MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V8

Table of Contents

1. Administrator Guide V8 - EN 7
1.1. Before You Start 8
1.1.1. Help Documentation 9
1.1.2. Overview of This Guide 10
1.1.3. Technical Support 11
1.1.4. What's New 12
1.2. About the System 14
1.2.1. What is Mirasys Software? 15
1.2.2. OS Compatibility 18
1.3. Configuring the System 20
1.4. Logging In 21
1.4.1. Locking System Manager 24
1.5. Management User Interface 25
1.6. VMS Servers 27
1.6.1. Adding and Removing VMS Servers 28
1.6.2. Configuring VMS Servers 30
1.6.3. Failover Servers 32
1.6.4. Failover Licensing 34
1.6.5. An Example Redundant Architecture With Failover 35
1.6.6. VMS Servers (Normal, Failover, Broken) 36
1.6.7. Failover Servers in System Manager 37
1.6.8. Adding and Removing Failover Servers 39
1.6.9. Restoring System To Normal State After Failover 40
1.7. Port Forwarding 41
1.7.1. Installer Option 42
1.7.2. System Manager 43
1.7.3. Automatic Router Configuration 44
1.7.4. Single Server Behind Router 45

1.7.5. More Than One Server Behind Router..... 46
1.7.6. More Than One Server On Multiple Sites..... 47
1.8. Cameras..... 48
1.8.1. Adding and Removing IP Cameras..... 49
1.8.2. Limiting the Camera Configuration to Certain Camera Drivers...52
1.8.3. IP Camera Search Modes..... 53
1.8.4. Camera Audio Channels..... 55
1.8.5. Editing Camera Settings..... 56
1.8.6. General settings..... 57
1.8.7. Motion Detection..... 60
1.8.8. Video Content Analytics..... 63
1.8.9. Privacy..... 65
1.8.10. Scheduler (Video)..... 67
1.8.11. Multi-Streaming..... 70
1.8.12. Edge Storage..... 71
1.8.13. Multi-Casting..... 72
1.9. Audio..... 74
1.9.1. Adding, Editing and Removing Audio Devices..... 75
1.9.2. Audio Settings..... 77
1.9.3. General Settings..... 78
1.9.4. Audio Detection..... 80
1.9.5. Scheduler (Audio)..... 81
1.9.6. Audio Communication Settings..... 82
1.10. Digital I/O..... 83
1.10.1. Digital I/O Settings..... 84
1.10.2. Logical I/O..... 88
1.10.3. Countdown I/O..... 93
1.11. Video Outputs..... 95
1.11.1. Video Output Settings..... 96
1.12. Alarms..... 98

1.12.1. Alarm Settings..... 99
1.12.2. Accessing the Alarm List..... 100
1.12.3. Adding a New Alarm..... 101
1.12.4. Editing an Alarm..... 106
1.12.5. Deleting an Alarm..... 107
1.12.6. Action Types and Settings..... 108
1.12.7. Holiday Schedules..... 115
1.13. Storage..... 117
1.13.1. Storage Settings..... 118
1.13.2. Adding Storage Space..... 119
1.13.3. Storage Settings..... 121
1.13.4. Automatic Deletion of Video, Audio and Text Data..... 122
1.13.5. Archiving..... 124
1.14. Text Channels..... 126
1.14.1. Text Channel Settings..... 127
1.15. Profiles..... 129
1.15.1. Adding and Editing Profiles..... 131
1.15.2. Adding Device Groups and Devices to a Profile..... 133
1.15.3. Adding Profile specific Web page instances..... 136
1.15.4. Editing Profile Specific Alarm Settings..... 137
1.15.5. Adding Maps to Profiles..... 139
1.16. Users..... 141
1.16.1. User Roles..... 142
1.16.2. Adding New User Groups..... 143
1.16.3. Adding New Users..... 144
1.16.4. Domain Based User Groups (LDAP)..... 145
1.16.5. Editing User Groups..... 147
1.16.6. Deleting User Groups..... 148
1.16.7. System manager enterprise role..... 149
1.16.8. Spotter role customization..... 153

1.16.9. Monitoring Users..... 160
1.16.10. Logging Users Off..... 161
1.16.11. Disabling or Activating a User Account..... 162
1.16.12. Two-factor authentication..... 163
1.17. System..... 166
1.17.1. General System Settings..... 167
1.17.2. Using the System in Dual-Password Mode..... 168
1.17.3. E-Mail Settings..... 169
1.17.4. Managing Server Addresses..... 171
1.17.5. Managing System Addresses (Master Server Addresses)..... 172
1.17.6. Updating VMS Servers..... 174
1.17.7. Exporting Log Files..... 177
1.17.8. Backing Up Settings..... 178
1.17.9. Restoring Settings..... 179
1.17.10. System Management Diagnostics..... 181
1.17.11. Server Diagnostics..... 183
1.17.12. Licenses..... 187
1.17.13. Watchdog..... 189
1.18. Installing New Drivers and Plugins..... 192
1.18.1. Installing External Driver Packages..... 193
1.18.2. Installing Metadata Drivers..... 195
1.18.3. Installing Client Drivers..... 196
1.18.4. Removing Drivers..... 197
1.18.5. Installing Spotter Plugins..... 200
1.19. TruCast..... 201
1.19.1. Supported Cameras..... 202
1.19.2. Network Optimization..... 203
1.19.3. Impact of Multistreaming and TruCast for Network Optimization and Storage..... 205
1.19.4. Other Information..... 206

1.19.5. Configuration..... 207
1.19.6. Using TruCast..... 209

1. Administrator Guide V8 - EN

Next

1.1. Before You Start

Top Previous Next

1.1.1. Help Documentation

This help documentation, for example, is available:

1. *Installation Guide*: This shows how to install the VMS servers and the client programs. It also shows how to add devices to the system.
2. *Administrator's Guide*: This shows how to use the System Manager program for configuring the system.
3. *Spotter User Guide*: Complete instruction on how to operate all features of the Mirasys Spotter program. (Not available in all languages.)
4. *VCA Installation and Configuration Guide:* Instructions on how to install and configure Mirasys Video Content Analytics.

The PDF help documentation is on the VMS installation limited and the full setup package that can be downloaded from the Mirasys Extranet.

You can also access the *Administrator's Guide* and the *User's Guide* by clicking **Help** in the System Manager or Spotter programs.

Top Previous Next

1.1.2. Overview of This Guide

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

Top Previous Next

1.1.3. Technical Support

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

Top Previous Next

1.1.4. What's New

The lists below include only select information. For a full list of new features and changes, please refer to the Release Notes included in the installation packages.

NOTE: Microsoft SQL Server Express 2014 or the full Microsoft SQL Server 2014 is required to be installed on the Master Server (in single server installations the only server is the Master Server) and on networked recording VMS servers (nodes or slaves) when Mirasys VCA (Video Content Analytics) is to be utilized.

New features in version 8:

- New Mirasys TruStore storage file system.

  IMPORTANT: The TruStore storage file system is not compatible with earlier storage, and old stored material will be removed at install. Archive or export any material you wish to retain when upgrading to Version 8.
- The spotter can be used to simultaneously connect to multiple different Master Servers (license controlled add-on feature). Server selection has been moved from the Spotter login window to the application launcher dialogue. It is also possible to directly create desktop shortcuts that connect to a certain Master Server.
- Spotter look and feel has been modernized, and more functions are now available from the device tree and the new title menu. Hotkeys can be used to change view modes on the fly. Certain view components also have detailed configuration options for advanced users.
- Controlled playback for user groups: Ability to restrict users to have playback access only to up to 24 hours into the past.
- Alarms can have a custom colour.
- The Workstation client application is no longer available!
- The user can specify to show certain or all alarms on the Spotter time slider.
- Support for multiple alarm popup monitors.
- Ability to open the camera to search and analyse plugins from the device tree.
- Fast Bookmark button.
- Data cache for activity data.
- I/O devices can be attached to take over a whole device tab grid cell, making them easier to operate.
- PTZ (dome) camera control "aiming point" has been changed to be less intrusive, and the size can be adjusted from the Spotter configuration file.

- TruStream support: for multi-streaming cameras. A spotter will automatically choose a stream that matches best the grid cell resolution that the camera is displayed in.
- Certain product variants contain both a dark and light visual theme for Spotter.
- The numeric keypad device number popup dialogue can be positioned freely anywhere on the Spotter window.
- The AVM operator console can be positioned in a fixed camera grid cell.

Top Previous Next

1.2. About the System

Top Previous Next

1.2.1. What is Mirasys Software?

Mirasys software is a distributed, digital video management system (VMS or DVMS) for video and audio surveillance applications.

The software can be used for monitoring real-time and recorded video, audio and text data, and to control PTZ cameras, I/O devices and IP cameras.

The software supports systems consisting of both analogue and/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 both separately and as 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.

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** (“nodes,” if the system consists of multiple servers)
- Client programs:
  - Mirasys VMS System Manager
  - Mirasys VMS Spotter for Windows
  - Mirasys VMS Spotter Mobile
  - Mirasys VMS WebClient

VMS Servers

The VMS servers record video and audio from multiple cameras and audio channels and write the data on hard disks. You can access a VMS Server locally or over a network by using the System Manager and Spotter programs, and monitor server functionality through the Spotter Diagnostics plugin.

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

In addition, you can connect these devices 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
- Monitors
- Printers
- Backup unit (NAS, SAN, or RAID, for example)

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. In a larger system, it is recommended that the Master Server is a dedicated server for this purpose alone.

NOTE: *Master Servers must have SQL Server Express 2014 or another 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 event.
- It stores alarms.
- It stores audit trail.

Client Programs

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

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

- Monitoring the system.

End-users use the **Spotter** program, for example, for these tasks:

- 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
- Control automatic license plate recognition systems via the optional, separately sold ANPR+ software

The **Workstation** client is the legacy client that is no longer supported. If you must use **Workstation** you need to use Mirasys VMS V7.5.10, or earlier.

NETWORK REQUIREMENTS

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

Please see the *Mirasys VMS Installation Guide*, the *Mirasys Networking White Paper* and the *Mirasys Network Storage White Paper* for information on networking recommendations, limitations and rules

Top Previous Next

1.2.2. OS Compatibility

Mirasys VMS V8 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 client application	Spotter for Windows client application
Windows 2012 Server Standard Edition	-	X	X	X	-
Windows 2012 Server R2	-	X	X	X	X
Windows 10	-	X	X	X	X
Windows Server 2016	-	X	X	X	X

NOTES:

- Mirasys VMS has not supported Windows XP since Mirasys VMS version 6.4. If Windows XP support is required, do not install Mirasys VMS 6.4, or any later releases.
- Make sure that the “Desktop Experience” feature is activated for Windows server operating systems.

- *No releases before Mirasys VMS V7.4 has support for Windows 10. Any older versions (V7.3 or older), if used with Windows 10, must be upgraded to the latest V7.4 release, or later versions.*

Top Previous Next

1.3. 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 that is 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.*

Top Previous Next

1.4. 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

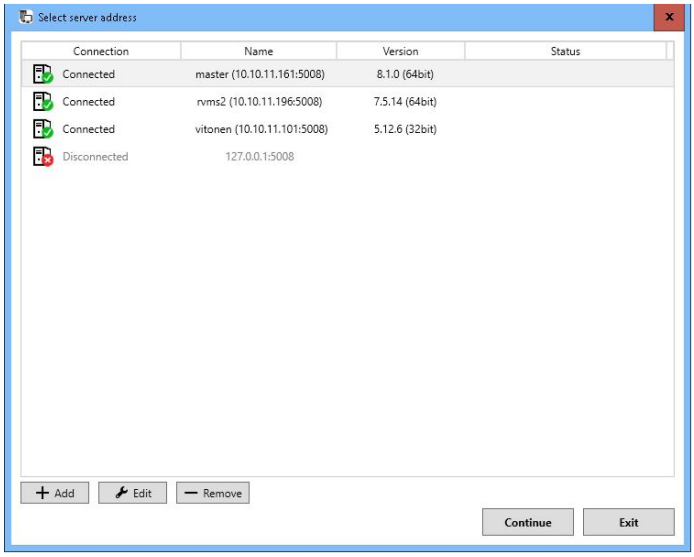
Password: 0308

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:

1. Do one of the following:
1. Double-click the shortcut icon **System Manager** on the desktop.
2. Click **Start**, point to **Programs** and then to **DVMS**. Click **System Manager**.

2. In systems that have only one Master Server address configured, the System Manager login screen is shown.
3. In systems that have multiple master addresses configured, or if the user presses the “Delete” key in the initial startup phase, the site selection screen is shown.
    b. On this screen, the user can add, remove or edit Master Server addresses, or choose a server to log on. After choosing a server and pressing the “Continue” button, the user is taken to the login screen.



4. On the login screen, type your user name in the **User name** box, and your password in the **Password** box.

Note: *The user name and password are case sensitive.*

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

After the program starts, the user interface is shown.

Note: *Only one user can be logged in with System Manager administrator rights at any given time. If additional users with administrator rights try to log into System Manager, they are given system monitoring rights, allowing them to view the system settings.*

To log off in order to change users:

1. Do one of the following:
3. On the menu bar, click **File** and then **Exit**.

4. On the menu bar, click **User** and then **Log off**.
5. On the status bar, click **Exit** (in the lower-right corner of the screen).
2. In the **Log Off** dialogue box, select **Log off current user** and click **OK.**

To quit the program:

1. Do one of the following:
6. On the menu bar, click **File** and then **Exit**.
7. On the menu bar, click **User** and then **Log off**.
8. On the status bar, click **Exit** (in the lower-right corner of the screen).
2. In the **Log Off** dialogue box, select **Exit** and click **OK.**

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.

Top Previous Next

1.4.1. 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:

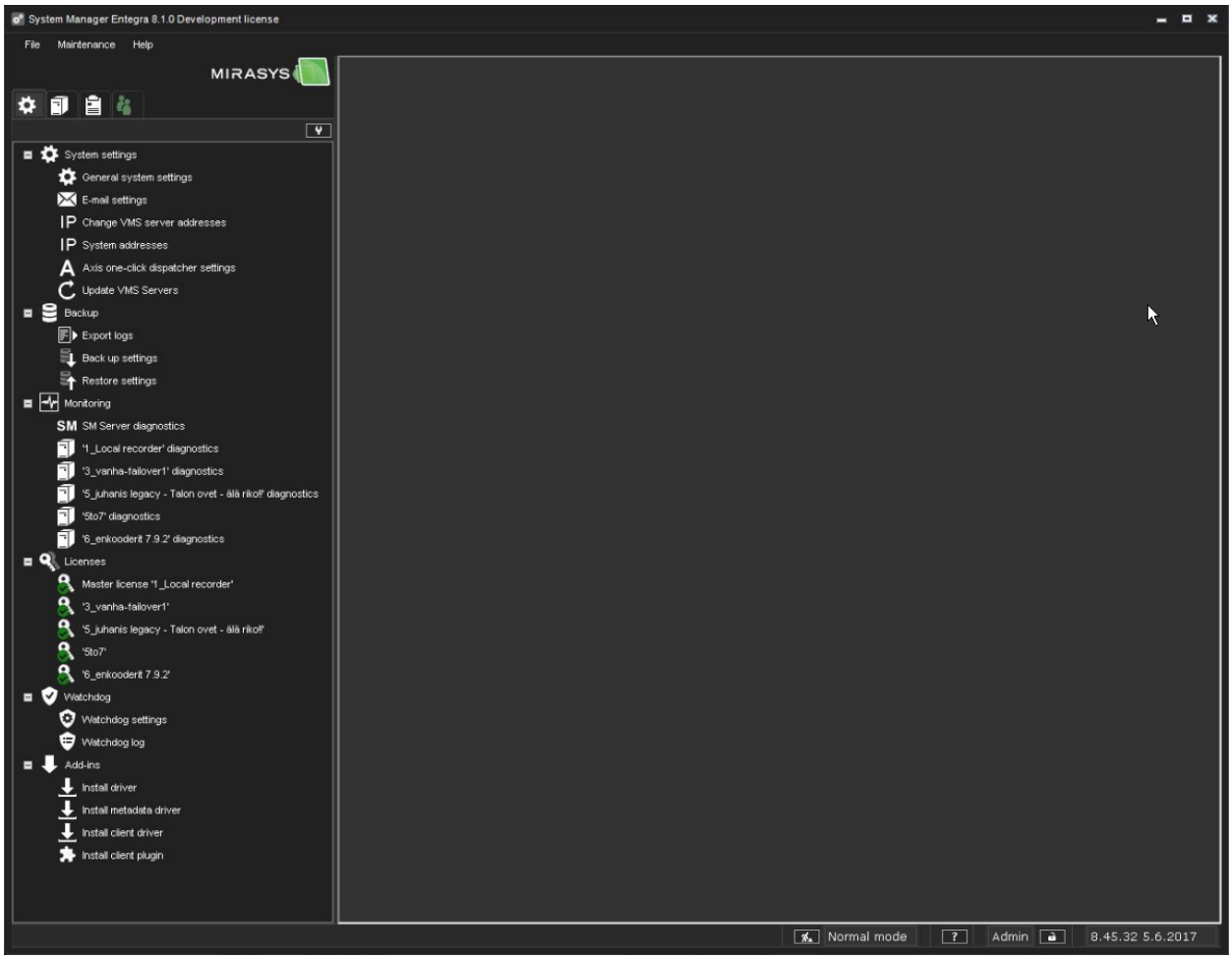
1. On the menu bar, click **File** and then **Lock Program**.
2. On the status bar, click **Lock program**.

To unlock the program:

3. 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.*

Top Previous Next

1.5. Management User Interface



The System Manager User interface

The System Manager User Interface contains these elements:

A. Menu bar.

- Click **File** and **Lock Program** to lock the program or click **Log Off** to log off from the program.
- Click **File** and **Import** or **Export** to introduce camera data for example location data.
- Click **Maintenance** and **Set maintenance state on** to control the failover transition state off.
- Click **Help** and then **About** to see information about the program version. Or click **Help** and then **Help Topics** to use the online guide.

B. Navigation pane. Contains these tabs: **System, VMS Servers, Profiles,** and **Users.**

C. Service list. Contains services, devices, users, and tools, depending on which tab has been selected from the **Navigation pane (B)**.

D. Status bar. Shows the current date and time and whether the system is in a Normal or Maintenance state. Also contains buttons for showing the online help, for locking the program, and for logging off from the program.

You can perform these tasks on the tabs:

1. Backup system settings, install new system drivers (camera, metadata or client drivers) or install client plugins, on the **System** tab. The tab also contains diagnostic tools, backup tools, and license information.
2. Add servers to the system and configure them on the **VMS Servers** tab.
3. Add and edit user profiles on the **Profiles** tab.
4. Add and edit user accounts on the **Users** tab.

Top Previous Next

1.6. VMS Servers

These sections describe how to add VMS Servers (nodes) to the system and how to configure their settings.

Top Previous Next

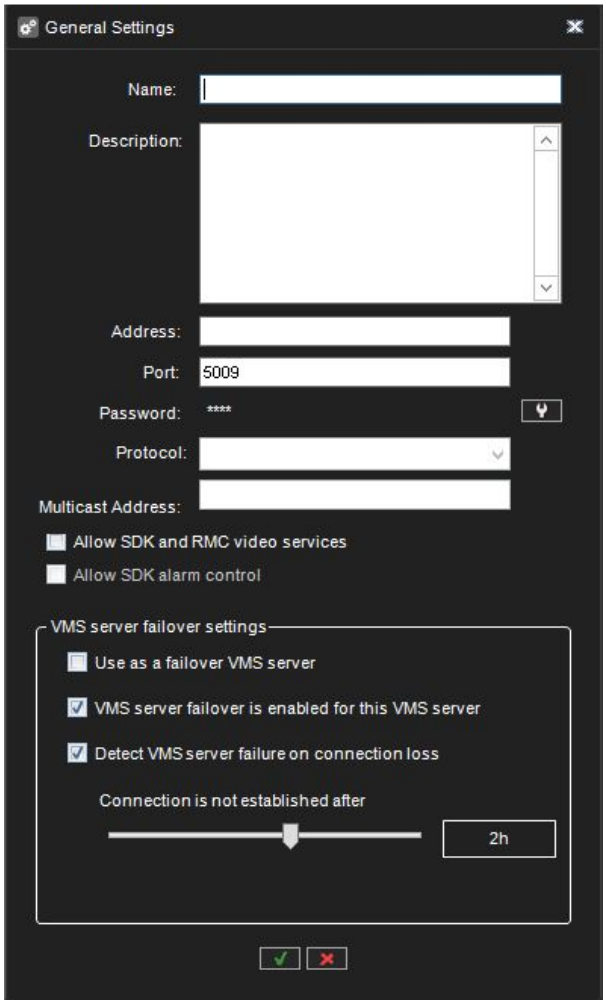
1.6.1. Adding and Removing VMS Servers

You can have (depending on the license) from 1 to 150 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:

1. Open the **VMS Servers** tab .
2. Click **Add VMS Server**
3. The **General Settings** dialog box is shown.



4. Do the following:
1. Type a descriptive name for the server.
2. Type a description of the server. The description is shown only on this tab.

3. Type the IP address or DNS name of the server.
4. To specify a password for the server or to change the existing password, click **Change Password** and type the password in the **New password** and **Confirm new password** boxes. If the server already has a password, you will be prompted for the existing password before the server is added to the system and the password changed.
5. If the server is used as part of an integrated system or with the Mirasys Remote Monitoring Center system, select **Allow SDK and RMC video services.**
6. If the server is to receive alarms from an integrated system, select **Allow SDK alarm control.**
7. If the server is to be used as a failover server, select the box. **"use as a failover VMS Server"**
5. Click **OK**. The server and the devices connected to it (for example, cameras and audio channels) are added to the list.
   Note: *If the server is password-protected, the system prompts for the password.*

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:

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

Top Previous Next

1.6.2. Configuring 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.
	Video outputs	Set video output settings.
	Audio communication	Set up a port or gate phone.
	Alarms	Set up alarm conditions and alarm actions.
	Storage	Add a hard disk to a server and set the storage times

		for video, audio, and alarm files.
	Text channels	Set the names and descriptions of text data channels here.

To access the settings, do one of the following:

1. Select the settings that you want to configure (for example, **Cameras**) and then click **Edit** in the lower-right corner of the navigation pane.
2. Double-click the settings that you want to configure.
3. Drag the settings from the **VMS Servers** tab to the workspace.

Top Previous Next

1.6.3. Failover Servers

Mirasys VMS supports failover video servers as a Mirasys VMS option.

Failover servers are VMS Servers that are 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 broken 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 ANPR+ or Reporting+) 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 as well as 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 normal server or a failover server. There can be any number of failover servers (0-n).

If the server is a normal 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. So, 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
- 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

The recording is continuous after the failover server has taken over to keep the operation of the system smooth. The only exception being the timeout time between disconnect and failover trigger. This is configured by the administrator.

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.

Top Previous Next

1.6.4. Failover Licensing

The Failover functionality uses automatic backups generated by the *SMServer* service when doing failover, and therefore the system must have an automatic backup option enabled; either as an Automatic Flash backup in Mirasys provided systems or a non-Flash based backup in hardware provided by another hardware distributor. This option is delivered as an optional license upgrade.

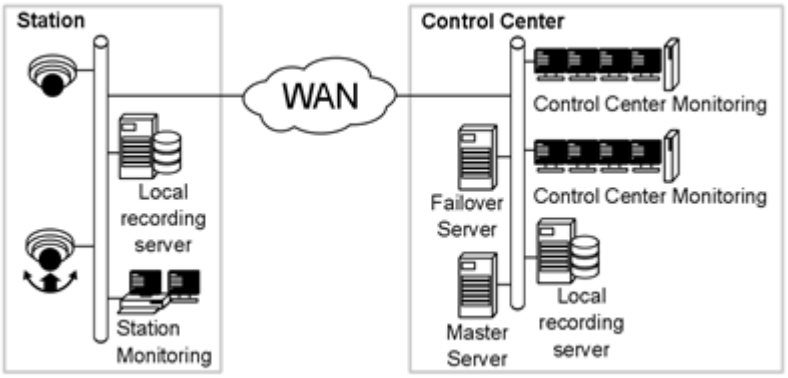
For the failover feature to function, the Master Server license has to have one or more failover servers in its license.

Broken servers will not reserve recording licenses from the license count.

All licenses in a failover installation should be of the same version.

Top Previous Next

1.6.5. An Example Redundant Architecture With Failover



A surveillance station has a local network connecting a local server that serves as the data recording device for the surveillance systems in the network; the surveillance devices themselves (e.g., IP cameras and PTZ cameras), some of which may support on-board data storage (Edge Storage); and a security station running a Spotter for Windows client.

The control centre houses the system network's failover and Master Server. The failover server can take over when a station's local VMS Server becomes unusable.

The Master Server serves as the central control entity of the system. Control centre monitoring is usually with AVM (Agile Virtual Matrix) multiple screen setups (desktop or video wall) with their own Display Servers.

The VMS Server and failover server need to be similar in terms of hardware and assigned drive letters. Please note that the Master Server needs to be installed on separate hardware.

Top Previous Next

1.6.6. VMS Servers (Normal, Failover, Broken)

When adding a new server, the user can select if the added server is a normal server or a failover server. If a server is added as a normal server, the user can adjust the following factors:

- VMS Server failure is detected on that server
- Whether to trigger failure if the server continuously disconnects
- The length of the disconnection to trigger the server failure

To be able to set a server as a failover server, there has to be a free failover license slot available.

The users can change server states (normal or failover) and failover settings from the server's general settings in the System Manager application.

When a server is added as a failover server, the System Manager sets the server to standby mode.

The device tree in the **VMS Servers** tab in System Manager shows failover and broken servers in their own groups (under *Failover VMS Servers* and *Broken VMS Servers*).

The *Failover VMS Servers* group shows server connection states and server general settings if the connection is available.

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.

Top Previous Next

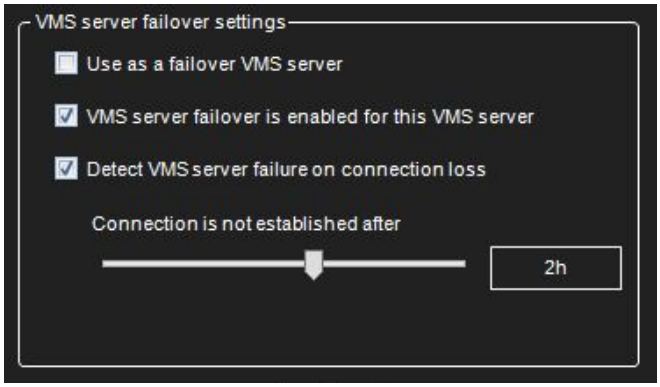
1.6.7. Failover Servers in System Manager

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 the duties of any server that is defined to be under failover protection.

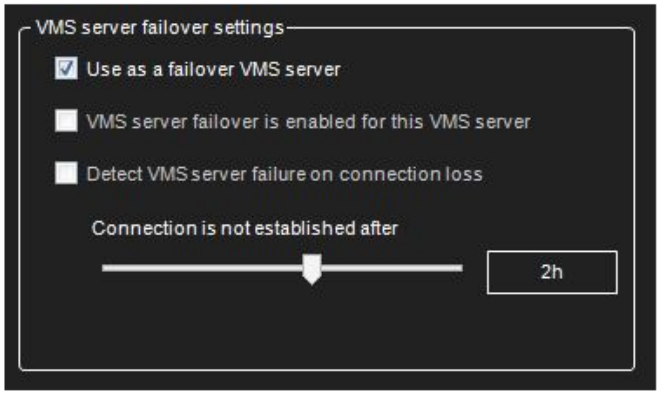
Failover servers must have the same file system (same drive letters) as the VMS Servers that are under failover protection, and they can only be used for IP camera backup purposes.

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 are moved under the *"Broken VMS Servers"* folder and any available failover server shall take the responsibilities of the broken 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 longer than a defined time period.



Example server that is under failover protection, if inaccessible longer than 2 hours, the failover switch would happen.



Adding a failover server

Failover servers in the VMS Server *list*

Top Previous Next

1.6.8. Adding and Removing Failover Servers

Adding and removing a failover server is done in the same way as a normal server, except, the check box **“use as a failover VMS Server”** is selected.

Top Previous Next

1.6.9. Restoring System To Normal State After Failover

To restore the system to normal operation mode after the failed server was repaired or investigated to contain no issues:

1. Open the **System** tab
2. Double-click **Restore settings**

and locate a system backup (.vbk) file that contains settings from the time when the system was in operation with the normal status.
3. Restore the system with this file. Be sure to select the option "**Do automatic settings backup after successful settings restore"**

Top Previous Next

1.7. Port Forwarding

The basic idea with port forwarding is that it is possible to access one or more VMS Servers or Master Servers that are behind a router that does Network Address Translation (NAT).

Typically, this kind of situation happens when the client is outside the network and needs to access servers inside a company network.

Top Previous Next

1.7.1. Installer Option

When installing a VMS Server, the installer offers the option to turn on the automatic port forwarding. The default state is off

Top Previous Next

1.7.2. System Manager

If the port forwarding is not activated when the system was installed, it can be activated from the system manager second tab “VMS Servers”.

Open the view “Port forwarding” and activate the selection “UPnP is in use”

Top Previous Next

1.7.3. 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 has to be enabled on the device.

The server has continuous UPnP device discovery when it is 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 that was done automatically, he can do this from the system manager.

After this, the server will remember that the settings were removed and will not do port forwarding again 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 because deleting the port forward mapping would disconnect the system and no further configuration would be possible.

If port forward settings are changed and the connection to the server has not returned after a while, then it might be necessary to reboot the router.

Servers need 4 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...)

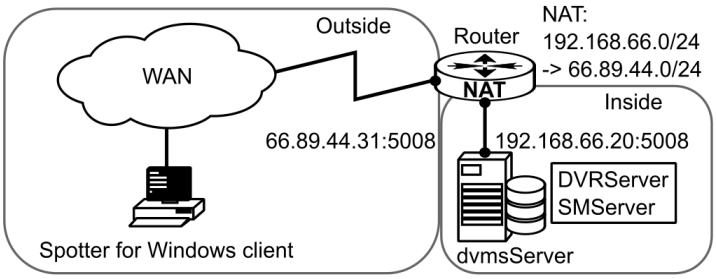
The second port is used for DVRServer process communication, (5009, 5013, 5017...)

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 is more than one server on-site, then the ports are 5009 +4, 5009 + 8 etc.

Top Previous Next

1.7.4. Single Server Behind Router

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



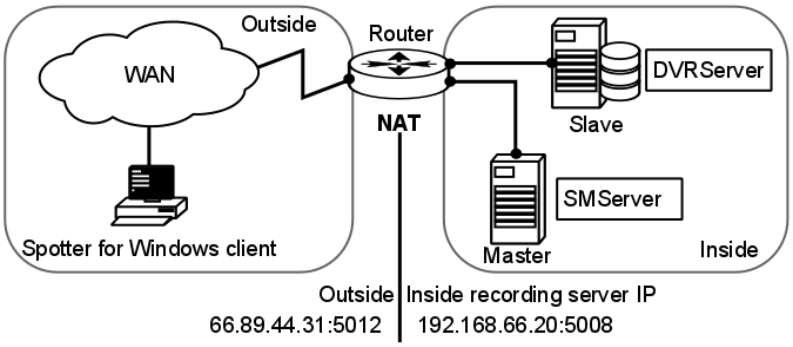
If the user is accessing a single server from the WAN, he needs to connect to the VMS Server with the outside IP address that the router has translated.

The user can check the port forwarding what the port in use is, but it is with high likelihood port 5008.

Top Previous Next

1.7.5. More Than One Server Behind Router

Scenario 2: More than one server behind a single router (WAN address)



If the user is configuring a larger 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, there will be a note shown to the user that he can choose between internal IP address and 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 (locally on the VMS Server, start System Manager to 127.0.0.1 and log in) and check the port forwarding settings.

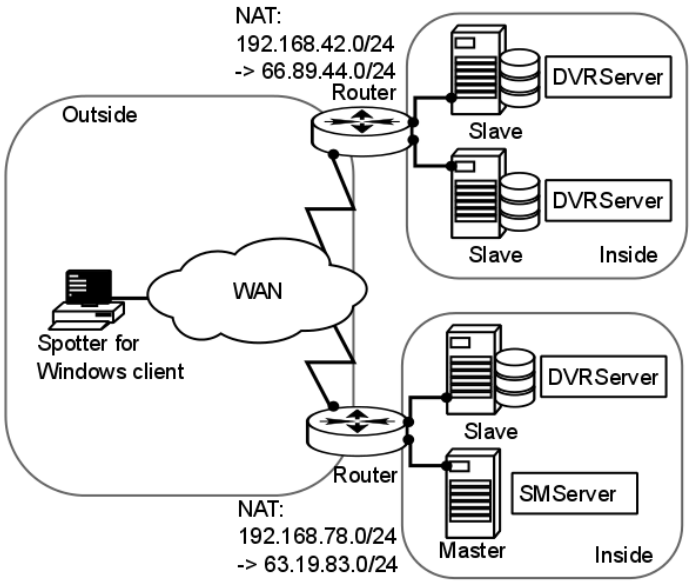
When adding a server to a Master Server when not on the local site (cannot use the local IP address) then the user must know the external IP address and have knowledge of the first port that the port forwarding was done to.

If the server that is added is a single, standalone server, the port is most likely 5009. If there are multiple servers on the same site, they most likely get the ports starting with 5009, 5013, 5017, 5021...

Top Previous Next

1.7.6. 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.

Top Previous Next

1.8. Cameras

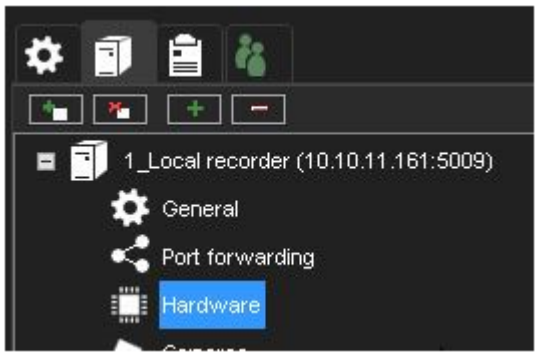
Before using the system manager application to search for the camera, first configure the camera to use an IP address or DNS name, user name and password for the cameras in the camera's internal settings, typically using a camera manufacturer's web browser interface. See the camera manual for details.

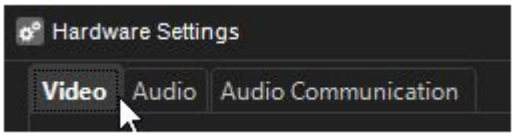
Please see the document *Supported IP Cameras* for information regarding tested IP camera models that can be added to the system.

Top Previous Next

1.8.1. Adding and Removing IP Cameras

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

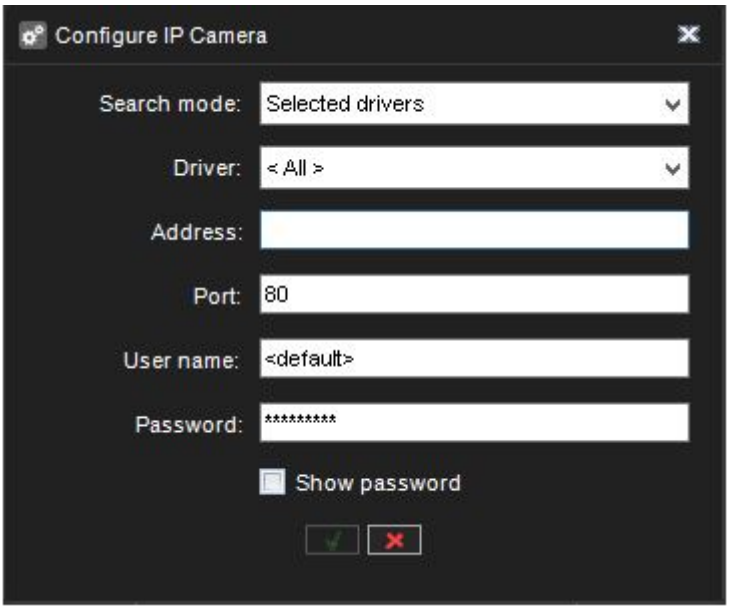




To add a new IP camera when the IP address is known:

1. On the **Video** tab, click **Add IP Camera**

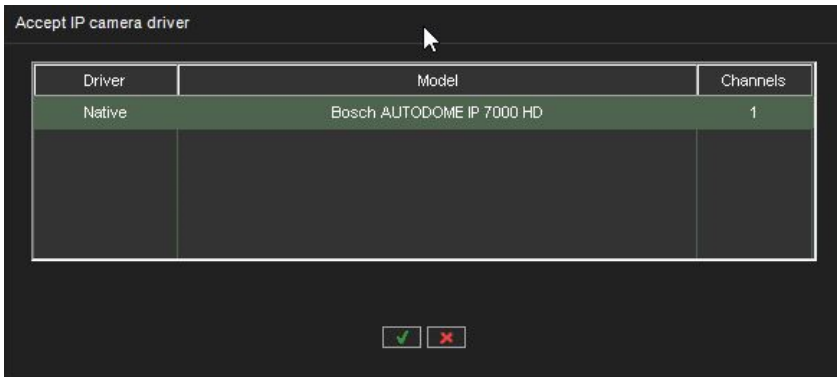
.



2. Type the IP address or DNS name of the camera or video server.
    - Change the port number if needed, usually, port 80 is used.

3. Type the user name and password for the camera.
4. Click **OK**.

The system will now communicate with the camera and display which drivers can be used to connect to the camera. The camera may support ONVIF Profile S. In this case, it may also be detected by the ONVIF driver. Select a driver from the list. Typically, it is recommended to use the Native driver if it exists.

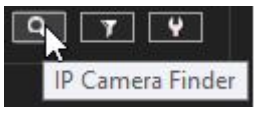


For multichannel devices, the **Channels** option can be used to add the device with less than the maximum number of channels.

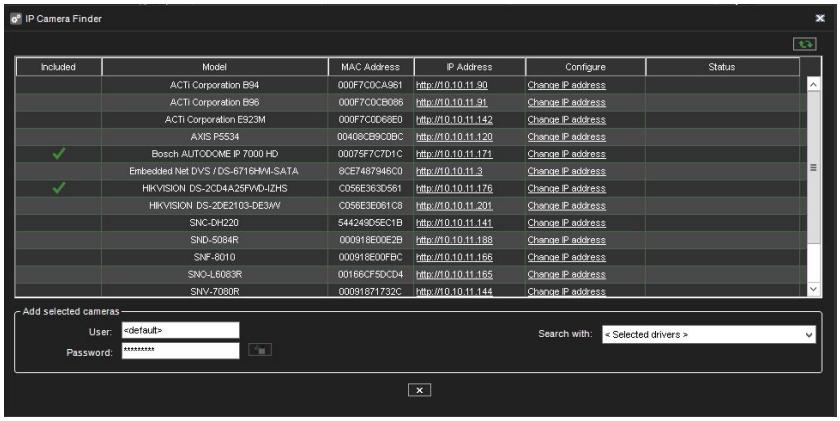
5. After selecting the driver and pressing the ok button, the camera is added and can be seen in the hardware list. It is still necessary to accept the dialogue with the OK button in the low part of the screen.

To add one or more IP cameras with the Camera Finder tool:

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.



2. Cameras can be selected from the list. Selecting multiple cameras is possible with SHIFT or CTRL keys.
3. Type the username and password for the cameras.
4. Click **Add Selected Cameras**

. The system adds the selected cameras to the system with the selected username and password.
5. 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.
6. Click **Close** to exit the **IP camera finder**.
7. Save the Hardware settings by pressing OK in the list:

To remove an IP camera:

1. On the **Video** tab
2. Click on an IP camera's name in the camera list.
3. Click **Remove Selected IP Camera** in the lower right corner of the tab.
4. When asked to confirm the deletion, click **OK**.

Top Previous Next

1.8.2. Limiting the Camera Configuration to Certain Camera Drivers

It is possible to limit the camera search to certain drivers only. This can be useful in installations where the cameras are only from a single manufacturer or a few different manufacturers.

This option speeds up the camera search and other operations.

This is achieved by selecting the “Selected drivers” button.

This opens a dialogue where the user can choose which drivers are used by the system.

Top Previous Next

1.8.3. IP Camera Search Modes

IP Camera Search Modes

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 of the drivers.
- ***Currently active drivers***: Search the camera using all drivers which are currently used. In case this option is selected, the system will use only drivers that are 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 would like 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 of the existing camera using *Modify* button will show dialogue with ***Currently active drivers*** search mode and driver name in mode option combo-box (except cameras added by the model of course). The system will not store last used

options for modifying cases because the options will be available for adding cameras only

Top Previous Next

1.8.4. Camera Audio Channels

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.

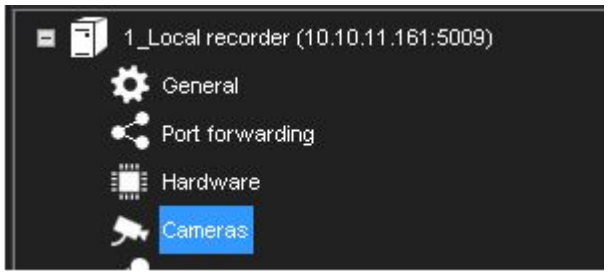
After IP audio inputs and outputs for a camera have been added to the system, they can be edited and removed through the **Audio** tab.

If the audio inputs and outputs are not found by the automated search tools, they can be added separately through the **Audio** tab.

Top Previous Next

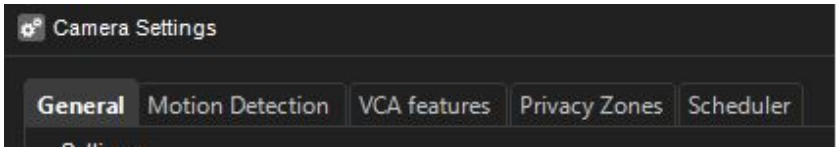
1.8.5. Editing Camera Settings

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



The cameras page consists of 5 tabs.

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



The full camera list with a summary of the main settings can be seen on the General tab.

Selecting a camera on the general tab camera list and then switching to other tabs will keep the same camera selected.

The other tabs also have a pull-down type control for switching to a different camera.

Top Previous Next

1.8.6. General settings

The camera settings part on the lower part of the window contains three tabs that contain the following parameters:

General.

- **Name.** The name of the camera. The system suggests names of the type *Camera 1, Camera 2*, and so on. You can change the name to better describe the location of the camera.
    - The name will be shown to the users in the Spotter program.
- **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 Listener. If there are multiple servers that have the same camera configured, then one of them should be made Active and the others should be Listener. This way, only the Active server settings are communicated to the camera.
- **Transport Mode**. This setting controls how the media stream is transported from camera to server. The available options are RTPoverUDP (default) and RTPoverRTSP. 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.
- **Codec.** The codec 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 the case of 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 (additional licensing option) and Mobotix MxPEG.
- **Description.** Here you can type a description of the camera that will be 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, which makes 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 make sure 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.

Streams

- **Bitrate mode.** This setting controls if the Variable bit rate (VBR) 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 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.** Set the record rate. The maximum rate depends on the video standard and the camera type.
- **Multiple streaming (multi-streaming)**

Advanced

This tab contains camera or driver-specific special settings. A driver update may bring additional values to this tab.

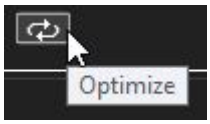
Selecting multiple cameras is possible with SHIFT or CTRL keys. Please note that if you select more than one camera, you cannot set parameters that are not supported by all selected cameras.

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 enable to addition of all desired cameras with desired settings. However, care should be taken to not 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.



Top Previous Next

1.8.7. Motion Detection

Each camera has an un-editable default motion detection mask. When the default mask is used, the system detects motion from the full image area.

In addition to the default mask, you can have four customizable masks for each camera. On the **Scheduler** tab of the camera settings and on the **Scheduler** tab of alarm settings, you can select a different mask to be used during each hour of the week.

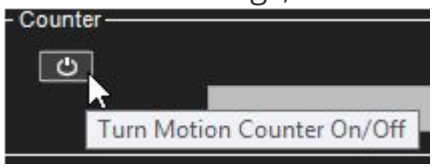
A mask contains these parameters:

1. Selected areas. The system detects motion in areas that are painted red.
2. Detection sensitivity.
3. Minimum quantity of movement.

To edit 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 name of the mask, 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.
8. To test the settings, click **Turn Motion Counter On/Off**



Detected motion is shown in red in the image, and the counter increments each time motion is detected. To adjust the sensitivity of the detection, turn the counter mode off and make the adjustments.

Drawing Tools:

Tool	Name	Description
	Pencil	Use to set the motion detection area. Select the pencil size by clicking one of the tool size buttons (large, medium, small).
	Eraser	Use to erase selected areas that you do not want to include. Select the eraser size by clicking one of the tool size buttons (large, medium, small).
	Lasso	Use to select areas using straight lines. If the pen tool is selected, using this tool adds to selected areas. If the eraser tool is selected, this tool removes from the selection. Click the image where you want to start the selection. Click again where you want to anchor the line and change direction. To complete the selection, click the starting point. The selected area is painted red or the red colour is removed.
	Fill/Clear	If the pen tool is selected, clicking this button selects the full 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 that 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).

Sensitivity and quantity

The system detects motion when:

4. Pixels change more than the set limit (**Sensitivity**).
5. 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 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 1 image per second.

Motion detection methods

Comparative detection 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.

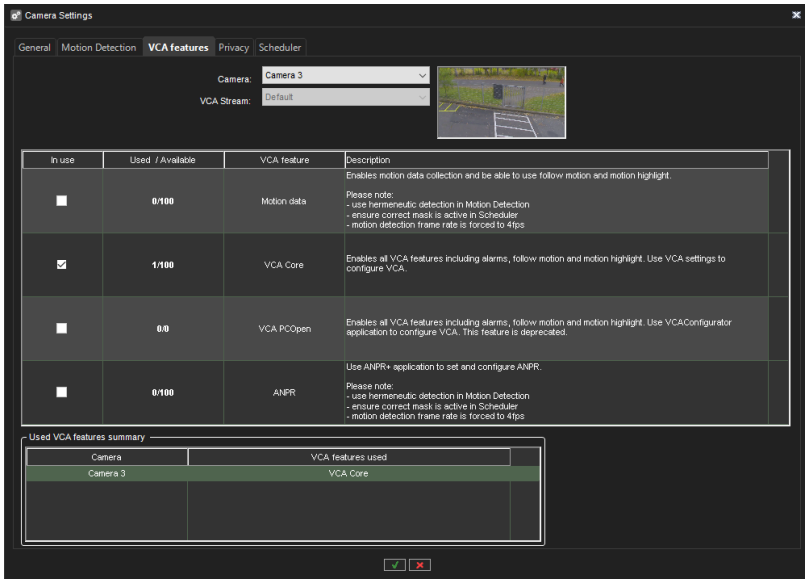
Hermeneutic detection is a sophisticated motion detection system for challenging weather conditions (e.g. heavy rain, “noisy” background image, etc.) and situations in which external video content analytics (VCA) tools are used. It should be noted that hermeneutic detection requires more processing resources than the other detection methods.

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

1.8.8. Video Content Analytics

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 camera that is configured to use multiple streaming) is used for VCA. This is achieved from the pull-down menu below the camera selector (see the following mage)



The VCA Features tab

In the basic state, the tab contains the following VCA features:

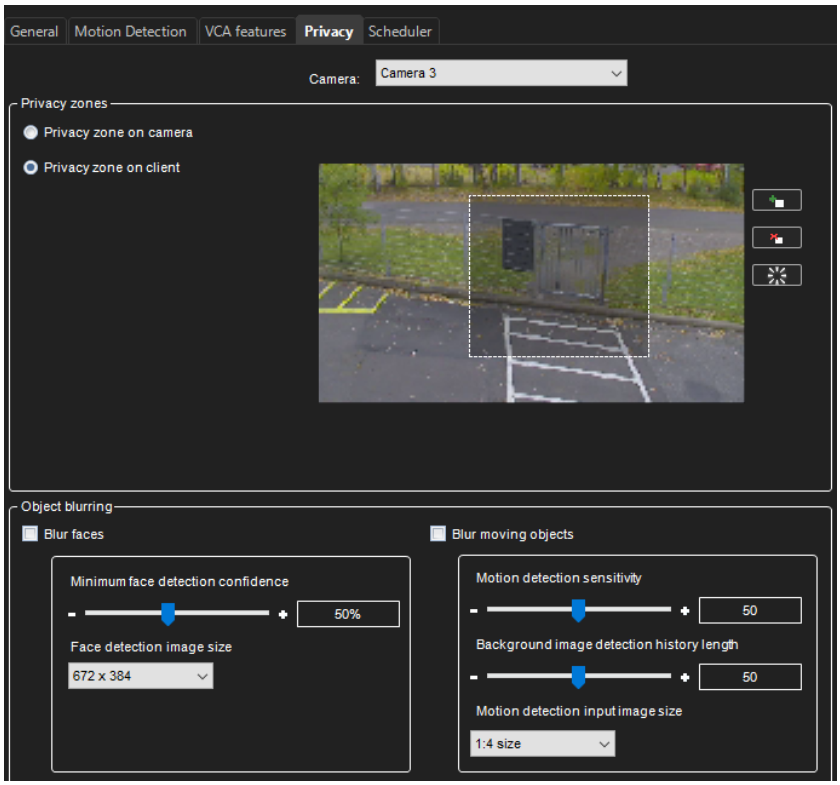
- **Motion data:** Internal VCA motion data, enabling data collection, motion following, and motion highlighting. Visualized in **Mirasys Spotter**.
- **VCA Core:** enables full VCA functionality. Configured through VCA settings in system manager.
- **VCA PCOpen:** Enables full external VCA functionality. Configured through the external VCA Configurator application. Visualized in **Mirasys Spotter**.
- **ANPR:** Automatic number plate recognition. Configured through the external ANPR+ application.

Please note that the VCA features are only available if enabled through the license. Some VCA features need to be configured through external applications.

1.8.9. Privacy

Under the Privacy menu, you can control the privacy zones of the camera as well as 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 applies also when exporting the materials.

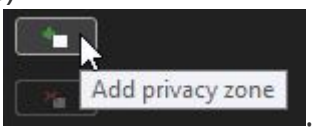


The Privacy tab.

A privacy zone can be chosen to be either

- on the camera (when supported by camera and driver) these privacy zones are camera-based areas that are not recorded or displayed in the camera view: image data from the areas is not transmitted by the camera to the server.
- 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 rights to do so.

To add a privacy zone:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select if you want the privacy zone to be **on the camera** or **on the client** (requires license update)
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**.

Note: *If the selected camera does not support privacy zones, the privacy zone controls are disabled.*

Note: *If the master or server license does not support client privacy screens, the privacy zone controls for the client are disabled.*

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**.

BLURRING

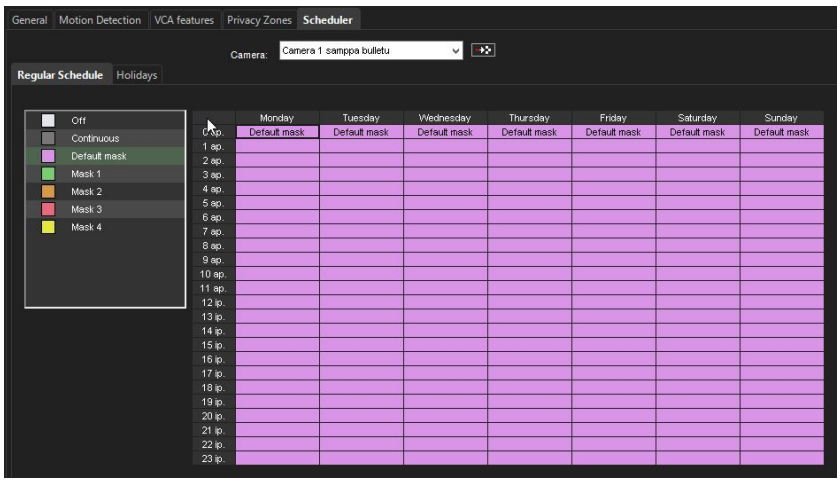
"Blur faces" and "Blur moving objects" settings are available to be set up as additional privacy. If the facial- or motion-based blurring is enabled for a camera, these are also available on the Spotter side (provided that the user has sufficient permissions.) The blurring will not be functional on the Spotter side- or for exports of the video material for the cameras if they have not been selected in the system administrator side.

Higher resolutions used for the algorithms mean higher accuracy for the algorithms- but also higher CPU loads.

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

1.8.10. Scheduler (Video)

By default, video is recorded when the system detects motion in the default mask.



However, you can set different options for each hour of the week. For example, use different motion detection masks during the day and during 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, simply click on the mask you want to activate, and then click on the scheduled hour where you want it to be used.

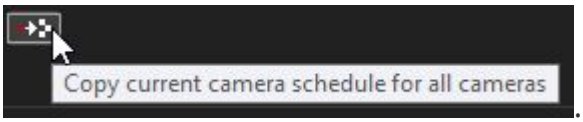
Tip: *To change more than one hour at the same time, drag with the mouse. You can also click the first cell, keep the SHIFT key pressed and then click the last cell. To change all hours in a column or a row, click the column or row heading. To change all hours of the week, click the cell above the hour's column (on the left side of the weekdays heading row).*

These options are available:

1. **Off**. Video is not recorded. However, possible alarms are recorded. Alarms are configured in **Alarm Settings**.
2. **Continuous.** The camera records all images. This option uses a lot of disk space.
3. **Default mask.** The camera records video using the default motion detection mask and default motion detection parameters.
4. **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:

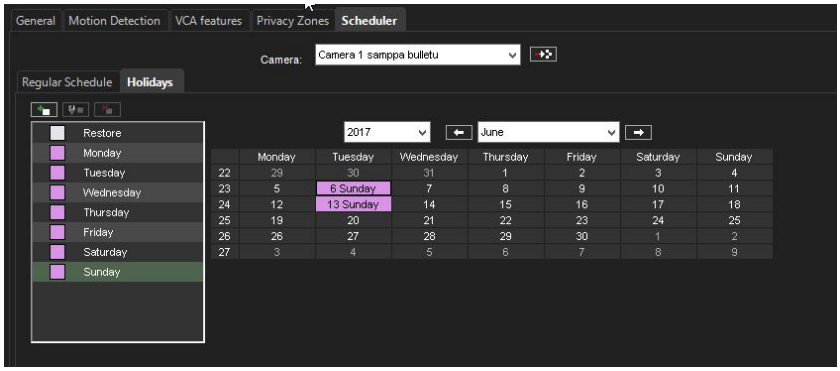
You can copy the currently selected recording schedule for all cameras in the system.

1. Click **Copy Schedule** 

.
2. When asked for confirmation, click **OK**.

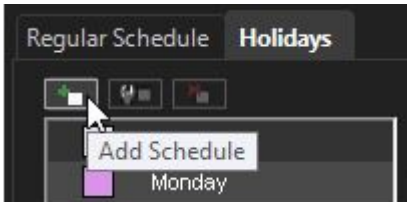
To set a holiday schedule:

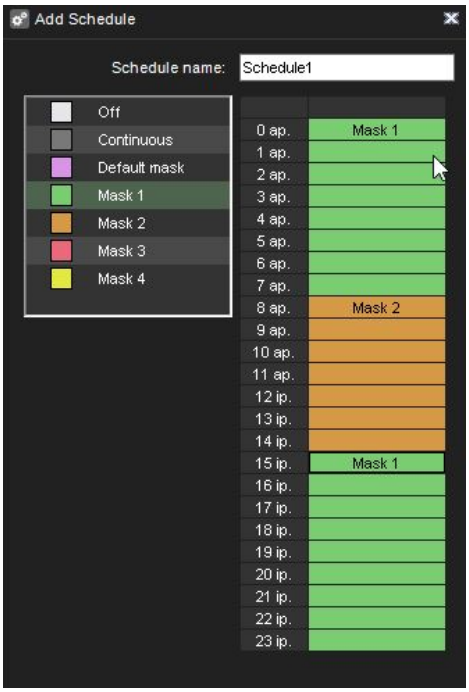
You can use different recording schedules for holidays. You can apply a daily schedule from the **Regular Schedule** or use a custom schedule.



1. On the **Holidays** tab, select the year and month.
2. From the left pane, click the schedule that you want to apply and then click the holiday in the calendar.

To add a custom schedule:

1. Click **Add Schedule** 



2. The **Add Schedule** dialogue box is shown.
3. Type a name for the schedule.
4. Click the mask that you want to apply and then click the hours that you want to apply the mask to.
5. 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:

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

To restore the original schedule:

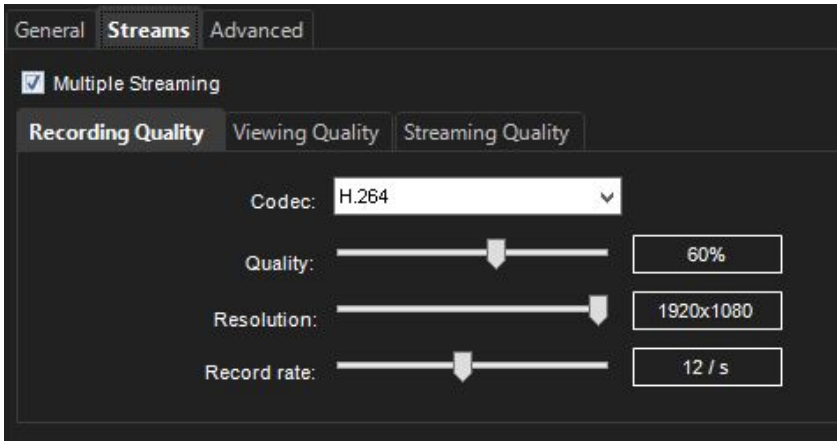
Click **Restore** and then click the day that you want to restore.

Top Previous Next

1.8.11. 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.

In Mirasys System Manager, multi-streaming is configured in-camera settings, **Streams** sub-tab.



Top Previous Next

1.8.12. Edge Storage

The Edge storage functionality enables uninterrupted recording during network blackouts. In practice, in the case of 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.

This feature is configured solely through the camera's configuration utility, and it does not require any modifications in System Manager. Please refer to the camera's documentation for instructions on enabling Edge storage.

Top Previous Next

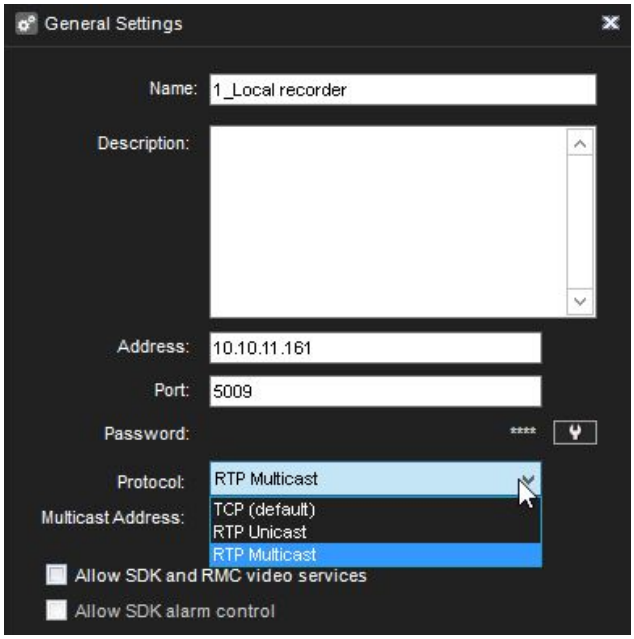
1.8.13. Multi-Casting

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 the camera's documentation for instructions on enabling multi-streaming. 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.

1.9. Audio

Top Previous Next

1.9.1. 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.
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.

Top Previous Next

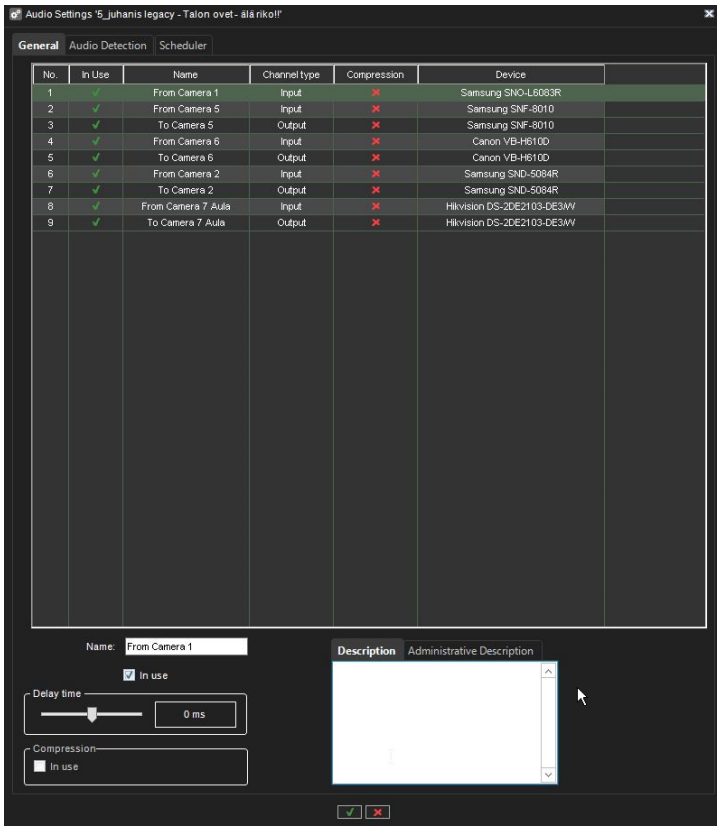
1.9.2. Audio Settings

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.

Top Previous Next

1.9.3. General Settings



The **General** tab in the **Audio** page lists the basic settings of all audio channels:

- **No.** The number of the channel.
- **In Use.** Shows if a channel is enabled or disabled.
- **Name**. The name of the channel.
- **Mono / Stereo**. Shows if a channel is a mono or stereo channel.
- **Compression**. Shows if compression is on or off. A checkmark means that compression is used.

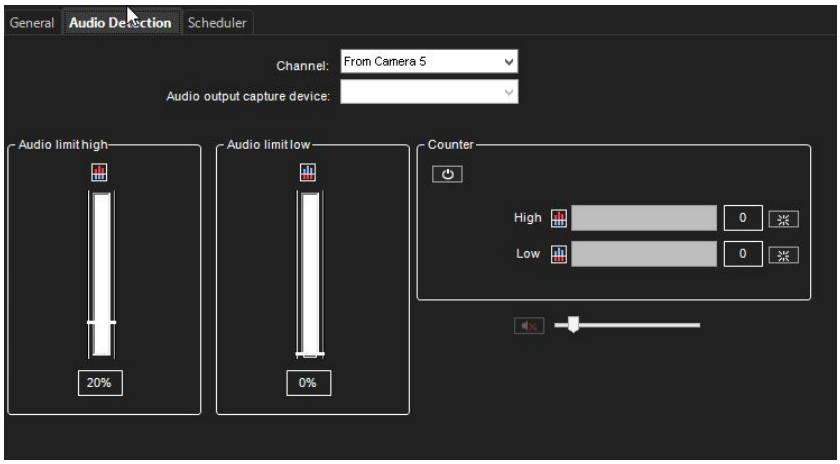
- **Capture Driver**. Shows what capture driver is used. Select the driver in **Hardware Settings**.

To change general settings:

1. Select the channel from the list.
2. You can change these settings in the lower part of the window:
1. **Name**. The name of the channel.
2. **In use**. Select to enable the channel. Clear the check box to disable the channel.
3. **Delay time**. Sets the delay time in synchronizing the audio stream with other devices. The delay time can be used to optimize the audio and video stream synchronization to, for example, enable better lip synchronization.
4. **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.
5. **Description**. Here you can type a description of the channel that will be shown to the users in the Spotter program.
6. **Administrative Description**. Here you can type a description of the channel that will be shown in the Spotter program to only system administrators.

Top Previous Next

1.9.4. 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**. 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. 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. 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. Audio detection is activated when the level drops below the limit.
5. To reset the counters, click the reset buttons.
6. Turn the counters off by clicking the **Turn Audio Counter On/Off** button.
7. To save the settings, click **OK**.

You can adjust the volume of audio and also mute the audio channel. These settings are not saved; they only change how audio is played in the audio settings.

- **Mute**. Mutes the audio channel.
- **Adjust Volume**. Adjusts the audio volume.

Top Previous Next

1.9.5. 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 week 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 high.** Set the limit on the **Audio Detection** tab.

The functionality of this view is similar to the video scheduler.

Top Previous Next

1.9.6. Audio Communication Settings

You can connect a call button, a microphone, and a speaker to a server and use them like a door or gate phone. Each server has one such audio communication channel. Audio is transmitted over a TCP/IP network.

When the call button is pushed, the system sends a call signal to the Spotter program. This is shown by an animated telephone icon on the user's desktop and a ringing sound.

The user can then answer the call, which opens a direct, two-way communication channel between the user and the person who pushed the call button.

The users can also open the communication channel when there is no call signal.

To connect the devices:

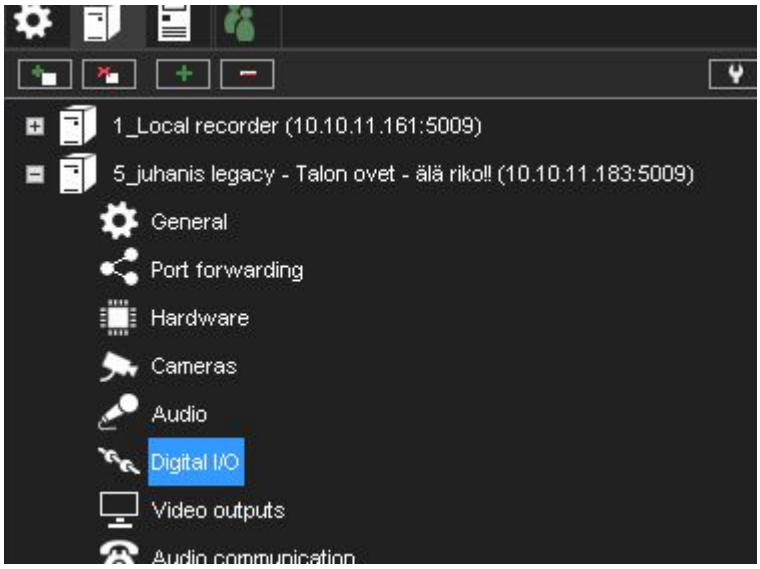
1. Connect a call button or an equivalent device to one of the digital inputs of the server.
2. Connect a microphone and a speaker to the server and to the user's workstation.

To set up audio communication:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Audio Communication** page from the menu.
3. Select the capture driver and the playback device.
4. In **Audio Communication Settings**, type a name for the communication channel (or use the default name).
5. Type a general description and an administrative description of the channel. All users can see the general description, whereas only system administrators can see the administrative description.
6. Select the digital input that the call button is connected to.

Top Previous Next

1.10. Digital I/O



Top Previous Next

1.10.1. Digital I/O Settings

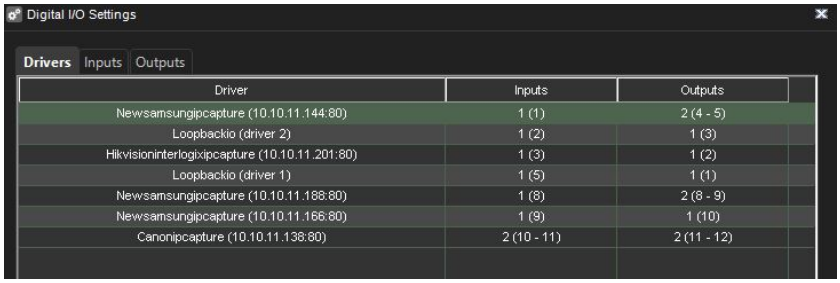
In **Digital I/O** settings, you can add digital input and output devices, and configure the input and output settings.

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.

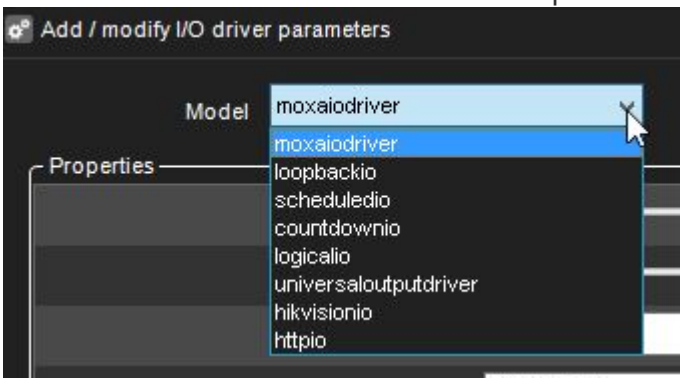
Once an I/O device driver has been added to the system, the device can be configured and taken into use through the **Drivers** tab.



To take an I/O device driver into use:

1. If necessary, install the device driver package.
2. Open the **VMS Servers** tab.
3. Select the correct server and open the **Digital I/O** page from the menu.
4. Click **Add I/O driver**

in the lower right corner of the screen.
5. Select the driver from the **Model** drop-down menu.



6. Configure the device settings in the **Properties** list.
7. To save the settings, click **OK**.

Note: *After configuring a digital I/O device driver, you may need to configure the inputs and/or outputs.*

To edit I/O device driver settings:

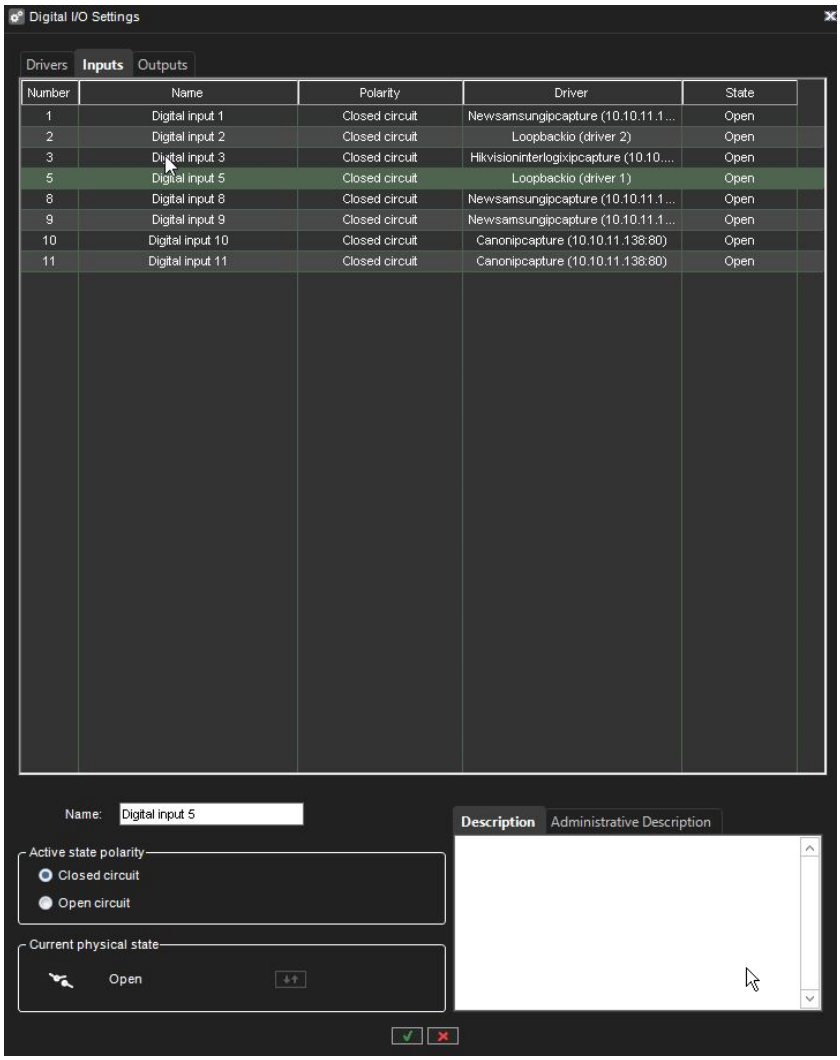
1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Double click on the device driver you want to edit.
4. Edit the device settings in the **Properties** list.
5. To save the settings, click **OK**.

To delete an I/O device driver:

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

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.



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

Active state polarity. Select the input and then select if the input is activated when the circuit is opened or closed.

Current physical state. Shows the state of a relay in real-time (**Open** or **Closed**).

Description. Here you can type a description of the selected input that will be shown to all users in the Spotter program.

Administrative Description. Here you can type a description of the selected input that will be 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 that will be shown to all users in the Spotter program.

Administrative Description. Here you can type a description of the selected output that will be shown in the Spotter program to only system administrators.

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

Top Previous Next

1.10.2. 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:

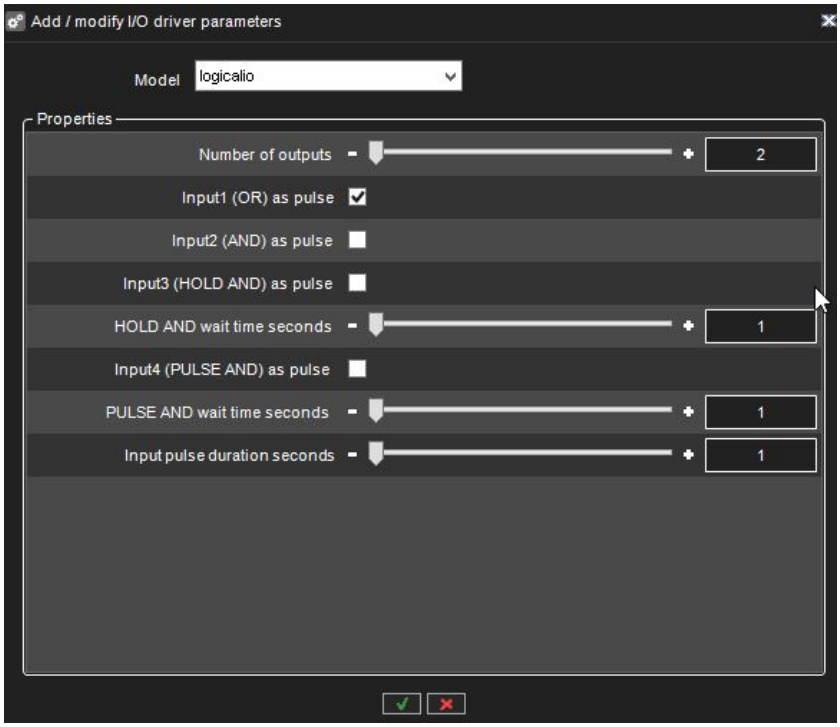
For example, if the customer wants to confirm that an Automatic Number Plate Recognition (ANPR) event is triggered when a car is in front of the camera, the Logical I/O can be used to create a “rule” that results in action only when VCA detects a car AND at the same time, there is an ANPR read event.

Another example could be that an entry “gate” with two doors is only allowing 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.

Logical IO and countdown IO are controlled by a license. If the license is not present, creating new IO will fail.

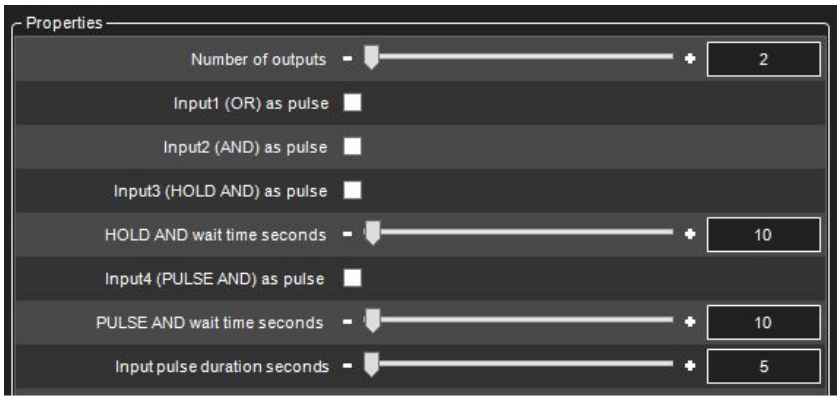
When a new Logical I/O is being added, the first option in the dialogue is how many output states are used as operands in the AND/OR decision making. The minimum number is 2 and the maximum is 32.



All Logical I/Os will automatically generate four inputs that can be used.

Input	Type
1	OR
2	AND
3	HOLD AND
4	PULSE AND

The following sections will describe the different inputs in more detail by using the below example:

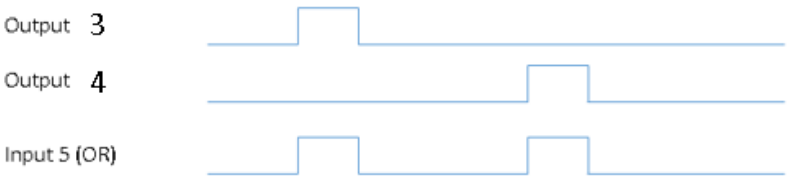


The example has 2 outputs that are the operands. These can be seen in the IO list as outputs 3 and 4.

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

"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.

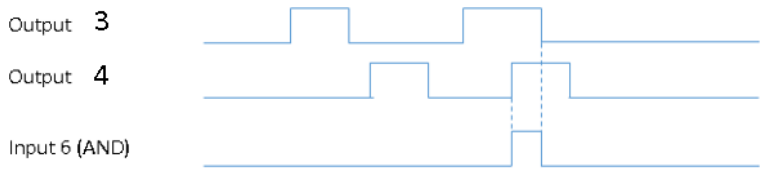


In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, input 5 will be turned on as a result.

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

"AND" Input

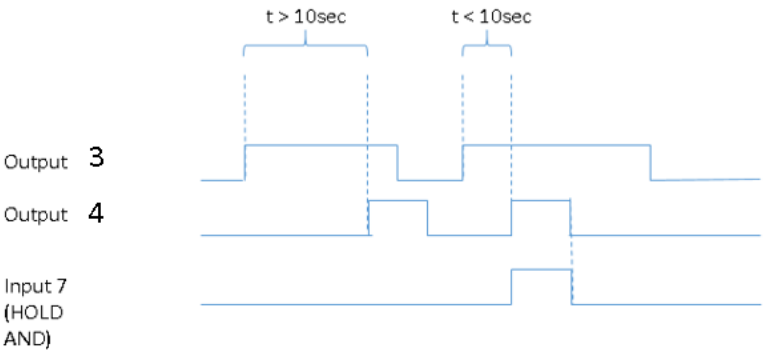
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on at the same time, input 6 will be turned on.



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

"HOLD AND" Input

HOLD AND input become active if all the outputs are active at the same time, and the time from the first activation to the last activation is less than the time defined in the HOLD AND wait time slider.



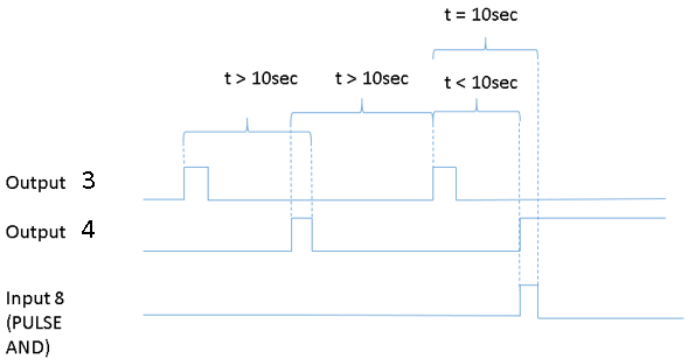
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

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.

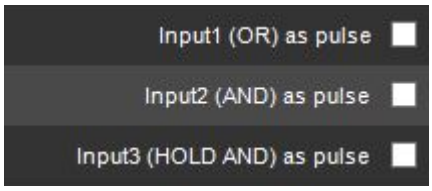
In our example, if output 3 has been active inside 10 seconds, and output 4 becomes active, then input 8 will be turned on.



Input 8 remains on 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, then 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.



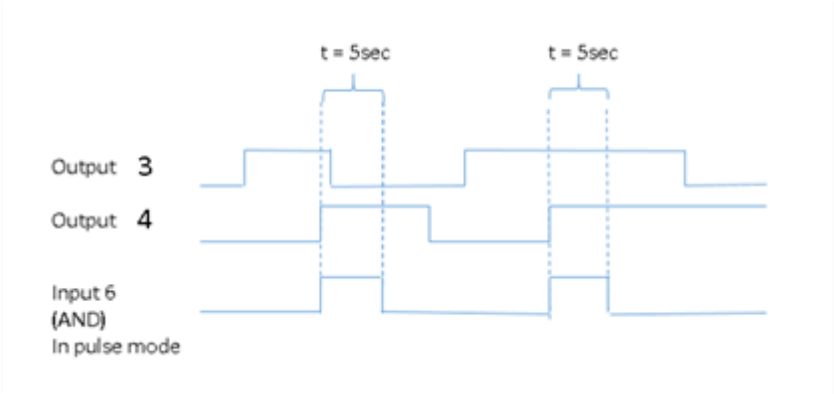
and

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:



Top Previous Next

1.10.3. 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 time period.

When a new Countdown I/O is created in System Manager, it automatically creates 4 inputs and 4 outputs.

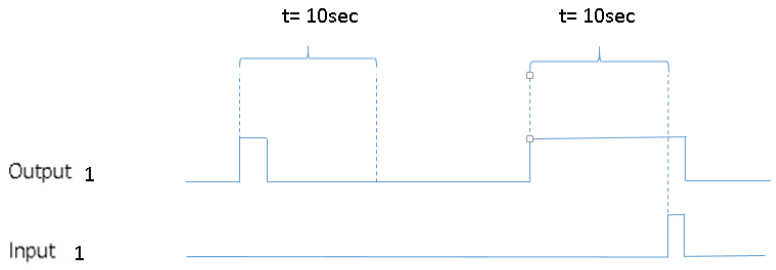
Countdown I/O has two basic modes. The first two input/output pairs are of type 1 and the last two pairs are of type 2.

Logical IO and countdown IO are controlled by a license. 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 1 is triggered and stays active for less than the defined duration, then there is no alarm. If the output is triggered and stays active for longer than the defined duration, then there is an alarm.



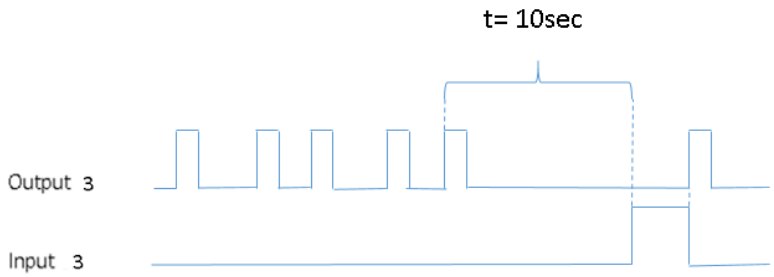
When creating a new Countdown I/O, the first two input-output pair is of this type.

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 in normal operation to get pulses from output 3 every 2-3 seconds. When the pulse is missing for longer than

10 seconds, the input state is changed to active. It stays active until the next output trigger is received.



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

Top Previous Next

1.11. Video Outputs

Video output support is only working on 32-bit servers. Since V8 is only provided as a 64-bit version, the use of this feature requires using a 32-bit VMS server with an earlier software version.

Top Previous Next

1.11.1. Video Output Settings

Video Output Settings

Video can be shown on external video monitors. In video output settings, you can change the names of the outputs and add camera tours. Users who have the right to edit camera tours can also add, edit, and delete camera tours in the Spotter program.

Using video outputs requires video output cards. For more information, see the *Installation Guide* or contact the system supplier.

To change the name of video output:

1. Select the monitor from the list and type a new name for the monitor.

To add a camera tour:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Video outputs** page from the menu.
3. Click **Edit Camera Tours**. The **Edit Camera Tours** dialogue box is shown.
4. Do as follows:
1. Click **Add Camera Tour**.
2. Type a name for the tour.
3. From the **Available Cameras** list, select the cameras that you want to add to the tour and click the right arrow.
   Tip: To select more than one camera, keep the SHIFT key pressed and click the first and last camera that you want to select. To add a camera to a selection or to remove a camera from a selection, keep the CTRL key pressed and click the camera that you want to add or remove.
4. To change the order of the cameras, drag a camera to a new position.
5. To remove a camera, select the camera and click **Remove Camera**.
6. To change the dwell time for a camera, select the camera and then drag the slider below the list.
5. To save the tour, click **OK**.

To edit a camera tour:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Video outputs** page from the menu.
3. Click **Edit Camera Tours**. The **Edit Camera Tours** dialogue box is shown.

4. From the tours list, select the tour that you want to edit. You can edit these settings:
2. To change the name of the tour, click **Change Tour Name** and then type a new name for the tour.
3. To change the order of the cameras, drag a camera to a new position in the list.
4. To remove a camera from the tour, select the camera, and then click **Remove Camera**.
5. To add a camera to the tour, select the camera from the **Available Cameras** list, and click the right arrow button.
5. To save the changes, click **OK**.

To delete a camera tour:

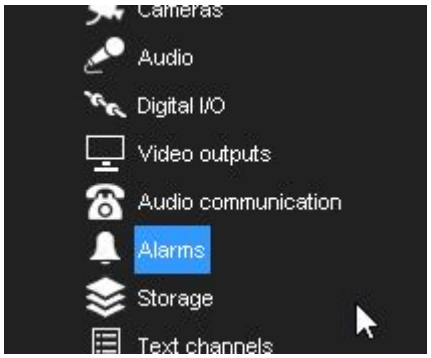
1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Video outputs** page from the menu.
3. Click **Edit Camera Tours**. The **Edit Camera Tours** dialogue box is shown.
4. From the tours list, select the tour that you want to delete.
5. Click **Delete Tour** adjacent to the list.
6. To save the changes, click **OK**.

To edit the descriptions of the outputs:

6. On the **Description** tab, you can type a description of the output that will be shown to all users in the Spotter program.
7. On the **Administrative Description** tab, you can type a description that will be shown only to system administrators.

Top Previous Next

1.12. Alarms



Top Previous Next

1.12.1. Alarm Settings

The alarm management tools enable the creation of server-specific alarms based on a variety of 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.

Top Previous Next

1.12.2. Accessing the Alarm List

To access the alarm list:

1. On the **VMS Servers** tab, select the server.
2. Double-click on **Alarms**.
3. All alarms configured for the server are displayed in the **Alarms** list.
4. You can click the arrow sign on the left side of an alarm's name to access further information about the alarm. The information can be hidden by re-clicking the arrow sign.

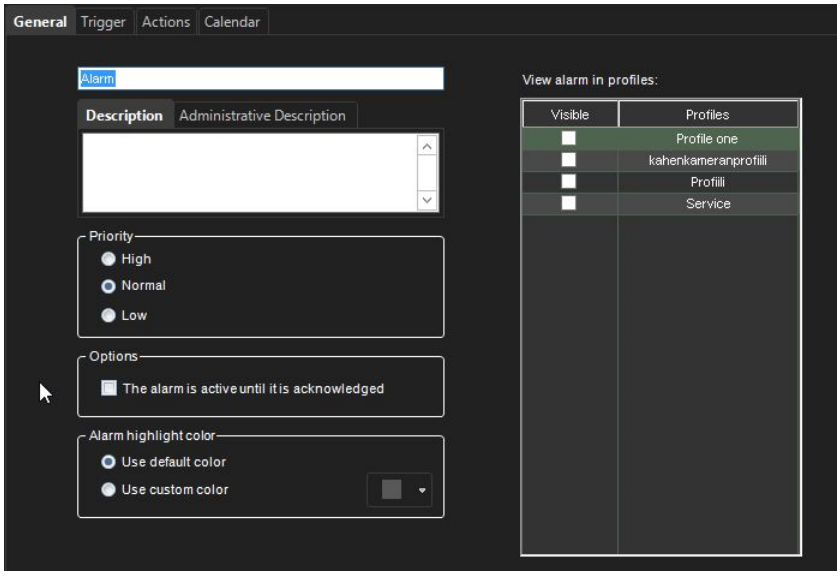
Top Previous Next

1.12.3. Adding a New Alarm

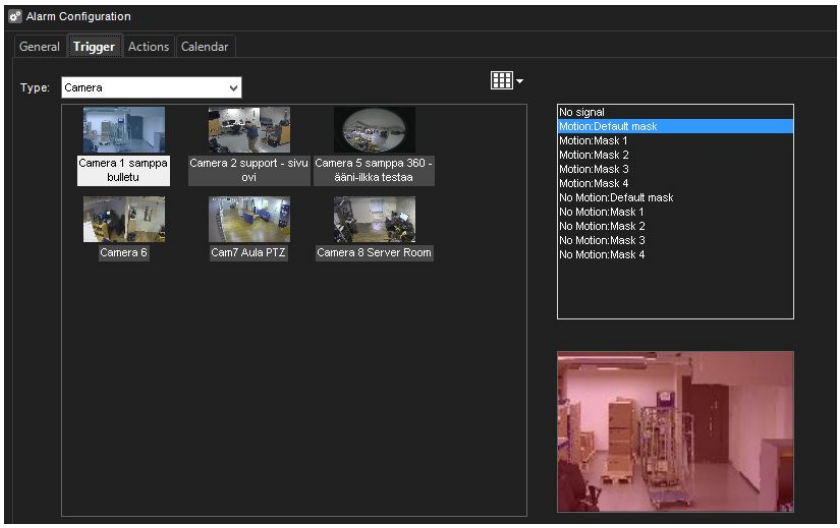
To create a new alarm:

1. Click **New Alarm**

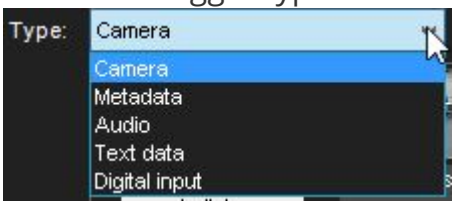
at the lower-left corner of the **Alarms** screen.
2. Type the name of the new alarm in the **Name** field.



3. Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.
4. Select whether the alarm is of **high**, **normal** 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 be also added to profiles through the **Profiles** tab.*
8. Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.



9. Select the trigger type from the **Type** drop-down menu.



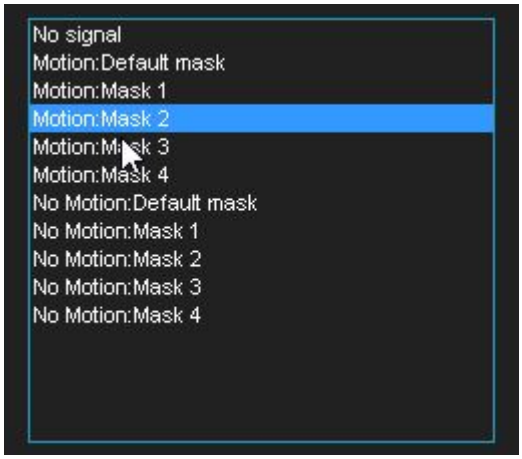
10. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.

This list contains a Metadata item. This option is now used to create alarms based on VCA metadata

- When this option is selected, the list of available metadata events from the driver is shown on the right side of the screen.
- Contact Mirasys for more information on how to configure VCA metadata-based alarms.

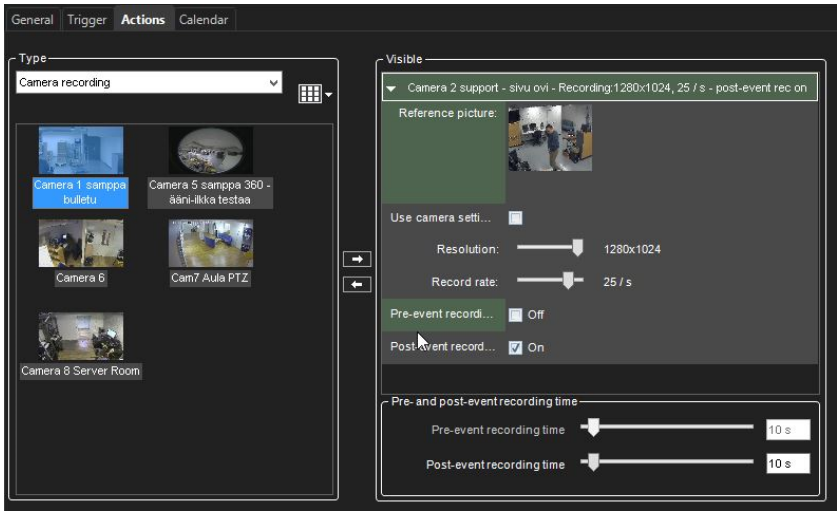
• Select the triggering condition from the condition list on the right side of the screen.

1. For camera-based triggers, you can select the mask that will be used in motion detection to trigger the alarm.

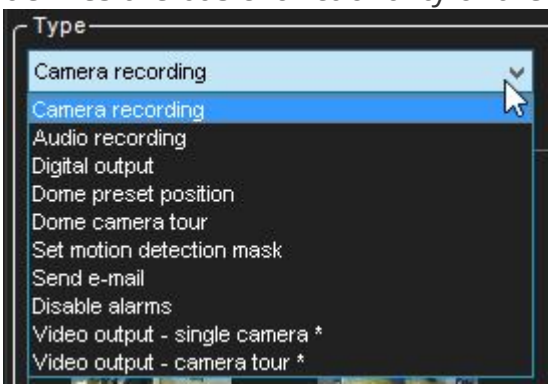


2. For audio-based triggers, you can set the alarm to trigger based on a high or low audio level.
3. For text data based (e.g., VCA, ANPR+, etc.) triggers, you can set the alarm to trigger based on a text data string. In addition, you can set an optional alarm ending trigger by marking **Define ending input** and selecting a string for ending the alarm.
4. For digital input-based triggers, the alarm is triggered based on the change of the input's polarity.

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.



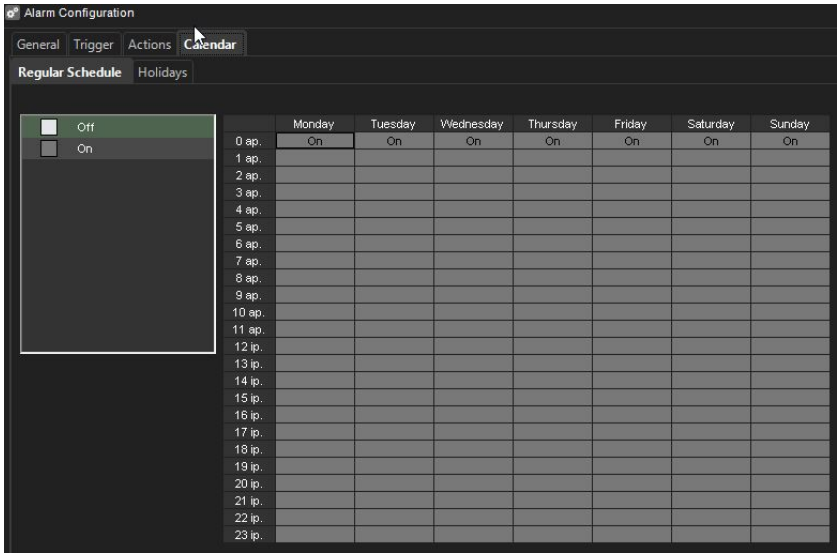
14. Select the device for which the selected action type will be used from the list below the **Type** drop-down menu. You can change the layout of the list by clicking the layout button.

15. Click **Add**

to add the device to the **Visible** list. The **Visible** list contains all actions that are taken once the alarm has been triggered.

Note: *You can add multiple actions to an alarm by repeating steps **13-15** for each desired action.*

16. After adding an action to the **Visible** list, you can edit its settings by clicking on the arrow sign on the left side of the name of the action in the **Visible** list. The available settings depend on the type of the selected action.
17. After editing all selected actions, open the **Calendar** tab. The calendar tab is used to define the schedule during which the alarm is active.



18. In the **Regular Schedule** sub-tab, you can create a weekly schedule for the alarm on an hourly basis. By default, the alarm is always active. To create a schedule for the alarm, select **Off** from the **On**/**Off** list on the left side of the screen and mark the hours the alarm is switched off for each weekday.
19. To add monthly or yearly schedules for specific dates, select the **Holidays** sub-tab. In the **Holidays** sub-tab, you can set holiday schedules, or set the alarm to function on a specific day with the schedule of another weekday.
20. Click **OK** to save the alarm.

NoteS:

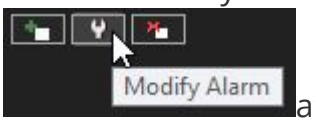
- If necessary, edit the alarm's profile-specific user rights.
- *It should be noted that alarms function regardless of whether they are associated with a user profile: assigning alarms to profiles affects how users can see and handle the alarms, but regardless of whether an alarm is assigned to a profile or not, the alarm functionalities remain operational until the alarm is removed via **System Manager**.*
- Even if the alarm is active, it will be automatically switched off when time reaches a point where the alarm schedule is defined to be off.

- *When the alarm schedule begins, and the alarm trigger is active, the alarm will be automatically activated.*

Top Previous Next

1.12.4. Editing an Alarm

To edit an alarm:

1. On the **VMS Servers** tab, select the server.
2. Double-click on **Alarms**.
3. Select the alarm you want to edit by clicking on its name.
4. Click **Modify Alarm** 

at the lower-left corner of the **Alarms** screen.
5. Edit the alarm as instructed in Adding a New Alarm.
6. Click the **OK** button to save the alarm.

Note: *If necessary, edit the alarm's profile-specific user rights.*

Top Previous Next

1.12.5. 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.

Top Previous Next

1.12.6. Action Types and Settings

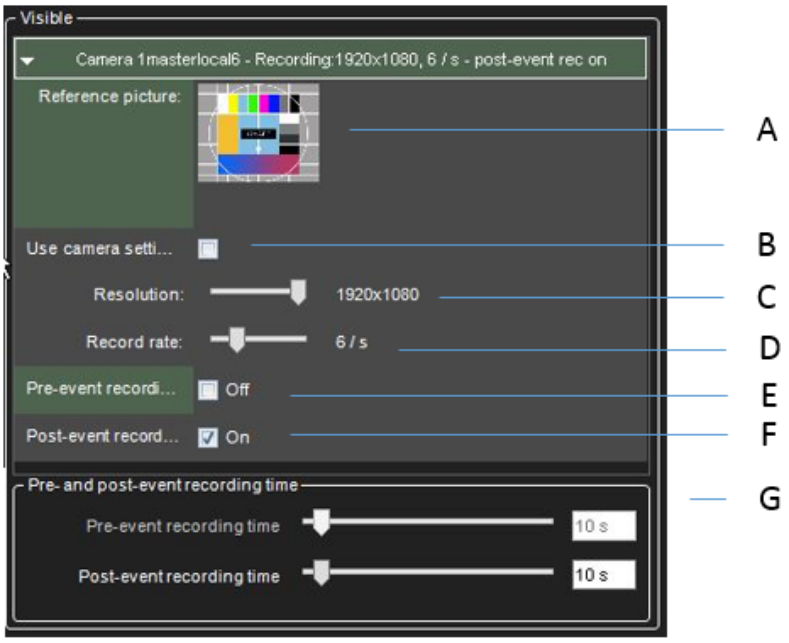
The list below contains the default action types and their parameters. Some of the action types listed above may not be available on all systems.

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. By marking this checkbox, the alarm recording will be performed using the camera-specific resolution and record rate setting.

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

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.

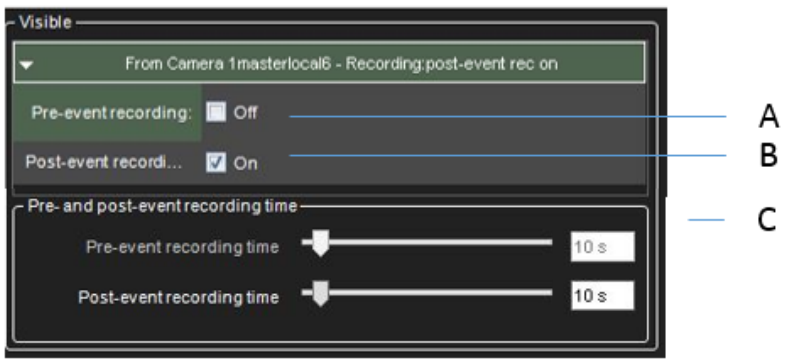
G) Pre- & post-event recording duration. These sliders can be used to set the pre- and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

Note *All devices (cameras and microphones) that 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:

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) that are 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.*

Video output - single camera

The **Video output - single camera** action can be used to display a video feed from a specific camera on a video monitor. When an alarm that contains this action type is triggered, the video feed from the selected camera is displayed on the selected video output.

The action includes the following fields and parameters:

- **Show in the monitor**. Use the drop-down menu to select the camera from which the video feed is displayed in the selected video output 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.*

Video Output - Camera Tour

The **Video output - camera tour** action can be used to display a pre-programmed camera tour on a video monitor. When an alarm that contains this action type is

triggered, the video feed from the selected camera tour is displayed on the selected video output.

The action includes the following fields and parameters:

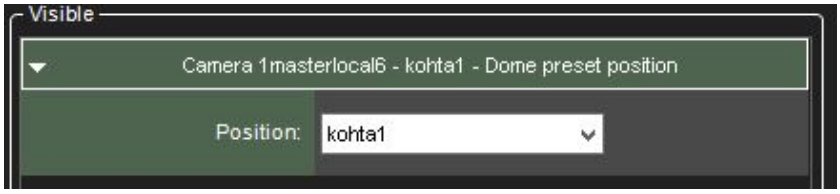
- **Show in the monitor**. Use the drop-down menu to select the camera tour from which the video feed is displayed in the selected video output during the alarm.

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) 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:

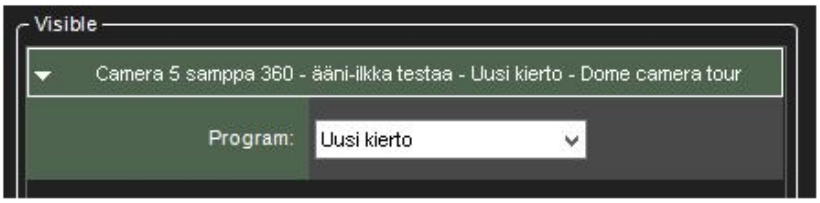
- **Position**. Use the drop-down menu to select the preset position to which the PTZ camera will move during the alarm.

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.



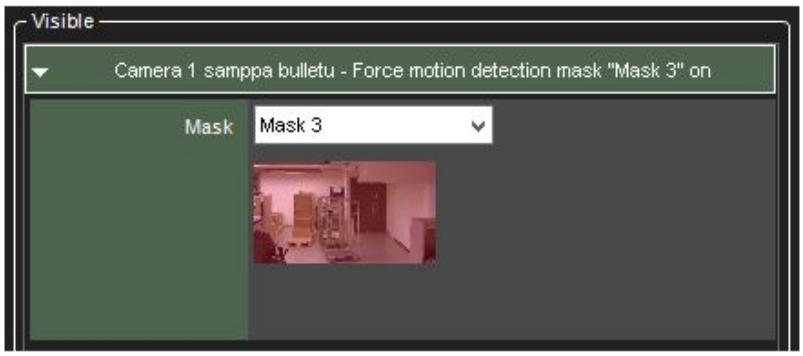
The action includes the following fields and parameters:

- **Program**. Use the drop-down menu to select the PTZ camera tour which will start running 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 be used to change the motion detection mask used by a specific camera during the alarm. When the alarm occurs, the motion detection mask used for the designated camera is changed to the alarm specific mask. After the alarm ends, the system restores the default mask.



The action includes the following fields and parameters:

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

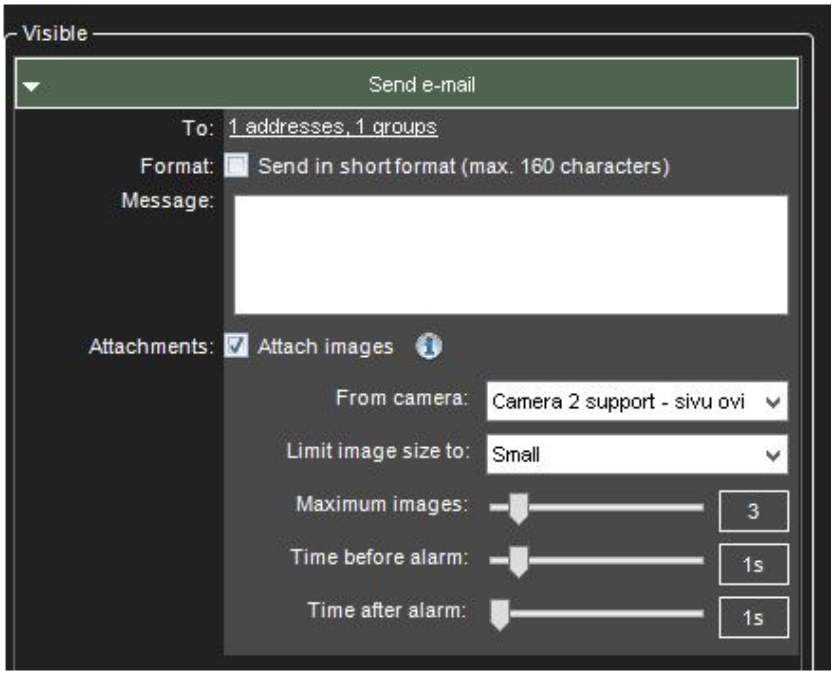
Note: *Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

Send E-Mail

The **Send e-mail** action can be used to send e-mail to any email address or group that is configured in the **E-mail settings** in the **System** tab.

You can choose which recipient or group should receive the alarm.

You can also include one or more unscaled or scaled-down images in the alarm email. To do this, uncheck the **Send in a short format** -option and check the **Attach images** –option



After this, you can choose a camera, size for the image scaling, desired number of images, and the time span from which the images are fetched.

NoteS:

- The number of images in this configuration is the maximum amount delivered. Fewer images might arrive
- Attaching images to alarm emails might lead to a high amount of 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, is recommended to select more than 1 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 normal.

1. 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.

NoteS:

- *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 or low and medium priority alarms or only low alarms.

This option allows certain alarms to remain active while others are suppressed.

The alarms are disabled only while the alarm that disables them is active.

Top Previous Next

1.12.7. Holiday Schedules

Alarm specific holiday schedules can be used to create schedules for specific dates or to 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 to 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:

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.

Top Previous Next

1.13. Storage

Mirasys VMS Version 8 comes with a new Mirasys TruStore storage file system.

IMPORTANT: The TruStore storage file system is not compatible with earlier storage, and old stored material will be removed at install.

Archive or export any material you wish to retain when upgrading to Version 8.

Mirasys TruStore removes limitations that were valid for earlier Mirasys legacy filesystem (used in VMS servers until version 7.5.x). With Mirasys TruStore:

- Storage drives can vary in size. It is no longer necessary to have all storage drives of the same size.
- Storage solutions for the single server can be of unlimited size. Previously the storage solution was recommended to be less than 25 TB per VMS server.
- Storage drive access has improved robustness for drive access failures.

Top Previous Next

1.13.1. Storage Settings

In storage settings, you can set the storage time of recorded video, audio and text data as well as alarm data. In addition, after adding a hard disk to a server, you can set it as additional data storage through the storage settings.

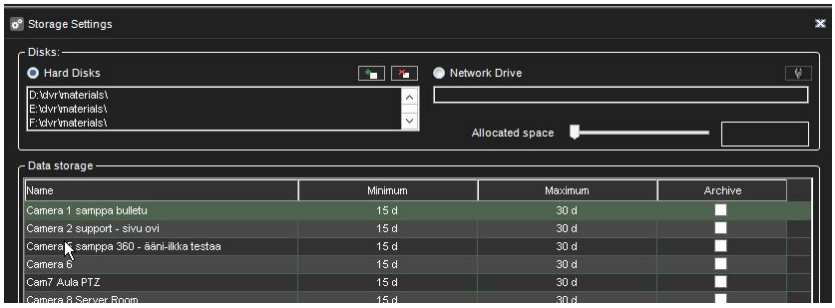
The storage settings are also used to configure the automatic archiving functionality, which enables the creation of backup copies of the server-specific video, audio and text data on a daily or weekly basis.

Top Previous Next

1.13.2. Adding Storage Space

If additional storage space is required, you can add new hard disks or map a network drive for data storage (i.e., NAS support).

There can be multiple network storage disks and local disks used simultaneously as seen in the picture.



Note: *When adding storage drives to legacy Mirasys filesystem (VMS server version 7.5.x or earlier), the storage drives are recommended to be all of the same capacity, and any single disk should be less than 10TB in size, and the total amount per VMS server should be less than 25 TB in size.*

The use of multiple storage disks has the benefit of allowing material write to be distributed to all the drives, making a loss of any single material drive less likely to wipe out large parts of the stored material.

To add a hard disk:

1. Install the new disk.
2. In **Storage Settings**, click **Add Disk** . The Add Disk dialogue box is shown. The **Minimum free space on the new disk box** shows how much free space the new disk must have.
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.

Top Previous Next

1.13.3. Storage Settings

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.

Video, audio and text data storage settings

Minimum. To prioritize recordings from one or more video, audio or text data channels, make sure 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 storage settings

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 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.

Log entries. This value specifies how many alarm events will be kept in the alarm log at the most. The system examines the number of log entries hourly and deletes the oldest entries if this value is 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. But if all storage space is used, the system first deletes the oldest alarm recordings before deleting other video or audio recordings.

Top Previous Next

1.13.4. 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 is checked daily.

As the size of a stored data stream can vary greatly 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:

1. If the material storage runs out of storage space, the system checks whether there is more than the allocated amount of alarm specific data stored in the data storage. If the stored alarm specific data exceeds the allocated amount, alarm data will be deleted to ensure free disk space. If the alarm specific data falls below the allocated range, normal video, audio and text data will be deleted instead.
2. After defining whether to delete alarm data or standard data, the system selects the channel which has the oldest recorded video, audio or text data segment and deletes data up to the defined minimum amount.
3. If enough space is not freed, the system will repeat step 2 until all selected channels (alarm specific data or standard recorded data) have been processed.
4. If enough space is not freed after all selected channels have been cleared to their defined minimum storage capacity, the system will repeat step 2 for all available channels (alarm specific data and standard recorded data) starting with the channel which has the oldest recorded video, audio or text data segment.
5. If enough space is still not freed, the system will repeat step 2 disregarding the defined minimum storage time.

Note: *To ensure that the need for automatic deletion due to a lack of disk space is minimized, it is a good idea to regularly monitor the disk usage and to 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 case of storage space issues.

Hint: *You can set a Watchdog event to notify you if the storage space runs low.*

Top Previous Next

1.13.5. Archiving

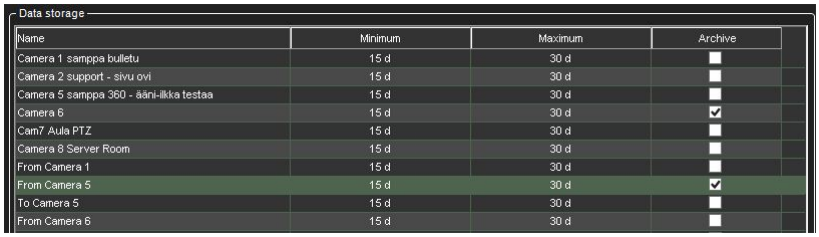
You can set the system to automatically archive video, audio and text data on a daily or weekly basis. The archive files can be automatically created on the server's hard disks or on a network drive.

The archive files can be opened on any Spotter client.

Note: *Archive files can be extremely large, 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.*

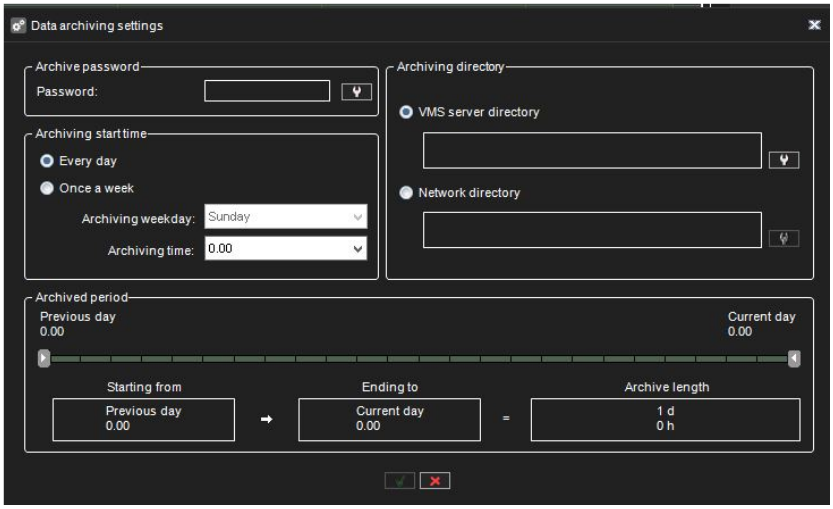
To set an automatic archiving schedule:

1. In the **Data storage** pane, click on the devices that you want to include in the automating archiving process.
   TIP: To select adjacent devices or folders, hold down the SHIFT key and then click the first and last device that you want to select. To add a device to a selection or to remove it from a selection, keep the CTRL key pressed and then click the device that you want to add or remove.
   Note: *Selecting a device group (folder) also selects its contents.*
2. Mark the **Archive** checkbox.



3. Click **Modify archive settings**

4. Set the archive password by clicking **Change archive password**



5. Select, whether to create the archive on a daily or weekly basis by selecting **Every day** or **Once a week**.
1. If you set archiving to occur on daily basis, use the **Archiving time** drop-down menu to select the time on which the archive files are created.
2. If you set archiving to happen on a weekly basis, use the **Archiving weekday** and **Archiving time** drop-down menus to select the date and time on which the archive files are created.
6. Use the **Archived period** slider to set the time period used in the archive files.
7. Select, whether to create the archives on a local drive (on the server) or on a network drive by selecting **VMS Server directory** or **Network directory**.
8. Click the **Change directory** or **Change network drive** button to set the directory in which the archives will be saved.
9. Click **OK** to set the archiving schedule.

Top Previous Next

1.14. Text Channels

Top Previous Next

1.14.1. Text Channel Settings

The servers can receive text data from devices such as cash registers or gas station pumps. A software license with text data channels and a text data capture driver is necessary.

The driver specifies what text data is recorded and what is shown to the users. It also specifies custom events and available search criteria.

In addition to the default text data drivers included in the software, new drivers can be installed as plugins.

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.

To add text data channels:

1. Click **Add channels** in the lower right corner of the **Text channel settings** screen.
2. Select the text data channel driver from the **Model** drop-down menu.
3. Use the **No. of data channels** slider control to select the number of channels you want to create.
4. Fill the driver-specific information into the fields in the **Properties** list.
5. Click **OK** to save the channels.

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 same 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 by using the* ***No. of channels*** *slider.*

Top Previous Next

1.15. Profiles

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

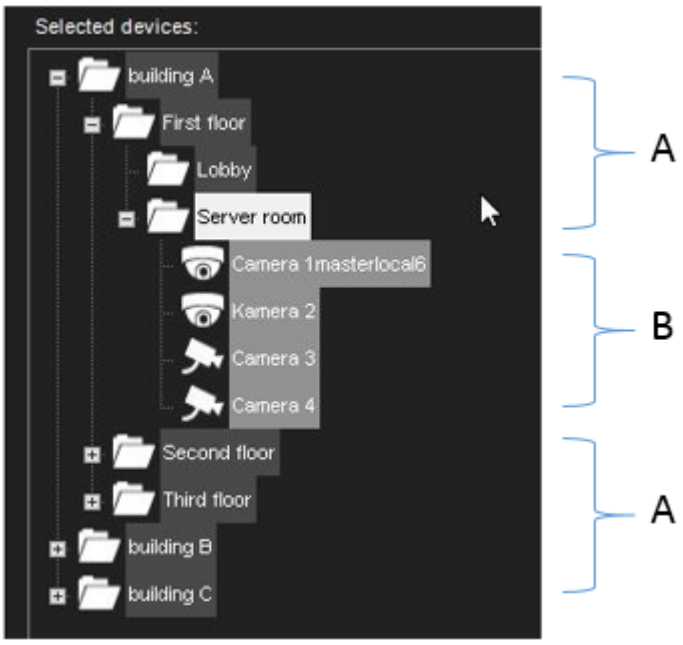
1. Cameras (fixed cameras and PTZ cameras)
2. Audio channels
3. Audio communication channel
4. Digital inputs (alarm inputs)
5. Digital outputs (control outputs)
6. Video outputs
7. Text channels
8. Alarms
9. Plugin instances
10. Web browser home pages

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.

Example 1*: Put devices into groups based on their location. For example, first add groups for different buildings (in the following figure, Building A, Building B, and Building C). Then add a group for devices that are on the first floor of the first building. Divide the first floor into subgroups. For example, add a group for all the devices that are in the lobby and then different groups for each department on the first floor. Finally, when you have added all groups and subgroups, add the devices to the groups.*

Example 2*: Put devices of the same type into the same group, for example, put all digital outputs into the same group.*

Note: *You can put a device into more than one group, so that you can, for example, put devices into groups based on both location and device type.*



A sample profile. ***A****. Device groups* ***B****. Cameras*

Top Previous Next

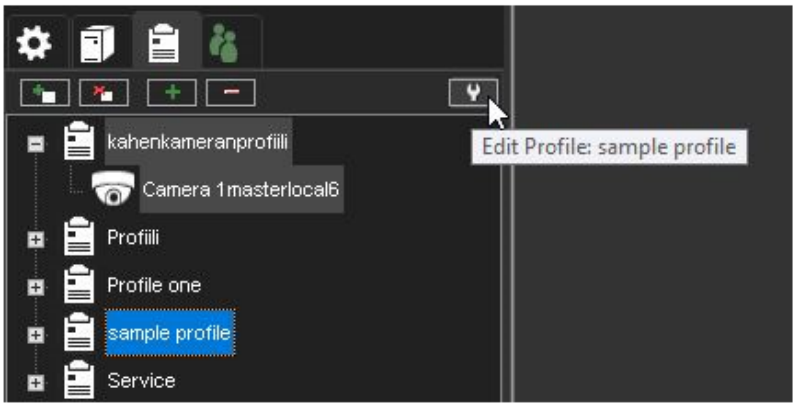
1.15.1. Adding and Editing Profiles

The system has one default profile, *Services*. The default profile contains the devices that the license key of the Master Server specifies.

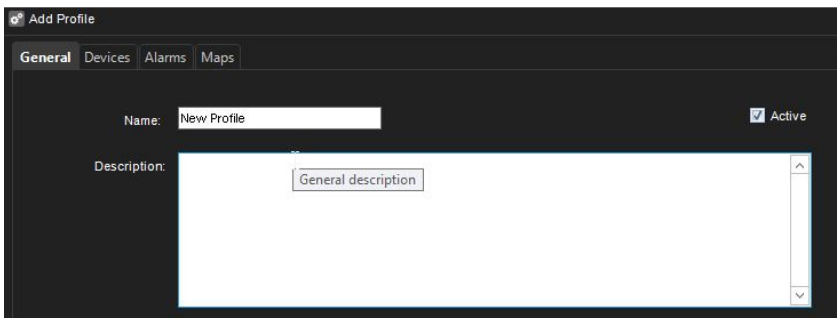
The devices are grouped by device type. For example, all cameras are in one group and all audio channels are in a different group.

You can use the default profile as such or edit it freely, for example, group cameras that are at the same location together. Or you can add new profiles. A profile can contain devices from different servers.

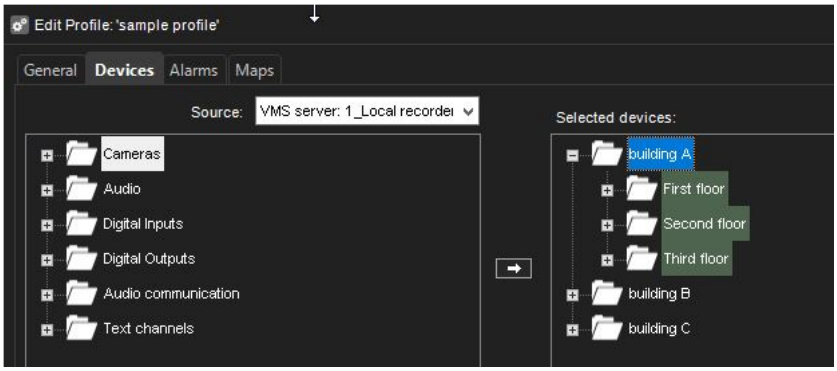
To add or edit a profile:

1. On the **Profiles** tab, do one of the following:
1. To edit a profile, click the profile that you want to edit and then click **Edit Profile** 

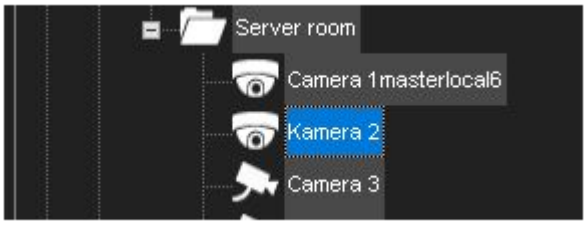
in the lower-right corner of the navigation pane. The **Edit Profile** dialogue box is shown.
2. To add a profile, click **Add Profile** in the lower-left corner of the navigation pane. The **Add Profile** dialogue box is shown.
2. On the **General** tab, you can change the name of the profile and type a description of the profile. To temporarily disable the profile, clear the **Active** check box. To again enable the profile, select the **Active** check box. The profile name is shown to the user in the Spotter program. The description is shown only in System Manager.

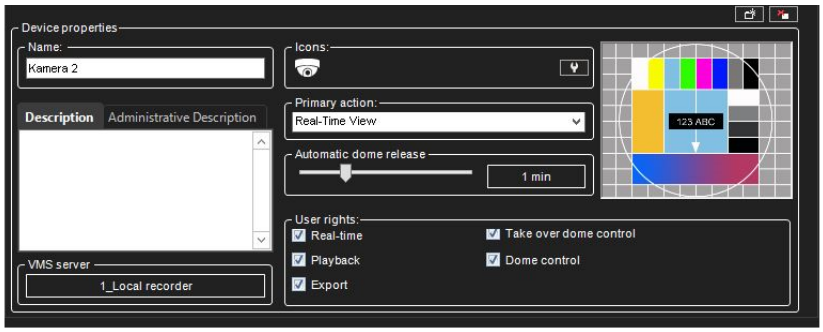


3. On the **Devices** tab, add device groups and devices to the profile. Or remove devices that you do not want the users to access. You can select devices from different servers or from other profiles and even copy existing profiles.



4. For each device, you can set user rights. Under **Selected devices**, click the device and then select or clear the appropriate checkboxes.





5. On the **Alarms** tab, you can select the alarms that you want to include in a profile. You can add only existing alarms. You can create alarms on the **VMS Servers** tab, under **Alarms**.
6. On the **Maps** tab, you can link maps and floor plans to device groups. Each device group can have its own map that shows where the devices are located. Users can access the devices directly from the map.
7. To delete a profile:

3. On the **Profiles** tab, select the profile and then click **Delete Profile** at the bottom of the navigation pane.

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

1.15.2. Adding Device Groups and Devices to a Profile

The tree structure that you create for a profile resembles the folder structure that is used for storing computer files.

The idea is to create a structure that makes it easy for the users the find and access devices.

The structure consists of devices and device groups. Devices resemble computer files, and device groups resemble computer folders.

First, create the device groups (folders). Note that you can add subgroups under the device groups. Then move the devices that you want the users of the profile to be able to access into the device groups.

You can add as many as 2000 devices and device groups to a profile and as many as eight levels of groups.

The structure that you create is what the users will see in the Spotter program.

To add device groups to a profile:

1. To add a new device group to a profile, click **Add Device Group**

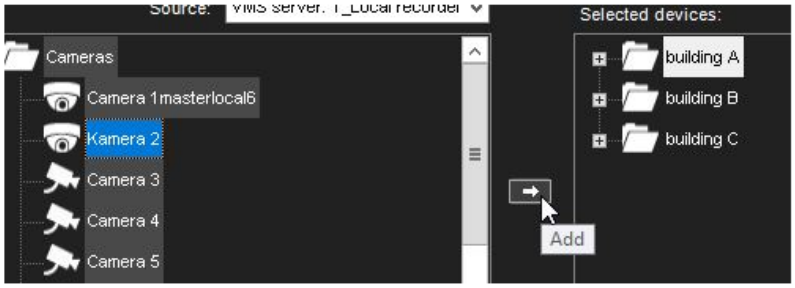
below the **Selected devices** pane. A new device group is shown.
Note: *A new device group is always added under the selected device group. To add a device group to the top level, make sure that none of the existing device groups is selected.*
2. Click the device group and type a name for it in the **Name** box in the **Device properties** section.
3. Type a description of the device group in **Description**.
4. To change the icon that is used for the device group, click **Change Icon**. Then select the icon that you want to use.
5. In **Device Group Options**, you can select the option **Devices are linked** to automatically open all device views from the same group when the user opens one of the device views. This option applies to real-time and playback views.
6. Add as many device groups as necessary.

TIP: Do not use the "ENTER" key while doing the group tree editing. ENTER key in this view will close the profile editing window. Instead, re-focus the mouse to some other area on the dialogue.

To remove a device group or device from a profile:

1. Click the device group or device and then click **Remove** .

To add devices to a profile:

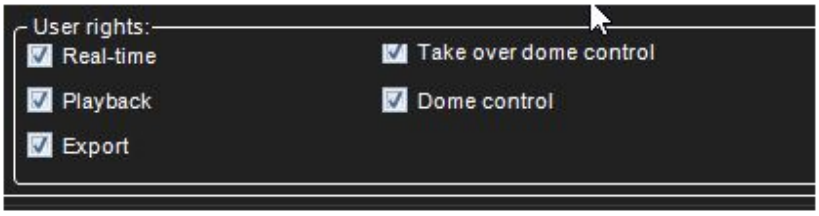
1. Select the source: a server or a profile. Available devices are shown in the left pane.
2. In the **Selected devices** pane, click the device group where you want to add a device.
3. Select the device or devices that you want to add and then click the right arrow 

You can also drag devices from the left pane to the right.
TIP: To select adjacent devices or folders, hold down the SHIFT key and then click the first and last device that you want to select. To add a device to a selection or to remove it from a selection, keep the CTRL key pressed and then click the device that you want to add or remove.
Note: *Selecting a device group (folder) also selects its contents.*
4. To select the icon for a device, select the device and then click **Change Icon**.
5. From the **Primary action** menu**,** select the action that will occur when a user double-clicks the device in Spotter.

6. If the device is a PTZ camera, you can set the profile-specific PTZ release time by using the **Automatic dome release** slider control. The setting defines the

time the user can be idle before PTZ controls are released and other users can access the controls.

7. Under **User rights**, select the functions that the user can activate.



8. For text channels, you can also select what data is shown in the device window. Click the **Device Window Options** tab to access the settings.

Device window options for text channels

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

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.

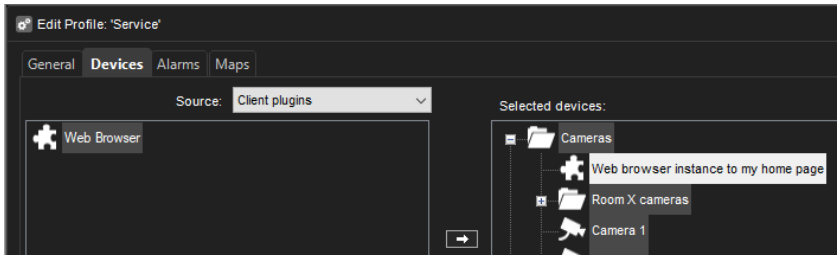
Top Previous Next

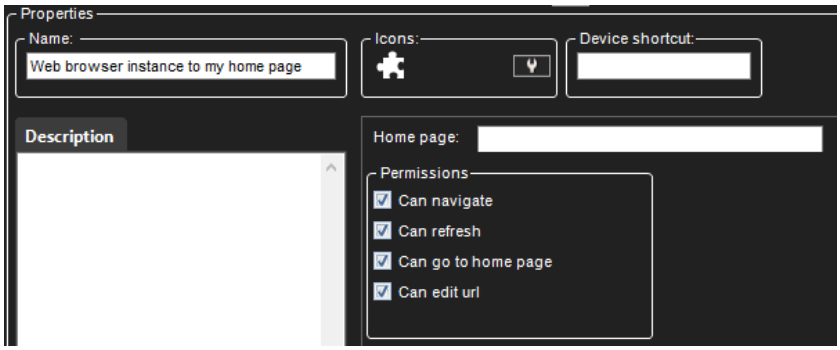
1.15.3. Adding Profile specific Web page instances

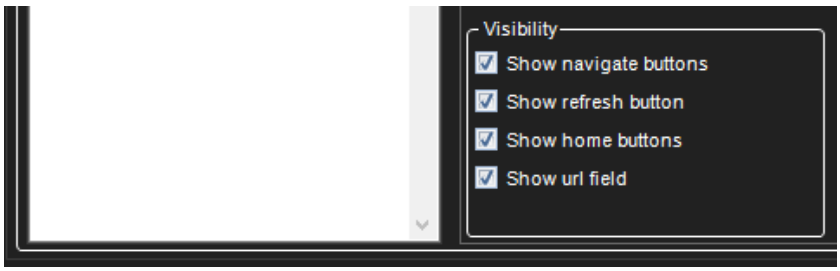
It is also possible to add instances of certain plugins to specific profiles. These can be used configured to access automatically to specific web pages.

Note that it is often possible to configure the username (and password) directly to the URL. It is also possible to prevent the user from browsing other pages.

These plugin instances allow bringing e.g. analytics web views, radar screens, and other backend systems to the user interface of the spotter.

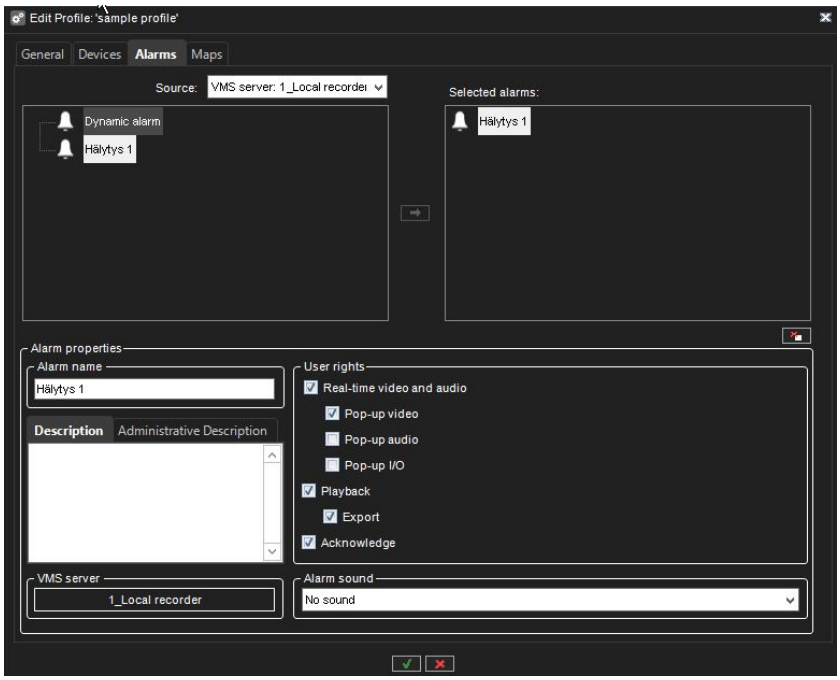






Top Previous Next

1.15.4. Editing Profile Specific Alarm Settings



On the **Alarms** tab, you can select the alarms that 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:

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.
4. 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.

The user rights include:

1. **Real-time video and audio**. Select to let the users see real-time alarm video or audio.
2. **Pop-up video**. Select to let users receive alarm video automatically.
3. **Pop-up audio**. Select to let users receive alarm audio automatically.
4. **Playback**. Select to let the user's playback alarm video.
5. **Export**. Select to let the users save alarm video on local media.
6. **Acknowledge**. Select to let the users acknowledge alarms.
4. To have the computer play a sound when an alarm occurs, select **Alarm sound** and then select the sound that is played. To test the sounds, select the sound from the list and click **Play**.
5. Save the settings by clicking **OK**.

Top Previous Next

1.15.5. Adding Maps to Profiles

You can attach a map or floor plan to each device group. You can then add icons to the map that show the location of the devices. By clicking the icons users can also access and operate devices directly from the map.

You can add map images that have been saved in BMP, JPEG, or PNG format.

There can be as many as eight levels of maps in the map hierarchy.

When you click the **Maps** tab, the highest group level is shown by default. You can move between group levels by selecting the level from the drop-down box. Click the **Up** arrow to move to a higher level.

The devices that have been selected to the profile are shown in the left pane.

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. 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 that you want to add to the map from the left pane and click the **Add to Map** arrow. Items that are already on the map appear dimmed in the left pane. If you add subgroup icons to the map, the icons will act as links to the subgroup maps. Users can move to a lower level map by double-clicking the subgroup icon.
   Tip: To select more than one device at the same time, keep the SHIFT or CTRL key pressed.
4. Select a device or device group from the map and then, under **Device properties,** you can set these options:

1. For cameras, you can select the direction that the camera icon points to.
2. 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.
3. If you need to fit a number of device icons in a small space, you can use placemarks. 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. Then drag the icon to a convenient position on the map.

To remove a site map:

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

To remove an icon from the map:

5. Select the icon and click **Remove**.

Top Previous Next

1.16. 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 to these.

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 devices the user group has access to in the system. One user group can have five profiles at the most.

All user accounts are protected by a username and a password.

Top Previous Next

1.16.1. User Roles

The system supports the following types of user roles (defined through user groups):

- **System Manager role:** Administrators are allowed to log in to System Manager and change all settings, for example, to change camera settings or add 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
- **[Product version] Spotter role:** End users are allowed to log in to Spotter but not to System Manager.

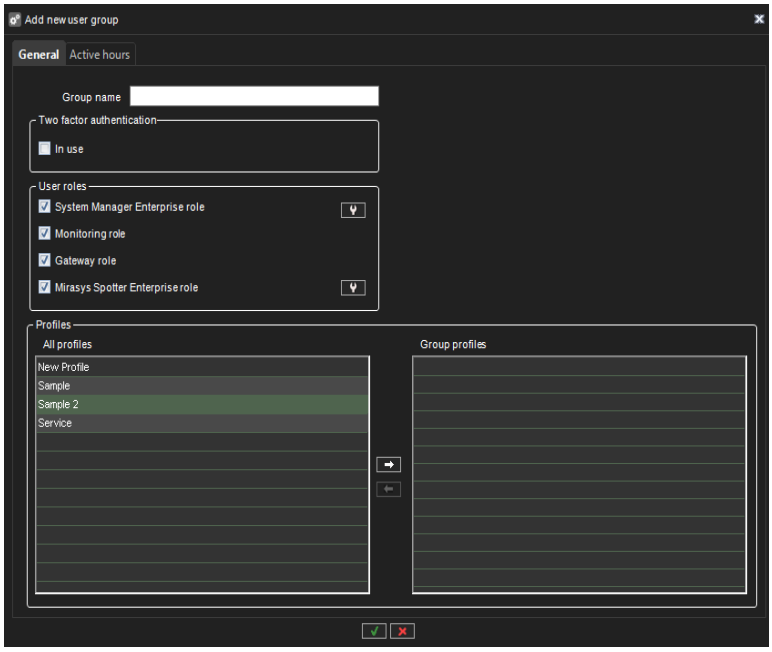
Top Previous Next

1.16.2. Adding New User Groups

To add a new user group to the system:

1. Click **Add User Group**

in the upper-left corner of the **Users** tab. The **Add User Group** dialogue box is shown:



2. Do the following:
1. Type a name for the group in the **Group name** box.
2. Select the user roles for the group.
3. 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.
   Tip: *To select more than one profile at a time, keep the SHIFT or CTRL key pressed.*
3. Click **OK** to save the new user group.

Top Previous Next

1.16.3. Adding New Users

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. 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:
1. Type a name for the account in the **Username** box.
2. To add a password to the account, click **Change password** and type the password two times.
3. Type an optional description about the user account.
4. Use the pull-down menu to select the user group into which you want to assign to the user.
5. Select the user interface language for the user.
6. To protect the program, you can use an automatic lock or automatic logoff. If the user does not use the program for the specified time, the program is locked or the user is logged off. The user can also manually lock the Spotter program at any time.
5. Click **OK** to save the new user account.

Note: Users can change their passwords and user interface language in the Spotter program.

Top Previous Next

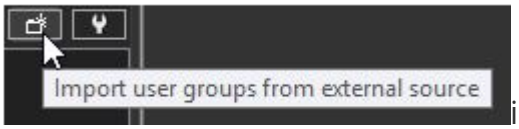
1.16.4. Domain Based User Groups (LDAP)

The system supports domain-level user rights integration (Microsoft Active Directory, LDAP), enabling users to be synchronized from domain groups. Domain-based users can log into the VMS system with their domain usernames and passwords.

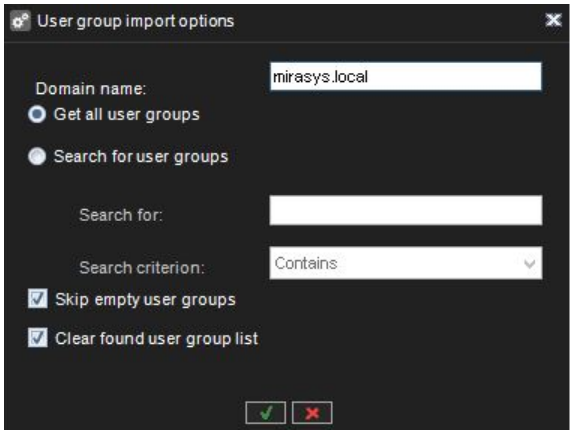
By default, user group rights are synchronized with their parent domain every 30 minutes. Please contact your system supplier if f you need to change the default interval.

This feature requires a license update.

To add a new domain-based user group to the system:

1. Click **Import User Groups** 

in the upper-left corner of the **Users** tab (next to the **Edit User Group** button). 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 **User group domain** dialogue box.



3. Select, whether to get all user groups or to search for specific groups. If you want to search specific groups by name, you can add a search criterion based on the text string is 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 empty user groups.
5. Select, whether to clear or keep previous search results.
6. Click **Ok**.

7. In the **Import user groups** window, select the user groups you wish to import from the domain.
8. Click **Ok** to import the selected groups.
9. Edit the imported user groups to set their user roles as instructed below.

Top Previous Next

1.16.5. Editing User Groups

To edit a user group (whether system or domain-based):

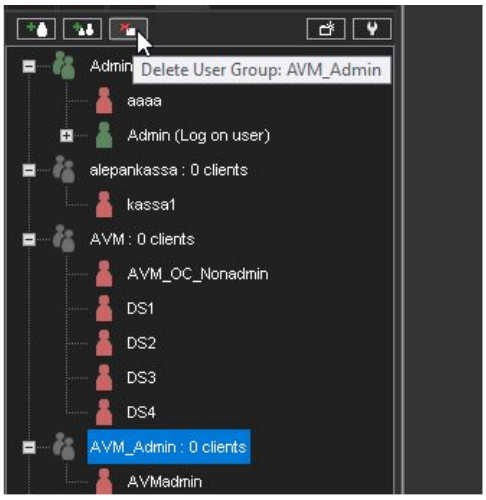
1. Open the **Users** tab.
2. Click on the user group you want to edit.
3. You can edit the following settings:
1. Type a name for the group in the **Group name** box.
2. Select the user roles for the group.
3. Select the profile or profiles you want to assign to the user group. Click the right arrow button or drag the profiles from the left pane to the right.
   Tip: *To select more than one profile at a time, keep the SHIFT or CTRL key pressed.*
4. Click **OK** to save the changes.

Top Previous Next

1.16.6. Deleting User Groups

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.



2. Click **Delete User Group** in the upper-left corner.
3. Click **OK** to delete the group.

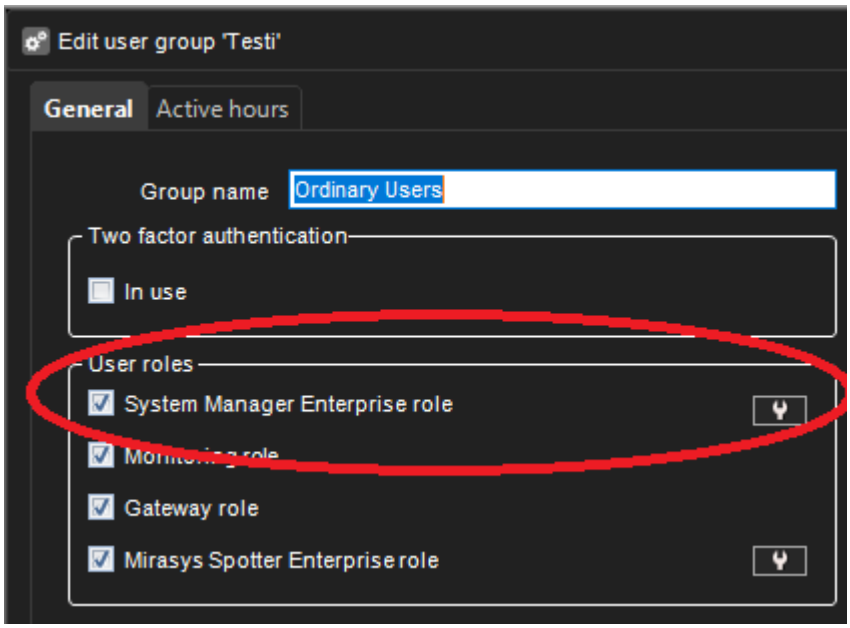
Note: *Domain-based (LDAP) user groups cannot be deleted through System Manager. If deleted, an LDAP group is removed from System Manager but the domain group is not affected.*

Top Previous Next

1.16.7. System manager enterprise role

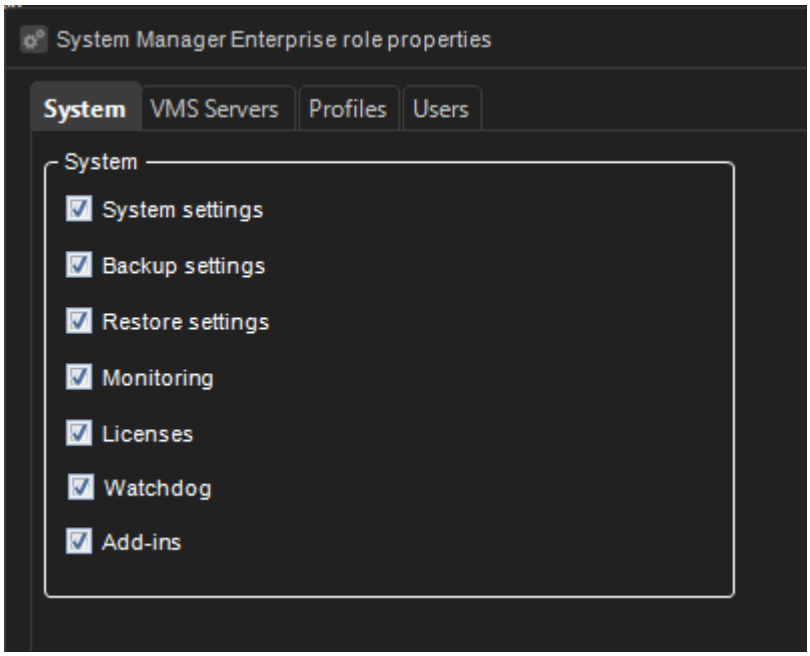
It is possible to set detailed permissions for the system manager for different user groups. This allows for instance implementing functionality for allowing different user groups for hardware maintenance and user administration, which is useful for large scale systems.

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.

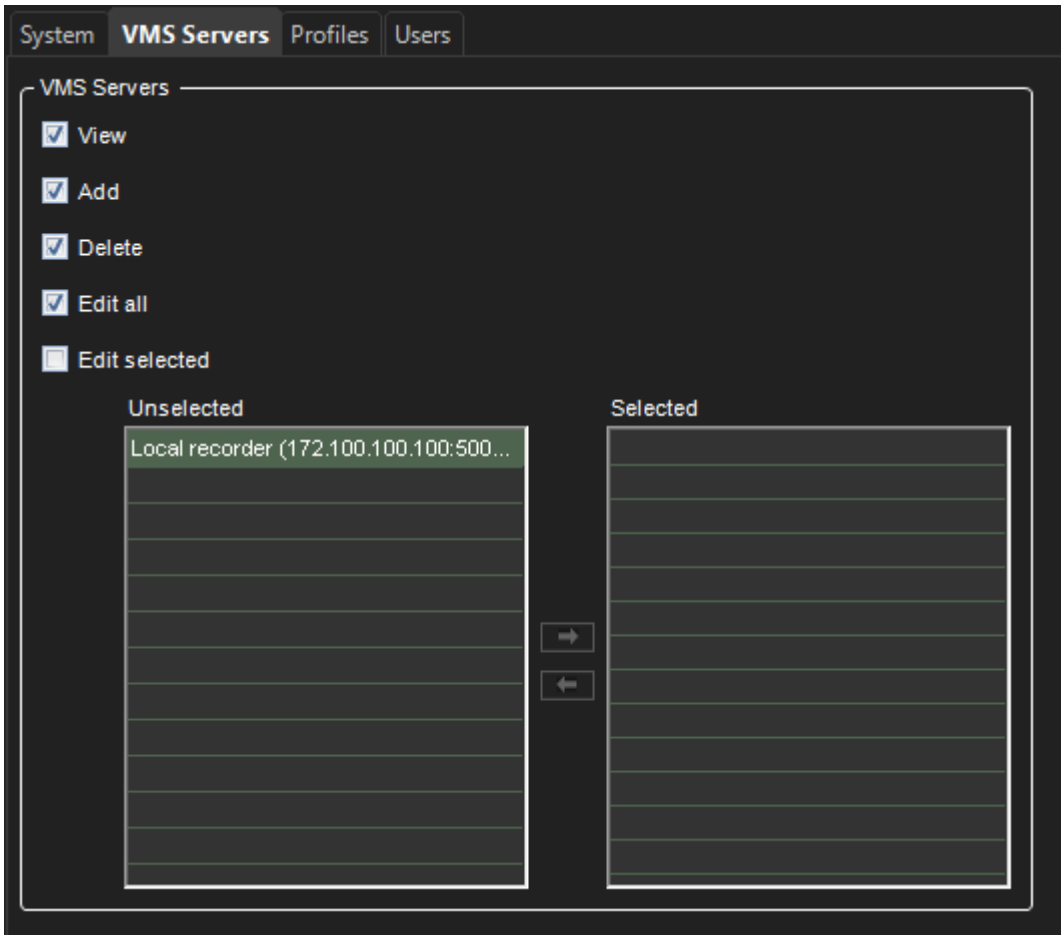


Under the role settings, there are tabs for setting the detailed level permissions for the user groups. The tabs (System, VMS Servers, Profiles, Users) correspond to the System Manager top-level dialogues:

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



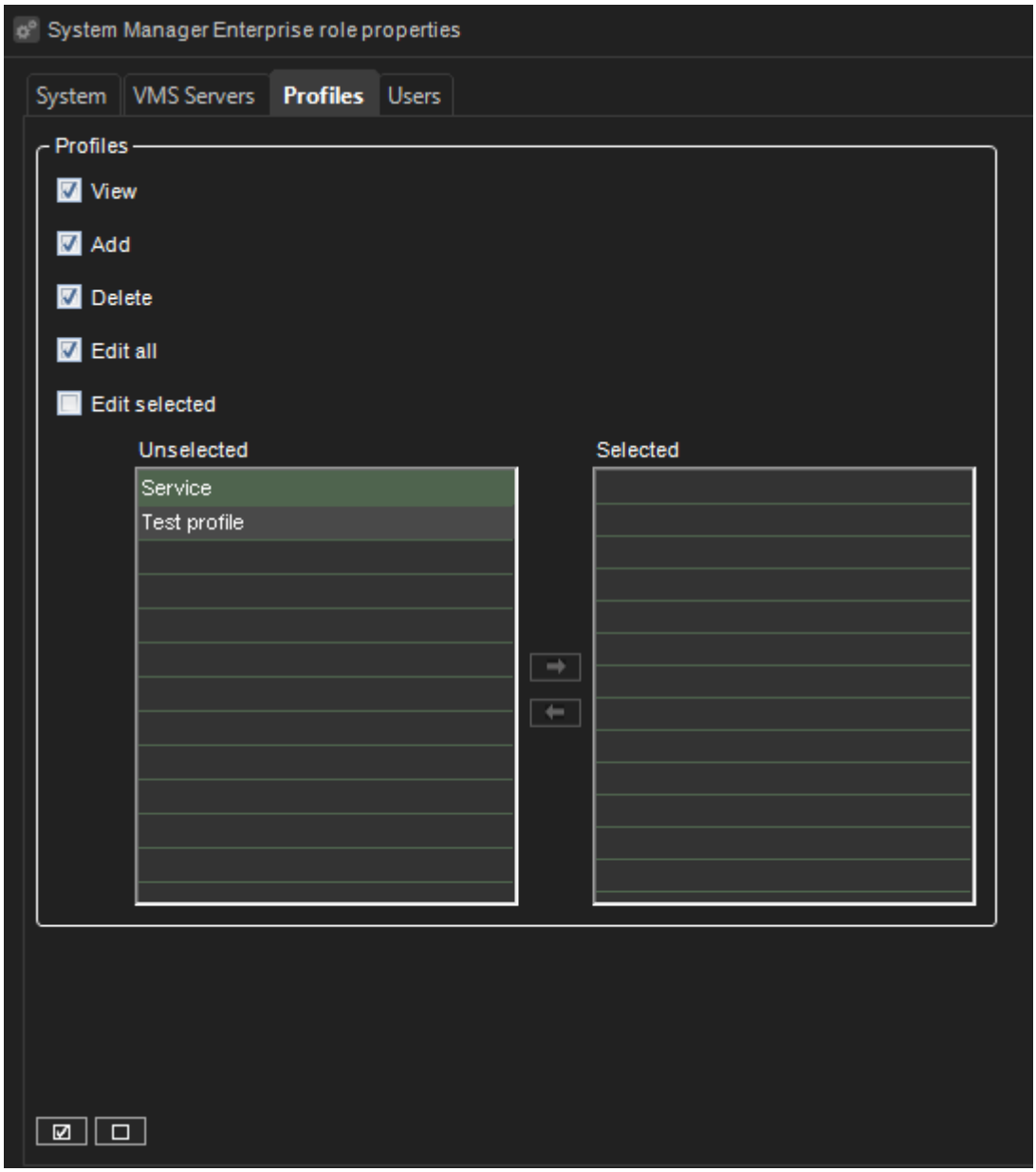
The servers tab allows permissions for a user group to View, Add, Delete and edit either all or only selected VMS Servers



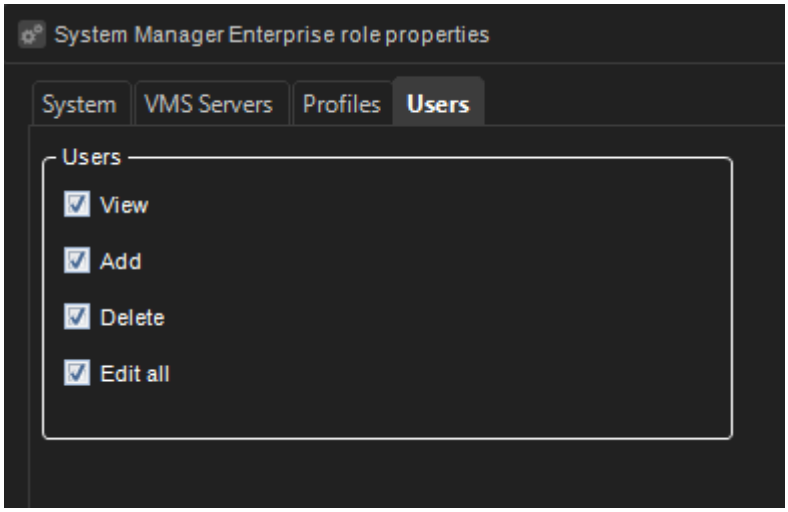
to be noted: if "Edit selected" is checked, the shuttle box below enables defining which specific servers this user group has access to. This is convenient in large installations in case-specific user groups are working with specific servers (e.g. if there are separate maintenance groups for different sites - and the recording servers are site-specific.)

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

“Edit selected” enables the shuttle bus selection for specific roles that the user groups can access (similar to the "servers" permission configuration.)



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



Edit all or Edit selected must be enabled for a user group for users to be able 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

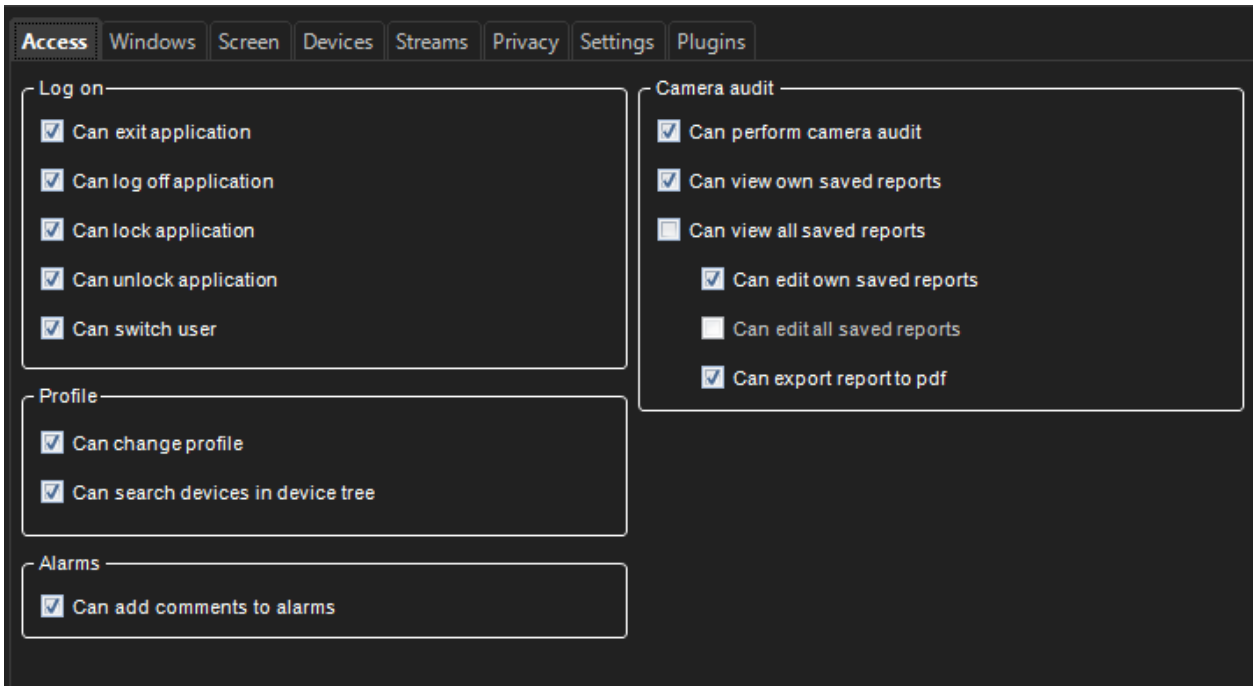
Top Previous Next

1.16.8. Spotter role customization

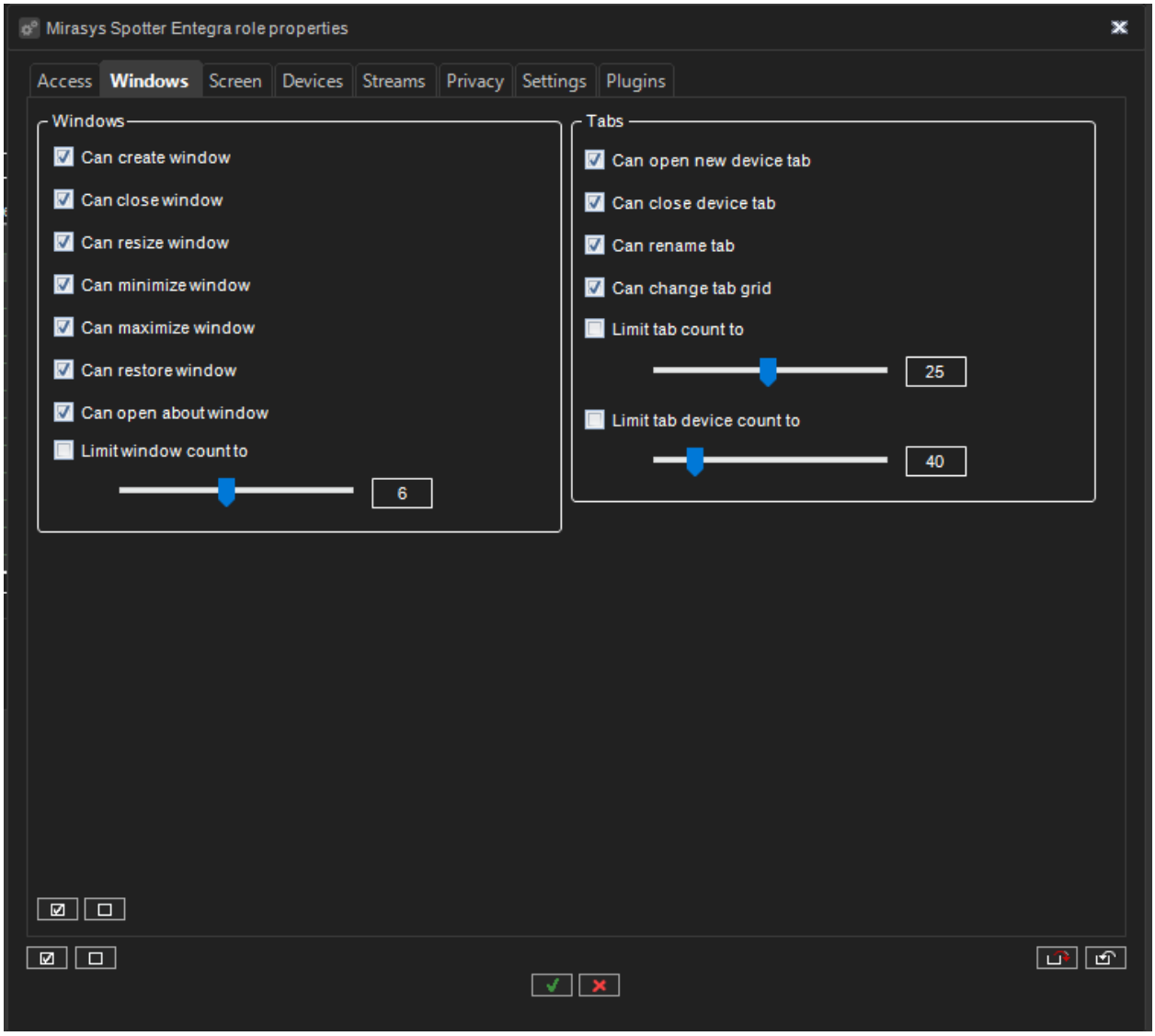
Custom user role properties can be edited by clicking the custom role properties edit button.

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

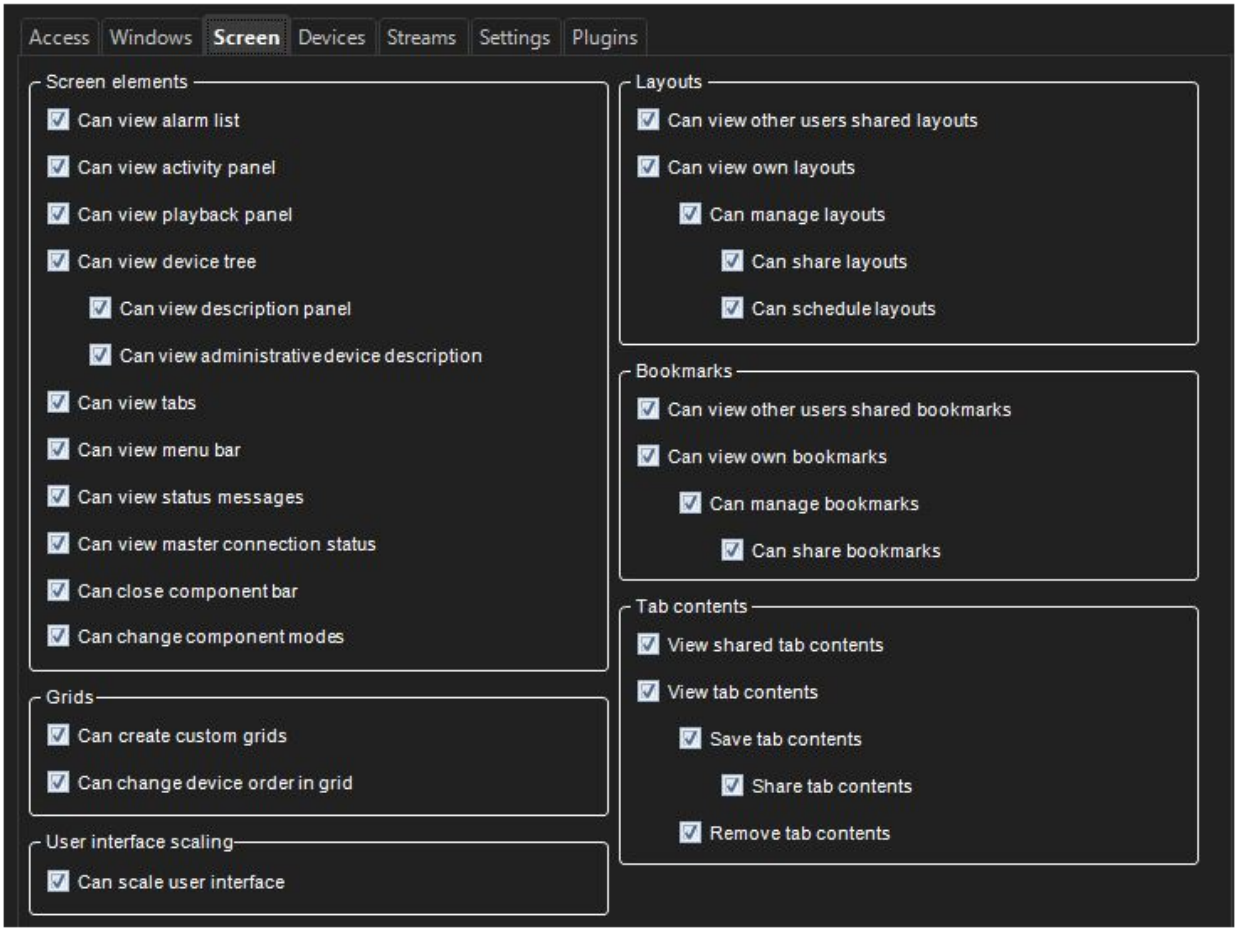
The first tab of the role customization contains options for the application access and accessing profiles, as well as alarm commenting.



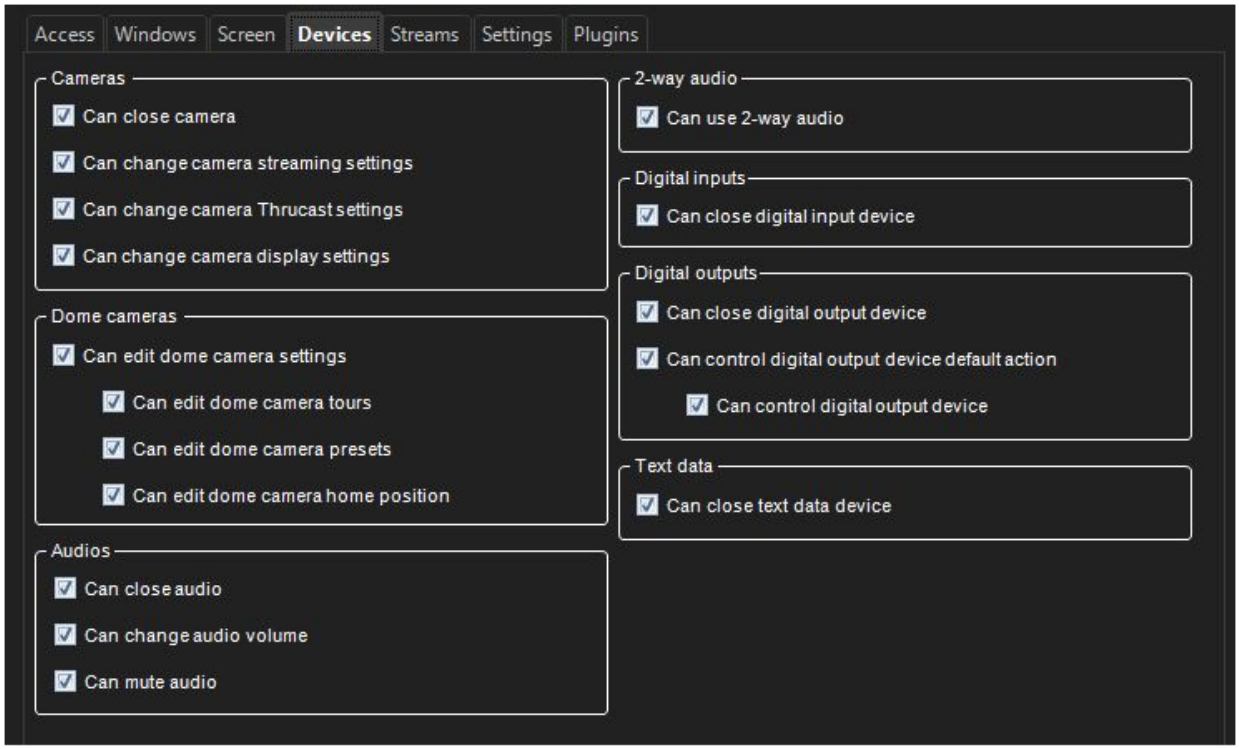
The second tab contains options for Spotter window management and tab management.



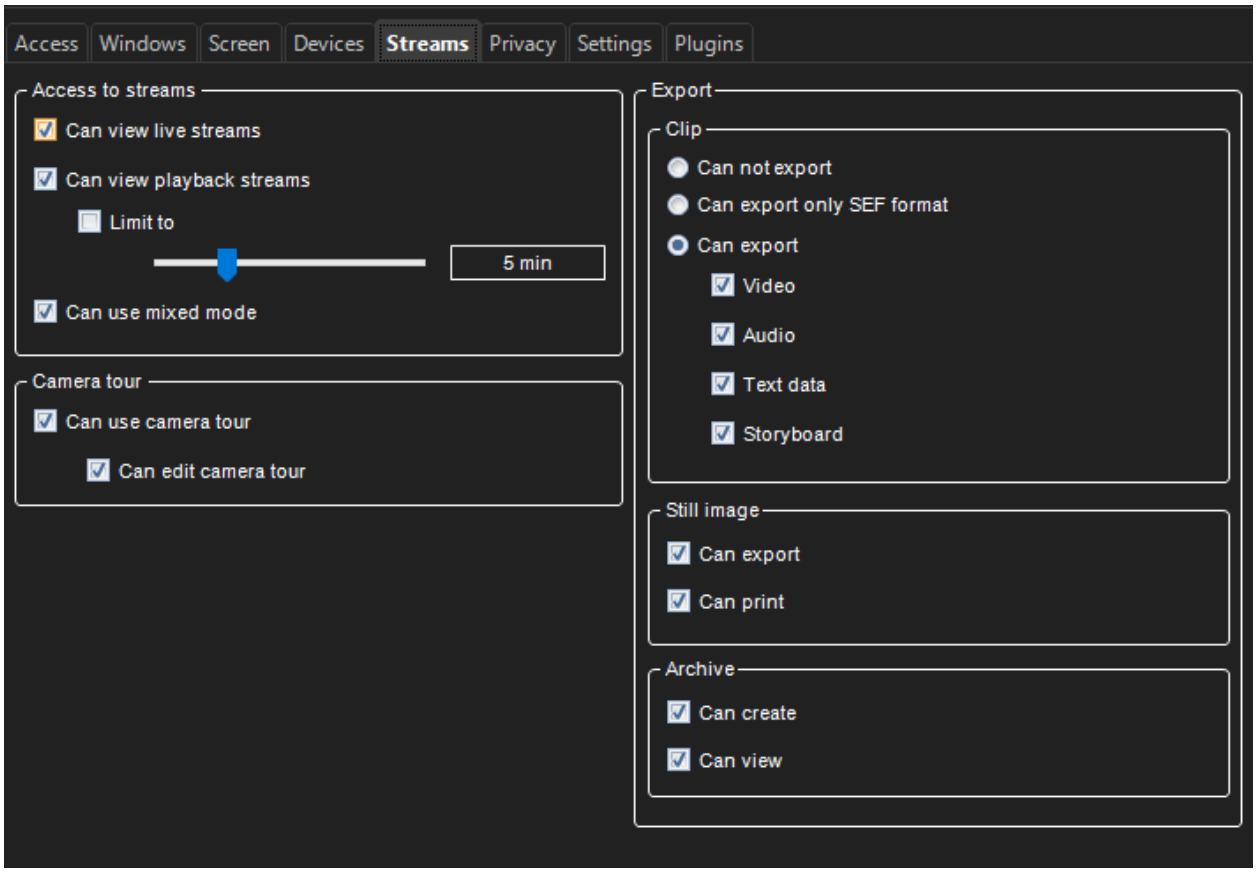
The third tab contains options for different screen element access and layout access, bookmarks, camera grid and saved camera tabs.



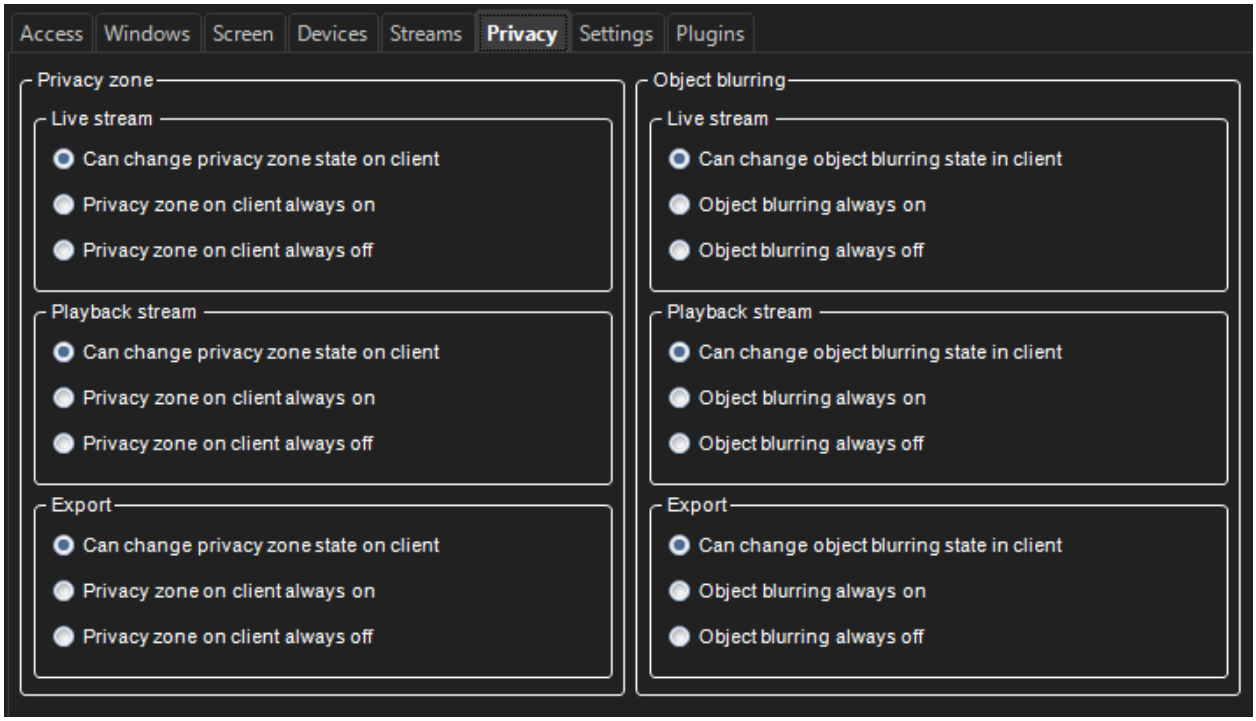
The fourth tab contains options for media control.



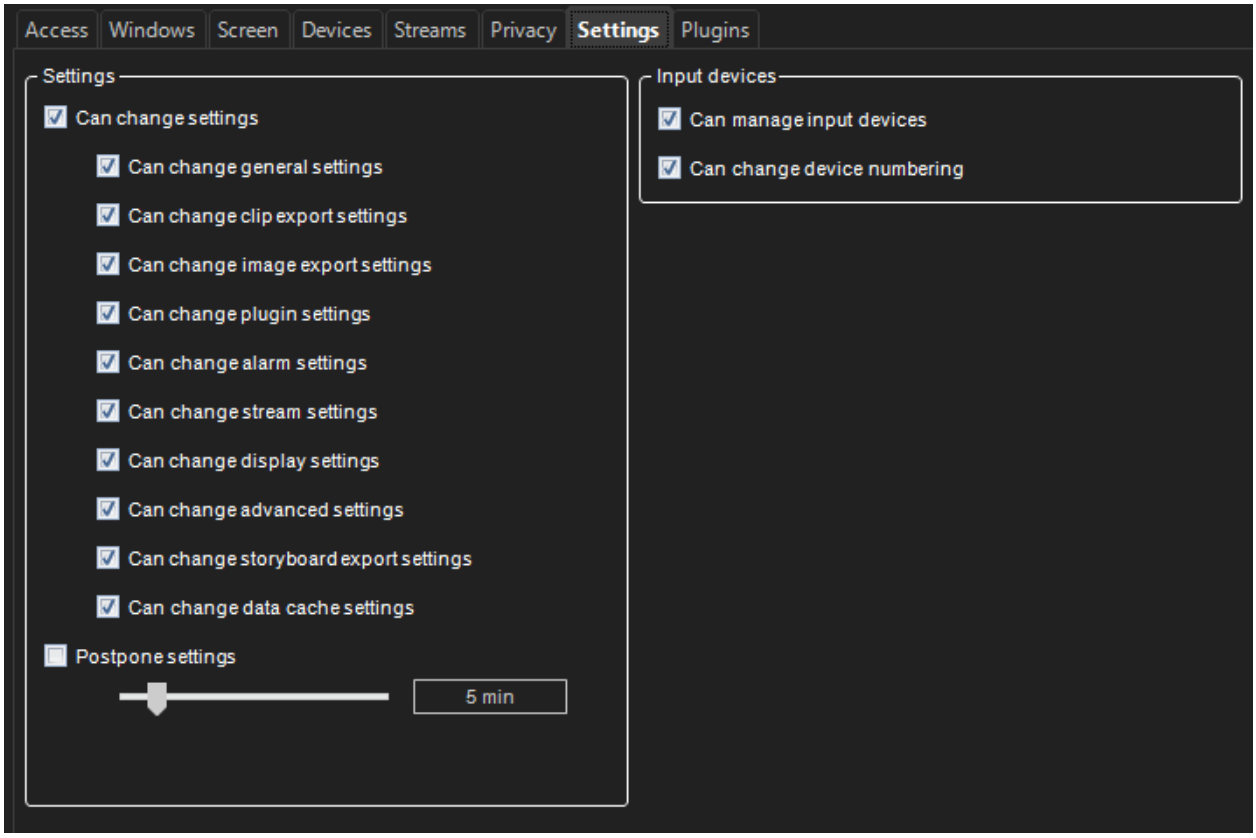
The fifth tab contains options for stream access and exporting.



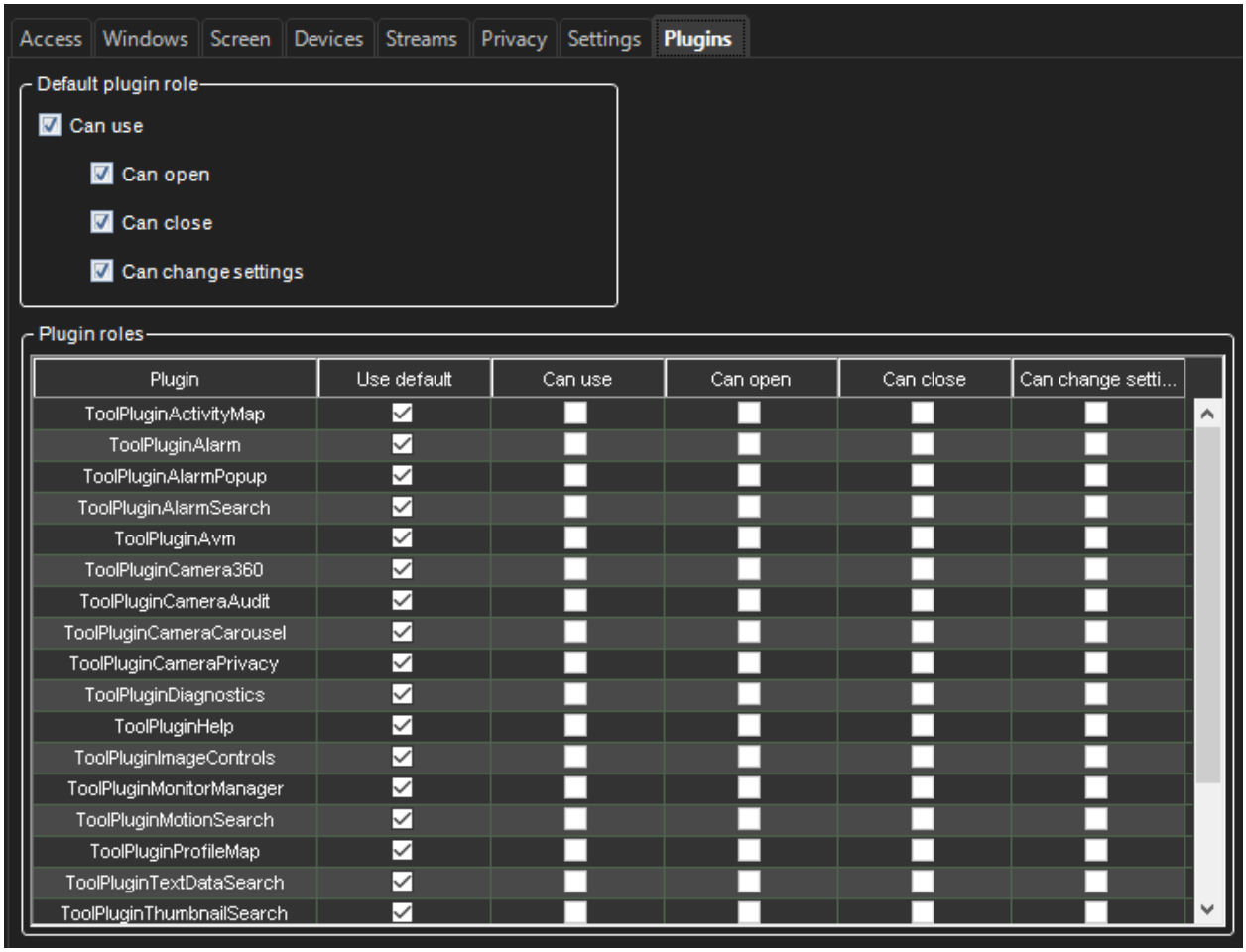
The sixth tab contains options for privacy.



The seventh tab contains options for Spotter settings.



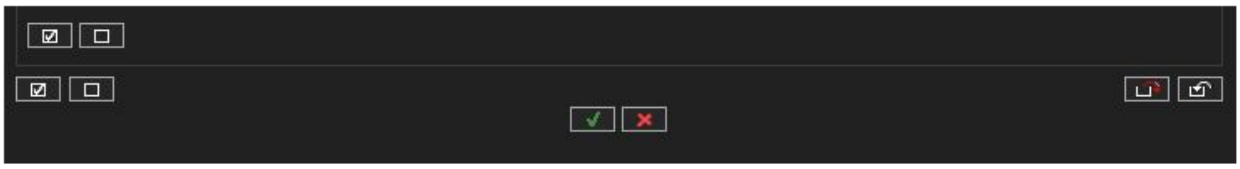
The final tab contains options for Spotter plugins.



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

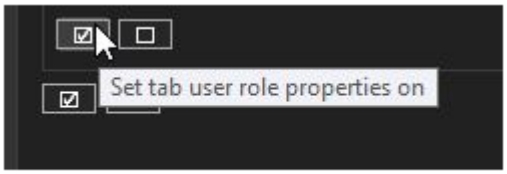
Exporting and Importing User Role Settings

There are six new buttons at the bottom of the Spotter user role settings window:

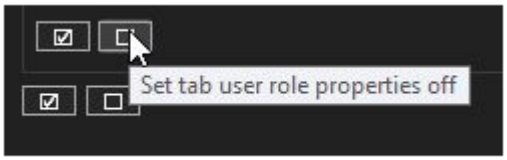


The first two buttons on the left will toggle the current user role settings tab checkboxes on and off for the current settings tab.

Clicking this button



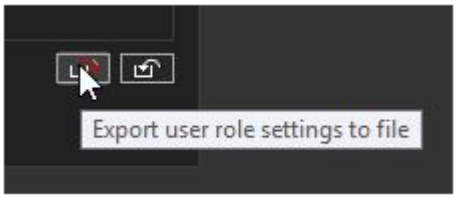
will select all the checkboxes in the current tab. Clicking the button next to it will deselect them again.



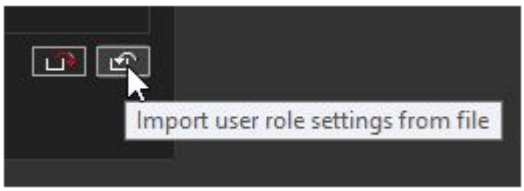
Below the tab specific select and deselect buttons are buttons to perform similar changes to all of the tabs.

This improvement makes it faster to create heavily customized roles.

After some changes have been made, it is then possible to export the settings to a ".sur" (Spotter User Role) file with this button:



These ".sur" files can then be used to quickly deploy a user group with specific settings to a new location with the import button



Top Previous Next

1.16.9. Monitoring Users

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

Icon	Description
	(Green). The user is logged on. Click the plus sign (+) to see the name of the program the user is logged on to and the IP address of the user's computer. In addition, the date and time of logon are shown.
	(Red). The user is not logged on.
	(Grey) The user account is disabled.

Top Previous Next

1.16.10. Logging Users Off

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

To log a user off:

1. Right-click the username on the **Users** tab and click **Log User Off**.

Top Previous Next

1.16.11. 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 and open the **Edit User Account** dialogue box.
2. Do one of the following:
1. To disable the account, clear the check box **Active**.
2. 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.*

Top Previous Next

1.16.12. Two-factor authentication

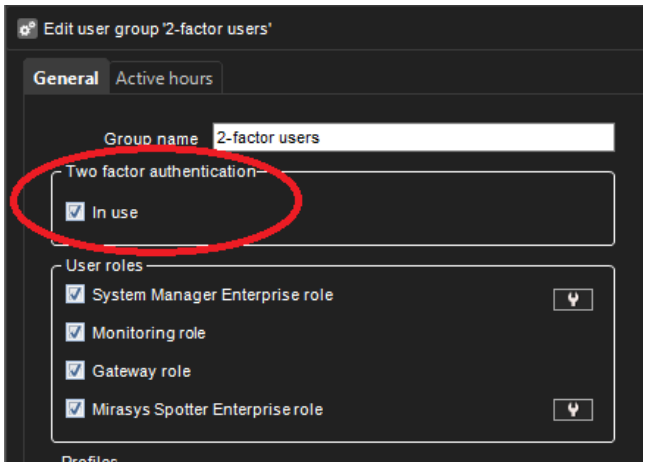
The two-factor authentication is functionality to improve the identification of the user logging in, by requiring not only the username and the password but also a code from an external physical device.

This makes it practically impossible for e.g. certain user groups (e.g. system administrators) to use shared credentials. (Using shared credentials would make it practically impossible to e.g. monitor specific user actions from the audit logs later on.)

The basic process in the 2-factor authentication is as follows:

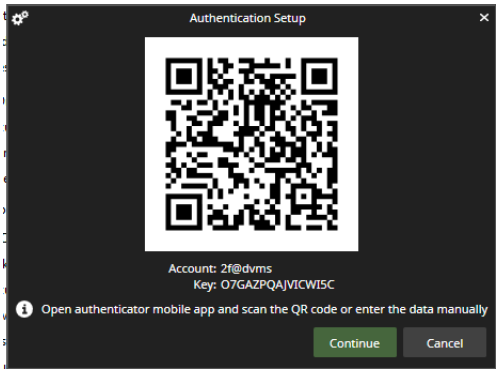
Setup:

0) Admin enables the 2-factor authentication for the specific user group.



1) When a 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.

2) The VMS and the authentication client have then synchronized the software with VMS. 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:

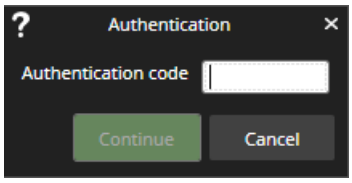


3) Thereafter the authentication client generates automatically new one-time passwords. (The passwords change periodically and are kept in sync as the clocks of the VMS and the authentication app have same time. Note that this does not require any direct data communication link between the software.)

Login:

1) The user provides the normal credentials to VMS (username, password)

2) The VMS requests an authentication code from the authentication app for each login.



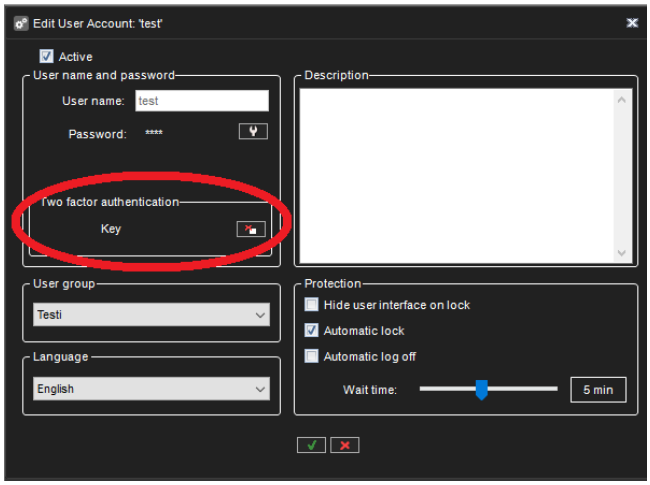
3) The user provides the one-time password from the authentication app. and the user types them to the VMS client.

Maintenance:

4) In case the user forgets his / her 2-factor secret key, the administrator can then reset the key from the system manager.

5) After 2-factor secret key reset, the user needs to update the secret key in the next time he/she logs in. (See step 2).

Administrator Guide V8



Top Previous Next

1.17. System

On the **System** tab, you can edit and backup system settings, monitor the system and examine diagnostic information about the system. On this tab, you can also change license keys for servers, for example, to add more camera channels and install new IP cameras, metadata and client plugin drivers. In addition, you can configure the software watchdog.

The tab contains these tools:

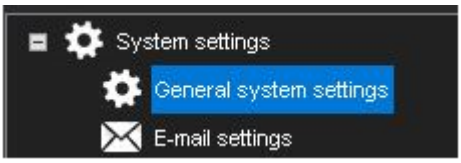
1. System settings
2. General system settings
3. E-mail settings
4. Change server addresses
5. System addresses
6. Update VMS Servers
7. Backup
8. Export files
9. Exporting log files
10. Backup system settings
11. Restore system settings
12. Diagnostics
13. SMServer diagnostics
14. DVRServer diagnostics
15. Licenses
16. Software Watchdog
17. Add-ins (drivers and plugins)

To open a tool, do one of the following:

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

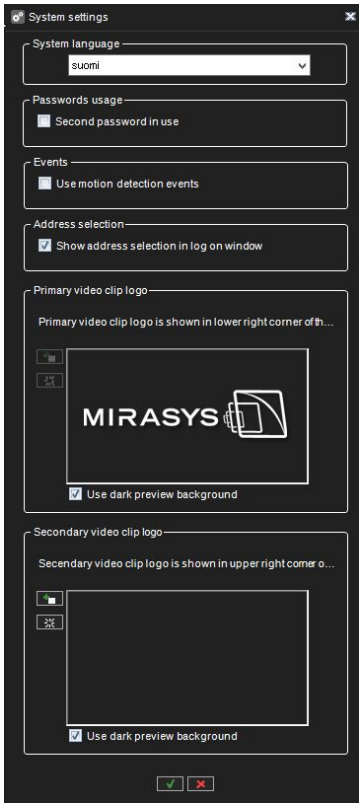
Top Previous Next

1.17.1. General System Settings



In this section, you can control:

- System language
- The password mode
- Login window site selection mode
- The setting for sending motion information to clients
- Logos that are attached to exported video clips

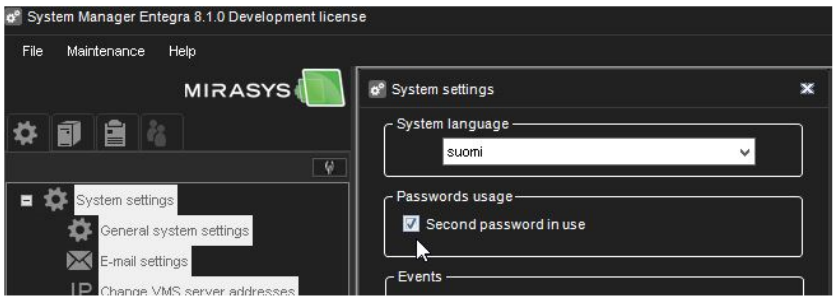


Top Previous Next

1.17.2. Using the System in Dual-Password Mode

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.

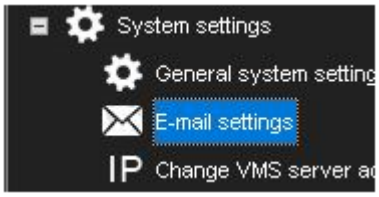


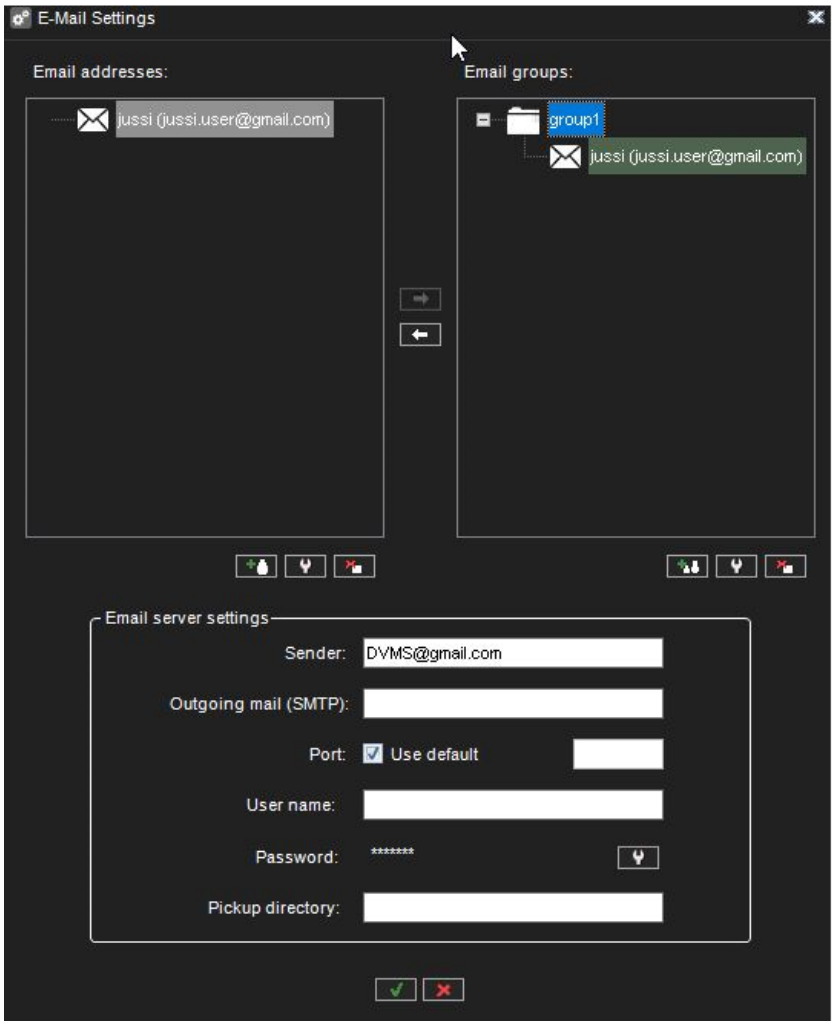
When this mode is selected, all users are required to give two passwords. The default second password is empty.

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, then both persons need to be present when reviewing videos.

Top Previous Next

1.17.3. E-Mail Settings





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

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 applicable fields.
5. Set the events for which notifications will be sent as instructed in the Software Watchdog.

Note: Emails are not sent to all system email recipients, but the administrator can control which Watchdog events and alarms are sent to which email recipients or groups.

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 to the **Name** and **Address** fields.
4. Click **OK**.

To add 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:

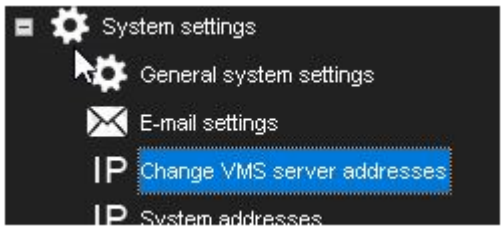
1. Highlight the desired group on the group list
2. Highlight the desired recipient(s) in the recipient list
3. click on the arrow to add the selected recipients to the selected group

Other available actions:

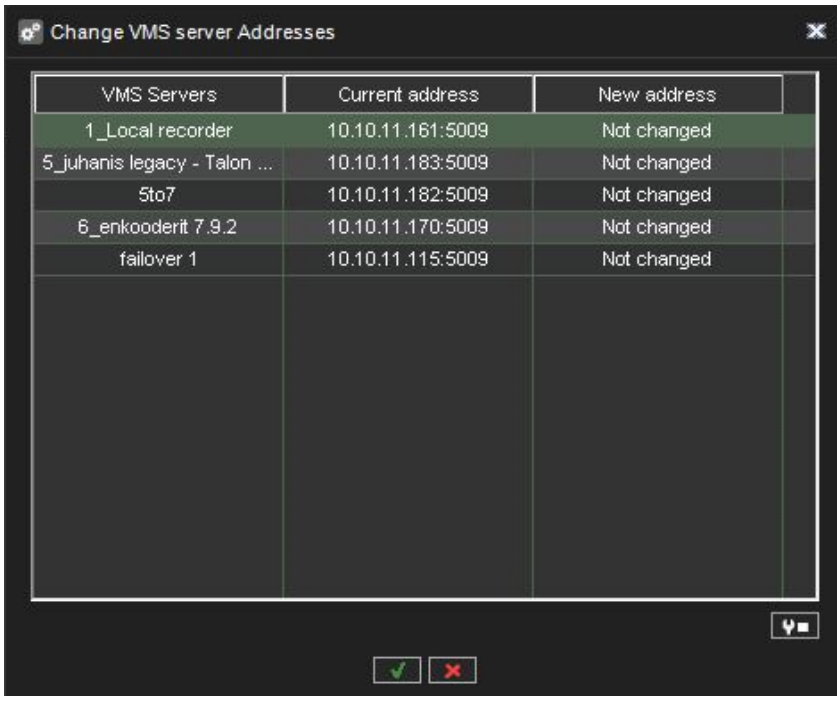
Editing of email names, addresses, group names and removing persons from groups is possible with the edit buttons. Persons can be removed from groups with the arrow . Persons and groups can be removed with the button

Top Previous Next

1.17.4. Managing 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.

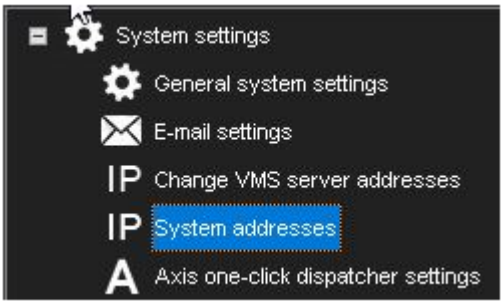


To change a server's IP address or DNS name:

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**.

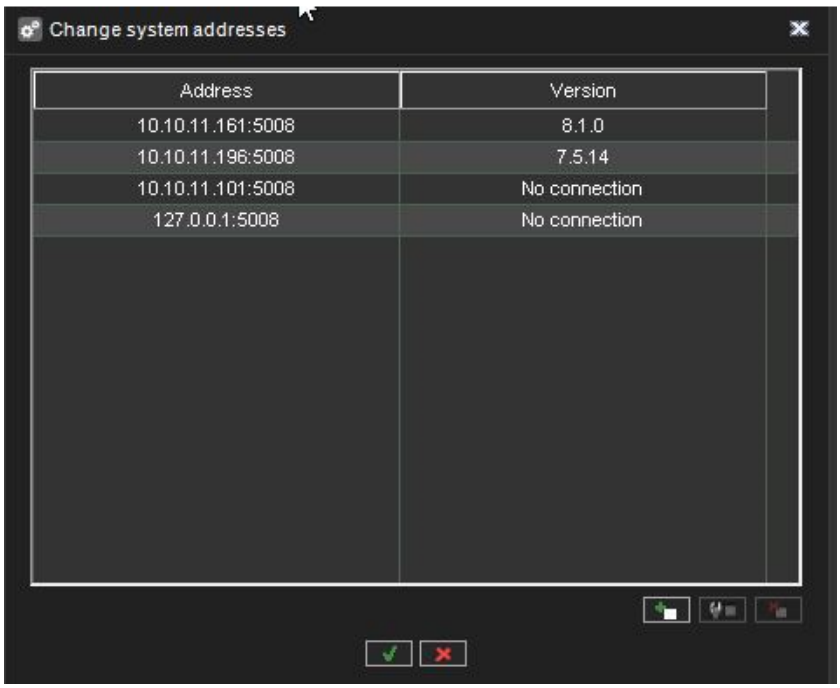
Top Previous Next

1.17.5. Managing System Addresses (Master Server 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.



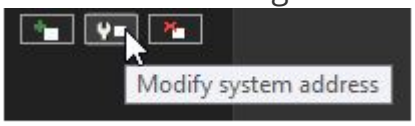
You can define multiple Master Server addresses that the client applications can connect to. The addresses can be provided as IP addresses (e.g. *http://195.168.0.1*) or DNS names (e.g. *http://www.example.com*).

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:

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** 

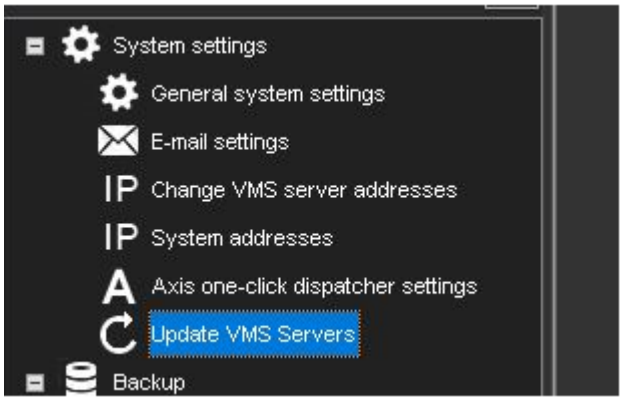
.
4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

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** .

Top Previous Next

1.17.6. Updating VMS Servers



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

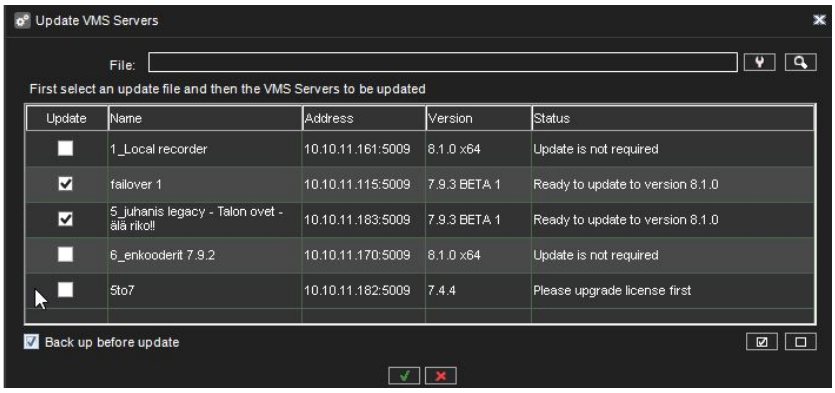
To update servers, first, select the installation file with the button.

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

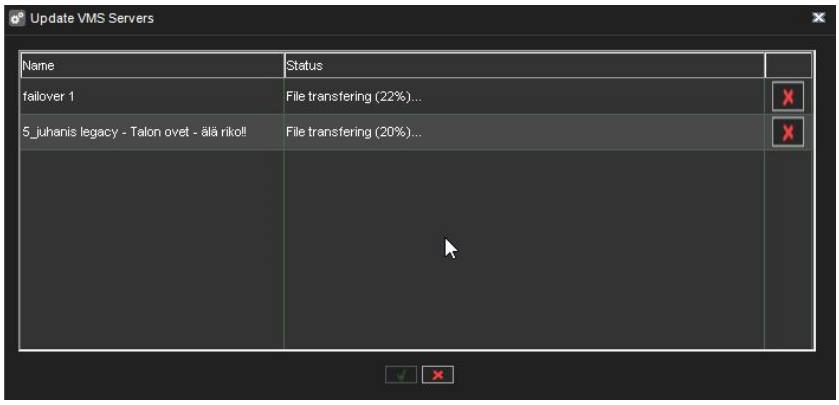
Note: *When performing a major version upgrade, for example from VMS 6.x to 7.x, it is usually necessary to first upgrade the server licenses, and only after this upgrade the VMS software.*

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 update.



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



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

NoteS:

- If the network connection is slow or intermittent, the progress dialogue might display no status information for the installation file transfer and update progress.
- 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 was selected to be updated, the System manager will be automatically closed soon 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 in exactly the same way as installing any DVMS version.*
- *After the update, the control panel of windows will show DVMS-x64 for 64-bit DVMS.*

Top Previous Next

1.17.7. Exporting Log Files

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.

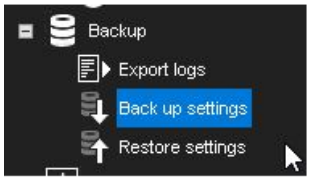
To export log files:

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

Top Previous Next

1.17.8. Backing Up Settings



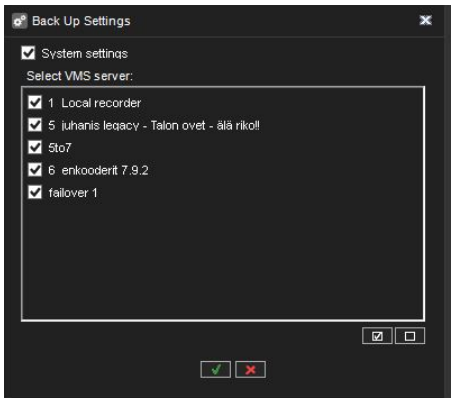
Backup system settings to be able to restore them if the hard disk that contains the settings fails. You can back up system settings and server settings.

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 disc, 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**.
3. Select the storage device and the folder where you want to save the backup file. To create a new folder, click the **New folder** button.
4. Type a name for the file and a description and click **OK**. The description is optional. The system creates the backup file.

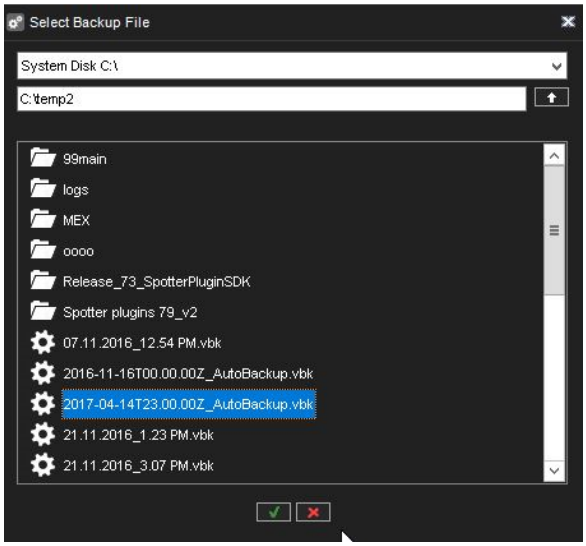
Top Previous Next

1.17.9. Restoring Settings

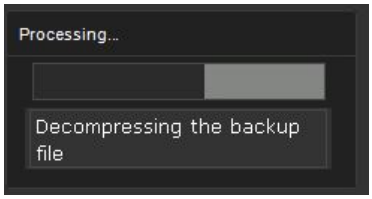
If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs.

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.
3. The dialogue box also shows a description of the settings.

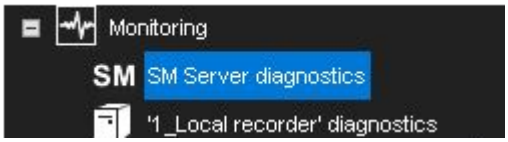


3. Select the system and server-specific settings that you want to restore and click **Start Restore**. The settings are restored.
4. Click **OK** to accept the new settings or **Start the restore process again** to return to the **Restore settings** dialogue.

The option **Do automatic settings backup after successful settings restore** is recommended especially when restoring the system after failover has happened.

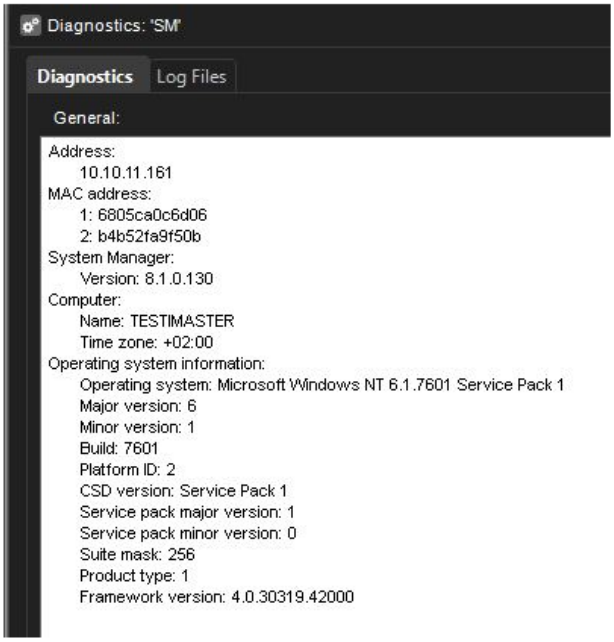
Top Previous Next

1.17.10. System Management 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:

1. SM Server version
2. Computer name and time zone
3. Operating system information
4. Major version
5. Minor version
6. Build
7. Platform ID
8. CSD version
9. Service pack major version
10. Service pack minor version
11. Suite mask
12. Product type
13. Framework version

Log Files

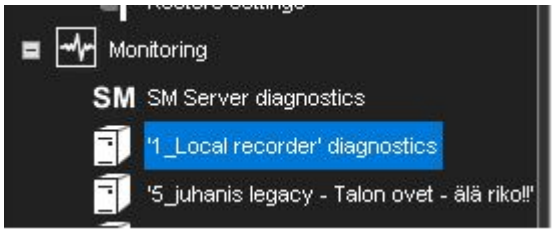
If there are problems with the system, you can access the system log files on the **Log Files** tab.

To examine a log file:

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

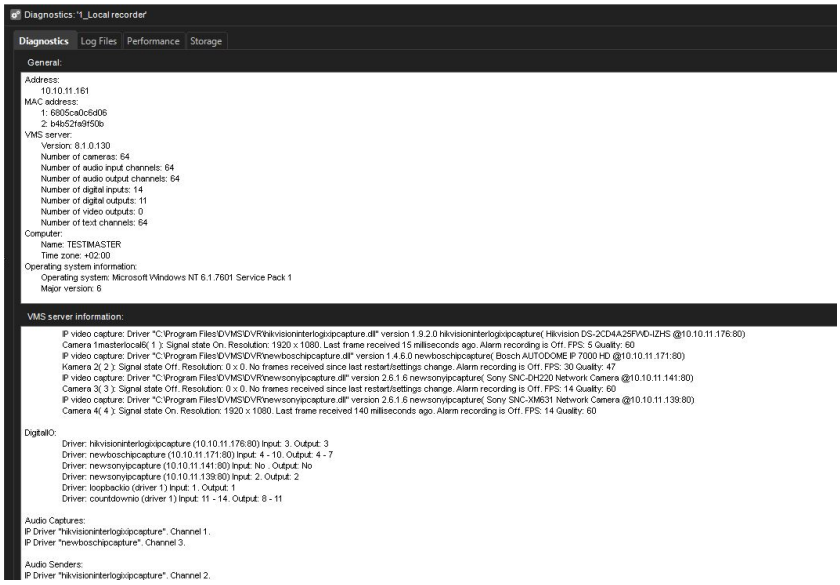
Top Previous Next

1.17.11. Server Diagnostics



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

Diagnostics



The **Diagnostics** tab shows this information:

1. Information about the server:
2. Software version
3. Model
4. Number of cameras, audio channels, digital inputs, digital outputs, and video outputs
5. The name of the computer and the time zone
6. Operating system information
7. Processor information
8. 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:

9. 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:

10. CPU usage.
11. Usage of physical memory.
12. Usage of virtual memory.
13. Network traffic.
14. 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.

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 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.

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.

Top Previous Next

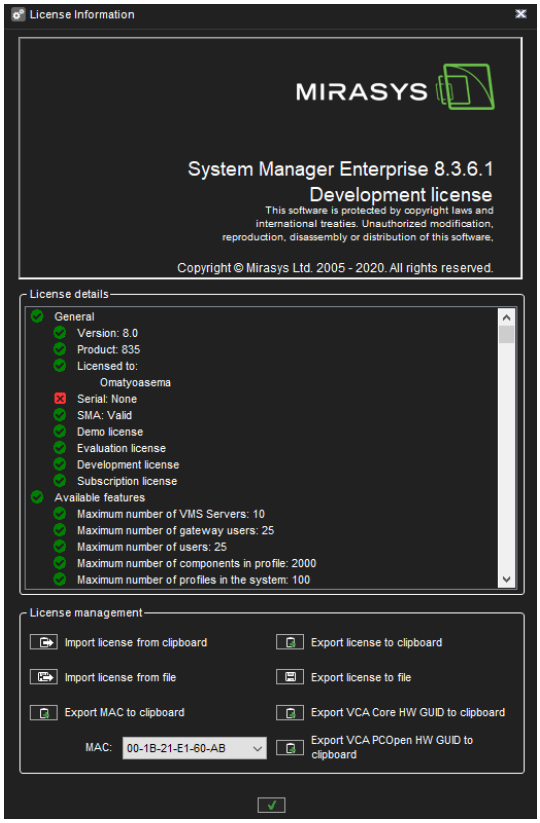
1.17.12. Licenses

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.



To import a license key:

1. On the **System** tab, under **Licenses**, double-click the server that you want to update.
2. In the License Information dialogue box, copy the MAC address and either:
    - Purchase a license key from the Mirasys Extranet
    - Or send the MAC address to your supplier, (or, in specific cases *orders@mirasys.com*)

In return, you will receive the license key as a text file.

3. After getting your license file:

In the License Information dialogue box, click **Import license from the file**.

4. Click **OK**. The system is updated immediately.

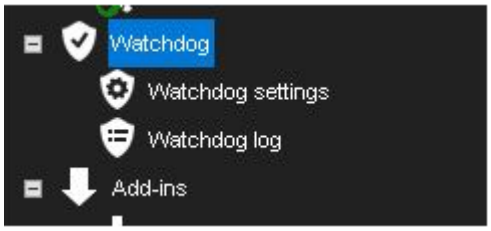
To export a license key:

1. On the **System** tab, under **Licenses**, double-click the name of a server to open its license window.
2. 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.
3. If exporting the license to a file, set the destination folder and the name of the file.
4. Click **OK**.

There is now also a button to copy VCA HW GUID to the clipboard. This allows users to fetch the VCA license without starting the VCA Configurator.

Top Previous Next

1.17.13. Watchdog



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

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

Watchdog Settings

In watchdog settings, you can select what events trigger a report to be sent to e-mail addresses specified in **System 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 restart if a critical hardware error occurs** to automatically restart the computer when serious hardware errors occur. The computer will not be restarted more than once a day.

Digital output notifications

In addition to e-mail notifications, notifications can be performed through digital outputs. Notifications through digital output are created as server-specific; you have 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**.

Watchdog Logs

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 own driver:

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

- WDEventProviderSMS.xml
- WDEventProviderSMTP.xml
- WDEventProviderTCP.xml

At the moment, these files need to be edited manually. Each XML file contains the documentation regarding the configuration options.

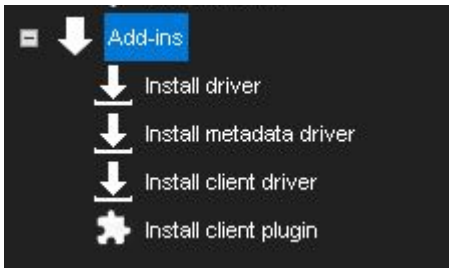
The new configuration options include filtered and conditional warnings (i.e. “send warning X only once in every 60 minutes” or “send warning X only if condition Y is not met in two minutes”), and customizable warning message format.

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 small error can cause fatal errors. Mirasys takes no responsibility for XML errors caused by editing the files.*

Top Previous Next

1.18. Installing New Drivers and Plugins



Top Previous Next

1.18.1. Installing External Driver Packages

To be able 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 by default all IP camera drivers that have been included in the previous versions of the software, as well as the drivers that have been released as plugins before the newest software release, as well as default I/O and text data drivers.

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

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** dialog box is shown.

3. Select the servers on which you want to install the driver.
4. If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**
5. Click **Install**. The **Status** column shows the text **Installed** if the driver is successfully installed. If the driver is not installed, the column shows an error message.
6. Click **Close** to exit the dialogue box.

NoteS*:*

- In case you need to update drivers for hardware other than IP cameras, please contact the supplier of the system.
- *A 32-bit system requires a 32-bit driver package, and a 64-bit system required a 64-bit driver package.*

Top Previous Next

1.18.2. Installing Metadata Drivers

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

Top Previous Next

1.18.3. Installing Client Drivers

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

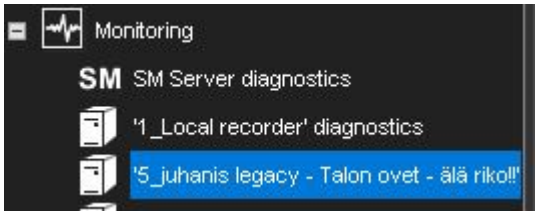
These are called (Managed) TruCast Client drivers.

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

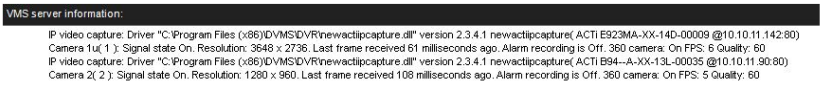
Top Previous Next

1.18.4. Removing Drivers

1. Identify driver you wish to remove/disable
2. Remove the cameras using the driver in question using System Manager
    a. Drivers installed on a server can be found through the System Manager's *Local VMS Server* diagnostics

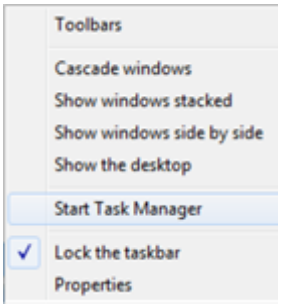


    i. All cameras using the same driver are grouped together in the Diagnostics screen
    ii. Device paths for the driver .DLL files are written in the diagnostic

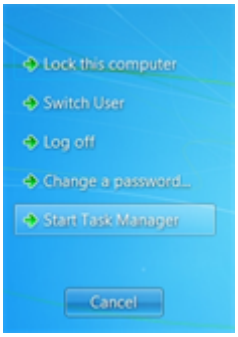


    b. The instructions for camera removal can be found in the chapter *Cameras*, subchapter *Adding and Removing IP Cameras*, page 32

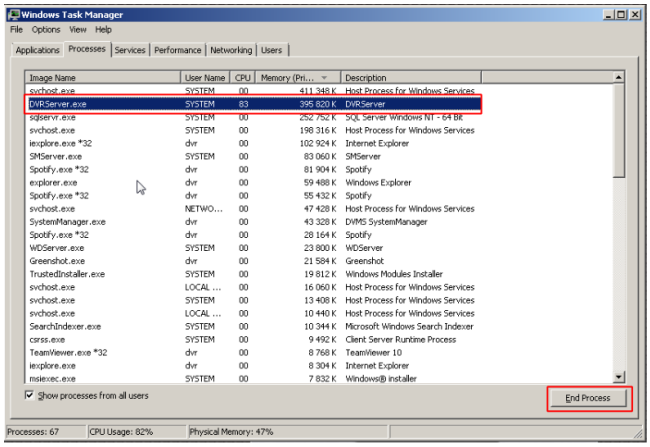
- Shut down the recording service (DVRServer process)
    a. Open the Task manager
        a. Open by right-clicking the taskbar and select Start Task Manager



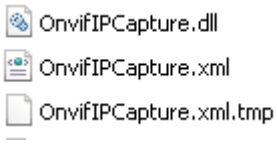
        b. Or open by using the **CTRL-ALT-DEL** key combination and select Start Task Manager



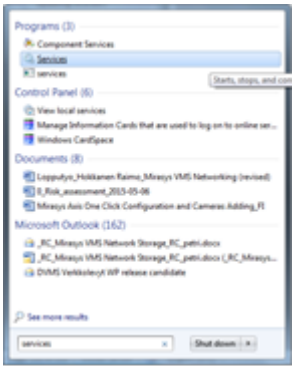
b. In Task Manager, select the *Processes* tab and select DVRServer.exe, then Right-click on the process and select End Process or click the *End Process* button.



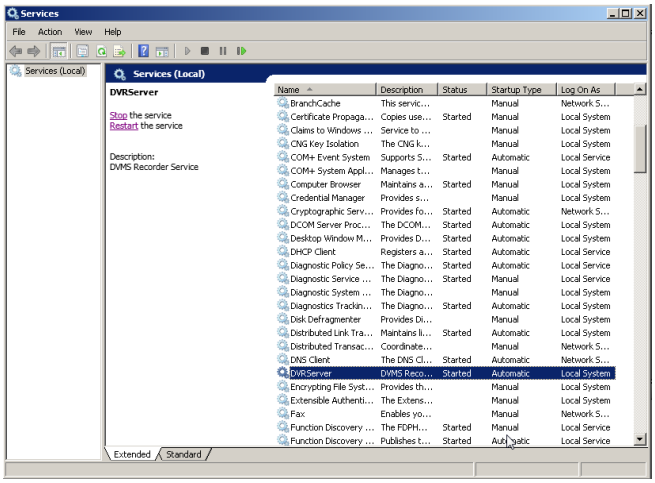
4. Delete the files 'X' from installation folder/directory 'Y'
   a. The folder path for the driver files are found in the diagnostics, usually in ~\Program Files\DVMS\DVR\ of the server's main hard drive
   b. Drivers create three files, the driver .dll, a .xml file and a temporary file for the .xml



5. Restart the recording service
   i. Open the Services program
      1. Open the Start Menu and type in "services" in the search bar



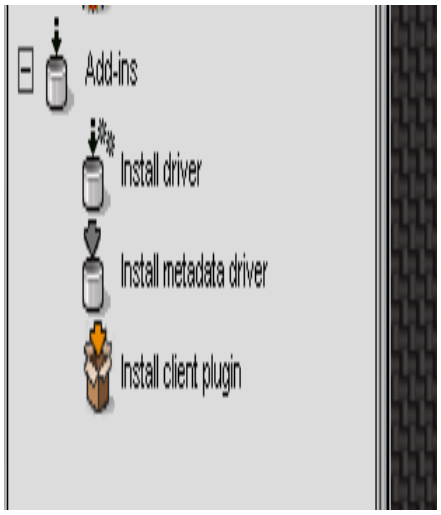
   c. Browse to the DVRServer service



c. Right-click the DVRServer service and select “Start”

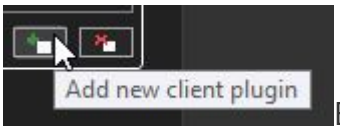
Top Previous Next

1.18.5. Installing Spotter Plugins



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. On the **System** tab, under **Add-ins**, open the **Install client plugin**.
2. In the plugin installation window, you can view all the installed plugins, add new plugins, and remove old plugins.
3. Find and select the plugin package (.zip file) and click **OK**. The **Install Plugin** dialogue box is shown.
4. Click **Add new plugin**. 

Browse for the correct file and select it.
5. 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.**
6. Configure the plugin through the Spotter user interface.

To remove a client plugin:

1. On the **System** tab, under Add-ins, open the **Install client plugin**.
2. In the plugin installation window, select **Remove client plugin**.

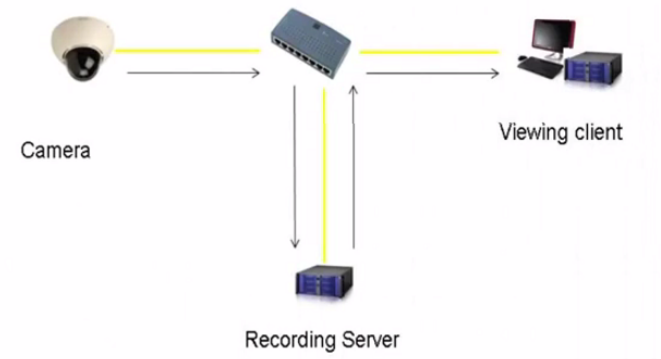
Top Previous Next

1.19. TruCast

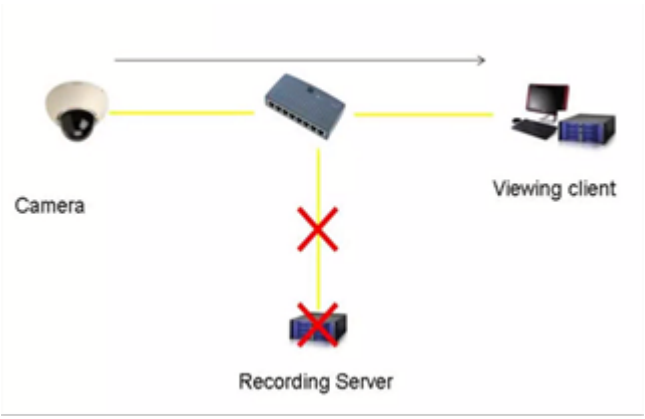
TruCast is the direct camera video streaming feature in Mirasys VMS.

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

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



If the connection to the VMS Server is lost, with TruCast the stream can come directly from the camera to the client.



It is possible to get the direct stream from the camera to the client also when the VMS Server connection is OK. This can be useful if users want to optimize network utilization.

Top Previous Next

1.19.1. 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 and
- ONVIF

Use the ONVIF TruCast driver for cameras that are not on the supported list.

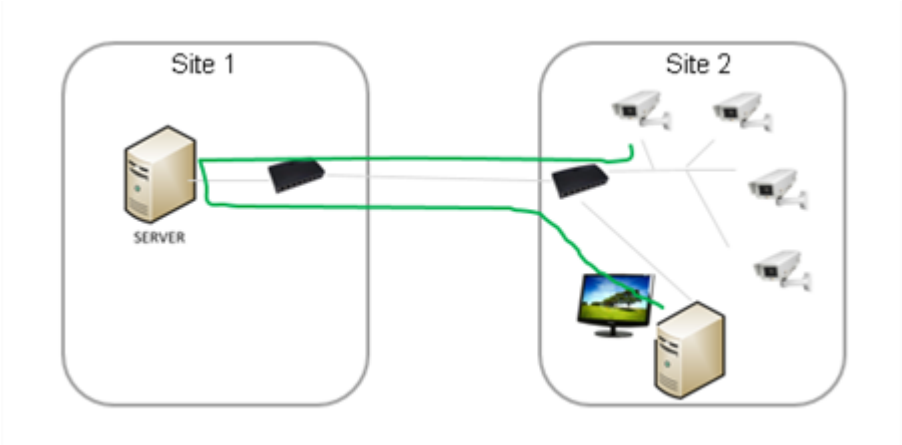
The use of the ONVIF driver requires that the camera is added to the VMS system with the ONVIF driver, not the camera's native driver.

Top Previous Next

1.19.2. Network Optimization

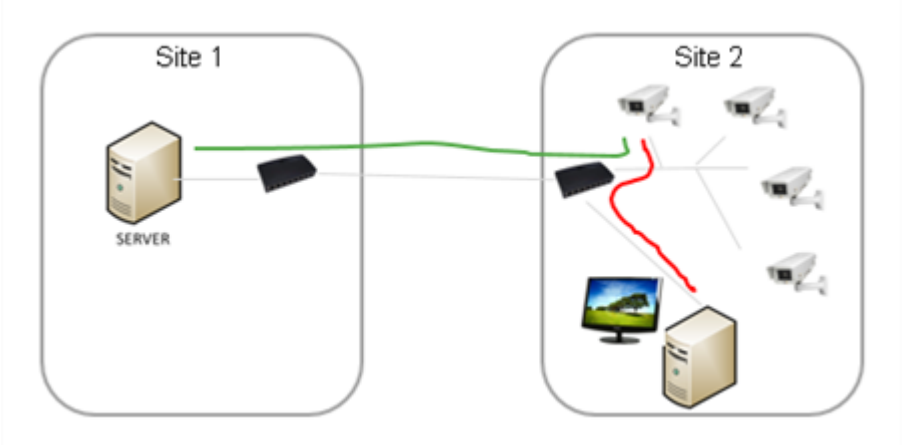
TruCast can be used to reduce network load in specific scenarios. Mainly the load reduction takes place when the server is located off-site (remote), and the viewing client is on-site (local to the cameras).

In 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.



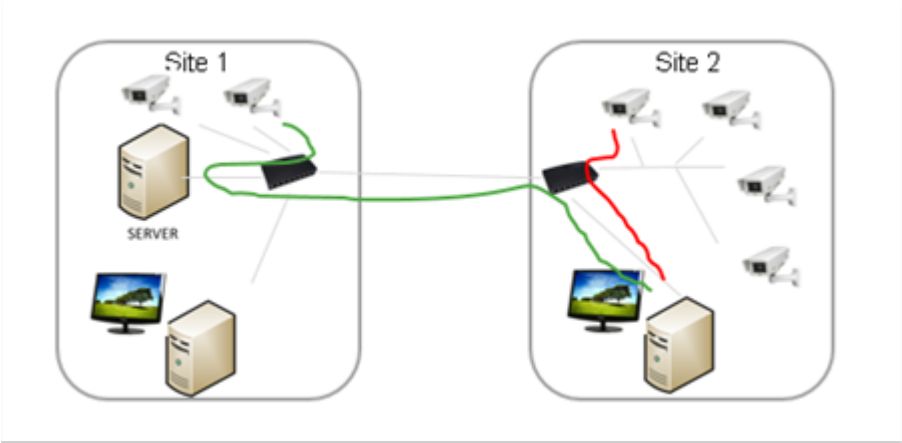
In this solution, the traffic between the two sites is increased.

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

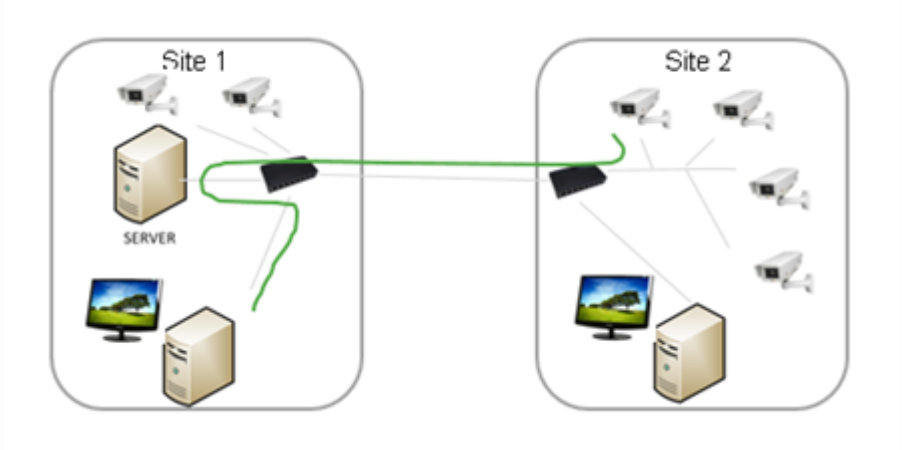


In example scenario 2, there are cameras on two sites and viewing clients on two sites.

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.



Users have complete control over which cameras are using TruCast and which cameras are viewed normally. The setting is memorized for each camera and for each user, and is also saved to Spotter layouts.

Top Previous Next

1.19.3. Impact of 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 taken into consideration 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 8 fps).

This reduces the storage and network requirements considerably.

Top Previous Next

1.19.4. Other Information

Impact of TruCast to 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 very difficult 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 that are being used.

These TruCast driver licenses, and the TruCast feature, are always enabled in the Mirasys V8 Entegra product version.

Multiple Viewers

Since each TruCast-viewer is opening 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 normally work ok.

Top Previous Next

1.19.5. Configuration

Installing Client Drivers

Before starting to use 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 full 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.

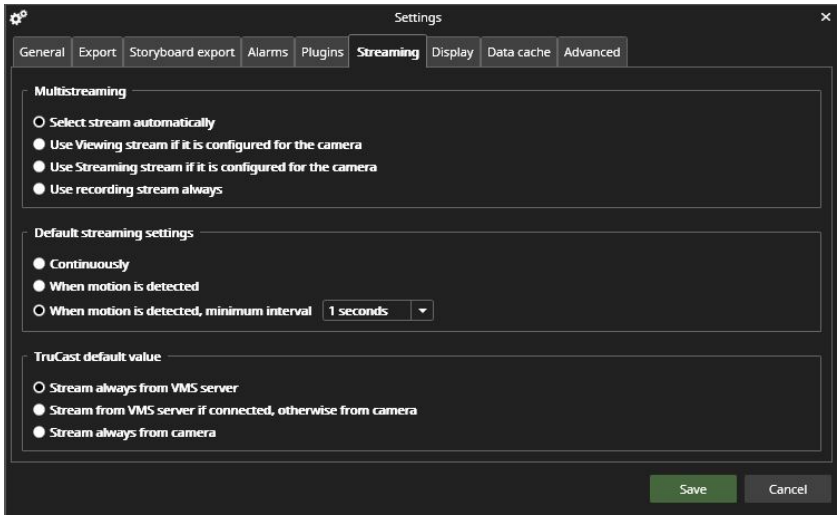
Please note that only those cameras which' client driver was installed will appear as TruCast enabled.

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 normally 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 normal and TruCast viewing.



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

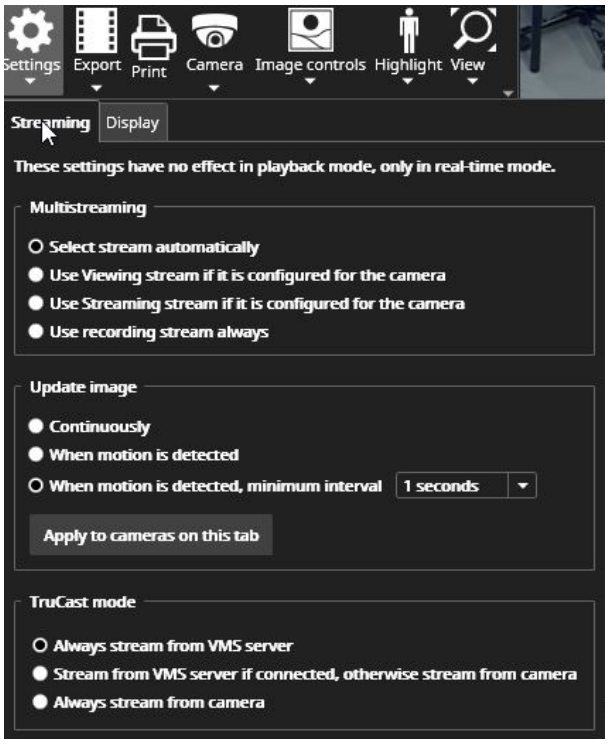
- Always stream from the VMS Server
- Stream from the VMS Server normally, but switch to TruCast if the connection to the server is lost
- Always stream using TruCast

Top Previous Next

1.19.6. 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 dialog is disabled.

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.

Copyrights

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V8

The contents of this document are provided “as is”, and Mirasys Ltd reserves the right to modify this document as necessary and without prior notice. Any products, services, or features discussed in this document are subject to change by Mirasys Ltd. or a third party when applicable. Mirasys Ltd does not guarantee the availability of all products, services, or features.

© Mirasys Ltd. All rights reserved.

No part of this document may be reproduced for any purpose, even in part, without an explicit permission from Mirasys Ltd.

Top Previous

Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com