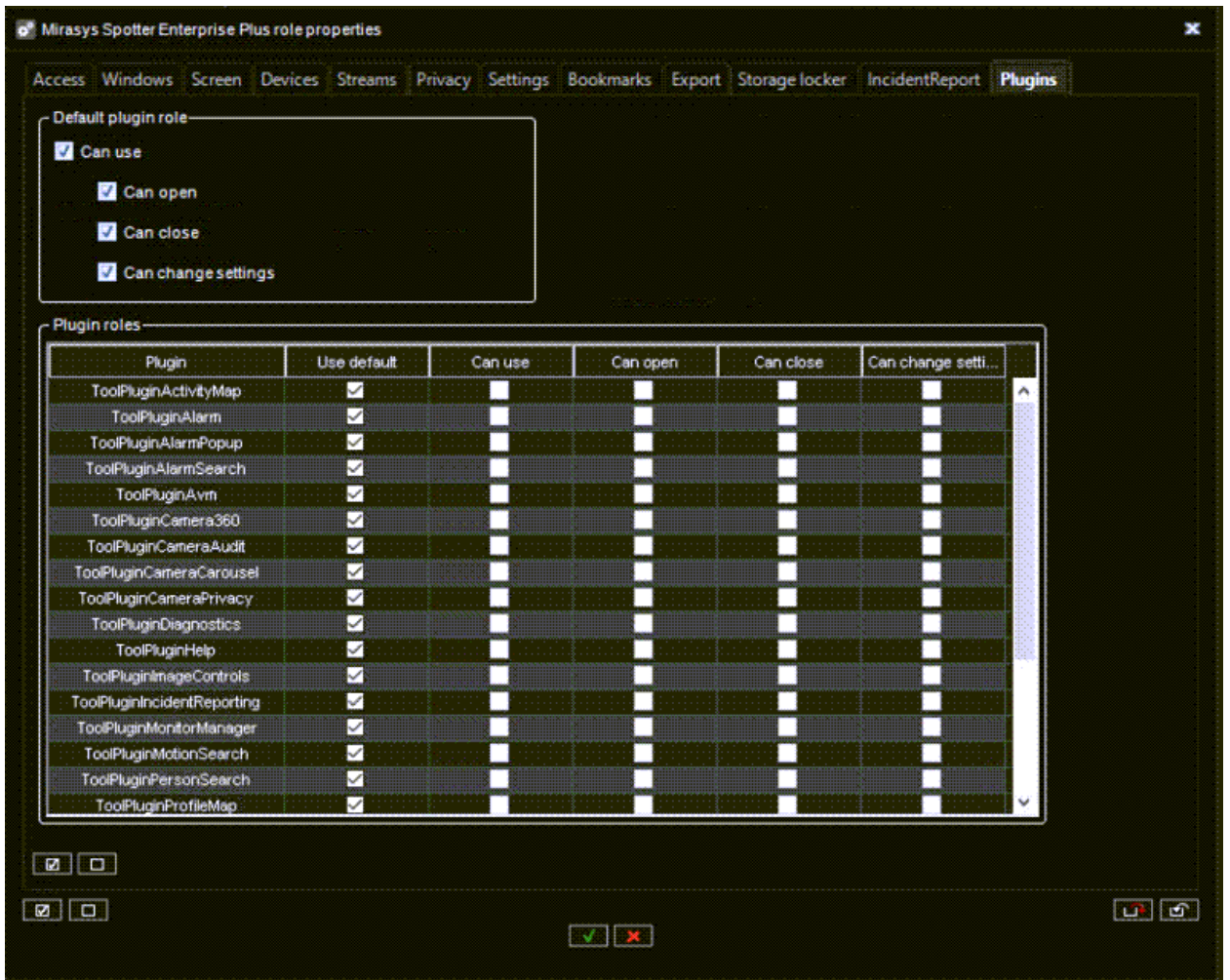
Administrator Guide V9 - EN



Plugins

The Plugins tab contains options for Spotter plugins.

Administrator Guide V9 - EN



Each plugin behaviour can be either default or custom. The default behaviour can be controlled from the "Default plugin role" controls.

Administrator Guide V9 - EN

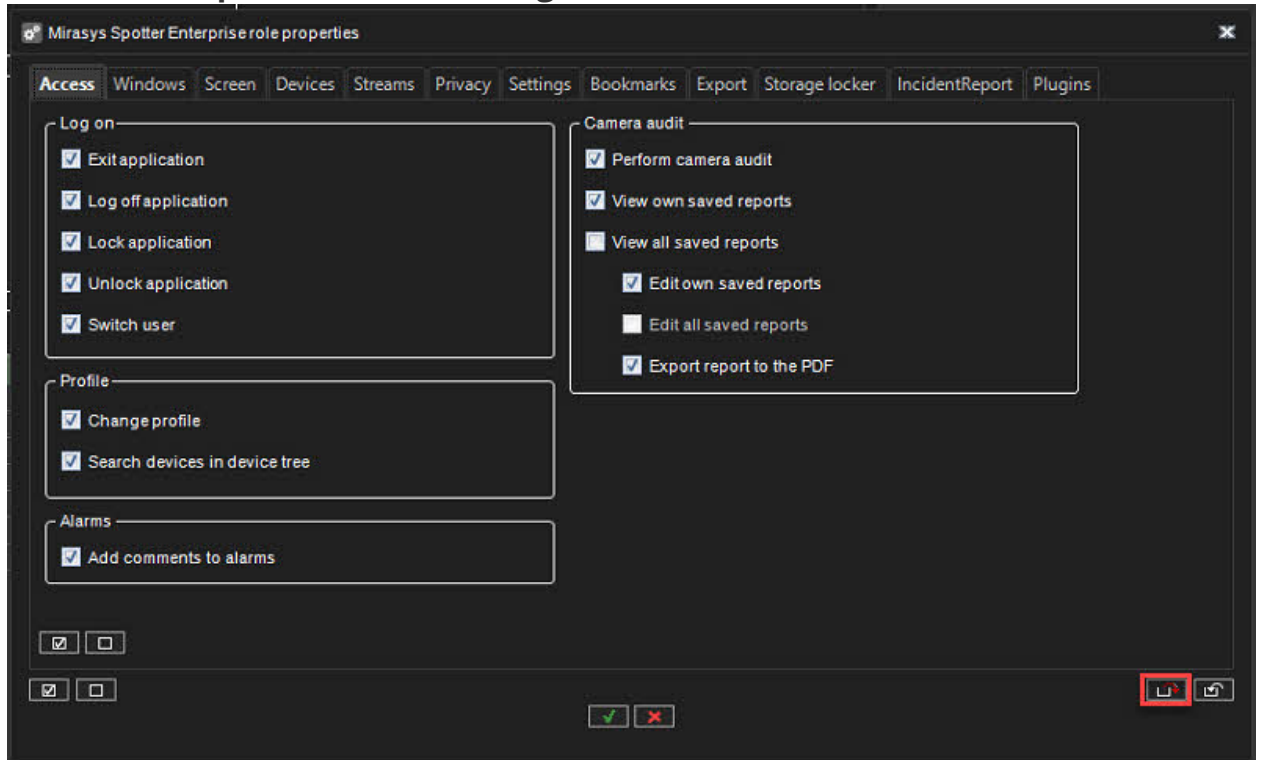
1.11.1.1.5. Spotter Web role

Spotter Web role enables new Spotter Web and Spotter Mobile usage

1.11.1.1.6. Exporting and Importing User Role Settings

Exporting User role settings

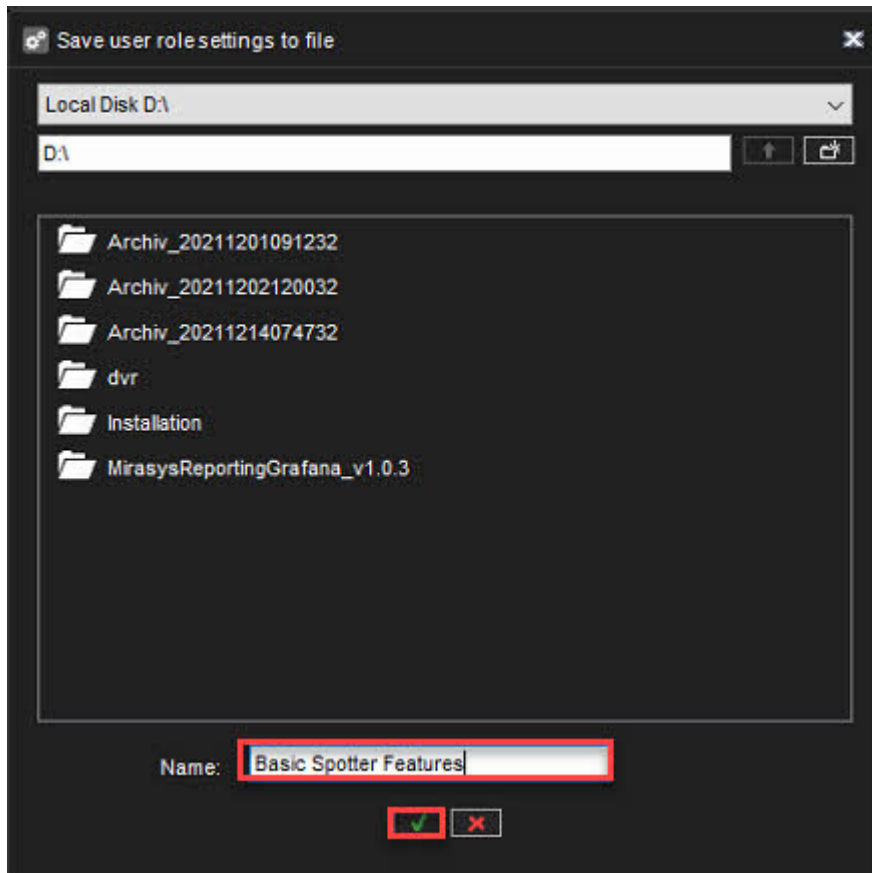
- Click **Export user role settings to file**



2. Select destination
3. Set the name of the file
4. Click **OK**

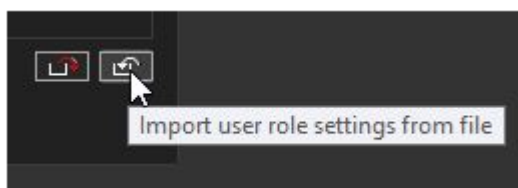


Administrator Guide V9 - EN



Importing User role settings

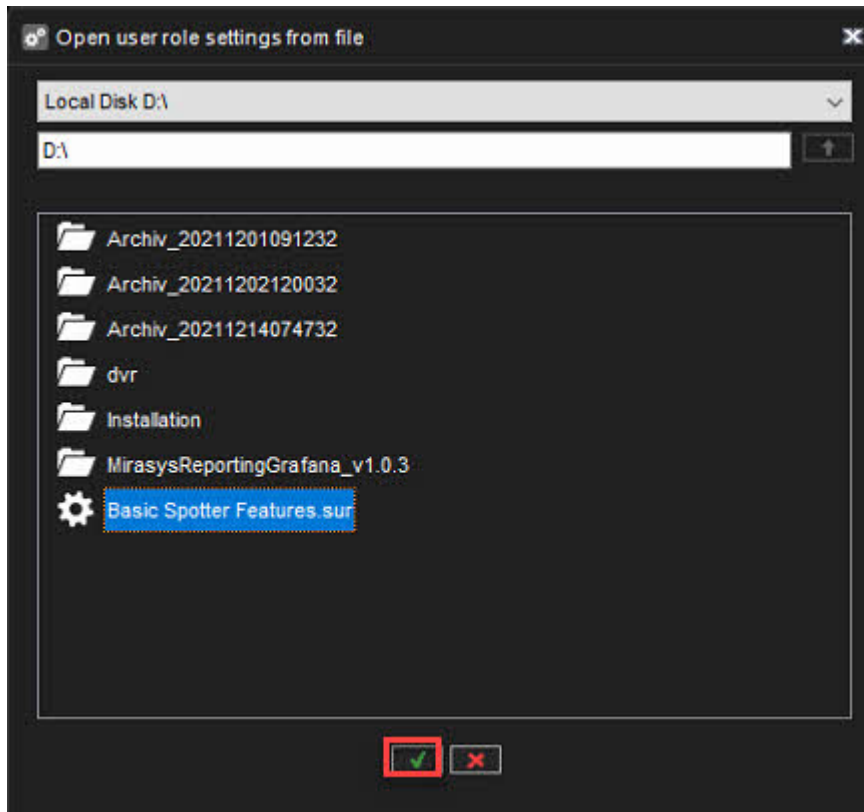
1. Click **Import user role settings from the file**



2. Select file(.sur)
3. Click **OK**



Administrator Guide V9 - EN

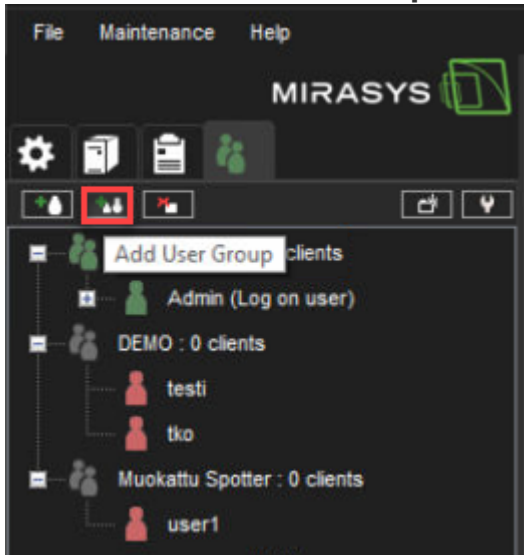




Administrator Guide V9 - EN

1.11.1.2. Creating a customer-specific User Group

1. Click **Add User Group**

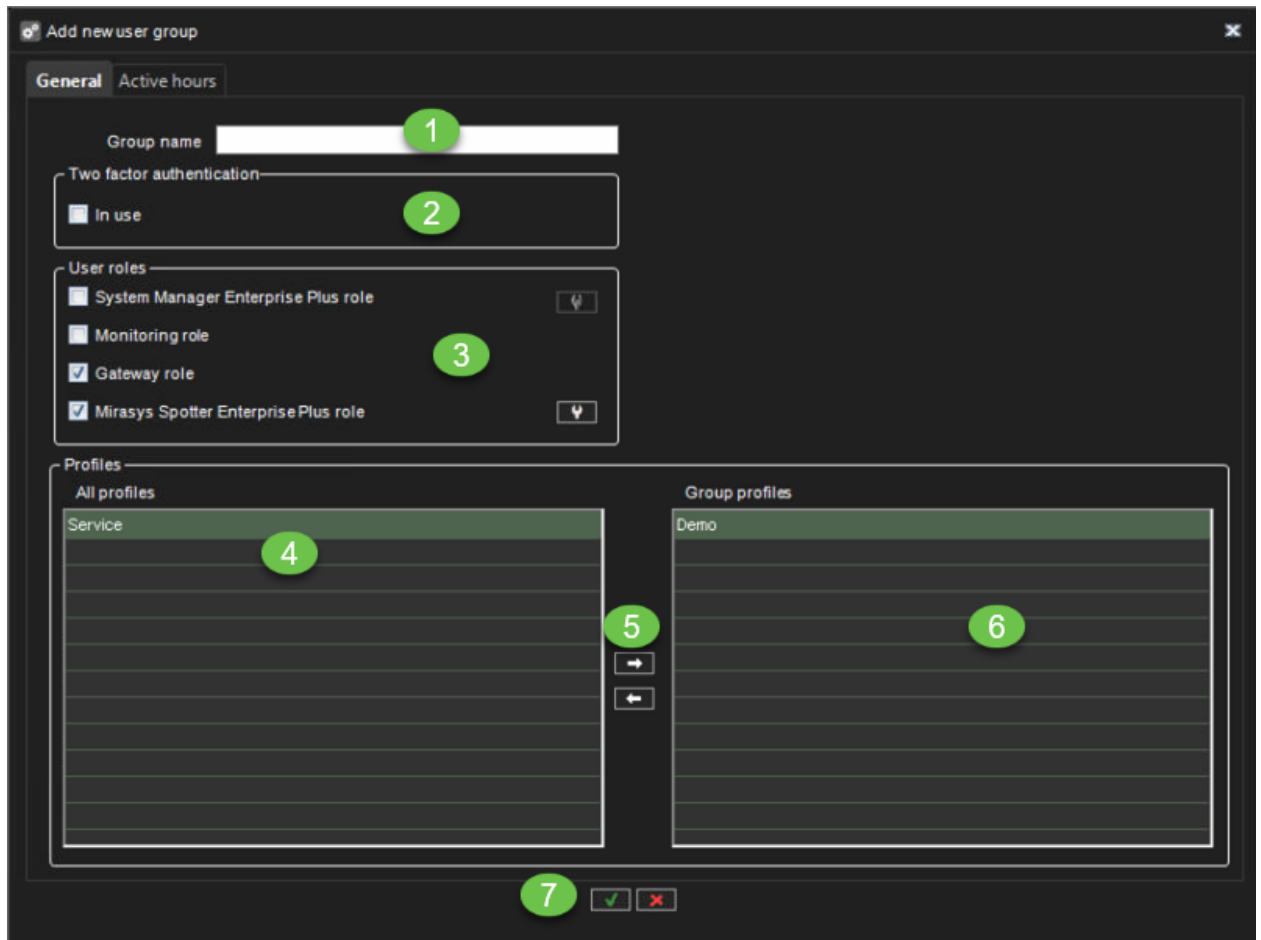


1. Type a name for the group in the **Group name** box
2. Enable **Two-factor authentication**, if needed
3. Select the **User roles** for the group.
4. Select the **Profile** or **Profiles** you want to assign to the user group.
5. Click the right arrow button or drag the profiles from the left panel to the group profiles box
6. Check that correct profiles is found
7. Click **Ok** to confirm user group creation

Tip: To select more than one profile at a time, keep the **SHIFT**, or **CTRL** key pressed.



Administrator Guide V9 - EN



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.

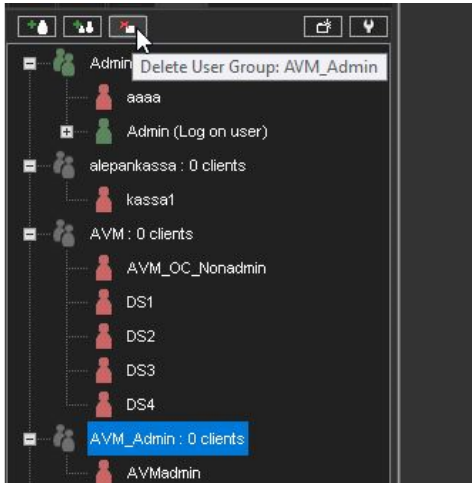
Deleting a user group



Administrator Guide V9 - EN

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.

Administrator Guide V9 - EN

1.11.1.3. Two-factor authentication

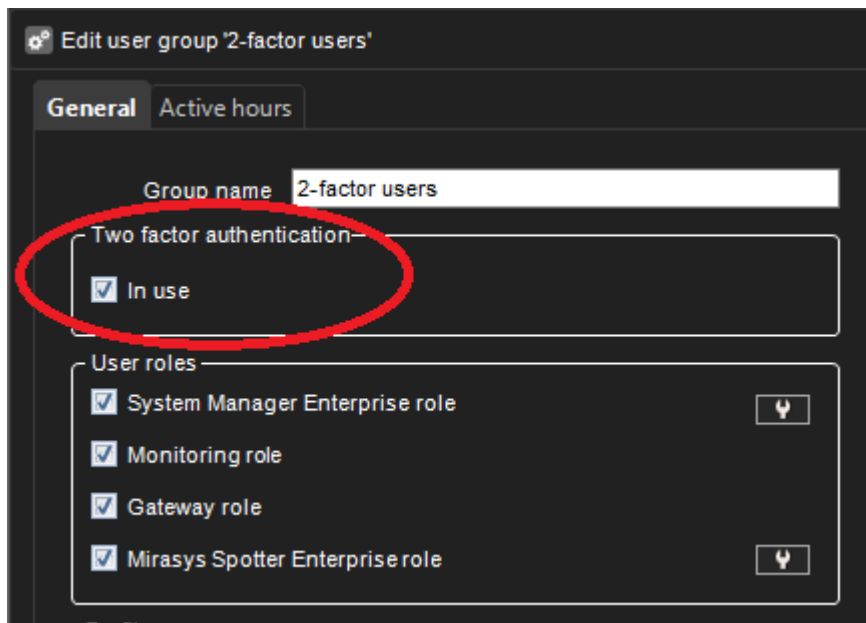
Two-factor authentication is functionality to improve the user's identification by requiring the username and password and a code from an external physical device.

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.)

Setup:

1. The admin enables the 2-factor authentication for the specific user group.

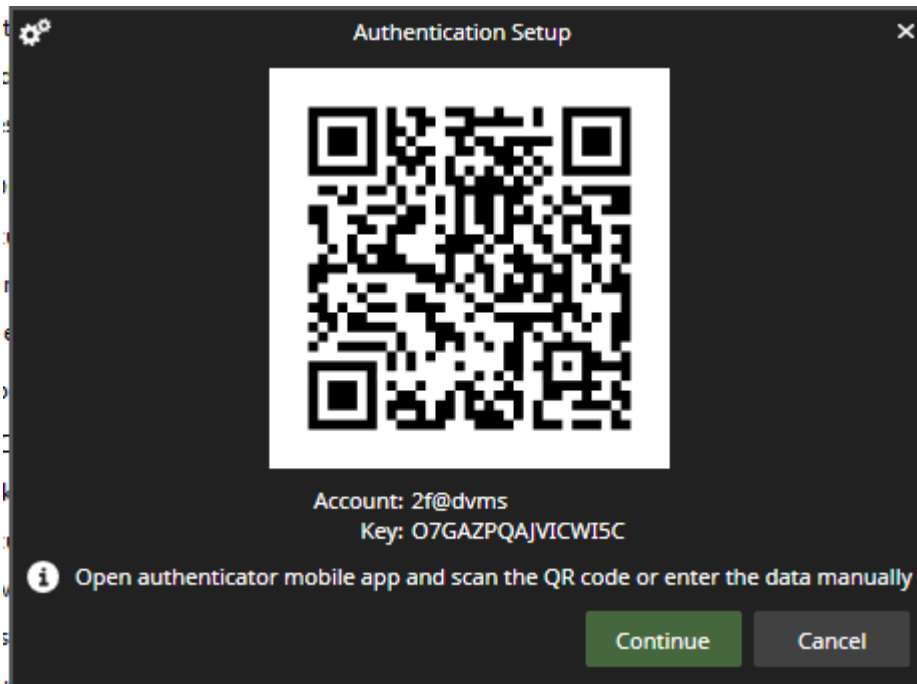


2. When the user in the group tries to log in for the first time, the user is requested to use or install the 2-factor authentication client (e.g. Authy, Google authenticator, MS Authenticator (available for free)) on his/her mobile device.
3. The VMS and the authentication client are then synchronized 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:



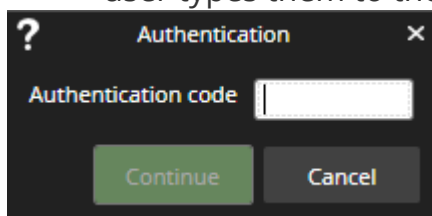
Administrator Guide V9 - EN



5. After that, the authentication client generates automatically 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.)

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.



Maintenance:

1. If the user forgets his / her 2-factor secret key, the administrator can then reset the key from the system manager.



Administrator Guide V9 - EN

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).

The screenshot shows the 'Edit User Account' window for user 'test'. The interface includes the following sections:

- Active:** A checked checkbox.
- User name and password:** Fields for 'User name' (test) and 'Password' (masked with ****).
- Two factor authentication:** A section circled in red, containing a 'Key' field with a red 'X' icon.
- Description:** A large empty text area.
- User group:** A dropdown menu showing 'Testi'.
- Language:** A dropdown menu showing 'English'.
- Protection:** A section with checkboxes for 'Hide user interface on lock' (unchecked), 'Automatic lock' (checked), and 'Automatic log off' (unchecked). Below these is a 'Wait time' slider set to '5 min'.

At the bottom of the window are green and red checkmark buttons.

1.11.1.4. Domain Based User Groups (LDAP)

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 you need to change the default interval.

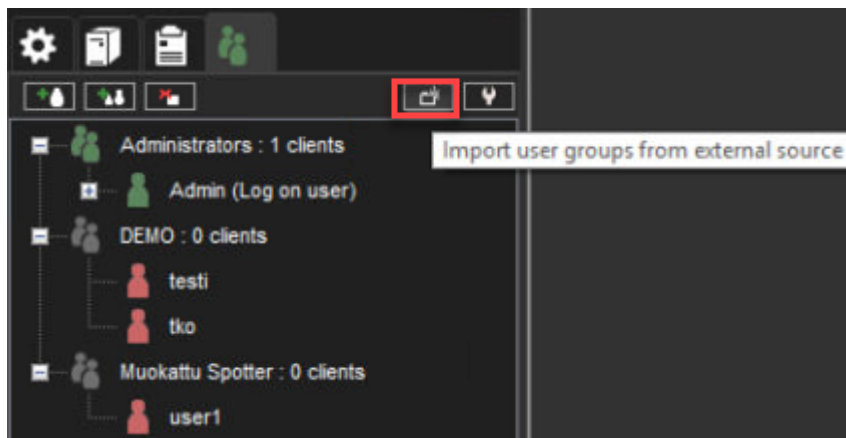
This feature requires a license update.

To add 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 Master Server needs to be connected to a domain for the button to be displayed.

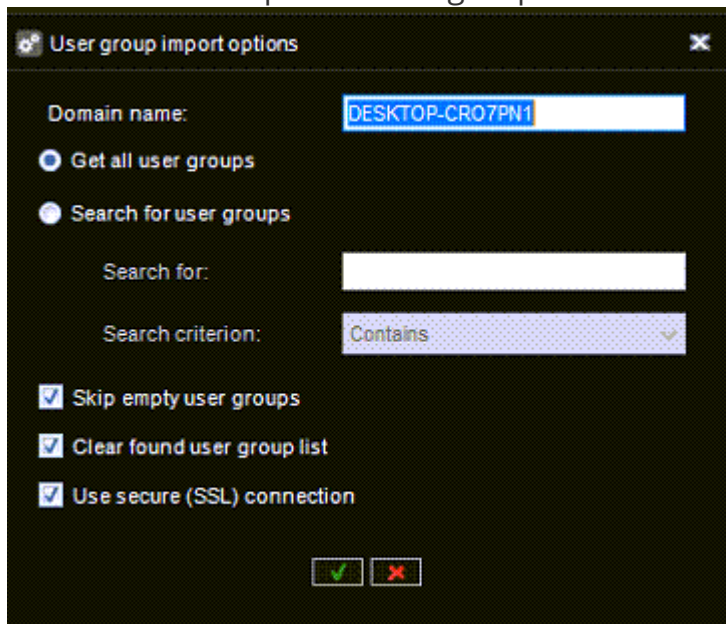
If the server is not connected to a domain, the button is not visible.



2. Type the name of the domain into the **Domain name** dialogue box.
3. Select whether to get all user groups or to search for specific groups.


Administrator Guide V9 - EN

- a. 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.



1.11.2. Creating a customer-specific user

To add a new user to the system:

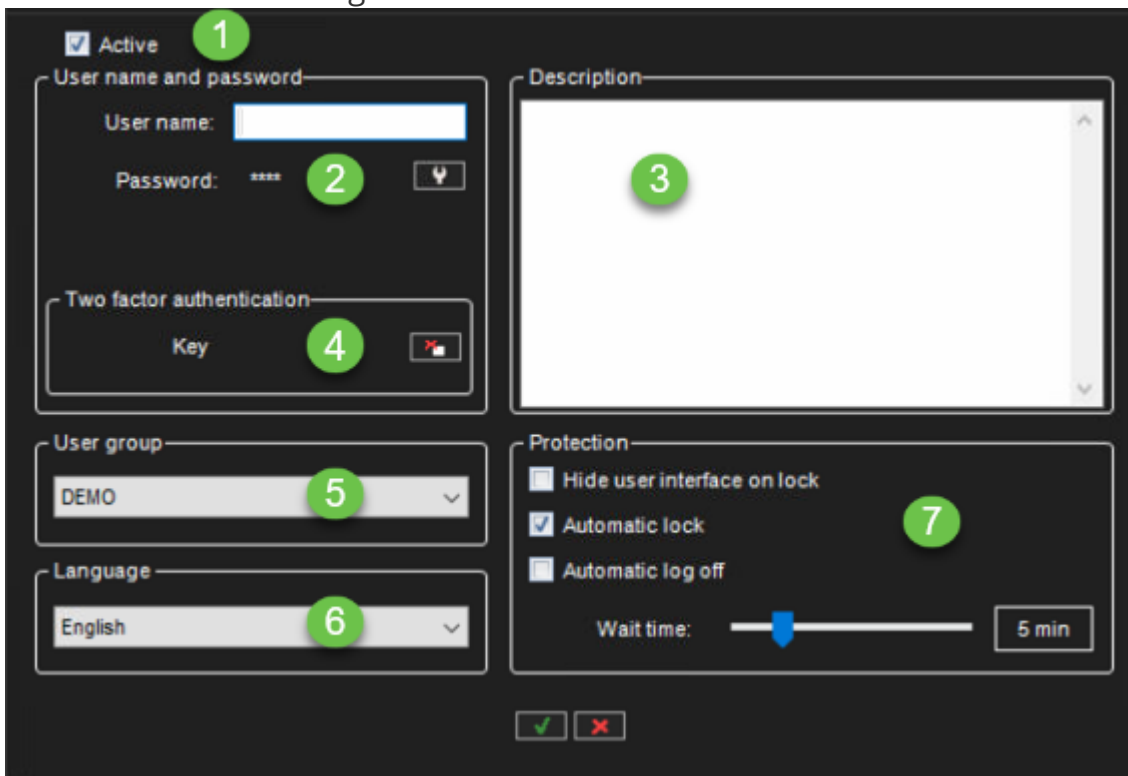
1. Open the **Users** tab.
2. Click the name of the user group to which you want to add the user.
 - a. Note that you can only add users to the system's native groups, not in domain-based groups.
3. Click **Add User**  in the upper-left corner of the **Users** tab. The **Add User** dialogue box is shown.
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.

1.11.3. User account settings

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



The screenshot shows a user account settings interface with the following elements:

- 1**: A checkbox labeled "Active" is checked.
- 2**: A "Password" field with a masked password "****" and a "Show/Hide" icon.
- 3**: A large "Description" text area.
- 4**: A "Two factor authentication" section with a "Key" field and a QR code icon.
- 5**: A "User group" dropdown menu currently showing "DEMO".
- 6**: A "Language" dropdown menu currently showing "English".
- 7**: A "Protection" section with three checkboxes: "Hide user interface on lock" (unchecked), "Automatic lock" (checked), and "Automatic log off" (unchecked). Below these is a "Wait time" slider set to "5 min".

At the bottom of the interface are two buttons: a green checkmark and a red 'X'.

1.11.4. Disabling or Activating a User Account

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.

When the user is again permitted to log in to the system, you can activate the account.

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**.
3. Click **OK**.

Note: Domain-based (LDAP) users cannot be deleted or removed with System Manager.



1.12. TruCast

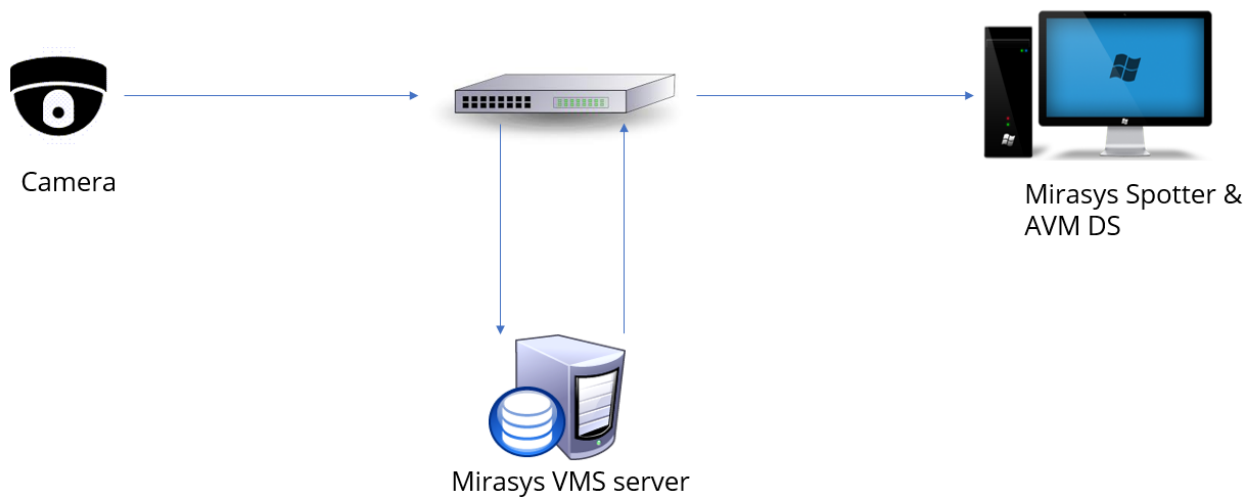
TruCast

TruCast is the direct camera video streaming feature in Mirasys VMS.

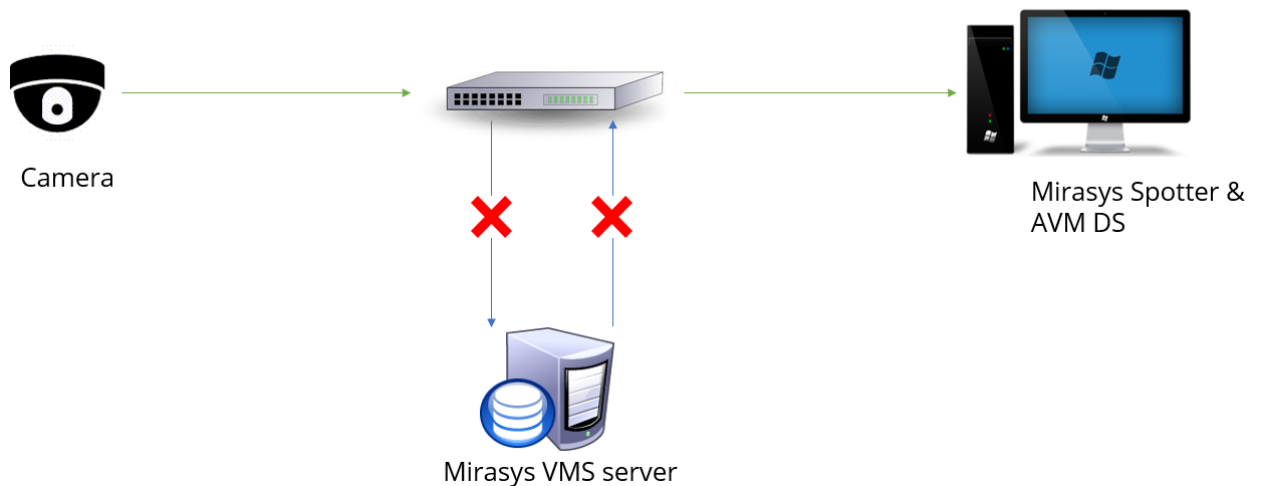
With TruCast, the video stream comes directly from the camera to the viewing client, the Spotter for Windows application.

In a standard streaming scenario, the stream to the client comes from the VMS Server.

Stream from the server to the client



Stream from the camera directly to the client



Administrator Guide V9 - EN

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.

1.12.1. Supported Cameras

Supported Cameras

TruCast 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 TruCast 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.



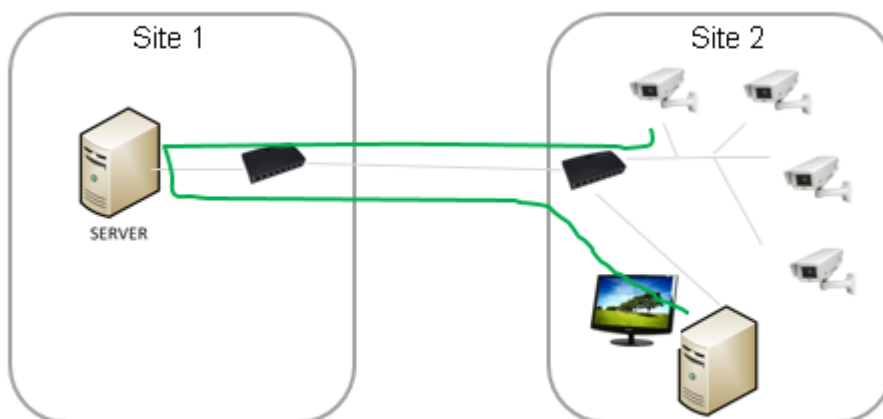
1.12.2. Network Optimization

Network Optimization

TruCast 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 TruCast, and the video goes first to the server and then from the server to the viewing client.

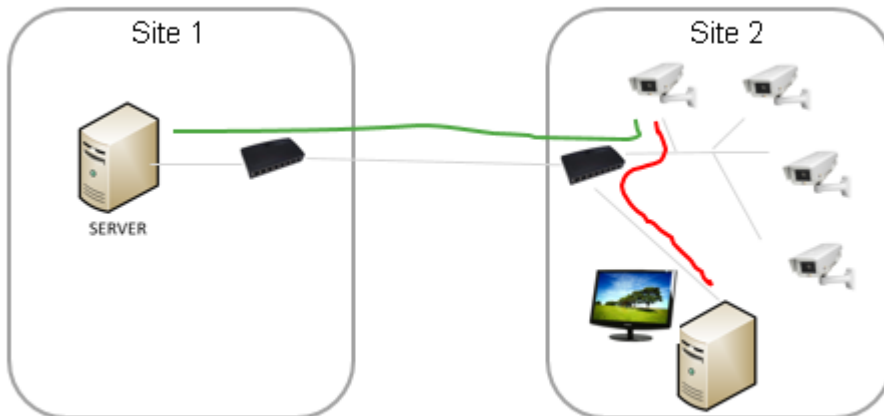


In this solution, the traffic between the two sites is increased.

If the stream is consumed directly from the camera with TruCast, the traffic between the two sites is reduced.



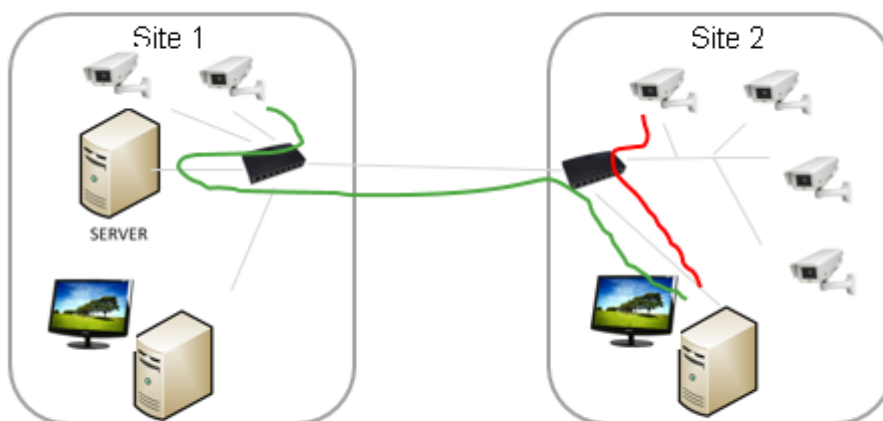
Administrator Guide V9 - EN



An example scenario 2, there are cameras on two sites and viewing clients on two sites.

For the Site 2 user, the use of TruCast makes more sense for the on-site cameras.

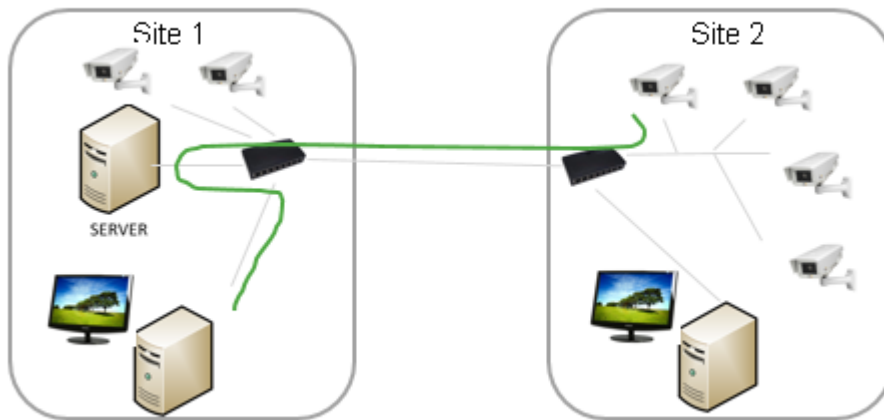
The user can choose to use TruCast for all cameras or only for the on-site cameras.



For the Site 1 user, the use of TruCast only reduces the amount of traffic from the server to the nearest network connection.



Administrator Guide V9 - EN



Users have complete control over which cameras are using TruCast and which cameras are viewed typically.

The setting is memorized for each camera and each user and saved to Spotter layouts.

1.12.3. Multistreaming and TruCast for Network Optimization and Storage

Since it is also possible to use a different stream for TruCast than the recording stream, this should be considered when planning the network capacity.

For example, users can choose to view live images with TruCast 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.

Impact of TruCast on Image Delay

Since the TruCast 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.

Features Not Supported in TruCast Streaming

TruCast does not support PTZ control or Audio

Also, currently, TruCast supports only live images. Playback (recorded images) is currently always received from the server.

Licenses

TruCast requires the VMS license to have the TruCast feature and the TruCast client driver identifiers used.

These TruCast driver licenses, and the TruCast feature, are always enabled in the Mirasys V9 product version.

Multiple Viewers

Since each TruCast-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.

Installing Client Drivers

Administrator Guide V9 - EN

Before using TruCast, 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 TruCast use.

Please note that only those cameras which' client driver was installed will appear as TruCast enabled.

Configuring multi-streaming

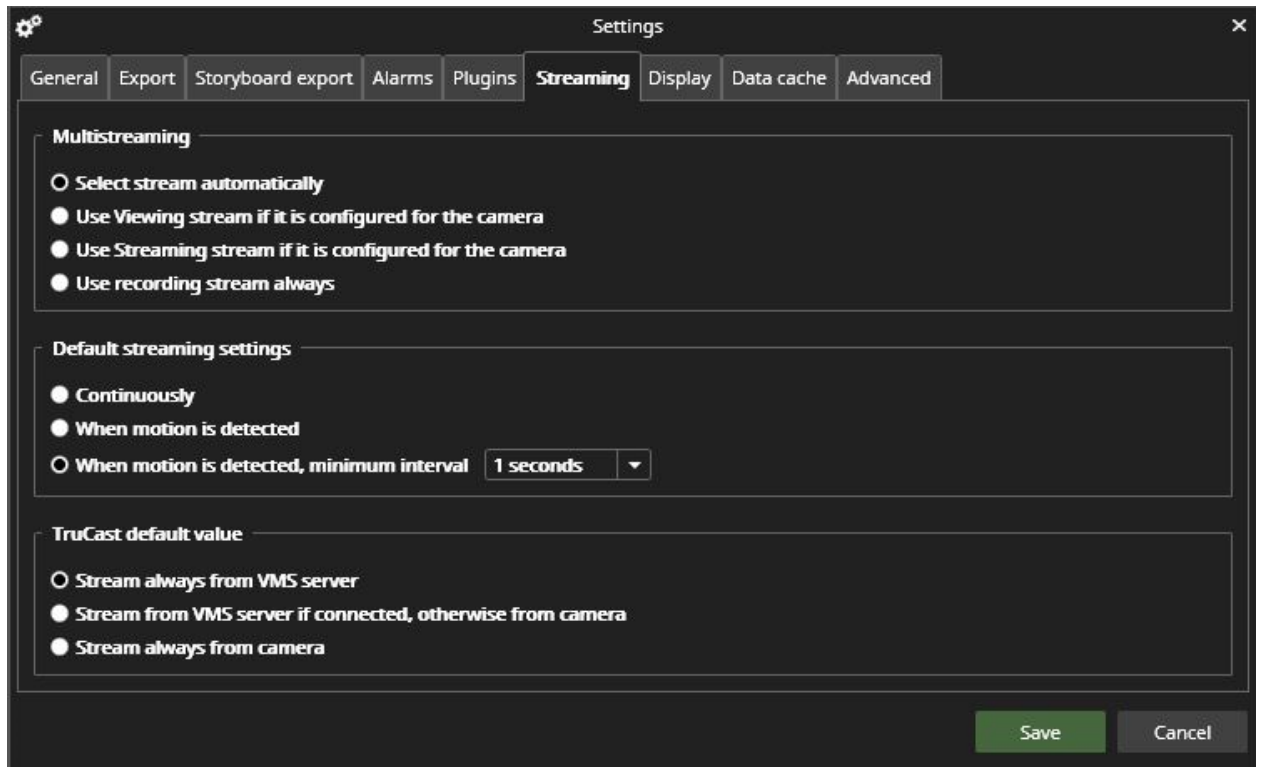
TruCast can use any stream from the camera, the Recording, Live viewing or Remote streams.

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 TruCast viewing.



Administrator Guide V9 - EN



TruCast Default Setting

The default setting for all cameras that have not been used for TruCast before can be defined in Spotter settings – streaming – TruCast default value.

The possible values are

- Always stream from the VMS Server
- Stream from the VMS Server normally, but switch to TruCast if the connection to the server is lost
- Always stream using TruCast

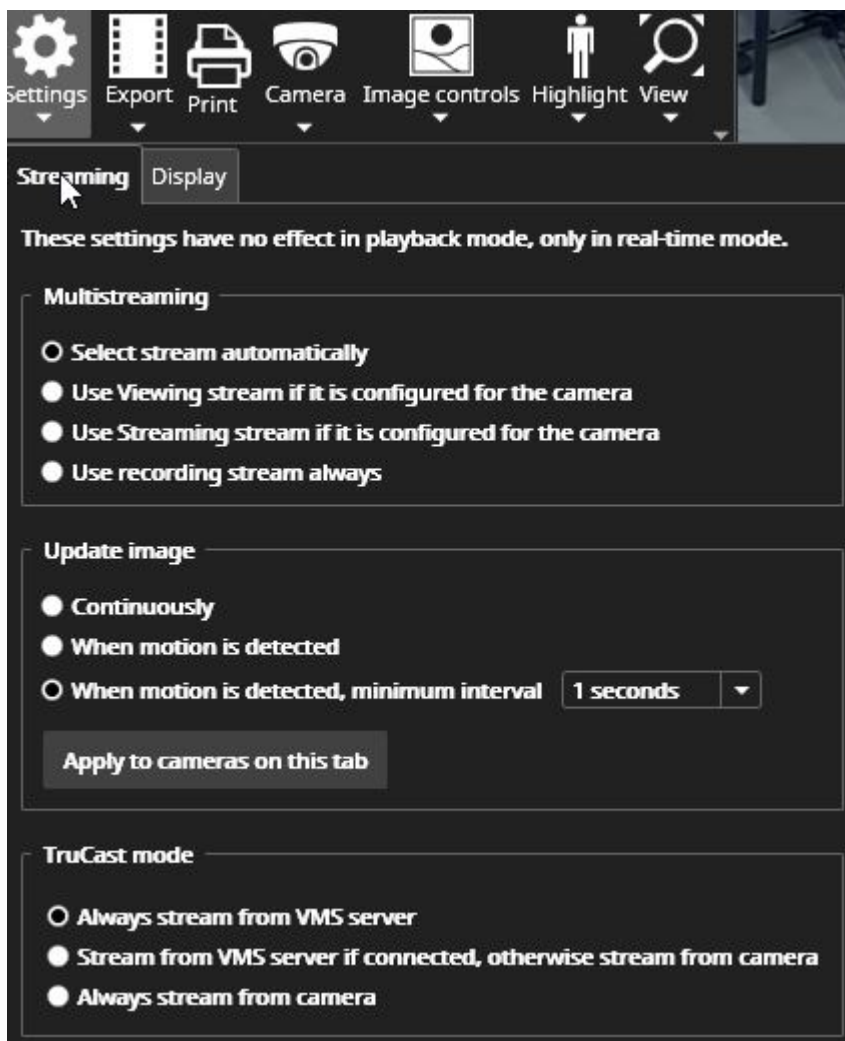


1.12.4. Using TruCast

Using TruCast

The user can see the cameras that have TruCast capability from the camera toolbar – settings.

For those cameras that have TruCast the setting is available.



For cameras that do not have TruCast, the lower part of the dialogue is disabled.

Administrator Guide V9 - EN

The setting is memorized for each camera separately.



When TruCast is active, there is a small arrow displayed on top of the camera in the device tree.

1.13. Failover Servers

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.

Analogue cameras connected to a server's capture card will not be transferred to the failover server. Only previously assigned IP cameras are reassigned during the switch.

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 Master 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 Master Server, one video recording VMS Server, and one standby failover server.

Failover migration will be triggered in the following conditions:

- The Master Server has lost the connection to a VMS Server, and the timeout set by the administrator has been reached

Administrator Guide V9 - EN

- A VMS Server has informed the Master 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 Master 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.

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.

1.13.1. Minimum requirements

Minimum Requirements

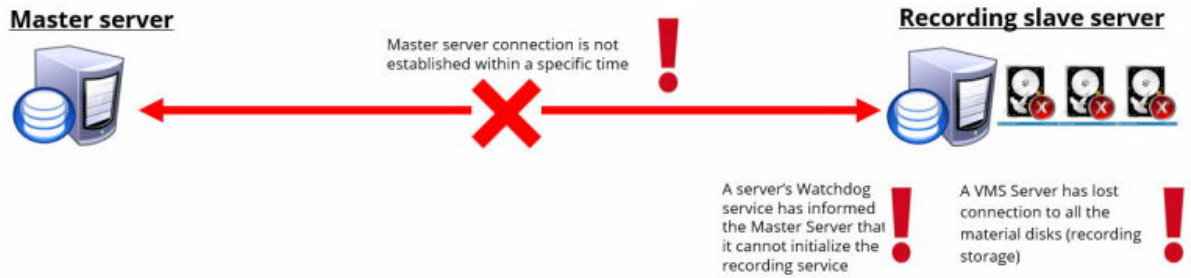
- **Master server installed on separate PC**
 - The license must contain an automatic backup feature
 - The license must contain one or more failover server
- **1 slave server for recording**

1 standby failover server

- The license must contain at least the same amount of video channels as recording slave server
- Same size material HDD and assigned drive letters

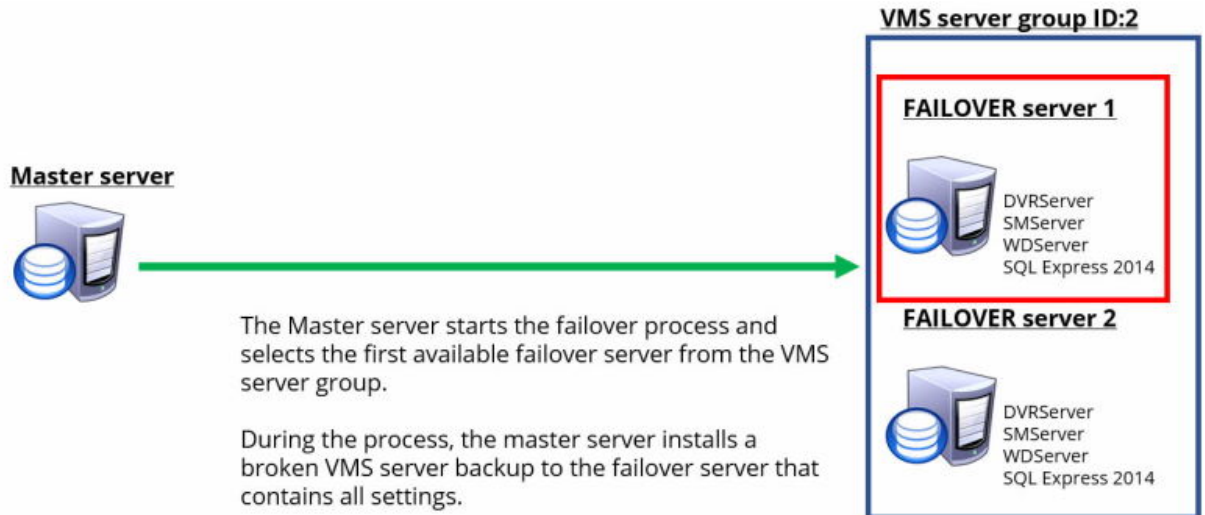


1.13.2. FAILOVER trigger conditions



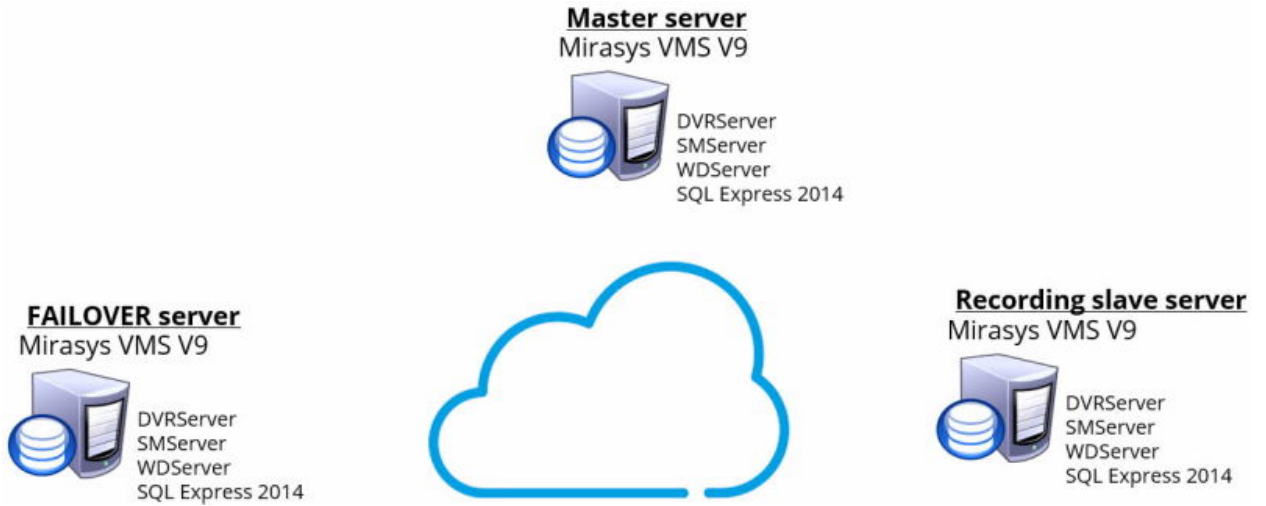


1.13.3. FAILOVER process





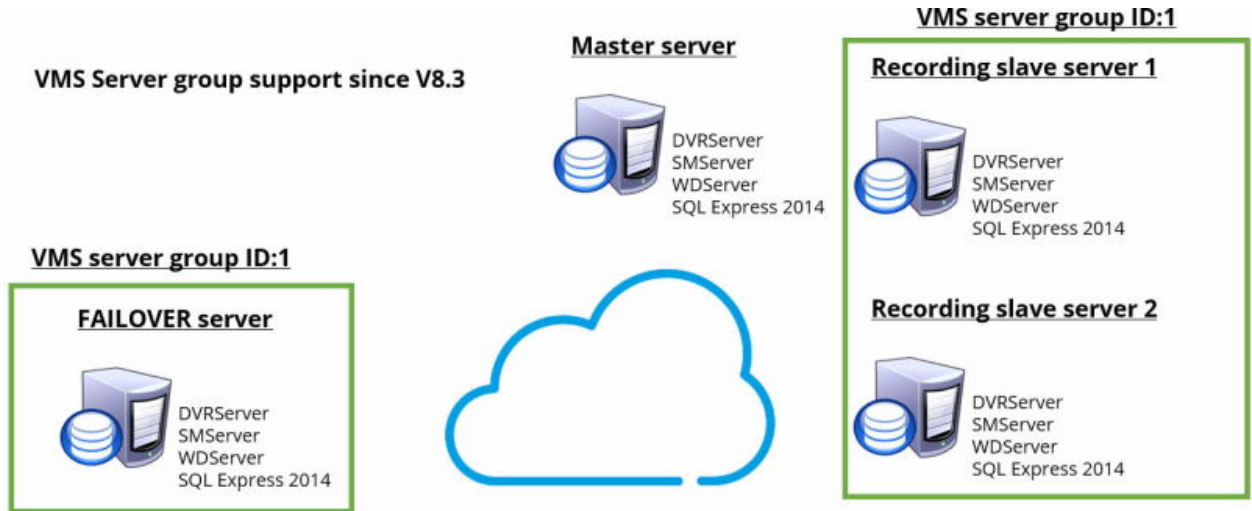
1.13.4. FAILOVER MINIMUM SCENARIO





Administrator Guide V9 - EN

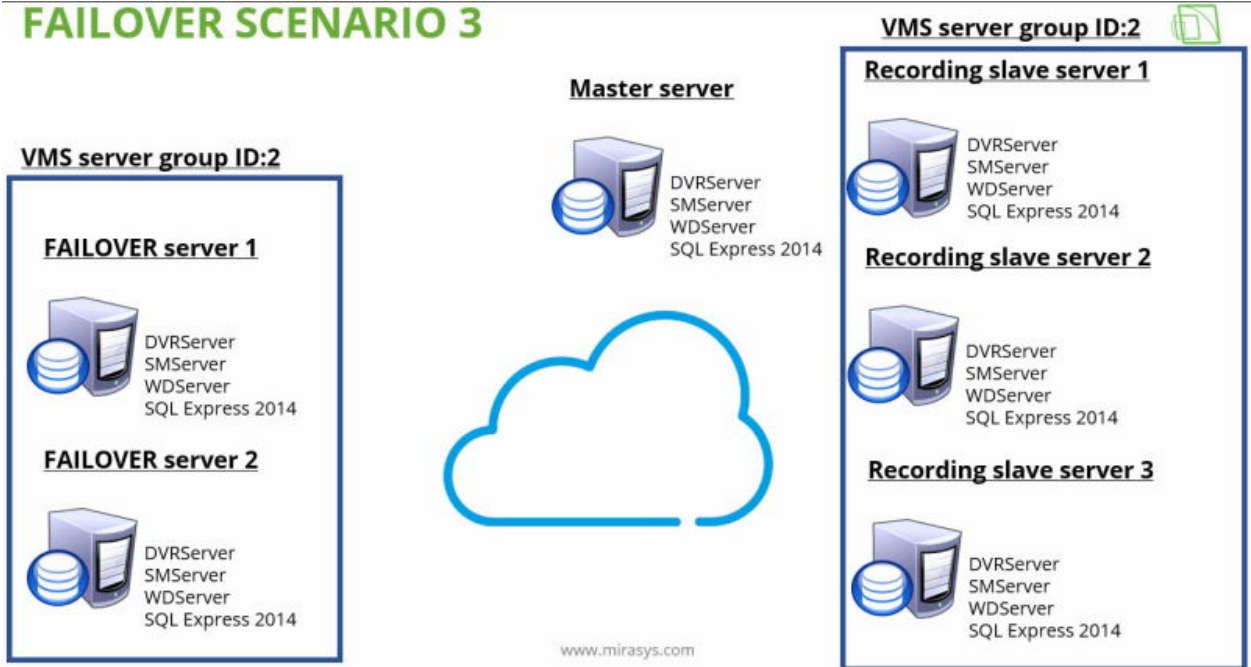
1.13.5. FAILOVER SCENARIO 2





1.13.6. FAILOVER SCENARIO 3

FAILOVER SCENARIO 3



1.13.7. VMS Server roles

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.

VMS Server role BROKEN

The Broken VMS Servers group displays connection states; the settings on broken servers cannot be changed.

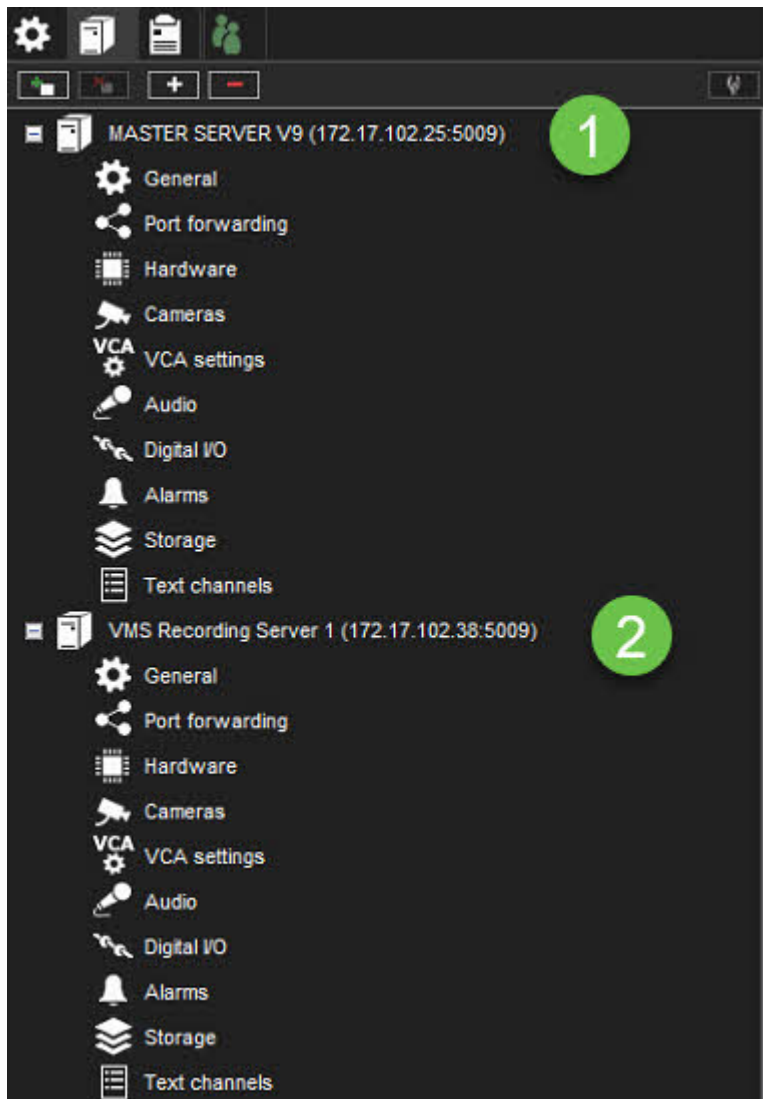
Users can, however, export server logs if there is a connection to a broken server.

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.

1.13.8. Building Failover system

Starting point

The master server and 1 recording slave server were added to the system

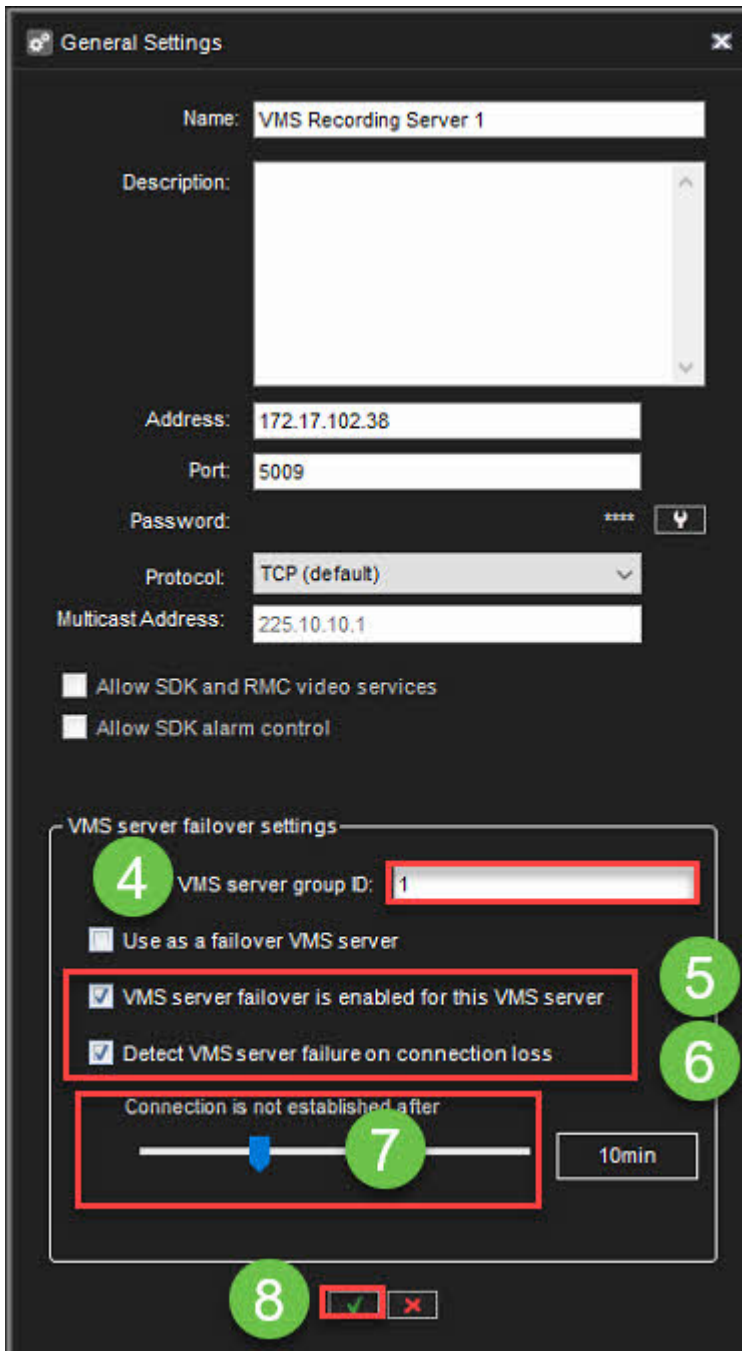


Enabling VMS failover server to the recording server

1. Open the **VMS Servers** tab
2. Select slave server 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**

Administrator Guide V9 - EN

7. Define value **Connection is not established an after**
8. Click **OK**



General Settings

Name: VMS Recording Server 1

Description:

Address: 172.17.102.38

Port: 5009

Password: ****

Protocol: TCP (default)

Multicast Address: 225.10.10.1

Allow SDK and RMC video services

Allow SDK alarm control

VMS server failover settings

4 VMS server group ID: 1

Use as a failover VMS server

5 VMS server failover is enabled for this VMS server

6 Detect VMS server failure on connection loss

7 Connection is not established after

10min

8 OK Cancel

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**

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland

Tel +358 (0)9 2533 3300

info@mirasys.com

www.mirasys.com



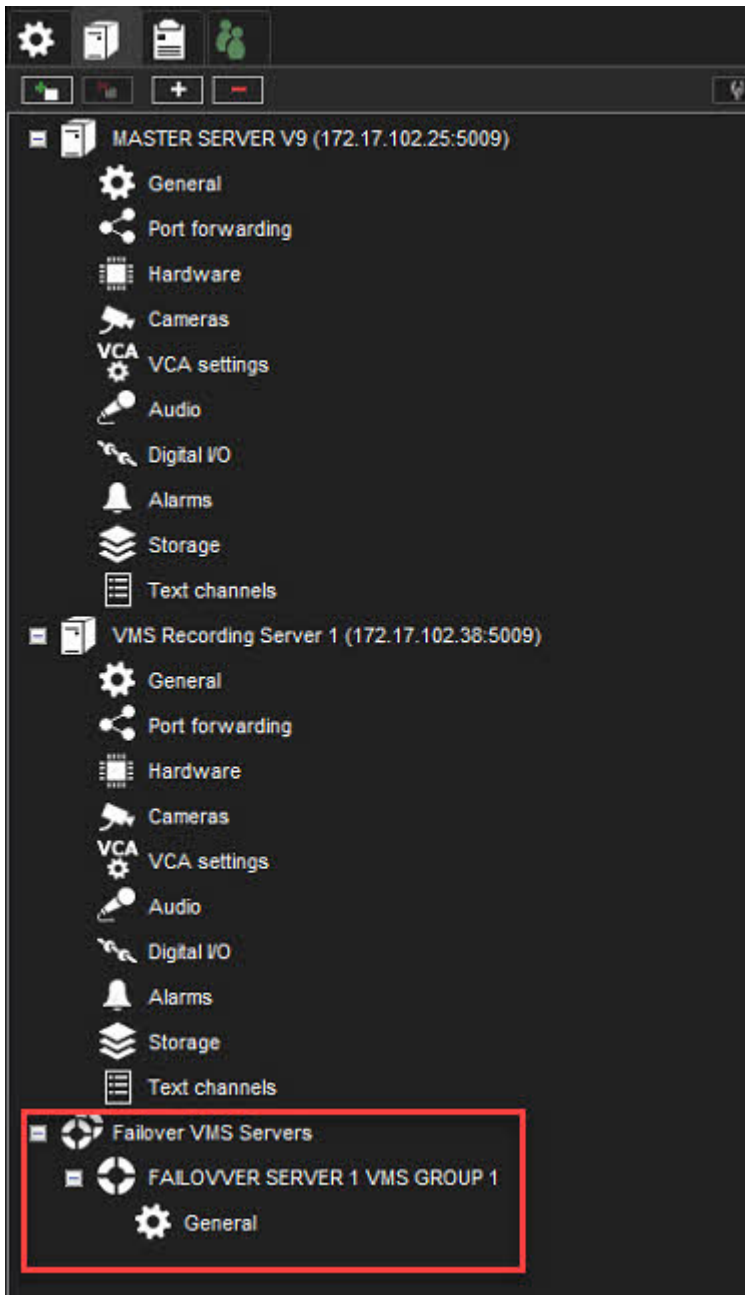
Administrator Guide V9 - EN

6. Enable **Use as a failover VMS server**
7. Click **OK**

After the adding, the VMS Server tab shows **Failover VMS Server** line



Administrator Guide V9 - EN



1.13.9. Restoring the fixed server to the system

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.

1.14. Easy LPR

EASY LPR is camera-based LPR detection. Supported cameras are:

- Hikvision 7-series LPR cameras
- Axis cameras, which support Vaxtor VaxALPR, version 2.2-20 and AXIS License Plate Verifier version 2.1-0
- Dahua ITC215-PW6M-IRLZF, firmware 2.625

EASY LPR main features

- Live monitoring from the one camera at the same time
- Plate number search from the one camera at the same time
- Plate number list Management
 - Black list
 - White list
- Importing and exporting plate number lists
- Uploading plate number list to the cameras
- Digital output controlling based on:
 - Other plate detected
 - Black list plate detected
 - White list plate detected

1.14.1. Configuration process

1. Configure LPR functionality to the used cameras. Please see the manufacturer website for more information
2. Add cameras to the Mirasys VMS
3. Check that Mirasys VMS license support LPR cameras
4. Enable Easy LPR

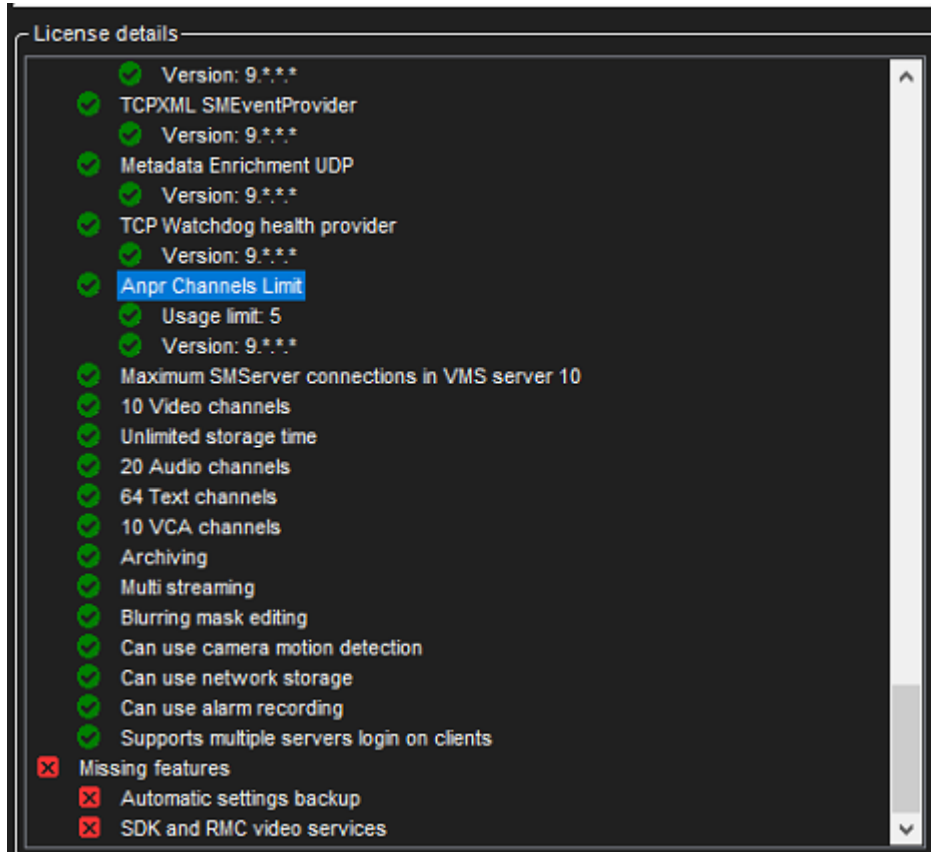


Administrator Guide V9 - EN

1.14.2. Licensing

Mirasys VMS server license defines that how many ANPR channels can be added.

The feature name is **Anpr Channels limit** and controllable value name **Usage limit**

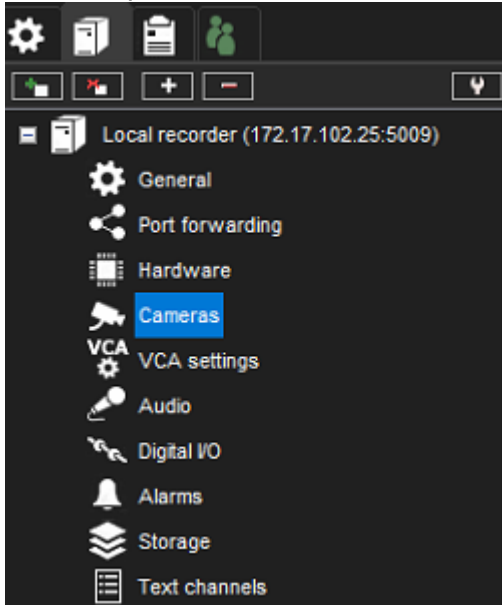




Administrator Guide V9 - EN

1.14.3. Enabling Easy LPR

1. Open **VMS servers**
2. Open **Cameras**



3. Click **VCA features**
4. Select LPR camera
5. Enable **Easy LPR**
6. Click **Save**



Administrator Guide V9 - EN

Camera Settings

General | Motion Detection | **VCA features** | Privacy | Scheduler

Camera: AXIS P1455-LE
VCA Stream: Default

In use	Used / Available	VCA feature	Description
<input type="checkbox"/>	0/10	Motion data	Enables motion data collection and be able to use follow motion and motion highlight. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps
<input type="checkbox"/>	0/10	VCA Core	Enables all VCA features including alarms, follow motion and motion highlight. Use VCA settings to configure VCA.
<input checked="" type="checkbox"/>	1/5	Easy LPR	Enables camera to be used in Easy LPR client plugin.

List of available VCA features

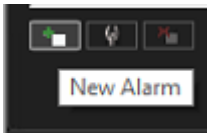
Used VCA features summary

Camera	VCA features used	Notes
AXIS P1455-LE	Easy LPR	

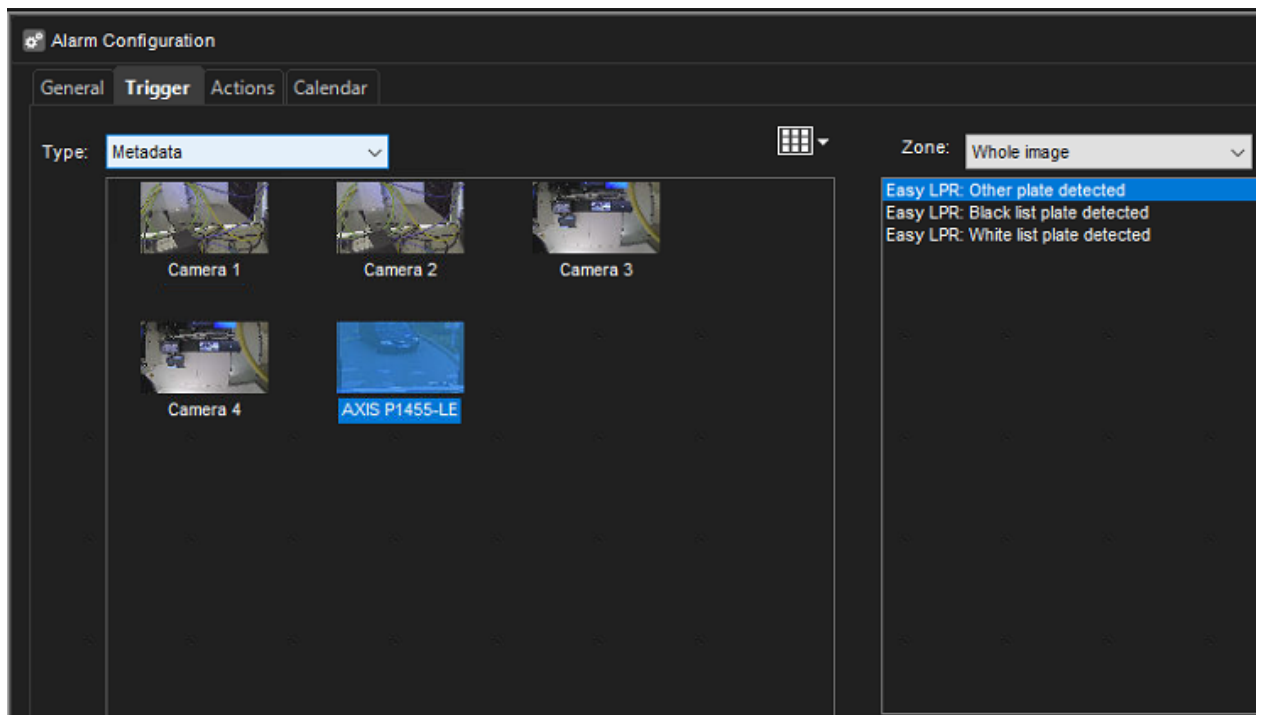
6

1.14.4. Creating an alarm from Easy LPR event

1. Go to the **VMS Servers** tab
2. Open **Alarms**
3. Click **New Alarm**



4. Enter all needed information in the **General** tab
5. Open **Trigger** tag
6. Select trigger type **Metadata**
7. Select LPR camera
8. Select correct event:
 - d. **Easy LPR: Other plate detected**
 - e. **Easy LPR: Black list plate detected**
 - f. **Easy LPR: White list plate detected**




8. Enter the actions of the alarms
9. Set calendar
10. Check overall view of the alarm
11. Click **OK** to confirm an alarm creation

Administrator Guide V9 - EN

Alarms

Name	Priority	Trigger	Actions
Black list plate detected	Normal	Metadata on channel AXIS P1455-L1-E	Record video from Camera 1

Name: Black list plate detected
Description: Normal
Priority: Normal
Requires Acknowledgment: No
Viewable in Profiles: v9.4
Metadata on channel: AXIS P1455-L1-E
Trigger: Activate on metadata event Easy LPR: Black list plate detected



Record video from Camera 1
Resolution: 3840x2160
Recording rate: 25/s
Pre-event recording: Off
Post-event recording: On
Pre-event recording time: 0 s
Post-event recording time: 10 s
Calendar: The alarm is always enabled
Special Days: