ernitec

EasyView System

Administrator Guide

Version 8

CONTENTS

BEFORE YOU START

HELP DOCUMENTATION

This help documentation, for example, is available:

- *Installation Guide*: Shows how to install the EASYVIEW servers and the client programs. It also shows how to add devices to the system.
- *System Administrator's Guide*: Shows how to use the System Manager program for configuring the system.
- *Viewing Client User Guide*: Complete instruction how to operate all features of Windows Viewing Client program. (Not available in all languages.)

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

OVERVIEW OF THIS GUIDE

This guide is intended for those who set up a EASYVIEW 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.

TECHNICAL SUPPORT

For technical support and warranty issues, please contact:

support@ernitec.com

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 EASYVIEW servers (nodes or slaves) when VCA (Video Content Analytics) is to be utilized.

New features in version 8:

- New 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.
- Viewing Client can be used to simultaneously connect to multiple different Master Servers (license controlled add-on feature). Server selection has been moved from the Viewing Client login window to the application launcher dialog. It is also possible to directly create desktop shortcuts that connect to a certain Master Server.
- Viewing Client 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 custom color.
- The Workstation client application is no longer available!
- The user can specify to show certain or all alarms on the Viewing Client time slider.
- Support for multiple alarm popup monitors.
- Ability to open camera to search and analysis plugins from 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 Viewing Client configuration file.
- TruStream support: for multi-streaming cameras. Viewing Client 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 Viewing Client.
- The numeric keypad device number popup dialog can be positioned freely anywhere on the Viewing Client window.
- The AVM operator console can be positioned in a fixed camera grid cell.

About the System

What is EASYVIEW Software?

EASYVIEW software is a distributed, digital video management system (EASYVIEW or DEASYVIEW) 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 analog and/or digital surveillance cameras, supporting the creation of analog, digital or hybrid (consisting of both analog and digital) surveillance systems.

A centralized surveillance system domain can consist of up to 150 local or remote EASYVIEW Servers.

What Does a System Contain?

The EASYVIEW system consists of these components:

- **1-150 EASYVIEW Servers**
    - **Master Server** (dedicated server – recommended -, one of the video recording EASYVIEW Servers, or the only server in a single-server, non-networked environment)
    - **EASYVIEW Server** ("nodes," if the system consists of multiple servers)
- Client programs:
    - EASYVIEW System Manager
    - EASYVIEW Viewing Client for Windows
    - EASYVIEW Viewing Client Mobile
    - EASYVIEW WebClient

EASYVIEW Servers

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

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

In addition, you can connect these devices to a EASYVIEW 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 EASYVIEW 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 **Viewing Client** 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 EASYVIEW V7.5.10, or earlier.

NETWORK REQUIREMENTS

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

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

OS Compatibility

EASYVIEW V8 supports the following operating systems:

Operating System	Server with analog camera support via capture cards	Server with only IP cameras or connected video servers (encoders)	Gateway server	System Manager client application	Viewing Client for Windows client application
Windows 7 Pro / Enterprise	32-bit EASYVIEW V7 or earlier only	X	X	X	X
Windows 8 Pro & Pro Retail	32-bit EASYVIEW V7 or earlier only	X	X	X	X
Windows 2008 Server R2 Enterprise	32-bit EASYVIEW V7 or earlier only	X	X	X	-
Windows 2008 Server R2 Foundation	-	X	X	X	-
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:

- *EASYVIEW has not supported Windows XP since EASYVIEW version 6.4. If Windows XP support is required, do not install EASYVIEW 6.4, or any later releases.*
- *Make sure that the "Desktop Experience" feature is activated for Windows server operating systems.*
- *No releases before EASYVIEW 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.*

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 "Viewing Client only" installer is provided.*

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

LOGGING IN

This section describes how to login and logoff from System Manager. Only system administrators or users with monitoring rights are allowed to login to System Manager.

Default username and password

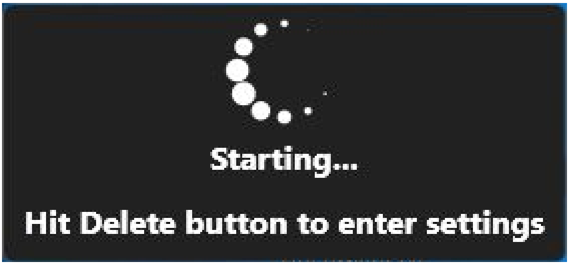
Username: `Admin`

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:

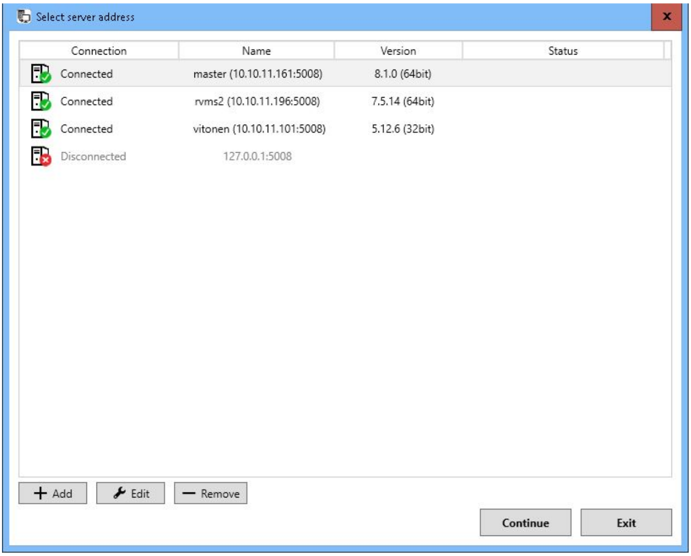
1. Do one of the following:
   - Double-click the shortcut icon **System Manager** on the desktop.
   - Click **Start**, point to **Programs** and then to **DEASYVIEW**. Click **System Manager**.



Starting...

Hit Delete button to enter settings

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 "Delete" key in the initial startup phase, the site selection screen is shown. 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, user is taken to the login screen.



Connection	Name	Version	Status
Connected	master (10.10.11.161:5008)	8.1.0 (64bit)	
Connected	rvms2 (10.10.11.196:5008)	7.5.14 (64bit)	
Connected	vitonen (10.10.11.101:5008)	5.12.6 (32bit)	
Disconnected	127.0.0.1:5008		

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

To quit the program:

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

LOCKING SYSTEM MANAGER

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

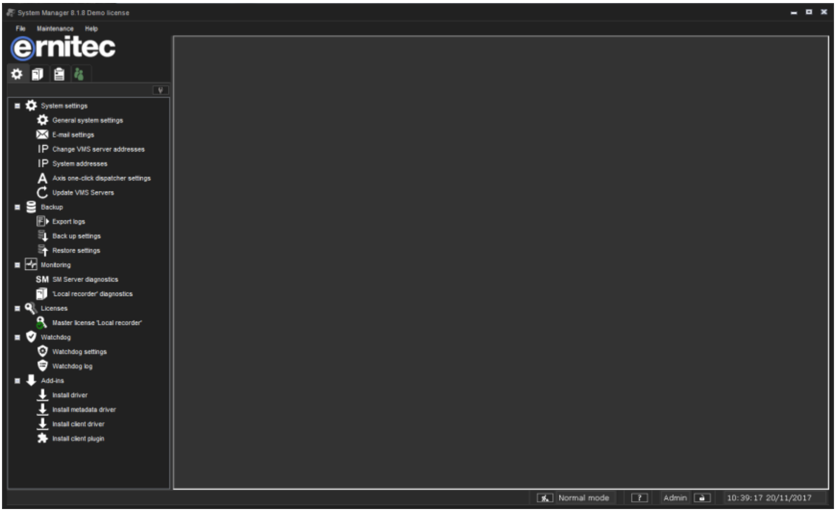
To lock the program, do one of the following:

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

To unlock the program:

- After locking the program, the login screen is shown. Type the user name in the **User name** box, and the password in the **Password** box.
  NOTE: *The password is case sensitive.*

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, EASYVIEW 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 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:

- 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.
- Add servers to the system and configure them on the **EASYVIEW Servers** tab.
- Add and edit user profiles on the **Profiles** tab.
- Add and edit user accounts on the **Users** tab.

EASYVIEW SERVERS

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

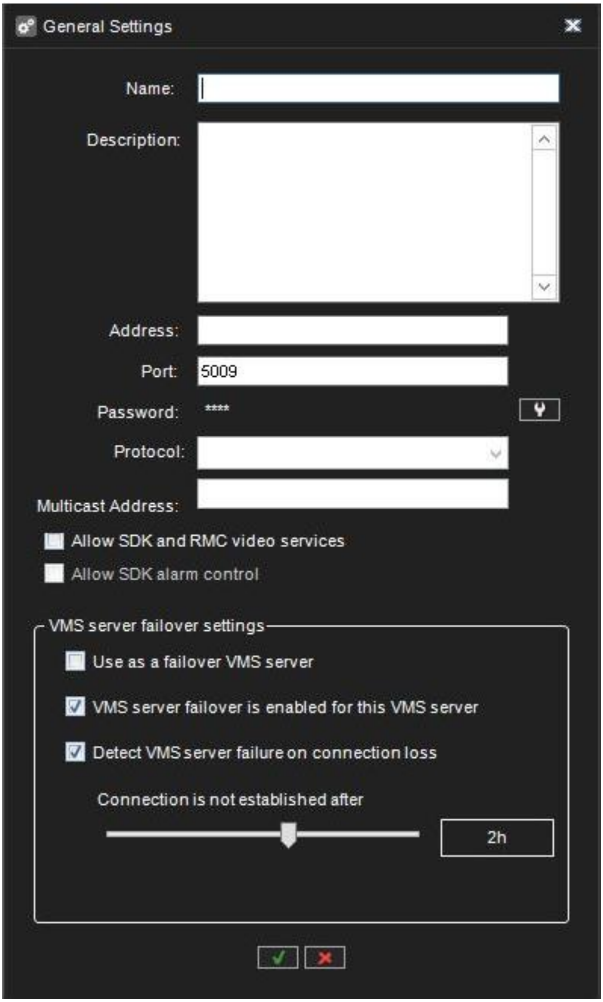
ADDING AND REMOVING EASYVIEW SERVERS

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 **EASYVIEW Servers** tab .
2. Click **Add EASYVIEW Server**
3. The **General Settings** dialog box is shown.



General Settings

Name:

Description:

Address:

Port: 5009

Password: ****

Protocol:

Multicast Address:

☐ Allow SDK and RMC video services

☐ Allow SDK alarm control

VMS server failover settings

☐ Use as a failover VMS server

☑ VMS server failover is enabled for this VMS server

☑ Detect VMS server failure on connection loss

Connection is not established after 2h

4. Do the following:

- Type a descriptive name for the server.
- Type a description of the server. The description is shown only on this tab.
- Type the IP address or DNS name of the server.

- 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.
- If the server is used as part of an integrated system or with the Remote Monitoring Center system, select **Allow SDK and RMC video services.**
- If the server is to receive alarms from an integrated system, select **Allow SDK alarm control.**
- If the server is to be used as failover server, select the box. **"use as a failover EASYVIEW 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 EASYVIEW 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.

CONFIGURING EASYVIEW SERVERS

On the **EASYVIEW 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**	User 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:

- Select the settings that you want to configure (for example, **Cameras**) and then click **Edit** 🔧 in the lower-right corner of the navigation pane.

- Double-click the settings that you want to configure.
- Drag the settings from the **EASYVIEW Servers** tab to the work space.

FAILOVER SERVERS

EASYVIEW supports failover video servers as a EASYVIEW option.

Failover servers are EASYVIEW Servers that are on a passive standby until the system recognizes that one of the active video recording EASYVIEW 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 Viewing Client 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.

Analog 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 failover server. There can be any number of failover servers (0-n).

If the server is 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 EASYVIEW Server, and one standby failover server.

Failover migration will be triggered in the following conditions:

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

- A EASYVIEW Server has informed the Master Server that connection to all the material disks (recording storage) on the server have 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

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.

FAILOVER LICENSING

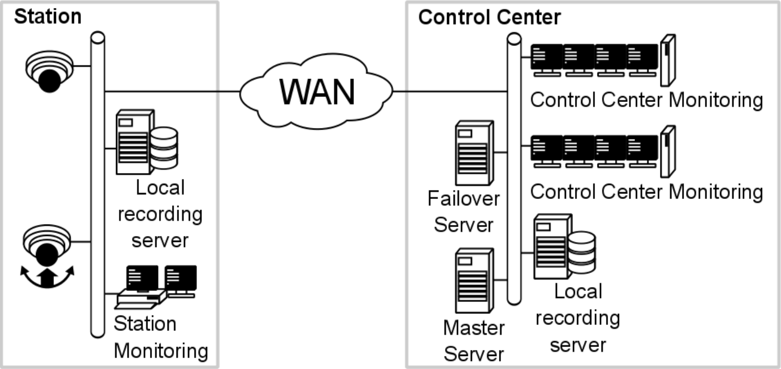
The Failover functionality uses automatic backups generated by the *SMServer* service when doing failover, and therefore the system must have automatic backup option enabled; either as an Automatic Flash backup in provided systems or a non-Flash based backup in hardware provided by another hardware distributor.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

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 Viewing Client for Windows client.

The control center houses the system network's failover and Master Server. The failover server can take over when a station's local EASYVIEW Server becomes unusable. The Master Server serves as the central control entity of the system. Control center monitoring is usually with AVM (Agile Virtual Matrix) multiple screen setups (desktop or video wall) with their own Display Servers.

The EASYVIEW 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.

EASYVIEW 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:

- EASYVIEW 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, System Manager sets the server to standby mode.

The device tree in the **EASYVIEW Servers** tab in System Manager shows failover and broken servers in their own groups (under *Failover EASYVIEW Servers* and *Broken EASYVIEW Servers*). The *Failover EASYVIEW Servers* group shows server connection states and server general settings if connection is available. The *Broken EASYVIEW 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.

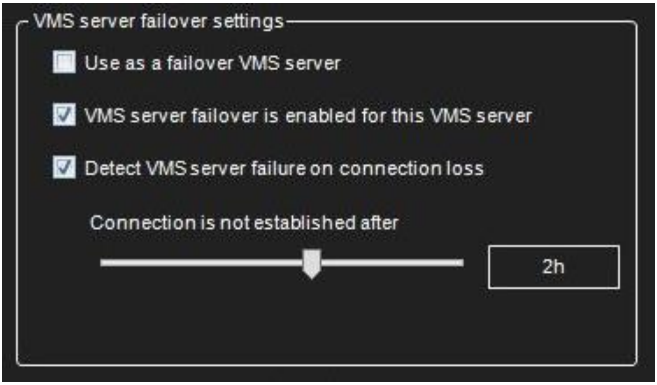
FAILOVER SERVERS IN SYSTEM MANAGER

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 same file system (same drive letters) as the EASYVIEW 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 *EASYVIEW Server* list. When any EASYVIEW Server is deemed to be broken or inaccessible, they are moved under the *"Broken EASYVIEW 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.



VMS server failover settings

□ Use as a failover VMS server

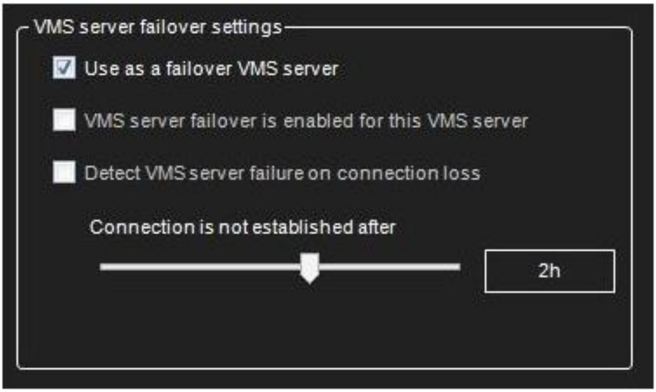
☑ VMS server failover is enabled for this VMS server

☑ Detect VMS server failure on connection loss

Connection is not established after

2h

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



VMS server failover settings

☑ Use as a failover VMS server

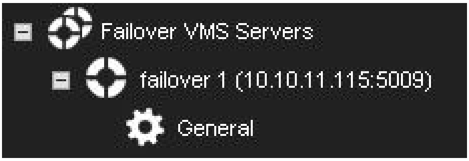
□ VMS server failover is enabled for this VMS server

□ Detect VMS server failure on connection loss

Connection is not established after

2h

Adding a failover server



Failover VMS Servers

failover 1 (10.10.11.115:5009)

General

Failover servers in the EASYVIEW Server *list*

Adding and Removing Failover Servers

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

Restoring System To Normal State After Failover

To restore 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 system was in operation with the normal status.
3. Restore the system with this file. Be sure to select option “**Do automatic settings backup after successful settings restore”**

PORT FORWARDING

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

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

INSTALLER OPTION

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

SYSTEM MANAGER

If the port forwarding is not activated when the system was installed, it can be activated from system manager second tab “EASYVIEW Servers”. Open the view “Port forwarding” and activate the selection “UPnP is in use”

AUTOMATIC ROUTER CONFIGURATION

When a EASYVIEW 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 on 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) address are detected.

If 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 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 connection to the server has not returned after a while, then it might be necessary to reboot the router.

Servers need 4 ports for server to server communication. The first server that does port forwarding will claim ports 5008, 5009, 5010 and 5011. The second server will claim ports 5012-5015, the third server ports 5016-5019. And so on. (Assuming all the ports are available).

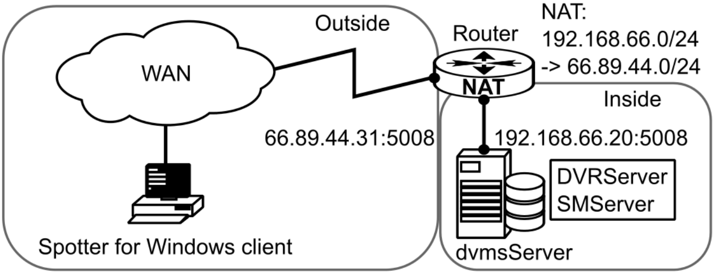
The first port is used for SMServer communication (5008, 5012, 5016…)

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

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

Single Server Behind Router

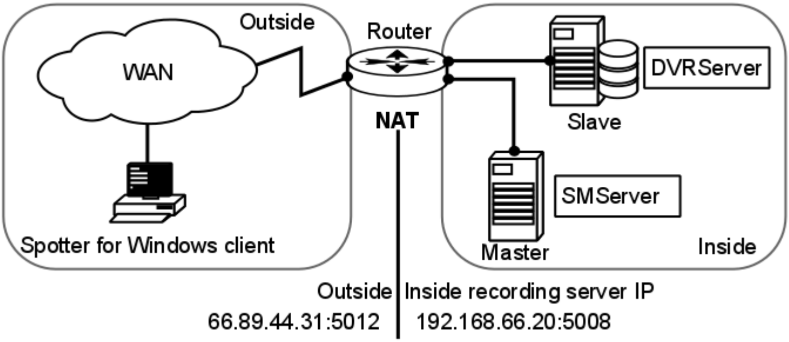
Scenario 1: Using a system with single server behind a router / firewall



If the user is accessing a single server from the WAN, he needs to connect to the EASYVIEW 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.

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 EASYVIEW Server, if the server has done automatic port forwarding, there will be a note shown to 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.

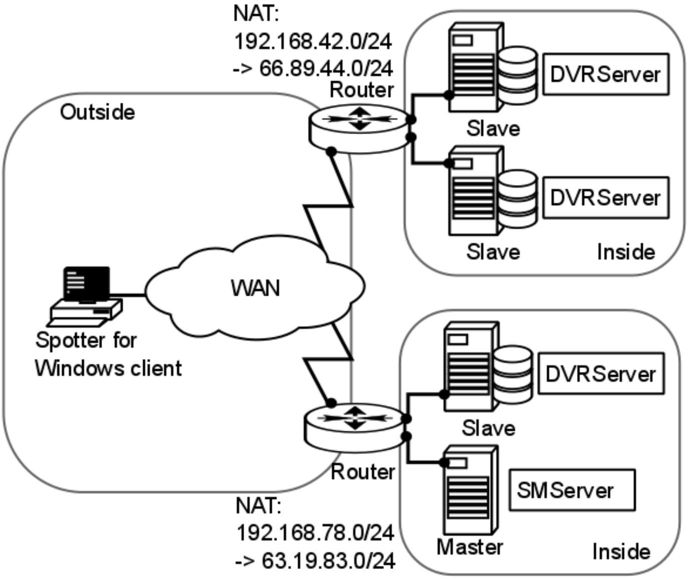
The exact ports that the server has done port forwarding to, can be found by starting the System Manager on the local server (locally on the EASYVIEW Server, start System Manager to 127.0.0.1 and log in) and check the port forwarding settings.

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 same site, they most likely get the ports starting with 5009, 5013, 5017, 5021…

More Than One Server On Multiple Sites

Scenario 3: More than one server on more than one site



Same principle applies as in Scenario 2, but this time NAT needs to be taken into account when assigning EASYVIEW Servers to the Master Server from the other site.

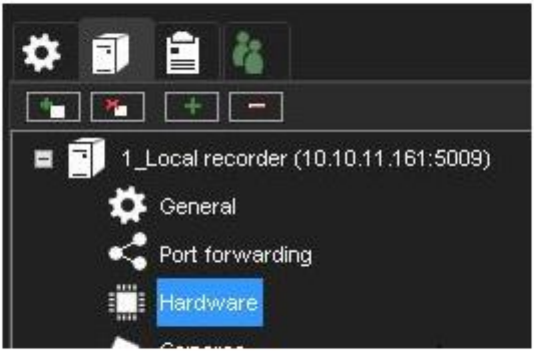
CAMERAS

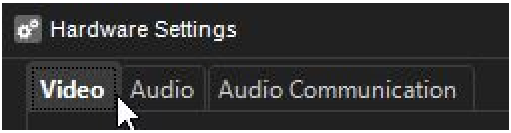
Before using the system manager application to search for the camera, first configure the camera to use an IP address or DNS name, user name and password for the cameras in the camera's internal settings, typically using a camera manufacturer's web browser interface. See the camera manual for details.

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

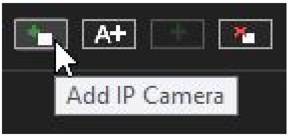
ADDING AND REMOVING IP CAMERAS

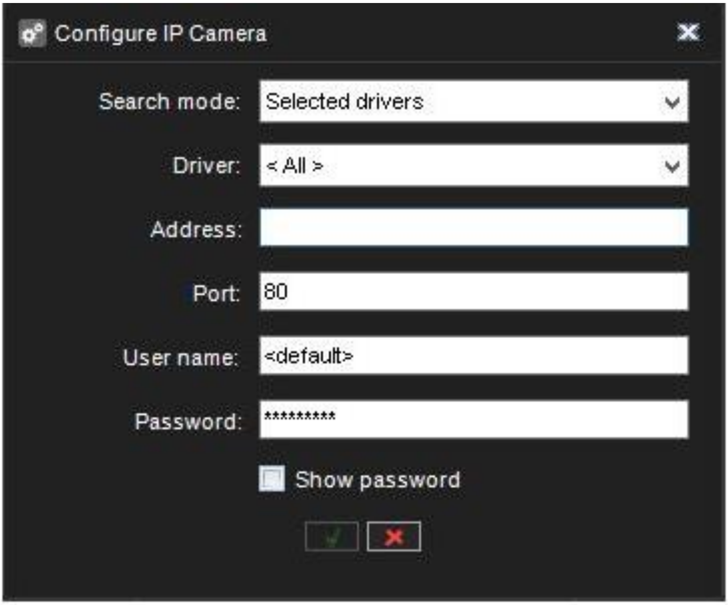
IP cameras or analog video servers (encoders) can be managed through the **Video** tab of **Hardware settings**.





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

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



Configure IP Camera

Search mode: Selected drivers

Driver: < All >

Address:

Port: 80

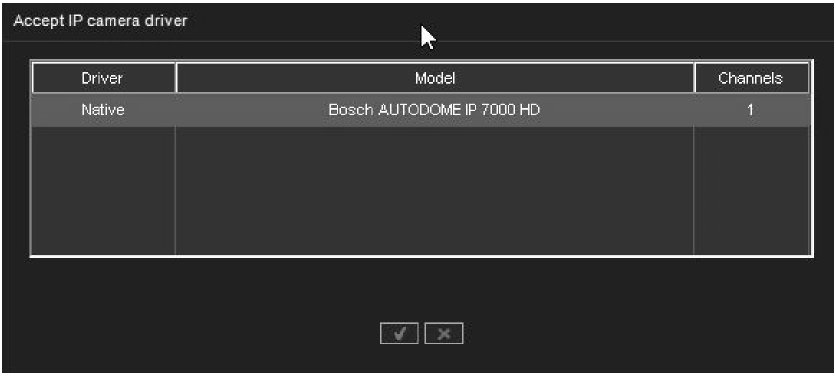
User name: <default>

Password: *********

□ Show password

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**.

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.

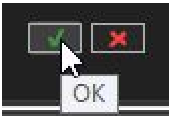


Accept IP camera driver

Driver	Model	Channels
Native	Bosch AUTODOME IP 7000 HD	1

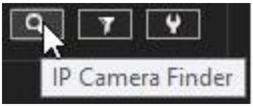
For multichannel devices, the **Channels** option can be used to add the device with less than the maximum number of channels.

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 dialog with the OK button in the low part of the screen.

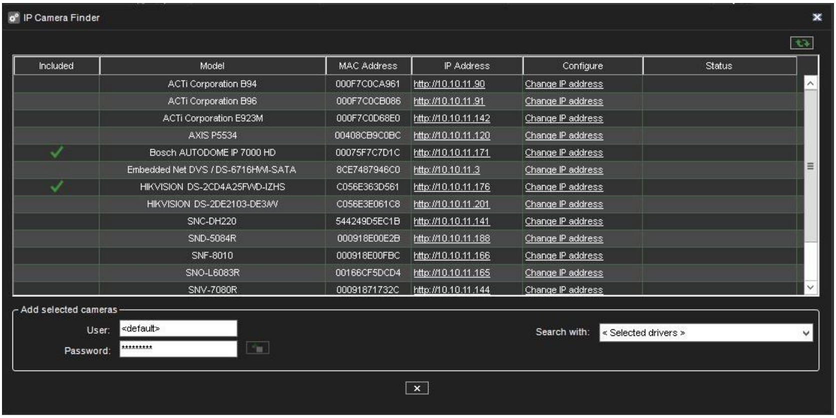


To add one or more IP cameras with the Camera finder tool:

1. Click the **IP camera finder**



The system will now scan 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.



IP Camera Finder

Included	Model	MAC Address	IP Address	Configure	Status
	ACTi Corporation B94	000F7C0CA961	http://10.10.11.90	Change IP address	
	ACTi Corporation B96	000F7C0CB086	http://10.10.11.91	Change IP address	
	ACTi Corporation E923M	000F7C0D68E0	http://10.10.11.142	Change IP address	
	AXIS P5534	00408CB9C0BC	http://10.10.11.120	Change IP address	
✓	Bosch AUTODOME IP 7000 HD	00075F7C7D1C	http://10.10.11.171	Change IP address	
	Embedded Net DVS / DS-6716HW-SATA	8CE7487946C0	http://10.10.11.3	Change IP address	
✓	HIKVISION DS-2CD4A25FWD-IZHS	C056E363D561	http://10.10.11.176	Change IP address	
	HIKVISION DS-2DE2103-DE3/W	C056E3E061C8	http://10.10.11.201	Change IP address	
	SNC-DH220	544249D5EC1B	http://10.10.11.141	Change IP address	
	SND-5084R	000918E00E2B	http://10.10.11.188	Change IP address	
	SNF-8010	000918E00FBC	http://10.10.11.166	Change IP address	
	SNO-L6083R	00166CF5DCD4	http://10.10.11.165	Change IP address	
	SNV-7080R	00091871732C	http://10.10.11.144	Change IP address	

Add selected cameras

User: <default>

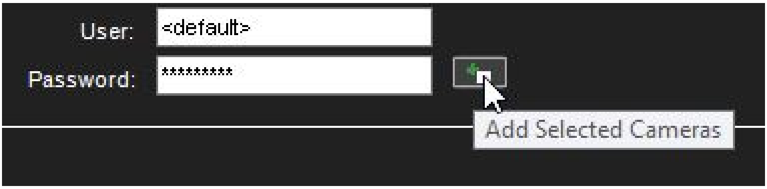
Password: *********

Search with: < Selected drivers >

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**



User: <default>

Password: *********

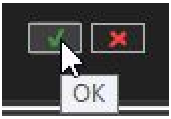
.

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:

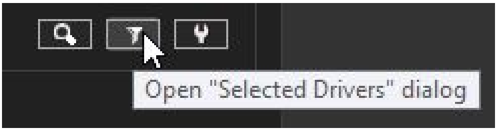
1. On the **Video** tab, click on an IP camera's name in the camera list.

2. Click **Remove Selected IP Camera** in the lower right corner of the tab.
3. When asked to confirm the deletion, click **OK**.

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 single manufacturer or a few different manufacturers. This option speeds up the camera search and also other operations.

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



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

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 dialog during 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 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 fail, the system will prompt whether the user wishes to search using all drivers. The driver currently used for 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 list of available models.

The ***Selected drivers*** -mode will be selected by default for adding of the new camera for the first time. Next time when the dialog is opened, the system will remember the previous mode and driver selection to allow user to add similar cameras faster.

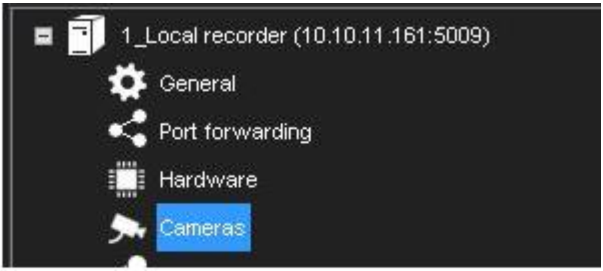
Opening of existing camera using *Modify* button will show dialog with ***Currently active drivers*** search mode and driver name in mode option combo-box (except cameras added by model of course). The system will not store last used options for modify cases because the options will be available for adding cameras only

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.

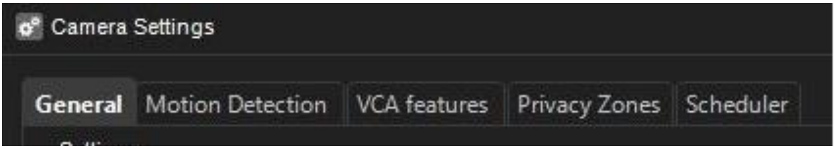
Editing Camera Settings

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

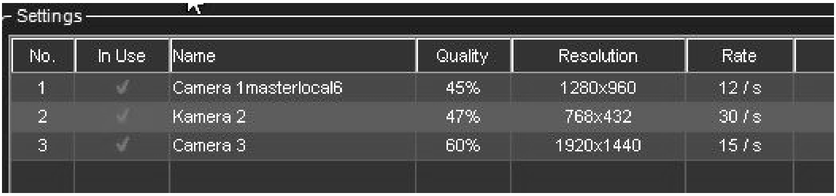


The cameras page consists of 5 tabs.

- 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.


Settings

No.	In Use	Name	Quality	Resolution	Rate	
1	✓	Camera 1masterlocal6	45%	1280x960	12 / s	
2	✓	Kamera 2	47%	768x432	30 / s	
3	✓	Camera 3	60%	1920x1440	15 / s	

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 different camera.

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 Viewing Client 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 Viewing Client client that the camera is a 360 camera, and Viewing Client 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 camera) then the other setting 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 case of analog cameras, the codec used by the system is JPEG. In 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 Viewing Client program.
- **Administrative Description**. Here you can type a description of the camera. The description will be shown in the Viewing Client program to only system administrators.
- **Reference image.** A reference images is an image captured from the camera, which makes it easier to identify the cameras. In addition, in the Viewing Client program, the users can compare what they see in the video view against the reference image to make sure that the camera is pointed at 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 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.

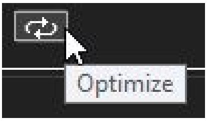
Selecting multiple cameras is possible with SHIFT or CTRL keys. Please note that if you select more than one cameras, you cannot set parameters that are not supported by all selected cameras.

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 add all desired cameras with desired settings. However, care should be taken to not overload the server in such 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.



MOTION DETECTION

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

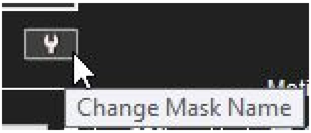
In addition to the default mask, you can have four customizable masks for each camera. On the **Scheduler** tab of the camera settings and on the **Scheduler** tab of alarm settings, you can select a different mask to be used during each hour of the week.

A mask contains these parameters:

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

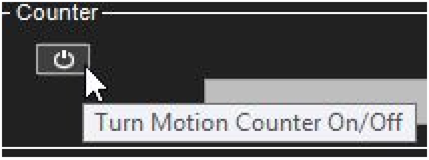
To edit a mask:

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.



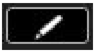
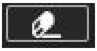
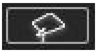
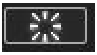
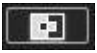
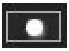
4. With the drawing tools presented in the following table, paint the areas red where you want the system to detect movement and remove the red from areas where you want to ignore movement.
5. Set the detection sensitivity.
6. Set the minimum quantity of movement.
7. Select the motion detection method: 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 counter mode off and make 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 color is removed.
	**Fill/Clear**	If the pen tool is selected, clicking this button selects all of the 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:

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

If there is a lot of background noise in the image, for example, changes in lighting conditions, decrease 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, the motion detection uses the 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.

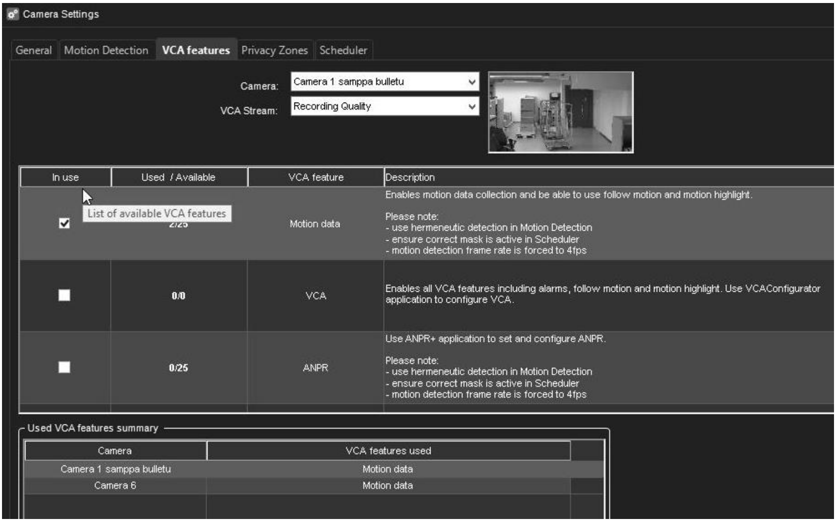
Adaptive detection compares each image to a background image. The system learns the background image and the movement that belongs there automatically. Thus, the system does not interpret, for example, moving leaves, as motion. In addition, if more than half of the pixels in an image change, the system 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.

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 following mage)



Camera Settings

Camera: Camera 1 samppa bulletu

VCA Stream: Recording Quality

In use	Used / Available	VCA feature	Description
☑	2/25	Motion data	Enables motion data collection and be able to use follow motion and motion highlight. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps
□	0/0	VCA	Enables all VCA features including alarms, follow motion and motion highlight. Use VCAConfigurator application to configure VCA.
□	0/25	ANPR	Use ANPR+ application to set and configure ANPR. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps

Used VCA features summary

Camera	VCA features used
Camera 1 samppa bulletu	Motion data
Camera 6	Motion data

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 **Viewing Client**.
- **VCA:** Enables full external VCA functionality. Configured through the external VCA Configurator application. Visualized in **Viewing Client**.
- **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.

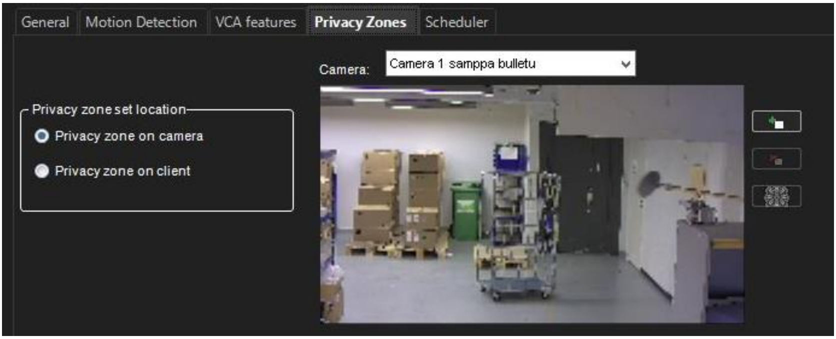
PRIVACY ZONES

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 Viewing Client 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

Privacy zone settings can be accessed in the **Privacy Zones** tab.

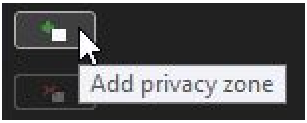


Camera: Camera 1 samppa bulletu

Privacy zone set location
● Privacy zone on camera
○ Privacy zone on client

The Privacy Zones tab

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 gray. 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.*

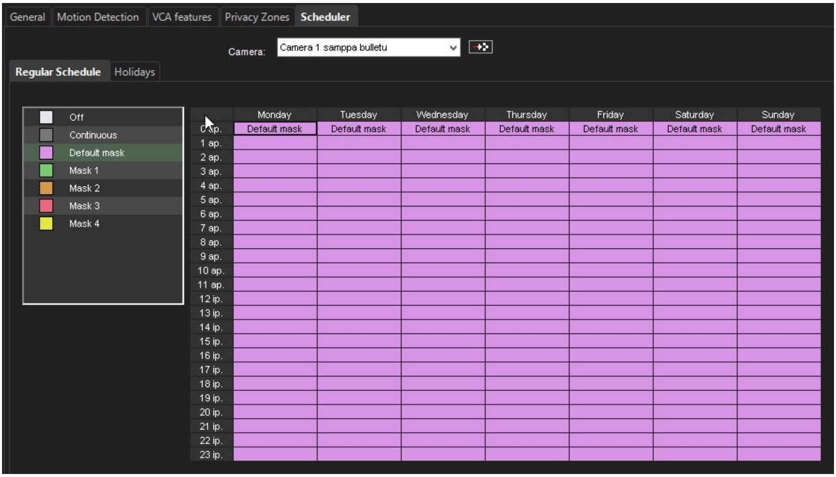
NOTE: *If the master or server license does not support client privacy screens, the privacy zone controls for client are disabled.*

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**.

SCHEDULER (VIDEO)

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



Camera: Camera 1 samppa bulletu

⬜ Off
⬛ Continuous
🟪 Default mask
🟩 Mask 1
🟧 Mask 2
🟥 Mask 3
🟨 Mask 4

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

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

First, set the regular week 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 schedule 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 hours-column (on the left side of the weekdays heading row).*

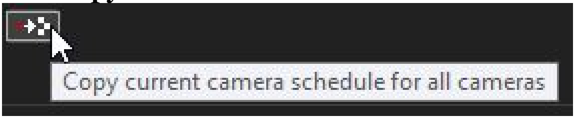
These options are available:

- **Off**. Video is not recorded. However, possible alarms are recorded. Alarms are configured in **Alarm Settings**.
- **Continuous.** The camera records all images. This option uses a lot of disk space.
- **Default mask.** The camera records video using the default motion detection mask and default motion detection parameters.
- **Custom mask.** The camera records video using a custom mask. Each camera can have as many as four custom masks.

To copy the current schedule for all cameras:

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

1. Click **Copy Schedule**

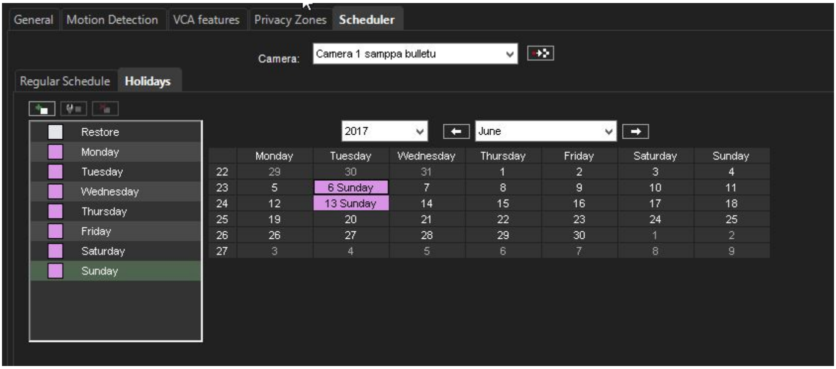


.

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

To set a holiday schedule:

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



Camera: Camera 1 samppa bulletu

2017 June

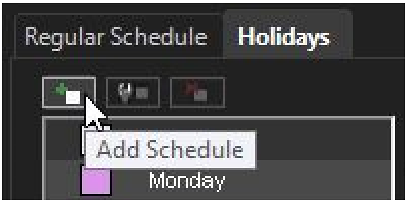
	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
22	29	30	31	1	2	3	4
23	5	6 Sunday	7	8	9	10	11
24	12	13 Sunday	14	15	16	17	18
25	19	20	21	22	23	24	25
26	26	27	28	29	30	1	2
27	3	4	5	6	7	8	9

1. On the **Holidays** tab, select the year and month.

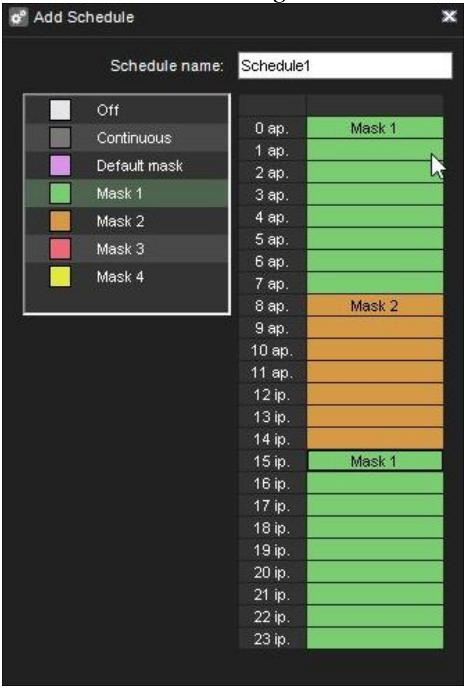
2. From the left pane, click the schedule that you want to apply and then click the holiday in the calendar.

To add a custom schedule:

1. Click **Add Schedule**



2. The **Add Schedule** dialog box is shown.



Schedule name: Schedule1

- ⬜ Off
- ⬛ Continuous
- 🟪 Default mask
- 🟩 Mask 1
- 🟧 Mask 2
- 🟥 Mask 3
- 🟨 Mask 4

0 ap.	Mask 1
1 ap.	
2 ap.	
3 ap.	
4 ap.	
5 ap.	
6 ap.	
7 ap.	
8 ap.	Mask 2
9 ap.	
10 ap.	
11 ap.	
12 ip.	
13 ip.	
14 ip.	
15 ip.	Mask 1
16 ip.	
17 ip.	
18 ip.	
19 ip.	
20 ip.	
21 ip.	
22 ip.	
23 ip.	

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:

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

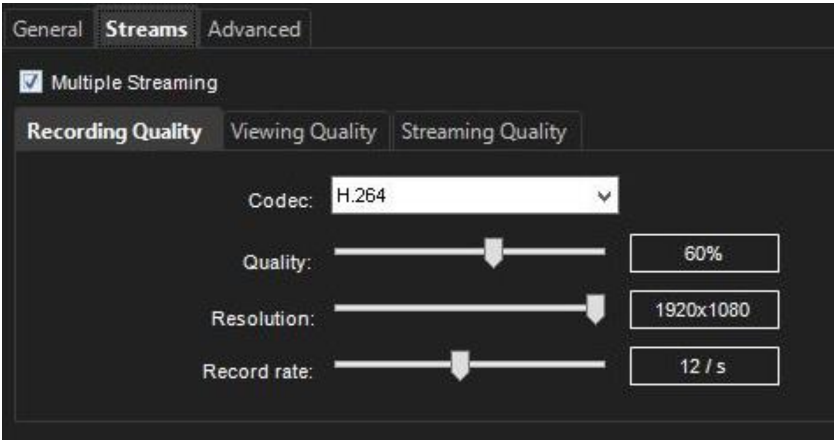
To restore the original schedule:

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

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



☑ Multiple Streaming

Codec: H.264

Quality: 60%

Resolution: 1920x1080

Record rate: 12 / s

EDGE STORAGE

The Edge storage functionality enables uninterrupted recording during network blackouts. In practice, in the case of network blackout, video feed can be stored on an SD memory card on the camera. Once 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.

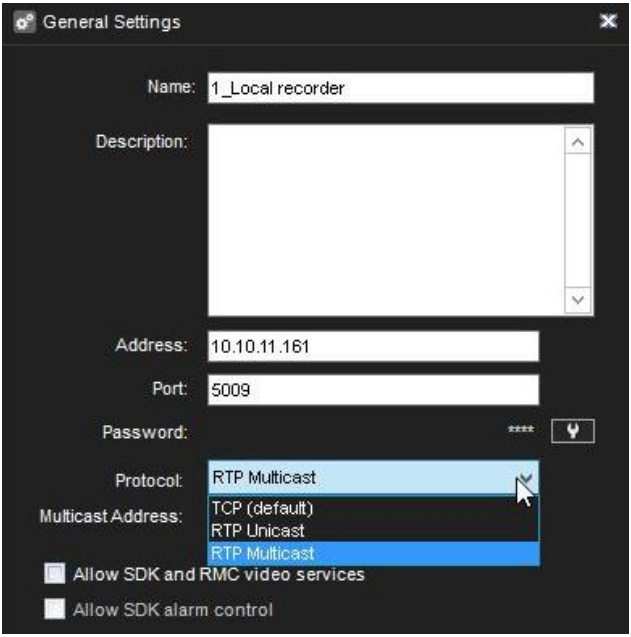
MULTI-CASTING

When a single workstation stream is opened multiple times, the server – and the network – faces 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:



General Settings

Name: 1_Local recorder

Description:

Address: 10.10.11.161

Port: 5009

Password: ****

Protocol: RTP Multicast

Multicast Address:

□ Allow SDK and RMC video services

□ Allow SDK alarm control

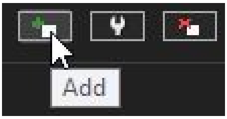
1. In the server's General settings, change the protocol from **TCP (default)** to **RTP Multicast**.
2. Edit the multicast address.
3. Repeat steps 1-2 for all required servers in the system. Note: Each multicast address needs to be separate.

AUDIO

ADDING, EDITING AND REMOVING AUDIO DEVICES

The system supports three basic types of audio components: one-way analog and IP audio channels, two-way IP audio channels, and a single audio communication channel.

To configure audio devices:

1. Open the **EASYVIEW 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:
   - **Mono**. Select to use two mono channels.
   - **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 **EASYVIEW 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** dialog box is shown.
6. Edit the information fields.
7. Click **OK**.

To remove an audio device:

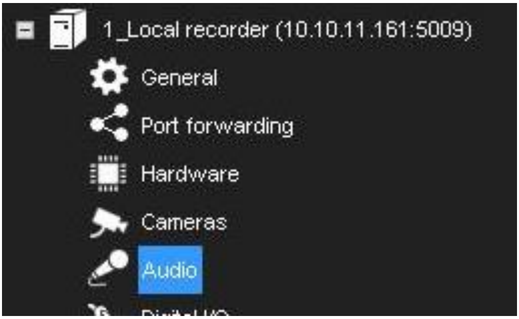
1. Open the **EASYVIEW Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the audio channel.
5. Click **Remove Last Audio Channel from the List** in the lower right corner of the tab.
   NOTE: *You cannot remove an audio device 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.

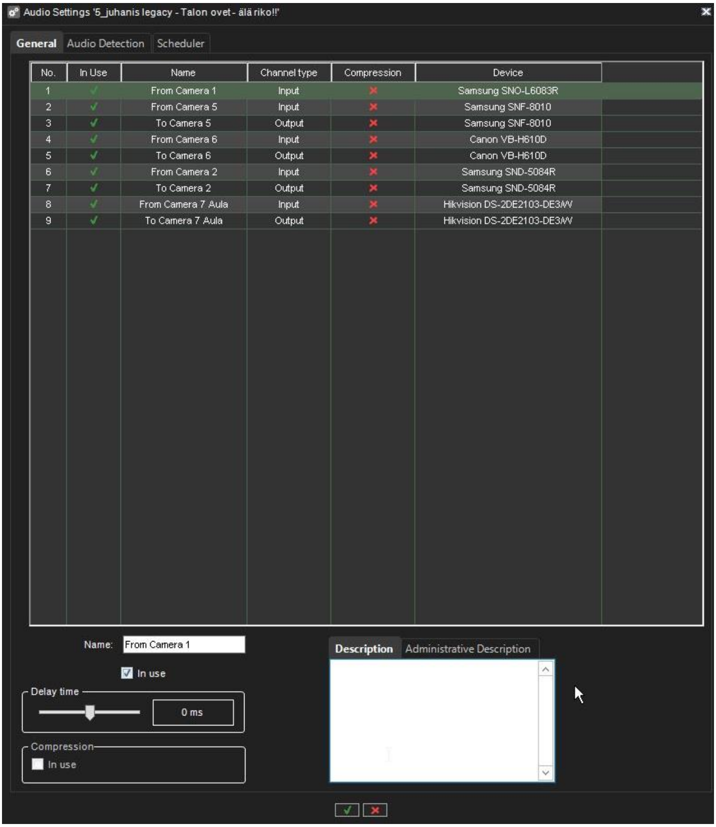
AUDIO SETTINGS

The system supports three basic types of audio components:

- **One-way analog 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 Viewing Client client. Only one Viewing Client 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.

GENERAL SETTINGS





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

No.	In Use	Name	Channel type	Compression	Device
1	✓	From Camera 1	Input	✗	Samsung SNO-L6083R
2	✓	From Camera 5	Input	✗	Samsung SNF-8010
3	✓	To Camera 5	Output	✗	Samsung SNF-8010
4	✓	From Camera 6	Input	✗	Canon VB-H610D
5	✓	To Camera 6	Output	✗	Canon VB-H610D
6	✓	From Camera 2	Input	✗	Samsung SND-5084R
7	✓	To Camera 2	Output	✗	Samsung SND-5084R
8	✓	From Camera 7 Aula	Input	✗	Hikvision DS-2DE2103-DE3/W
9	✓	To Camera 7 Aula	Output	✗	Hikvision DS-2DE2103-DE3/W

Name: From Camera 1

☑ In use

Delay time: 0 ms

Compression: ☐ In use

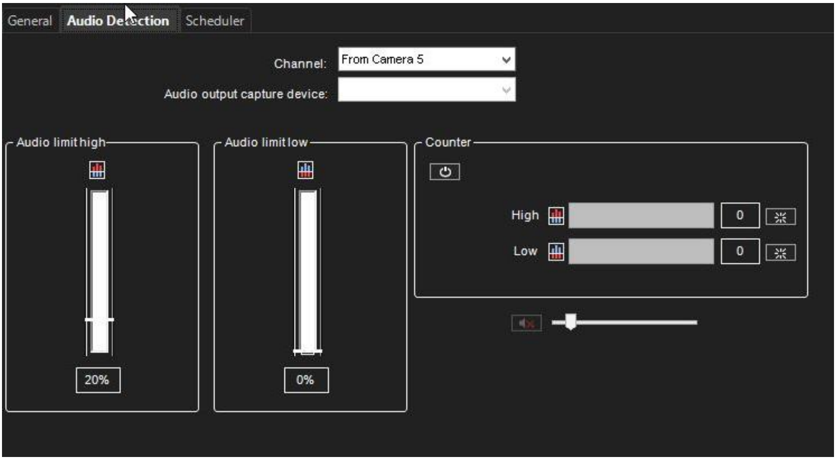
The **General** tab in the **Audio** page lists the basic settings of all audio channels:

- **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 check mark 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:
   - **Name**. The name of the channel.
   - **In use**. Select to enable the channel. Clear the check box to disable the channel.
   - **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.
   - **Compression**. Select to use compression. Compressed audio files use less disk space, but the quality of audio is a bit lower. Clear the check box to not use compression.
   - **Description**. Here you can type a description of the channel that will be shown to the users in the Viewing Client program.
   - **Administrative Description**. Here you can type a description of the channel that will be shown in the Viewing Client program to only system administrators.

AUDIO DETECTION



General | Audio Detection | Scheduler

Channel: From Camera 5

Audio output capture device:

On the **Audio Detection** tab in 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.

SCHEDULER (AUDIO)

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

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

- **Off.** Audio is not recorded. However, possible alarms are recorded.
- **Continuous.** All audio is recorded.
- **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.

AUDIO COMMUNICATION SETTINGS

You can connect a call button, a microphone, and a speaker to a server and use them as 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 Viewing Client 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:

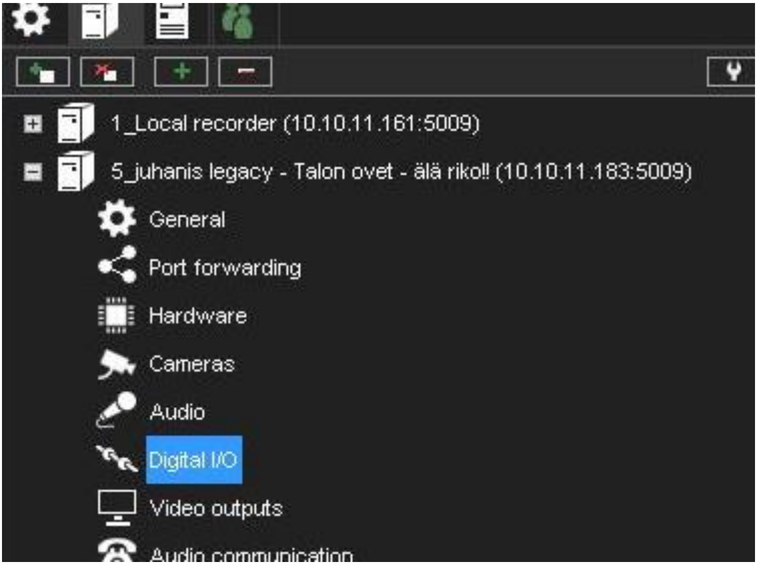
1. Connect a call button or an equivalent device to one of the digital inputs of the server.
2. Connect a microphone and a speaker to the server and to the user's workstation.

To set up audio communication:

1. Open the **EASYVIEW Servers** tab.
2. Select the correct server and open the **Audio Communication** page from the menu.

1. Select the capture driver and the playback device.
2. In **Audio Communication Settings**, type a name for the communication channel (or use the default name).
3. 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.
4. Select the digital input that the call button is connected to.

DIGITAL I/O



1_Local recorder (10.10.11.161:5009)

5_juhanis legacy - Talon ovet - älä riko!! (10.10.11.183:5009)

- General
- Port forwarding
- Hardware
- Cameras
- Audio
- Digital I/O
- Video outputs
- Audio communication

DIGITAL I/O SETTINGS

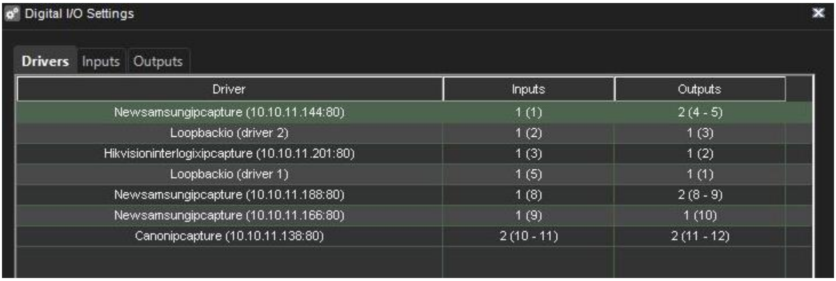
In **Digital I/O** settings, you can add digital input and output devices, and configure the input and output settings.

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.

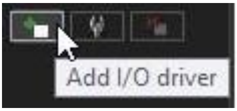
Once an I/O device driver has been added to the system, the device can be configured and taken into use through the **Drivers** tab.

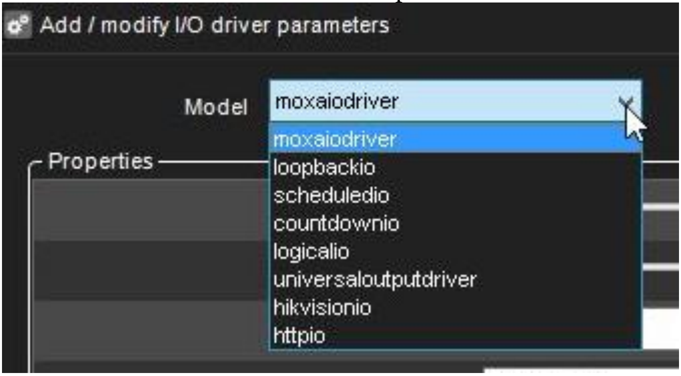

Digital I/O Settings

Drivers | Inputs | Outputs

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

To take an I/O device driver into use:

1. If necessary, install the device driver package.
2. Open the **EASYVIEW 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.


Add / modify I/O driver parameters

Model: moxaiodriver

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:

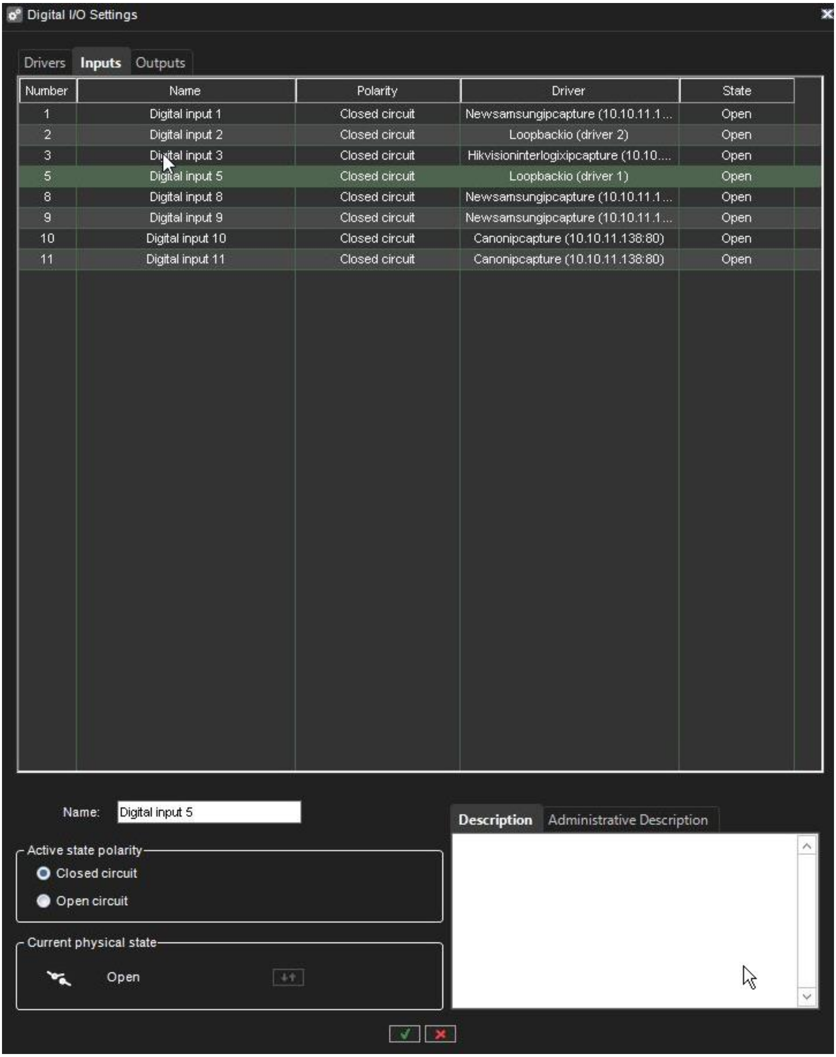
1. Open the **EASYVIEW Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Double click on the device driver you want to edit.
4. Edit the device settings in the **Properties** list.
5. To save the settings, click **OK**.

To delete an I/O device driver:

1. Open the **EASYVIEW 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.



Number	Name	Polarity	Driver	State
1	Digital input 1	Closed circuit	Newsamsungipcapture (10.10.11.1...	Open
2	Digital input 2	Closed circuit	Loopbackio (driver 2)	Open
3	Digital input 3	Closed circuit	Hikvisioninterlogixipcapture (10.10....	Open
5	Digital input 5	Closed circuit	Loopbackio (driver 1)	Open
8	Digital input 8	Closed circuit	Newsamsungipcapture (10.10.11.1...	Open
9	Digital input 9	Closed circuit	Newsamsungipcapture (10.10.11.1...	Open
10	Digital input 10	Closed circuit	Canonipcapture (10.10.11.138:80)	Open
11	Digital input 11	Closed circuit	Canonipcapture (10.10.11.138:80)	Open

Name: Digital input 5

Active state polarity
- ● Closed circuit
- ○ Open circuit

Current physical state: Open

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

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

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

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

Administrative Description. Here you can type a description of the selected input that will be shown in the Viewing Client 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 Viewing Client program.

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

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

LOGICAL I/O

With Logical I/O it is possible to create actions based on the OR and AND operators.

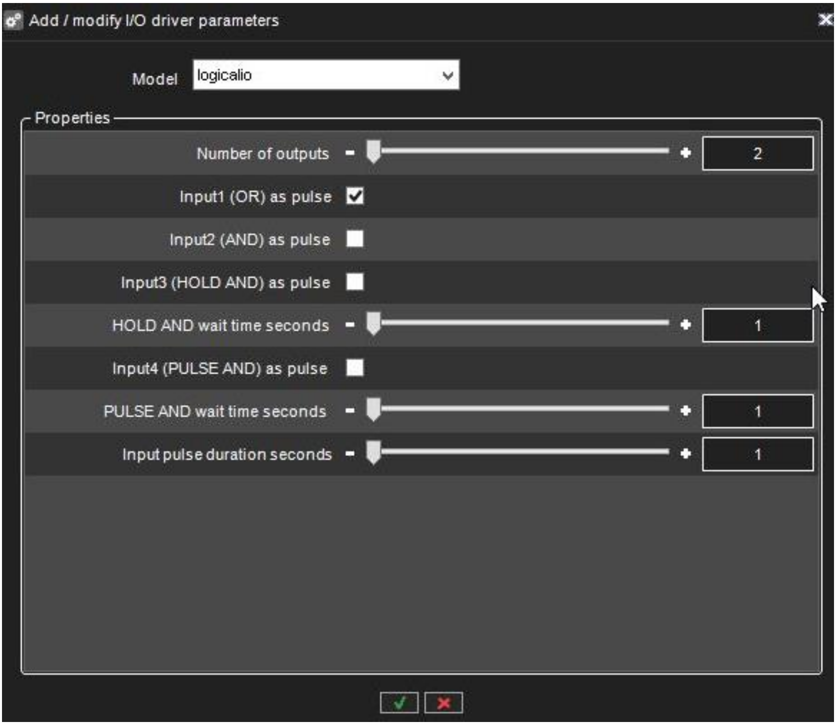
For example, if customer wants to confirm that an Automatic Number Plate Recognition (ANPR) event is triggered when a car is in front of the camera, the Logical I/O can be used to create a “rule” that results in an action only when VCA detects a car AND at the same time there is an ANPR read event.

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 license. If license is not present, creating new IO will fail.

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



Add / modify I/O driver parameters

Model: logicalio

Properties

Number of outputs: 2

Input1 (OR) as pulse ☑

Input2 (AND) as pulse □

Input3 (HOLD AND) as pulse □

HOLD AND wait time seconds: 1

Input4 (PULSE AND) as pulse □

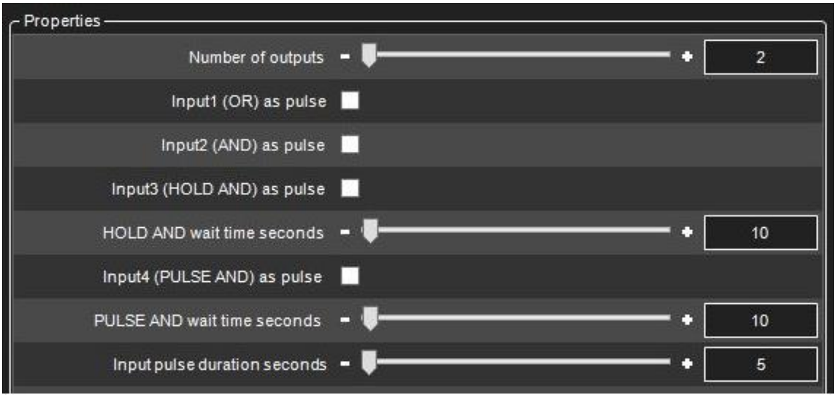
PULSE AND wait time seconds: 1

Input pulse duration seconds: 1

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:



Properties

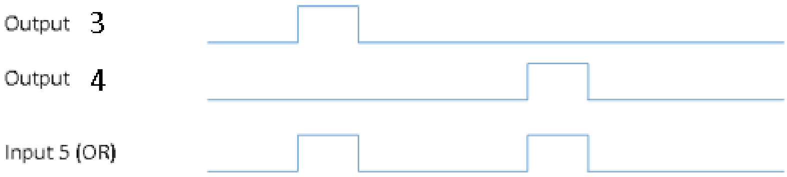
Number of outputs	2
Input1 (OR) as pulse	□
Input2 (AND) as pulse	□
Input3 (HOLD AND) as pulse	□
HOLD AND wait time seconds	10
Input4 (PULSE AND) as pulse	□
PULSE AND wait time seconds	10
Input pulse duration seconds	5

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.

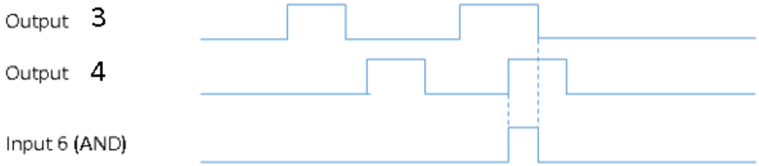


In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, the input 5 will be turned on as a result.

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

"AND" INPUT

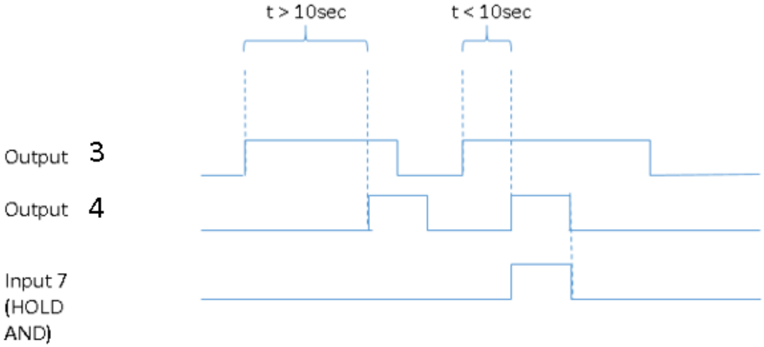
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on at the same time, the input 6 will be turned on.



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 becomes 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.



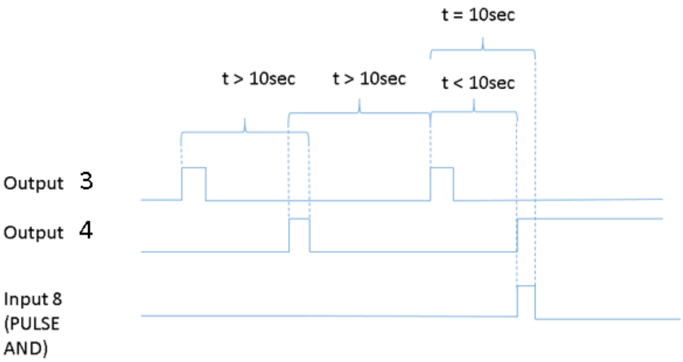
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, the input 7 will become active.

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 becomes active if all outputs *have been* active within a specified time.

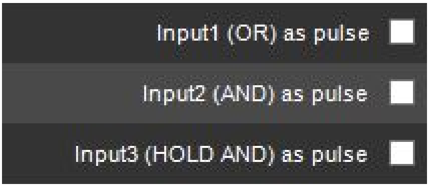
In our example, if output 3 has been active inside 10 seconds, and output 4 becomes active, then the input 8 will be turned on.



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 has elapsed from output 3 activation, the 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.

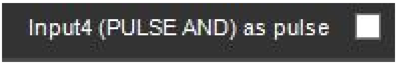


Input1 (OR) as pulse □

Input2 (AND) as pulse □

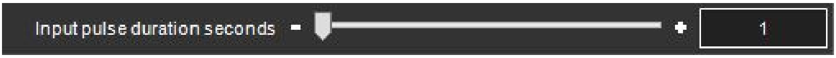
Input3 (HOLD AND) as pulse □

and



Input4 (PULSE AND) as pulse □

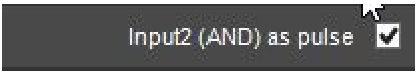
The pulse duration can also be adjusted.



Input pulse duration seconds 1

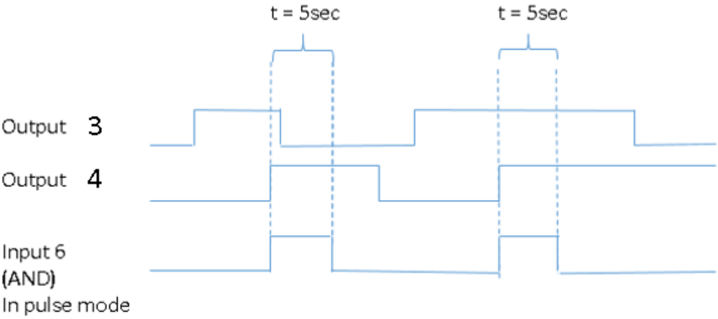
If the pulse mode is in use, the input will turn off after the set pulse duration.

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



Input2 (AND) as pulse ☑

It would mean behavior like this:



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.

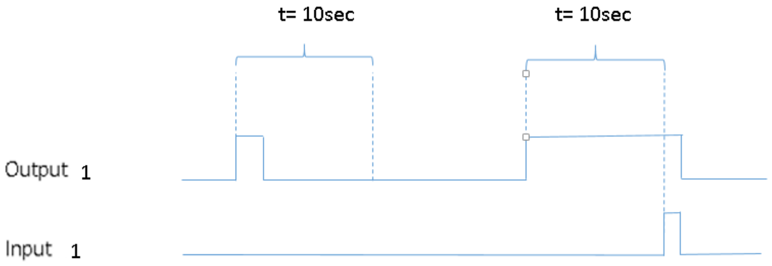
Countdown I/O has two basic modes. The first two input/output pairs are of type 1 and the last two pairs are of type 2.

Logical IO and countdown IO are controlled by license. If 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.

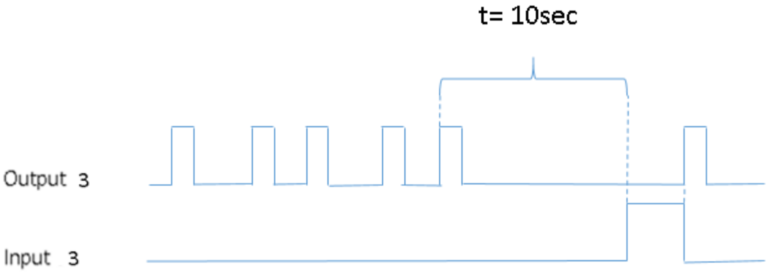


When creating a new Countdown I/O, the first two input-output pair is of this type.

EXPECTED TRIGGER MODE (TYPE 2)

Secondly, it is possible to trigger 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.

VIDEO OUTPUTS

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

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 Viewing Client 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 a video output:

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

To add a camera tour:

1. Open the **EASYVIEW 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** dialog box is shown.
4. Do as follows:
   a. Click **Add Camera Tour**.

   b. Type a name for the tour.

   c. 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.

d. To change the order of the cameras, drag a camera to a new position.

e. To remove a camera, select the camera and click **Remove Camera**.

f. 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 **EASYVIEW 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** dialog box is shown.
4. From the tours list, select the tour that you want to edit. You can edit these settings:
    - To change the name of the tour, click **Change Tour Name** and then type a new name for the tour.
    - To change the order of the cameras, drag a camera to a new position in the list.
    - To remove a camera from the tour, select the camera, and then click **Remove Camera**.
    - 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:

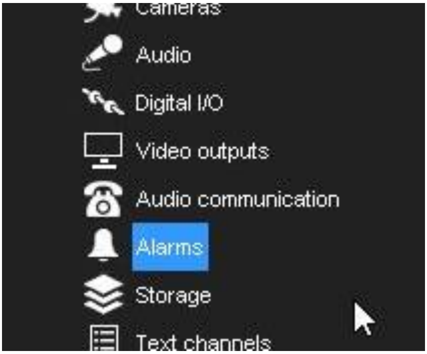
1. Open the **EASYVIEW Servers** tab.
2. Select the correct server and open the **Video outputs** page from the menu.
3. Click **Edit Camera Tours**. The **Edit Camera Tours** dialog box is shown.
4. From the tours list, select the tour that you want to delete.
5. Click **Delete Tour** adjacent to the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

6. To save the changes, click **OK**.

To edit the descriptions of the outputs:

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

ALARMS

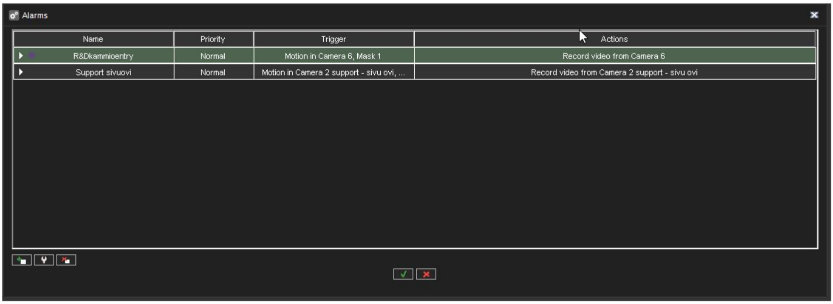


ALARM SETTINGS

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 **EASYVIEW Servers** tab.

ACCESSING THE ALARM LIST



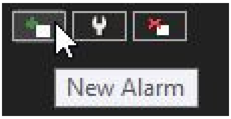
Name	Priority	Trigger	Actions
R&Dkammioentry	Normal	Motion in Camera 6, Mask 1	Record video from Camera 6
Support sivuovi	Normal	Motion in Camera 2 support - sivu ovi, ...	Record video from Camera 2 support - sivu ovi

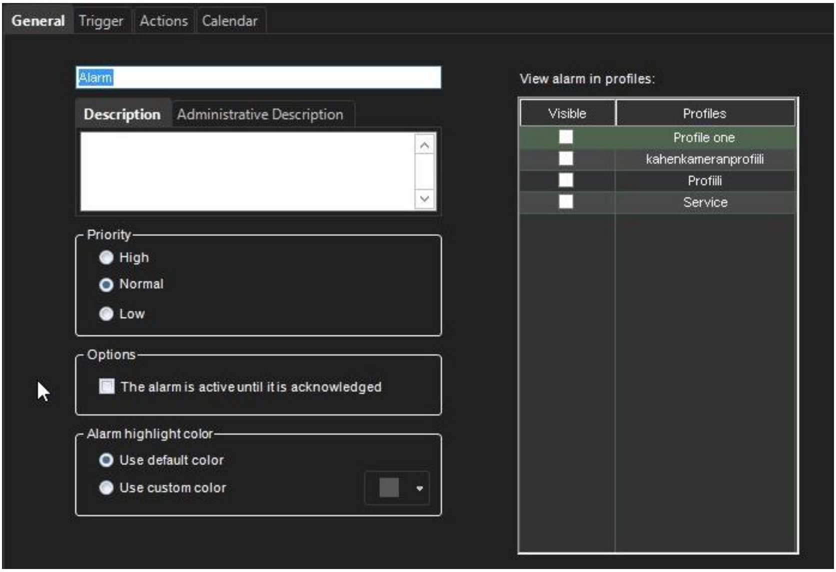
To access the alarm list:

1. On the **EASYVIEW 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.

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 to the **Name** field.



Alarm

Priority
○ High
● Normal
○ Low

Options
□ The alarm is active until it is acknowledged

Alarm highlight color
● Use default color
○ Use custom color

View alarm in profiles:

Visible	Profiles
□	Profile one
□	kahenkameranprofiili
□	Profiili
□	Service

3. Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.

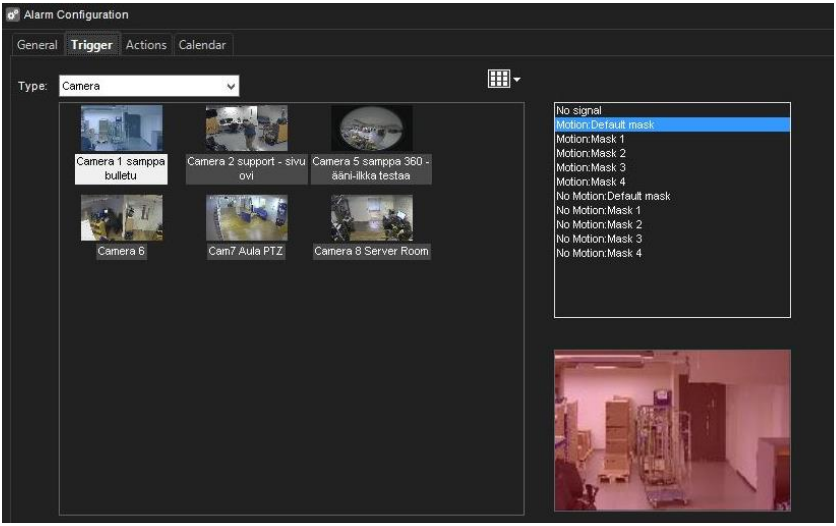
4. Select whether the alarm is of **high**, **normal** or **low priority**. The priority is used to define the order in which alarms are executed in case of multiple simultaneous alarms.

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 **Viewing Client** application.

6. **Alarm highlight color** allows administrators to define a custom color 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.*

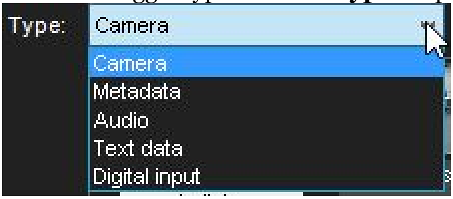
8. Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.



Alarm Configuration

Type: Camera

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



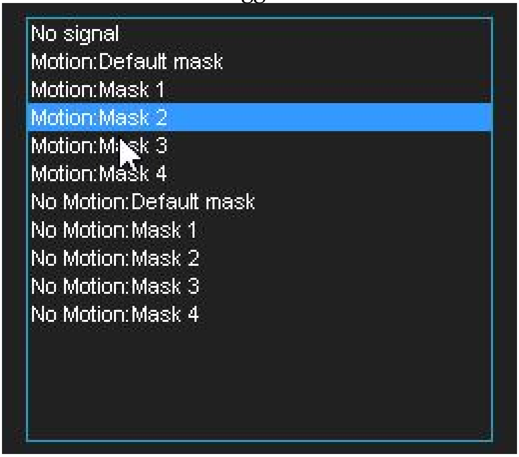
10. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.

    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.

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

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

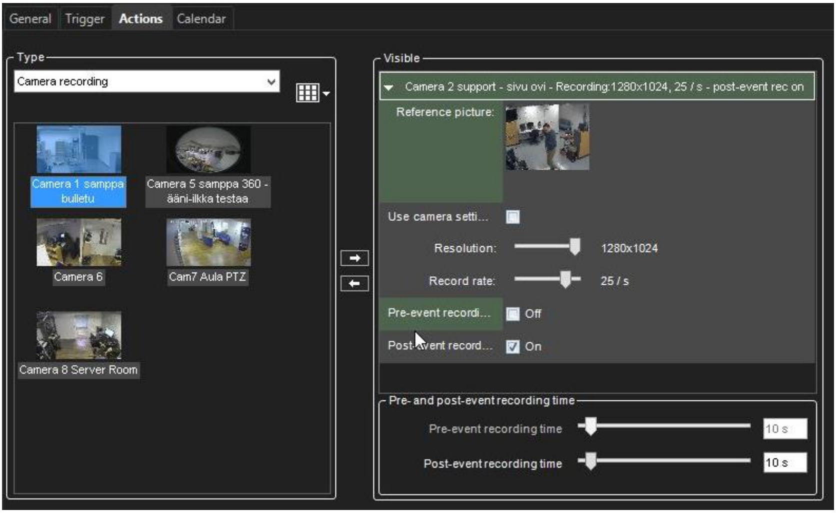


- For audio based triggers, you can set the alarm to trigger based on a high or low audio level.
- For text data based (e.g., VCA, ANPR+, etc.) triggers, you can set the alarm to trigger based on a text data string. In addition, you can set an

optional alarm ending trigger by marking **Define ending input** and selecting string for ending the alarm.

- 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.



Type: Camera recording

Visible

Camera 2 support - sivu ovi - Recording:1280x1024, 25 / s - post-event rec on

Reference picture:

Use camera setti... ☐

Resolution: 1280x1024

Record rate: 25 / s

Pre-event recordi... ☐ Off

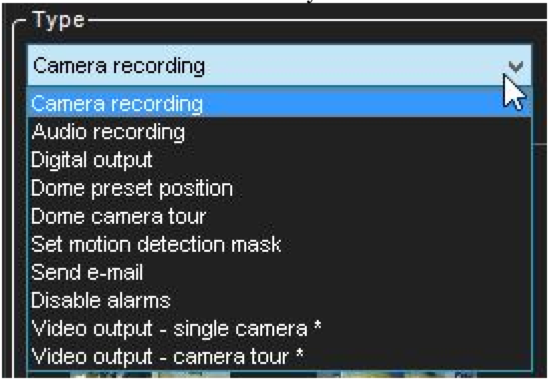
Post-event record... ☑ On

Pre- and post-event recording time

Pre-event recording time 10 s

Post-event recording time 10 s

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



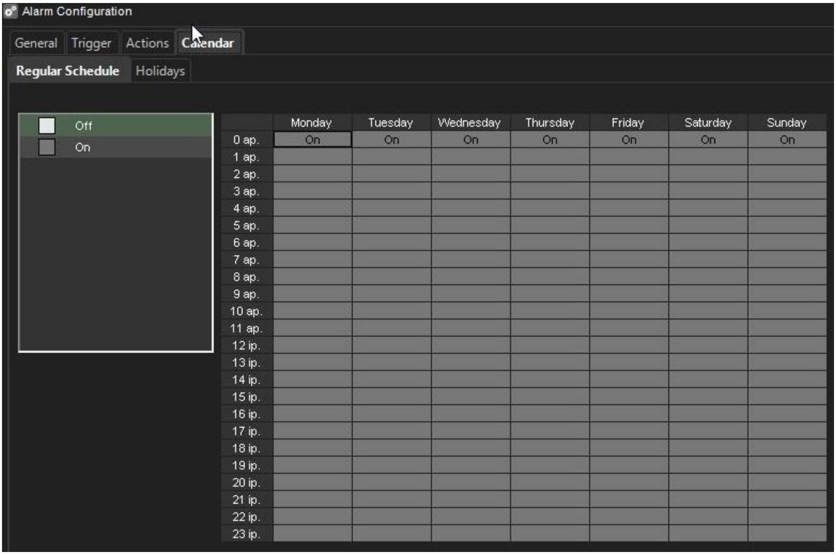
14. Select the device for which the selected action type will be used from the list below the **Type** drop-down menu. You can change the layout of the list by clicking the layout button.

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.



Alarm Configuration

General | Trigger | Actions | Calendar

Regular Schedule | Holidays

□ Off
□ On

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

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.

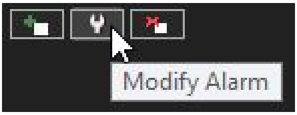
20. Click **OK** to save the alarm.

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 alarm is active, it will be automatically switched off when time reaches a point where alarm schedule is defined to be off.*
- *When alarm schedule begins, and alarm trigger is active, the alarm will be automatically activated.*

EDITING AN ALARM

To edit an alarm:

1. On the **EASYVIEW 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.*

DELETING AN ALARM

To delete an alarm:

1. On the **EASYVIEW 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.

ACTION TYPES AND SETTINGS

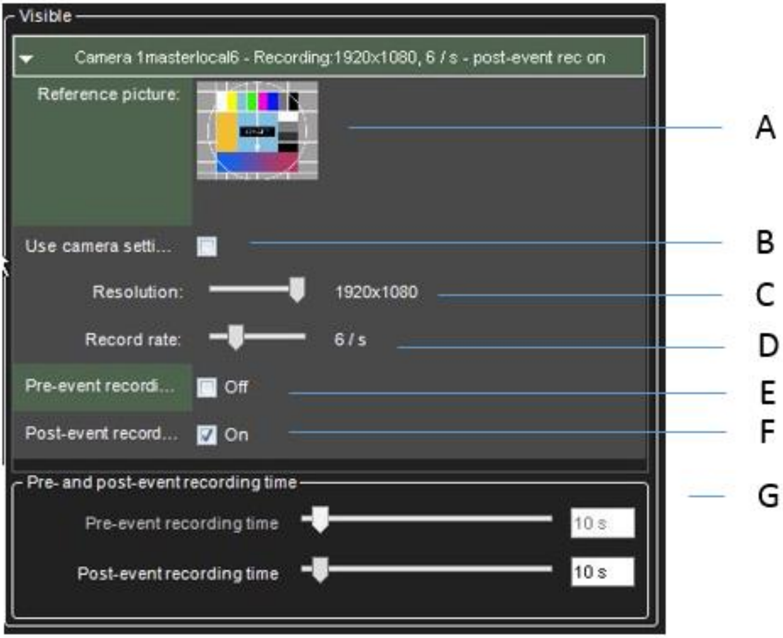
The list below contains the default action types and their parameters. Some of the action types listed above may not be available on all systems.

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 **Viewing Client**, 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.



Visible

Camera 1masterlocal6 - Recording:1920x1080, 6 / s - post-event rec on

Reference picture:

Use camera setti... □

Resolution: 1920x1080

Record rate: 6 / s

Pre-event recordi... □ Off

Post-event record... ☑ On

Pre- and post-event recording time

Pre-event recording time 10 s

Post-event recording time 10 s

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 pre-event recording on. The duration of 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 pre-event recording can be set through the **Post-event recording time** slider.

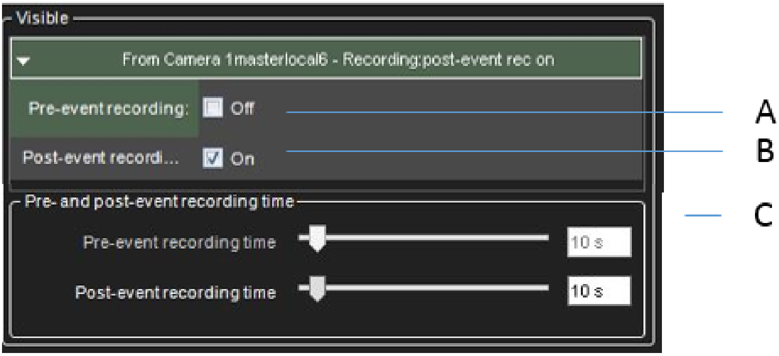
G) Pre- & post-event recording duration. These sliders can be used to set the pre- and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

NOTE: *All devices (cameras and microphones) that are connected to the alarm and have their pre- and post-event recording activated 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 **Viewing Client**, 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.



Visible

From Camera 1masterlocal6 - Recording:post-event rec on

Pre-event recording: ☐ Off

Post-event recordi... ☑ On

Pre- and post-event recording time

Pre-event recording time 10 s

Post-event recording time 10 s

The action includes the following fields and parameters:

A) Pre-event recording. Mark this checkbox to set pre-event recording on. The duration of 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 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 share the same pre- and post-event recording durations.*

DIGITAL OUTPUT

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 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:

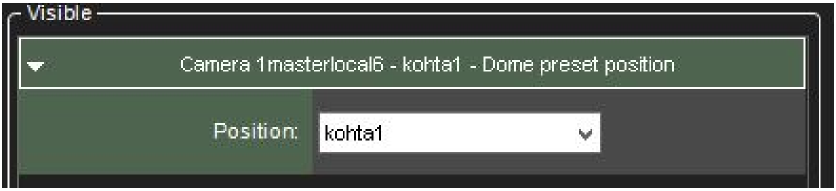
- **Show in monitor**. Use the drop-down menu to select the camera tour from which the video feed is displayed in the selected video output during the alarm.

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 *EASYVIEW Viewing Client 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 to be displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording** has been selected for the PTZ camera.



Visible

Camera 1masterlocal6 - kohta1 - Dome preset position

Position: kohta1

The action includes the following fields and parameters:

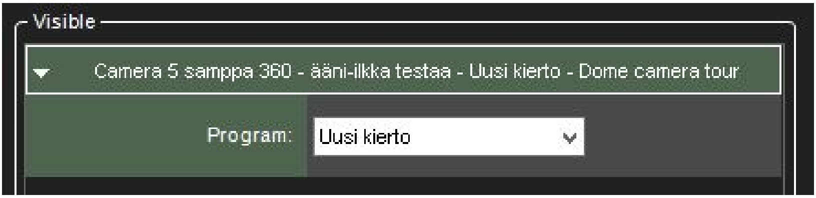
- **Position**. Use the drop-down menu to select the preset position to which the PTZ camera will move during the alarm.

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 *EASYVIEW Viewing Client 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 to be displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording** has been selected for the PTZ camera.



Visible

Camera 5 samppa 360 - ääni-ilkka testaa - Uusi kierto - Dome camera tour

Program: Uusi kierto

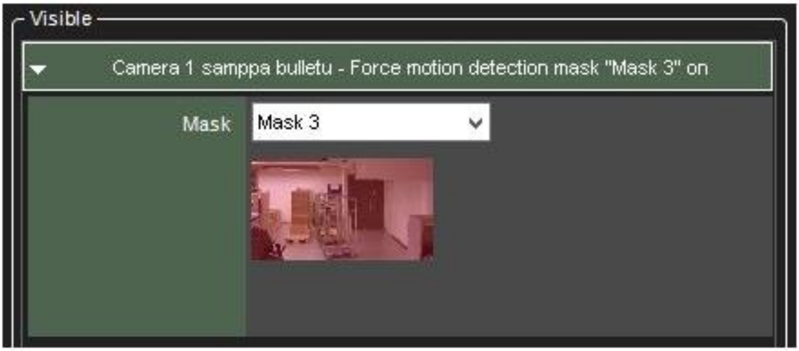
The action includes the following fields and parameters:

- **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.



Visible

Camera 1 samppa bulletu - Force motion detection mask "Mask 3" on

Mask: Mask 3

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.

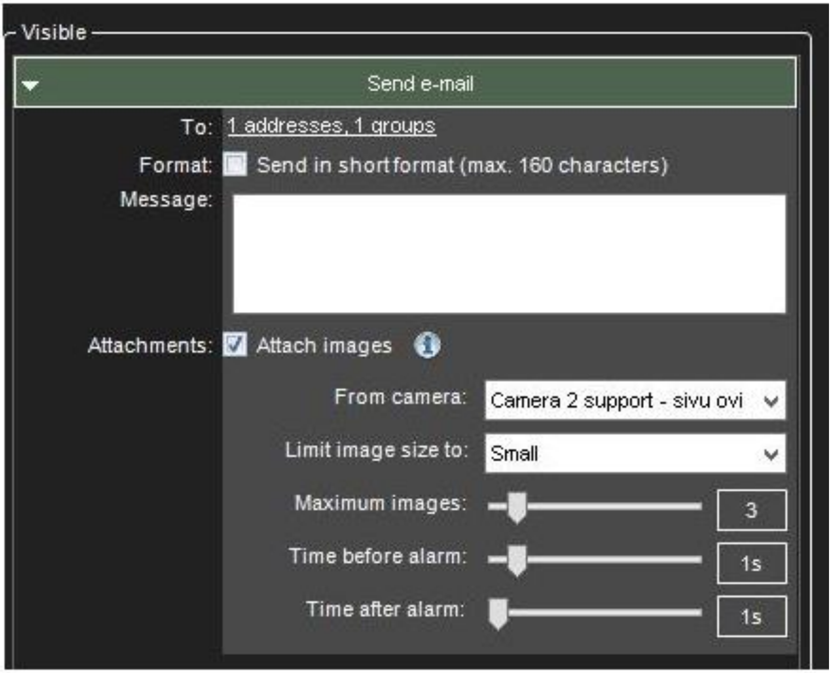
NOTE: *Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

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 **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 to the alarm email. To do this, uncheck the **Send in short format** -option and check the **Attach images** –option



Visible

Send e-mail

To: 1 addresses, 1 groups

Format: □ Send in short format (max. 160 characters)

Message:

Attachments: ☑ Attach images

From camera: Camera 2 support - sivu ovi

Limit image size to: Small

Maximum images: 3

Time before alarm: 1s

Time after alarm: 1s

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

NOTES:

- *The number of images in this configuration is the maximum amount delivered. Less images might arrive*
- *Attaching images to alarm emails might lead to high amount of data traffic, so it is recommended to test the configuration settings to find 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.

- 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 alarm name in 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.

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.

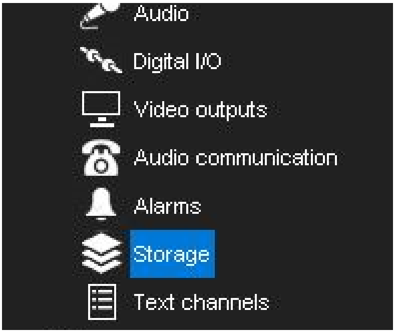
To delete a custom schedule:

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.

STORAGE



EASYVIEW Version 8 comes with new 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.

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

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

STORAGE SETTINGS

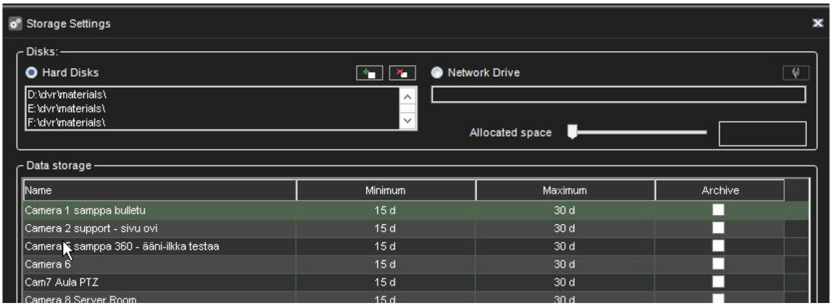
In storage settings, you can set the storage time of recorded video, audio and text data as well as alarm data. In addition, after adding a hard disk to a server, you can set it as additional data storage through the storage settings.

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

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.



Storage Settings

Disks:

● Hard Disks

D:\dvr\materials\
E:\dvr\materials\
F:\dvr\materials\

○ Network Drive

Allocated space

Data storage

Name	Minimum	Maximum	Archive
Camera 1 samppa bulletu	15 d	30 d	□
Camera 2 support - sivu ovi	15 d	30 d	□
Camera 5 samppa 360 - ääni-ilkka testaa	15 d	30 d	□
Camera 6	15 d	30 d	□
Cam7 Aula PTZ	15 d	30 d	□
Camera 8 Server Room	15 d	30 d	□

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

Use of multiple storage disks has the benefit of allowing material write to be distributed to all the drives, making 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 dialog box is shown. The **Minimum free space on 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 user name and password into the **User name** 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 dialog box is shown.
3. Storage size cannot be configured for iSCSI disks.
4. Click ok to store settings. Repeat for other disks.

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.

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 has 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 the 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.*

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 Viewing Client client.

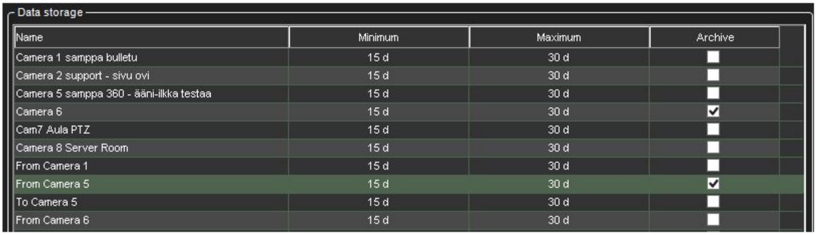
NOTE: *Archive files can be extremely large, and thus they can fill storage space quickly. Archive files should be regularly copied and removed from the server hard disks or network drives on which they are automatically saved.*

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.*

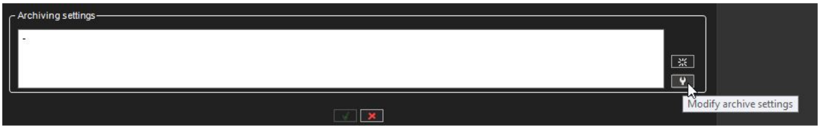
2. Mark the **Archive** checkbox.



Data storage

Name	Minimum	Maximum	Archive
Camera 1 samppa bulletu	15 d	30 d	□
Camera 2 support - sivu ovi	15 d	30 d	□
Camera 5 samppa 360 - ääni-ilkka testaa	15 d	30 d	□
Camera 6	15 d	30 d	☑
Cam7 Aula PTZ	15 d	30 d	□
Camera 8 Server Room	15 d	30 d	□
From Camera 1	15 d	30 d	□
From Camera 5	15 d	30 d	☑
To Camera 5	15 d	30 d	□
From Camera 6	15 d	30 d	□

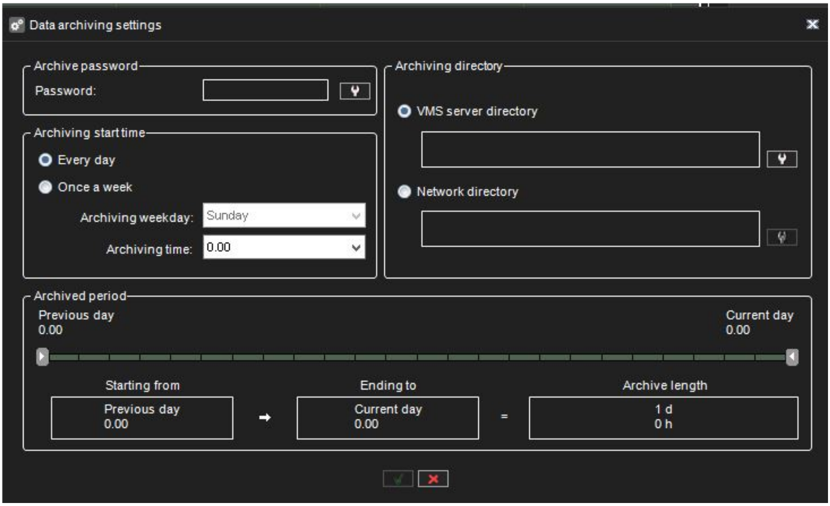
3. Click **Modify archive settings**



Archiving settings

-

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



Data archiving settings

Archive password
Password:

Archiving directory
● VMS server directory
○ Network directory

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

Archived period
Previous day 0.00
Current day 0.00

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

5. Select, whether to create the archive on a daily or weekly basis by selecting **Every day** or **Once a week**.

- If you set archiving to happen on a daily basis, use the **Archiving time** drop-down menu to select the time on which the archive files are created.
- 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 **EASYVIEW 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.

TEXT CHANNELS

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 are 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 to 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:
   a. Select a text data channel from the channel list.
   b. Type a name for the channel into the Name field.
   c. Type a general description and an administrative description of the channel into the respective fields. All users can see the general description, whereas only system administrators can see the administrative description.

d. 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:

   a. Select a text data channel from the channel list.

   b. Click **Modify channels** .

   c. Edit the driver specific information to the fields in the **Properties** list.

   d. 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.*

PROFILES

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

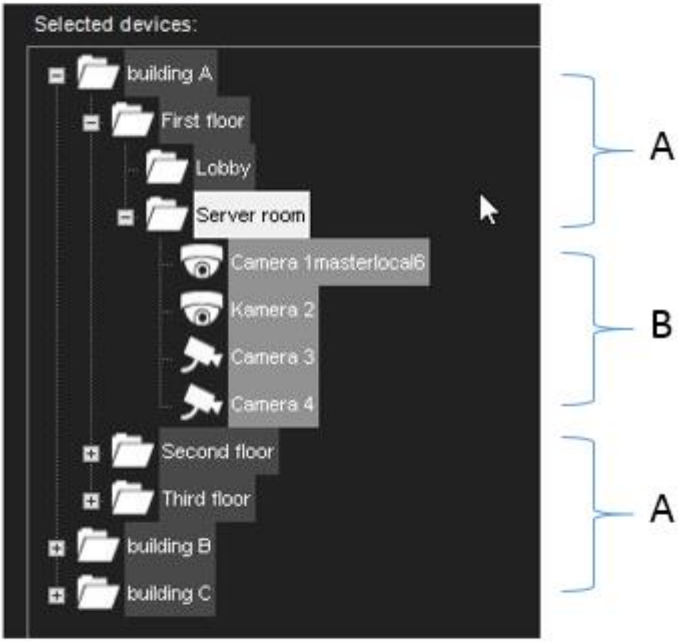
- Cameras (fixed cameras and PTZ cameras)
- Audio channels
- Audio communication channel
- Digital inputs (alarm inputs)
- Digital outputs (control outputs)
- Video outputs
- Text channels
- Alarms

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*

ADDING AND EDITING PROFILES

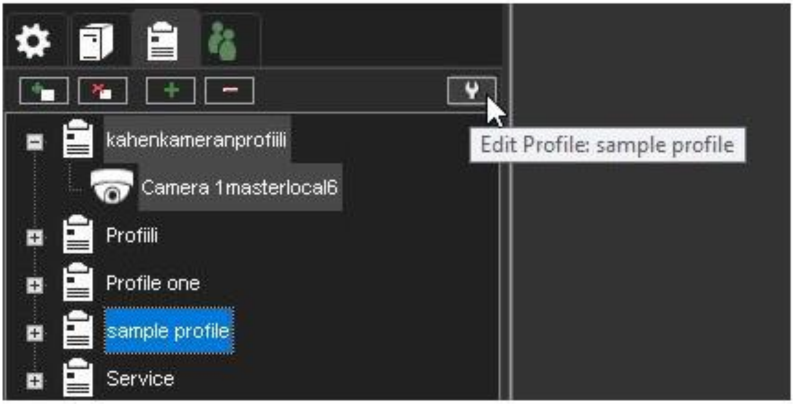
The system has one default profile, *Services*. The default profile contains the devices that the license key of the Master Server specifies. The devices are grouped by device type. For example, all cameras are in one group and all audio channels in a different group.

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:

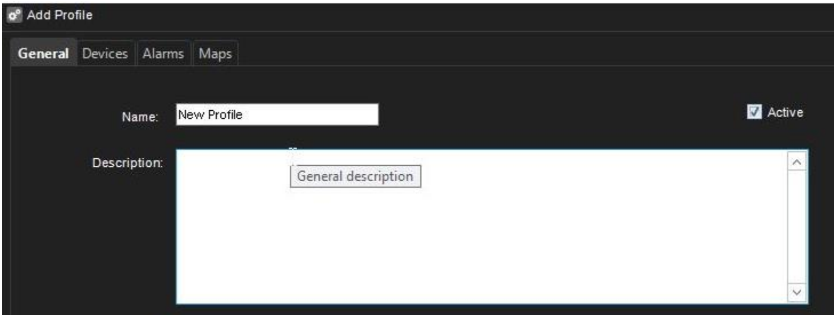
   - To edit a profile, click the profile that you want to edit and then click **Edit Profile**



in the lower-right corner of the navigation pane. The **Edit Profile** dialog box is shown.

- To add a profile, click **Add Profile** in the lower-left corner of the navigation pane. The **Add Profile** dialog 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 Viewing Client program. The description is shown only in System Manager.

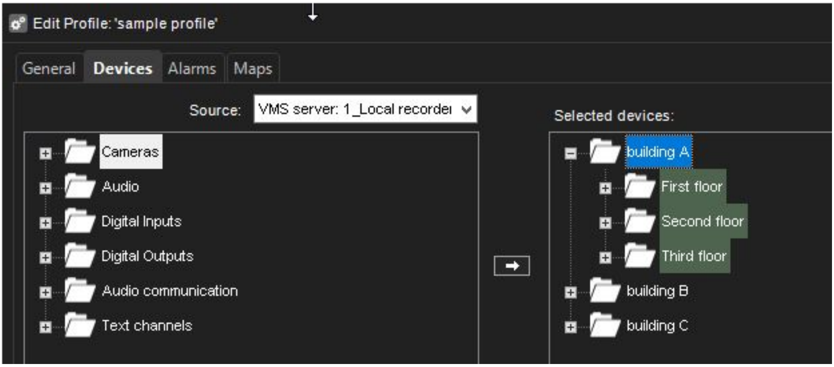


Name: New Profile

☑ Active

Description:

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.

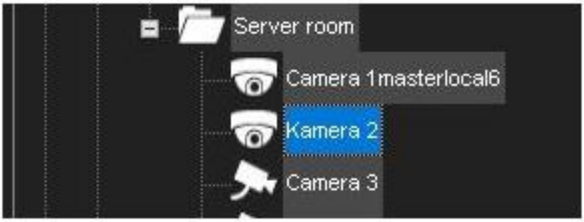


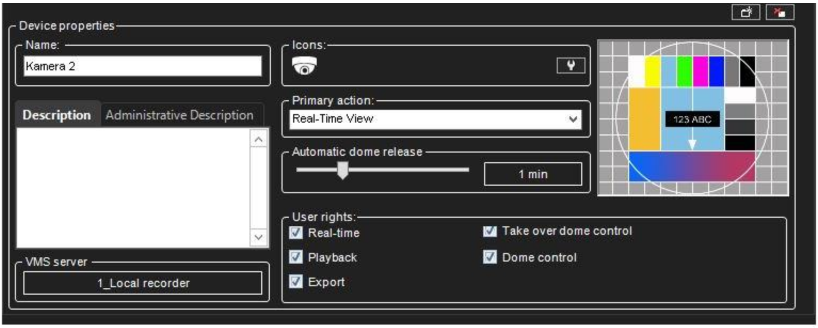
Edit Profile: 'sample profile'

Source: VMS server: 1_Local recorder

Selected devices:

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





Device properties

Name: Kamera 2

Icons:

Primary action: Real-Time View

Automatic dome release: 1 min

VMS server: 1_Local recorder

User rights:

☑ Real-time

☑ Playback

☑ Export

☑ Take over dome control

☑ Dome control

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 **EASYVIEW 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:

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

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.

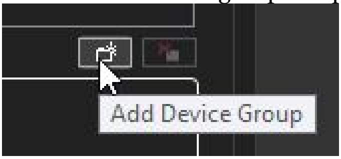
The structure consists of devices and device groups. Devices resemble computer files, and device groups resemble computer folders. First create the device groups (folders). Note that you can add subgroups under the device groups. Then move the devices that you want the users of the profile to be able 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 Viewing Client 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.

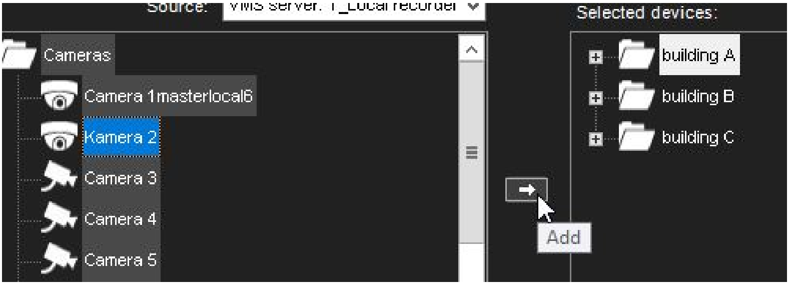
TIP: Do not use “ENTER” key while doing the group tree editing. ENTER key in this view will close the profile editing window. Instead, re-focus the mouse to some other area on the dialog.

To remove a device group or device from a profile:

- 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

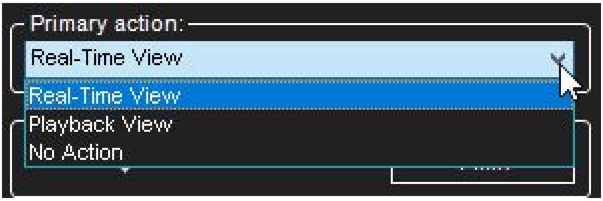


You can also drag devices from the left pane to the right.
TIP: To select adjacent devices or folders, hold down the SHIFT key and then click the first and last device that you want to select. To add a device to a selection or to remove it from a selection, keep the CTRL key pressed

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**.

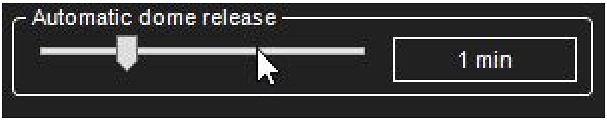
5. From the **Primary action** menu, select the action that will occur when a user double-clicks the device in Viewing Client.



Primary action:

Real-Time View

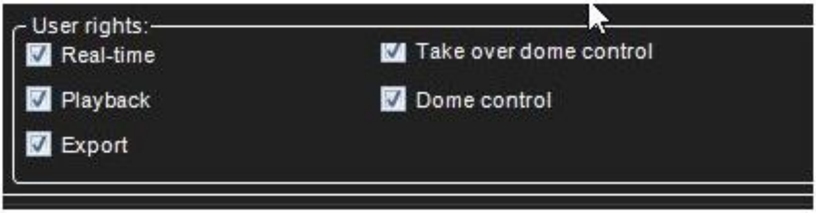
6. If the device is a PTZ camera, you can set the profile specific PTZ release time by using the **Automatic dome release** slider control. The setting defines the time the user can be idle before PTZ controls are released and other users can access the controls.



Automatic dome release

1 min

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



User rights:

☑ Real-time

☑ Playback

☑ Export

☑ Take over dome control

☑ Dome control

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 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.

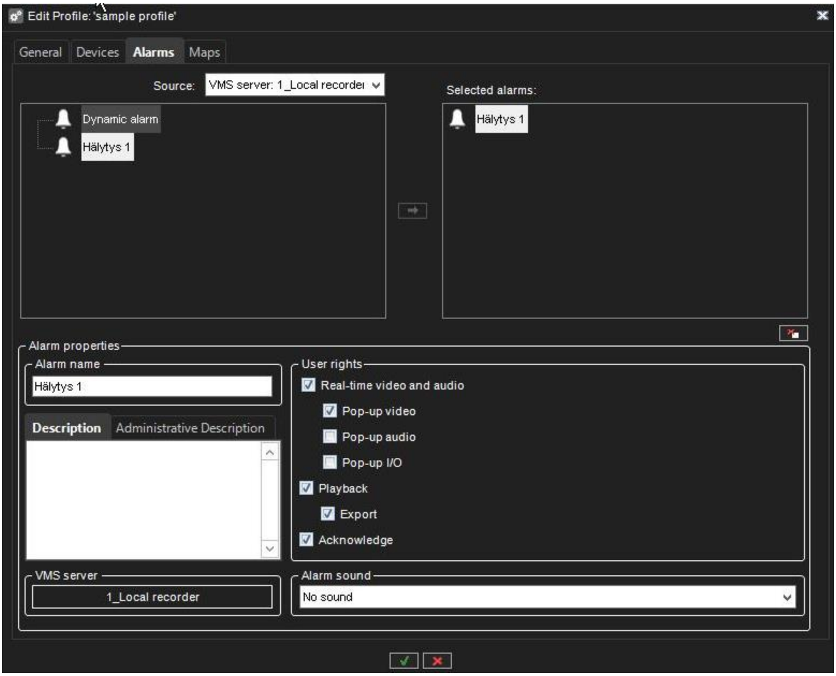
Show header. Select to show identification data specified by the text data capture driver.

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).

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

EDITING PROFILE SPECIFIC ALARM SETTINGS



Source: VMS server: 1_Local recorder

Selected alarms: Hälytys 1

Alarm properties

Alarm name: Hälytys 1

User rights

☑ Real-time video and audio

☑ Pop-up video

☐ Pop-up audio

☐ Pop-up I/O

☑ Playback

☑ Export

☑ Acknowledge

VMS server: 1_Local recorder

Alarm sound: No sound

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. 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:

- **Real-time video and audio**. Select to let the users see real-time alarm video or audio.
- **Pop-up video**. Select to let users receive alarm video automatically.
- **Pop-up audio**. Select to let users receive alarm audio automatically.
- **Playback**. Select to let the users play back alarm video.
- **Export**. Select to let the users save alarm video on local media.
- **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**.

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:
   - For cameras, you can select the direction that the camera icon points to.
   - 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.
   - 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:

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

To remove an icon from the map:

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

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 user name and a password.

User Roles

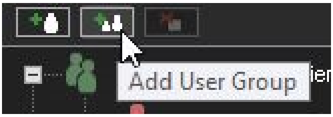
The system supports the following types of user roles (defined through user groups):

- **System Manager role:** Administrators are allowed to login 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 login 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 DEASYVIEW gateway
- **[Product version] Viewing Client role:** End users are allowed to login to Viewing Client but not to System Manager.

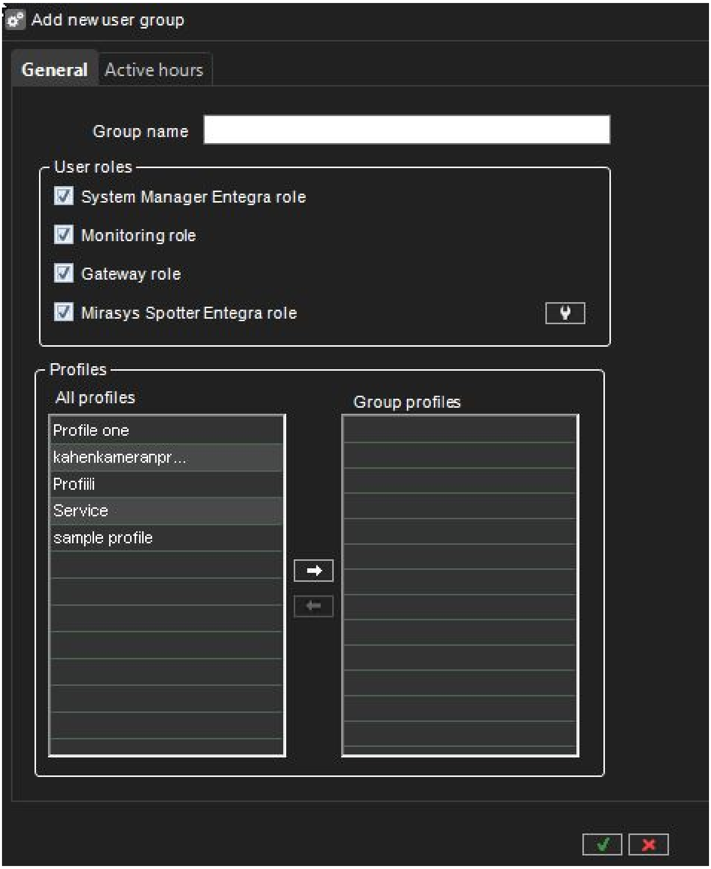
Adding New User Groups

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** dialog box is shown:



Add new user group

Group name

User roles

☑ System Manager Entegra role

☑ Monitoring role

☑ Gateway role

☑ Mirasys Spotter Entegra role

Profiles

All profiles	Group profiles
Profile one	
kahenkameranpr…	
Profiili	
Service	
sample profile	

2. Do the following:

- Type a name for the group in the **Group name** box.
- Select the user roles for the group.
- 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.

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** dialog box is shown.
4. Do the following:
   - Type a name for the account in the **User name** box.
   - To add a password to the account, click **Change password** and type the password two times.
   - Type an optional description about the user account.
   - Use the pull-down menu to select the user group into which you want to assign to the user.
   - Select the user interface language for the user.
   - 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 Viewing Client 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 Viewing Client program.

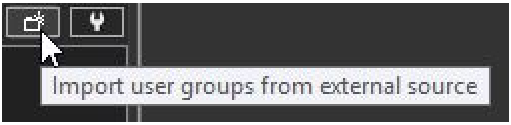
DOMAIN BASED USER GROUPS (LDAP)

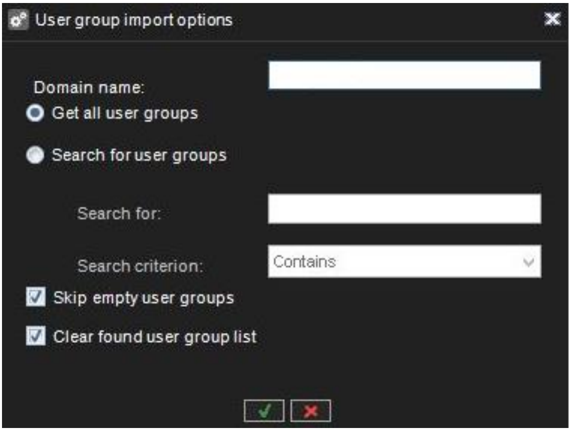
The system supports domain level user rights integration (Microsoft Active Directory, LDAP), enabling users to be synchronized from domain groups. Domain based users can log into the EASYVIEW system with their domain usernames and passwords.

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**  Import user groups from external source 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.



User group import options

Domain name:

● Get all user groups

○ Search for user groups

Search for:

Search criterion: Contains

☑ Skip empty user groups

☑ Clear found user group list

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 being equal to the group name, contained in the group name, or the group name starting or ending in the text string.
4. Select, whether to skip or include 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.

EDITING USER GROUPS

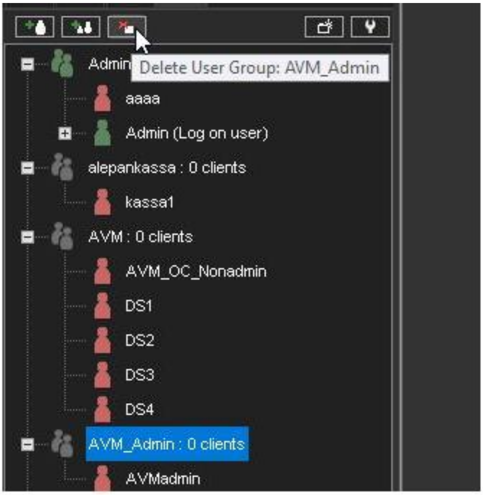
To edit a user group (whether system or domain based):

1. Open the **Users** tab.
2. Click on the user group you want to edit.
3. You can edit the following settings:
    - Type a name for the group in the **Group name** box.
    - Select the user roles for the group.
    - 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.

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.



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

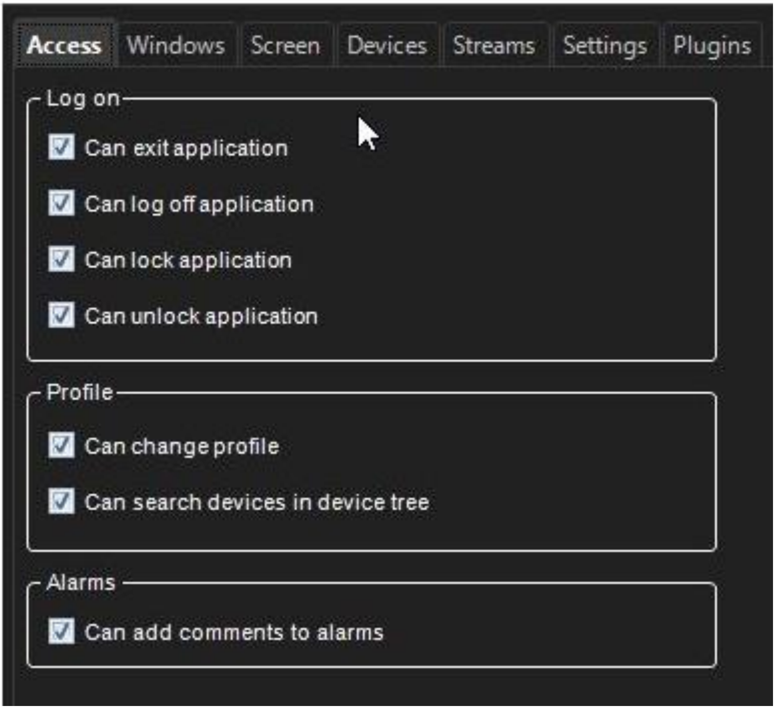
NOTE: *Domain based (LDAP) user groups cannot be deleted through System Manager. If deleted, a LDAP group is removed from System Manager but the domain group is not affected.*

VIEWING CLIENT ROLE CUSTOMIZATION

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

The **Viewing Client** custom roles can be customized with close to 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.



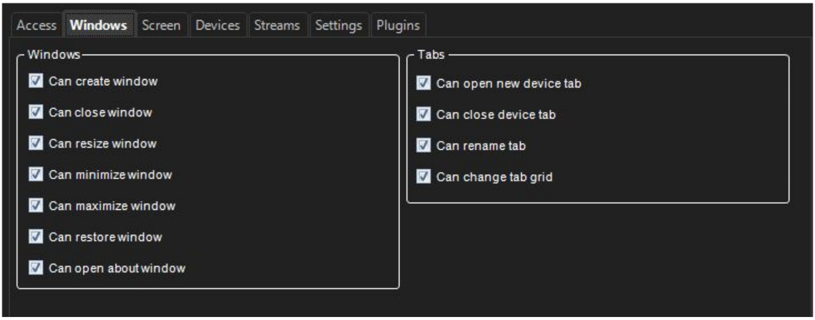
Access | Windows | Screen | Devices | Streams | Settings | Plugins

Log on
- ☑ Can exit application
- ☑ Can log off application
- ☑ Can lock application
- ☑ Can unlock application

Profile
- ☑ Can change profile
- ☑ Can search devices in device tree

Alarms
- ☑ Can add comments to alarms

The second tab contains options for Viewing Client window management and tab management.

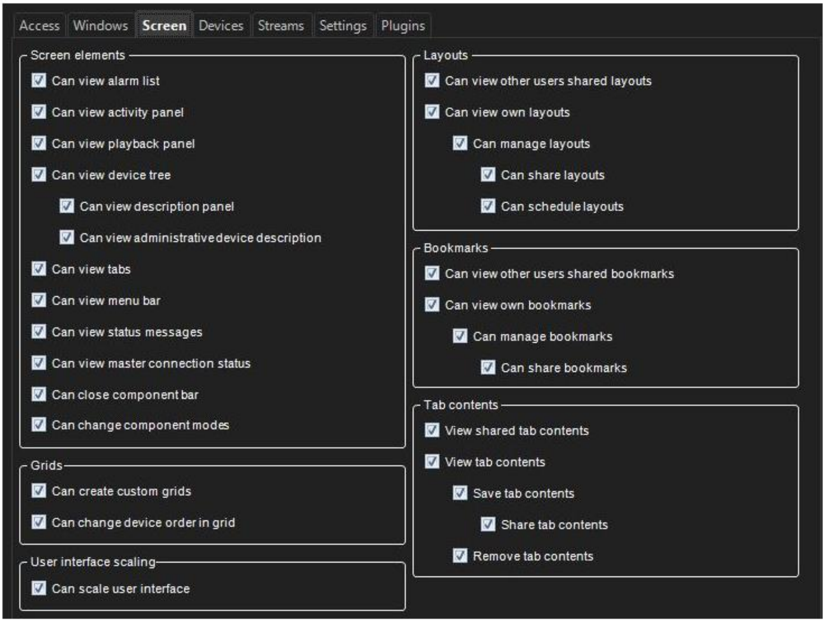


Access | Windows | Screen | Devices | Streams | Settings | Plugins

Windows
- ☑ Can create window
- ☑ Can close window
- ☑ Can resize window
- ☑ Can minimize window
- ☑ Can maximize window
- ☑ Can restore window
- ☑ Can open about window

Tabs
- ☑ Can open new device tab
- ☑ Can close device tab
- ☑ Can rename tab
- ☑ Can change tab grid

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



Screen elements

- ☑ Can view alarm list
- ☑ Can view activity panel
- ☑ Can view playback panel
- ☑ Can view device tree
  - ☑ Can view description panel
  - ☑ Can view administrative device description
- ☑ Can view tabs
- ☑ Can view menu bar
- ☑ Can view status messages
- ☑ Can view master connection status
- ☑ Can close component bar
- ☑ Can change component modes

Grids

- ☑ Can create custom grids
- ☑ Can change device order in grid

User interface scaling

- ☑ Can scale user interface

Layouts

- ☑ Can view other users shared layouts
- ☑ Can view own layouts
  - ☑ Can manage layouts
    - ☑ Can share layouts
    - ☑ Can schedule layouts

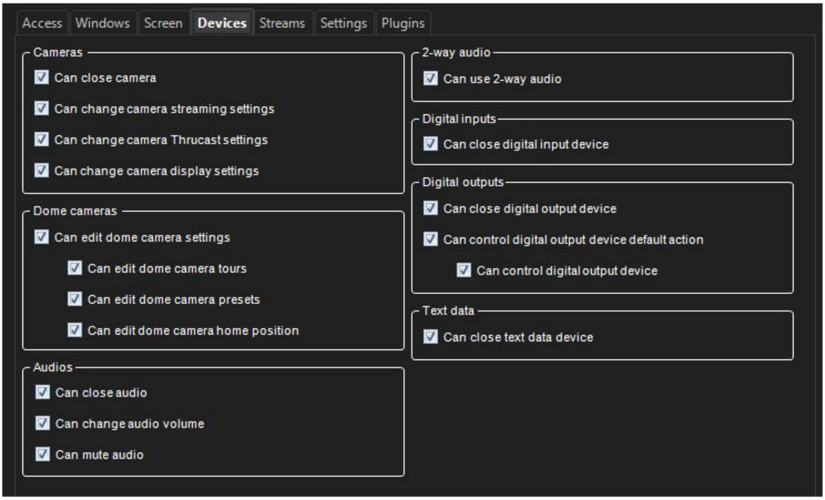
Bookmarks

- ☑ Can view other users shared bookmarks
- ☑ Can view own bookmarks
  - ☑ Can manage bookmarks
    - ☑ Can share bookmarks

Tab contents

- ☑ View shared tab contents
- ☑ View tab contents
  - ☑ Save tab contents
    - ☑ Share tab contents
  - ☑ Remove tab contents

The fourth tab contains options for media control.



Cameras

- ☑ Can close camera
- ☑ Can change camera streaming settings
- ☑ Can change camera Thrucast settings
- ☑ Can change camera display settings

Dome cameras

- ☑ Can edit dome camera settings
  - ☑ Can edit dome camera tours
  - ☑ Can edit dome camera presets
  - ☑ Can edit dome camera home position

Audios

- ☑ Can close audio
- ☑ Can change audio volume
- ☑ Can mute audio

2-way audio

- ☑ Can use 2-way audio

Digital inputs

- ☑ Can close digital input device

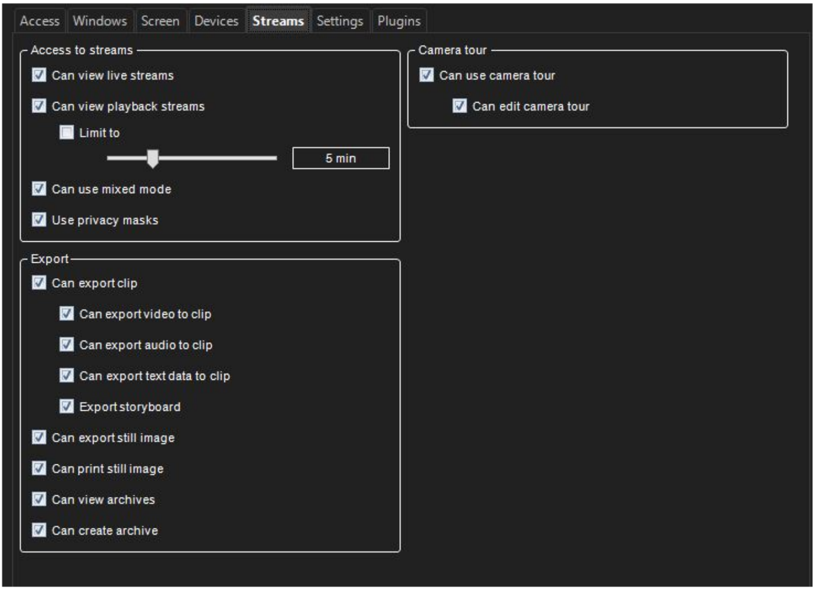
Digital outputs

- ☑ Can close digital output device
- ☑ Can control digital output device default action
  - ☑ Can control digital output device

Text data

- ☑ Can close text data device

The fifth tab contains options for stream access and exporting.



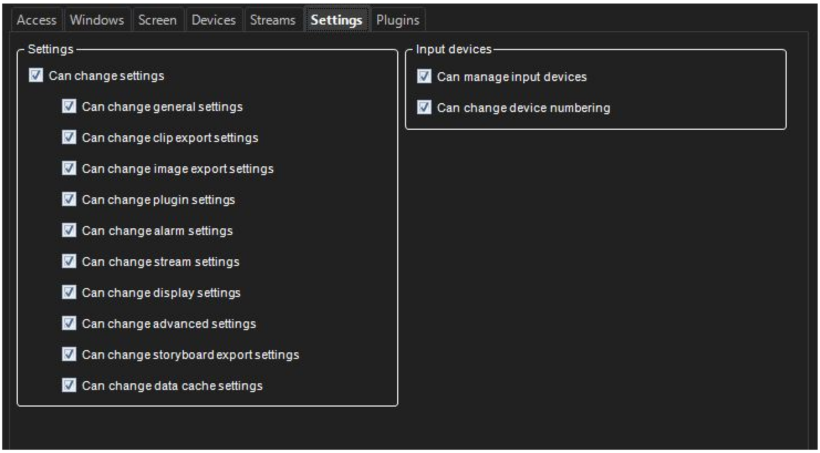
Access | Windows | Screen | Devices | **Streams** | Settings | Plugins

Access to streams
- ☑ Can view live streams
- ☑ Can view playback streams
  - □ Limit to
  - 5 min
- ☑ Can use mixed mode
- ☑ Use privacy masks

Camera tour
- ☑ Can use camera tour
  - ☑ Can edit camera tour

Export
- ☑ Can export clip
  - ☑ Can export video to clip
  - ☑ Can export audio to clip
  - ☑ Can export text data to clip
  - ☑ Export storyboard
- ☑ Can export still image
- ☑ Can print still image
- ☑ Can view archives
- ☑ Can create archive

The sixth tab contains options for Viewing Client settings.

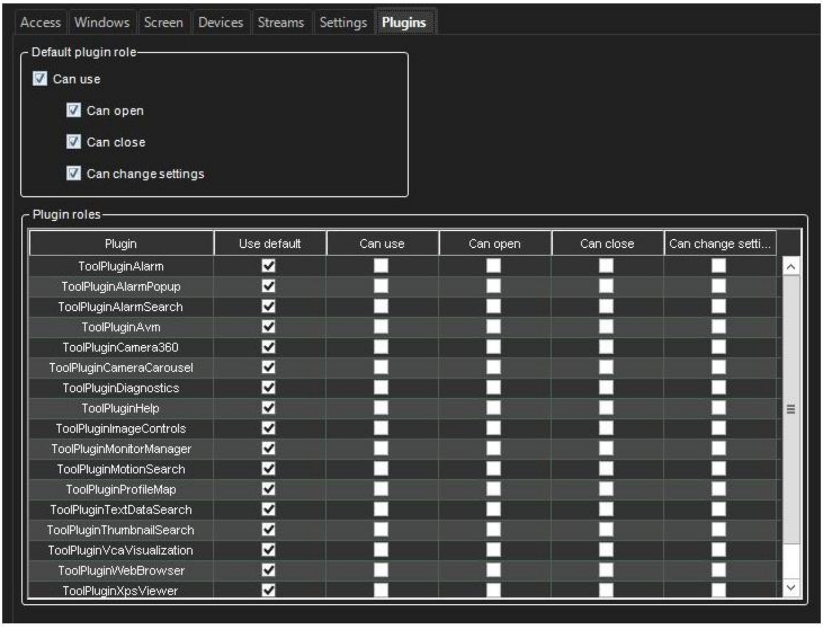


Access | Windows | Screen | Devices | Streams | **Settings** | Plugins

Settings
- ☑ Can change settings
  - ☑ Can change general settings
  - ☑ Can change clip export settings
  - ☑ Can change image export settings
  - ☑ Can change plugin settings
  - ☑ Can change alarm settings
  - ☑ Can change stream settings
  - ☑ Can change display settings
  - ☑ Can change advanced settings
  - ☑ Can change storyboard export settings
  - ☑ Can change data cache settings

Input devices
- ☑ Can manage input devices
- ☑ Can change device numbering

The final tab contains options for Viewing Client plugins.



Default plugin role

☑ Can use

☑ Can open

☑ Can close

☑ Can change settings

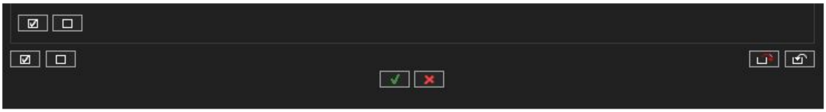
Plugin roles

Plugin	Use default	Can use	Can open	Can close	Can change setti...
ToolPluginAlarm	☑	□	□	□	□
ToolPluginAlarmPopup	☑	□	□	□	□
ToolPluginAlarmSearch	☑	□	□	□	□
ToolPluginAvm	☑	□	□	□	□
ToolPluginCamera360	☑	□	□	□	□
ToolPluginCameraCarousel	☑	□	□	□	□
ToolPluginDiagnostics	☑	□	□	□	□
ToolPluginHelp	☑	□	□	□	□
ToolPluginImageControls	☑	□	□	□	□
ToolPluginMonitorManager	☑	□	□	□	□
ToolPluginMotionSearch	☑	□	□	□	□
ToolPluginProfileMap	☑	□	□	□	□
ToolPluginTextDataSearch	☑	□	□	□	□
ToolPluginThumbnailSearch	☑	□	□	□	□
ToolPluginVcaVisualization	☑	□	□	□	□
ToolPluginWebBrowser	☑	□	□	□	□
ToolPluginXpsViewer	☑	□	□	□	□

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

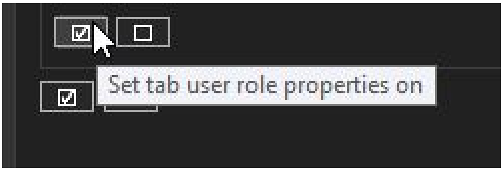
Exporting and Importing User Role Settings

There are six new buttons in the bottom of the Viewing Client user role settings window:

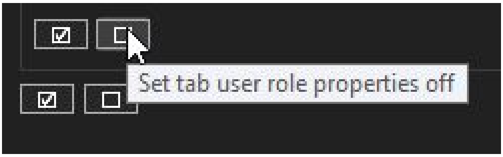


The first two buttons on the left will toggle the current user role settings tab check boxes on and off for the current settings tab.

Clicking this button



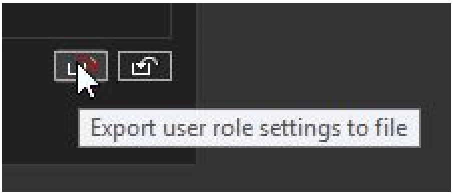
will select all the check boxes in the current tab. Clicking the button next to it will deselect them again.



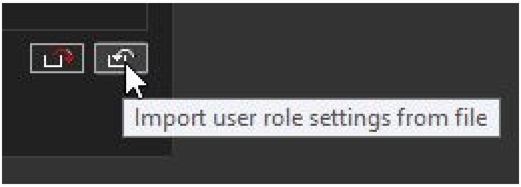
Below the tab specific select and deselect buttons are buttons to perform similar changes to all of the tabs.

These 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” (Viewing Client 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



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.

Logging Users Off

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

To log a user off:

- Right-click the user name on the **Users** tab and click **Log User Off**.

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 login 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** dialog box.

2. Do one of the following:

   - To disable the account, clear the check box **Active**.
   - To activate the account, select the check box **Active**.

3. Click **OK**.

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

SYSTEM

On the **System** tab, you can edit and back up 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 camera, metadata and client plugin drivers. In addition, you can configure the software watchdog.

The tab contains these tools:

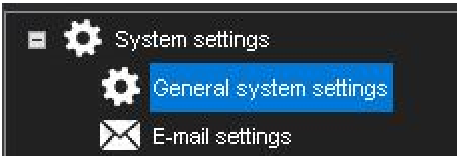
- System settings
  - General system settings
  - E-mail settings
  - Change server addresses
  - System addresses
- Update EASYVIEW Servers
- Backup
  - Export files
- Exporting log files
- Back up system settings
- Restore system settings
- Diagnostics
  - SMServer diagnostics
  - DVRServer diagnostics
- Licenses
- Software Watchdog

- Add-ins (drivers and plugins)

To open a tool, do one of the following:

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

General System Settings



In this section, you can control:

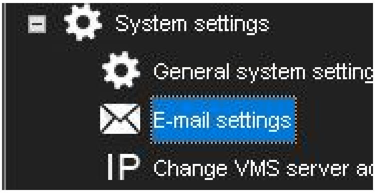
- System language
- The password mode
- Login window site selection mode
- Setting for sending motion information to clients
- Logos that are attached to exported video clips

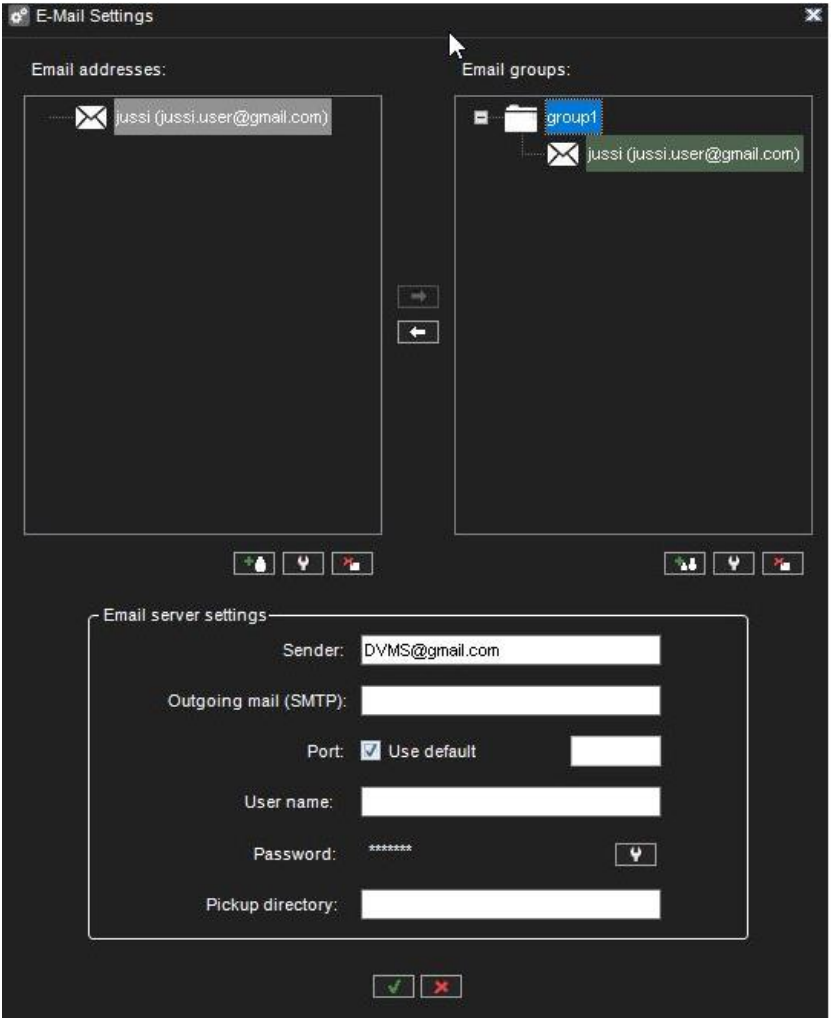
Using the System in Dual-Password Mode

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. Default second password is empty. This feature allows to limit that no single person can review videos alone. If one password is known to one person, and the other password is known to other person, then both persons need to be present when reviewing videos.

E-Mail Settings





Sender: DVMS@gmail.com

Outgoing mail (SMTP):

Port: ☑ Use default

User name:

Password: *******

Pickup directory:

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:

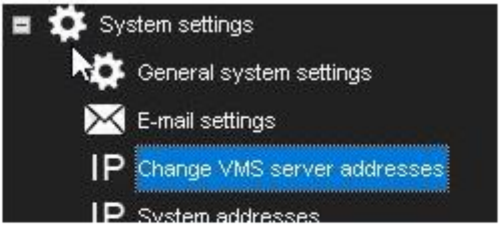
1. Highlight the desired group on the group list
2. Highlight the desired recipient(s) in the recipient list

3. click on the arrow ➡ to add the selected recipients to the selected group

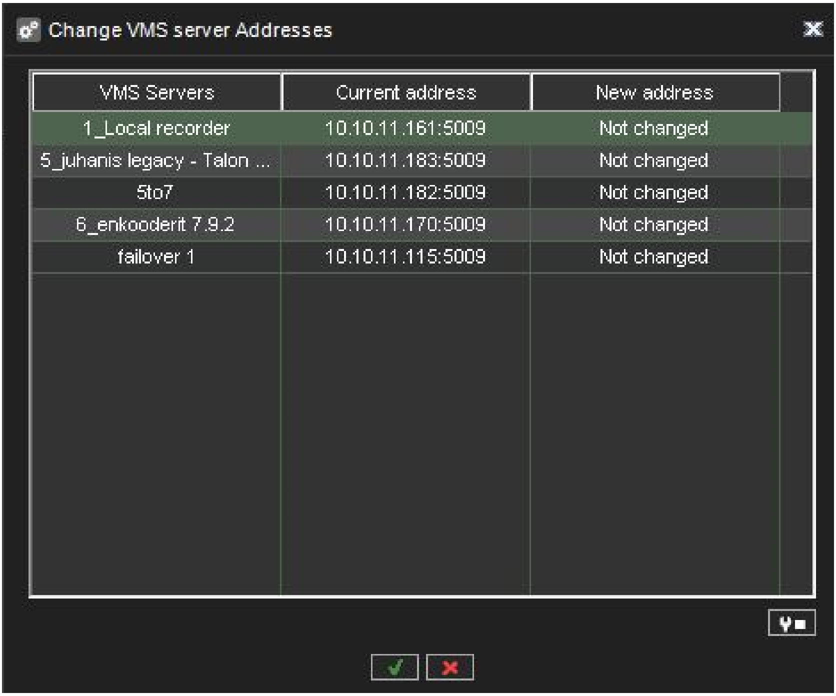
Other available actions:

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

Managing Server Addresses



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

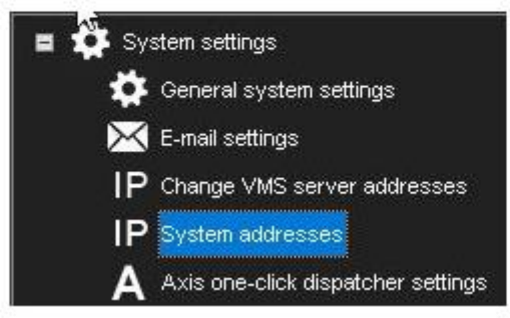


VMS Servers	Current address	New address
1_Local recorder	10.10.11.161:5009	Not changed
5_juhanis legacy - Talon ...	10.10.11.183:5009	Not changed
5to7	10.10.11.182:5009	Not changed
6_enkooderit 7.9.2	10.10.11.170:5009	Not changed
failover 1	10.10.11.115:5009	Not changed

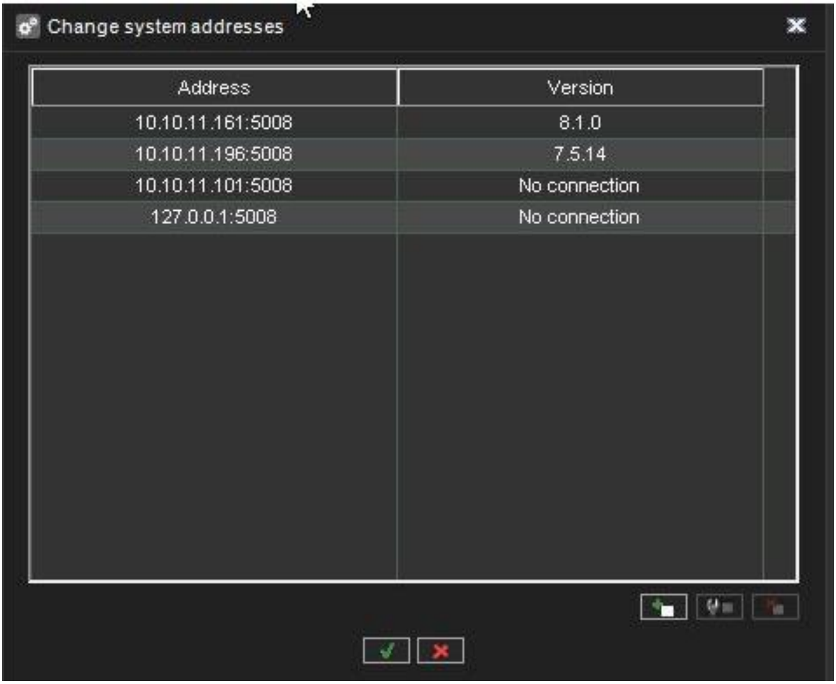
To change a server's IP address or DNS name:

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

MANAGING SYSTEM ADDRESSES (MASTER SERVER ADDRESSES)



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



Address	Version
10.10.11.161:5008	8.1.0
10.10.11.196:5008	7.5.14
10.10.11.101:5008	No connection
127.0.0.1:5008	No connection

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*).

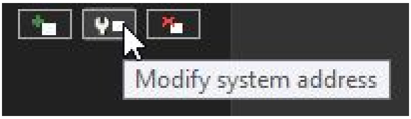
NOTE: *Users can connect to any of the defined Master Server addresses provided that they have a compatible username and password for the Master Server.*

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.

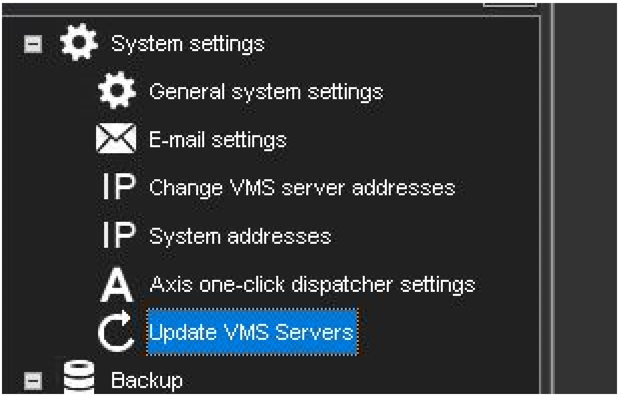


3. Click **Modify system address** .
4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

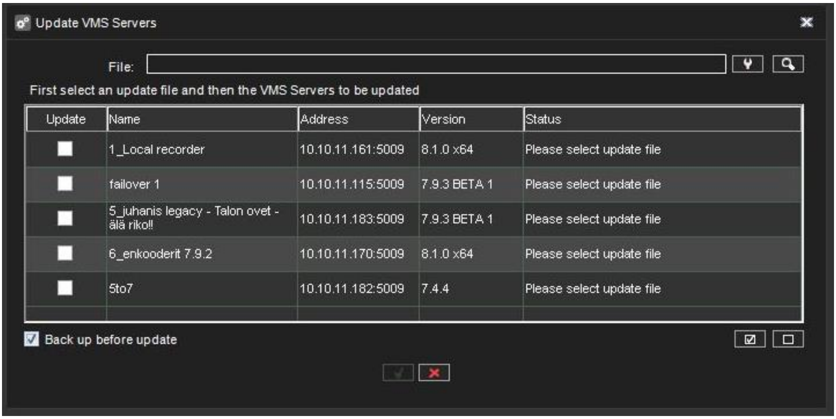
To remove a Master Server address:

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

UPDATING EASYVIEW SERVERS



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



Update VMS Servers

File:

First select an update file and then the VMS Servers to be updated

Update	Name	Address	Version	Status
□	1_Local recorder	10.10.11.161:5009	8.1.0 x64	Please select update file
□	failover 1	10.10.11.115:5009	7.9.3 BETA 1	Please select update file
□	5_juhanis legacy - Talon ovet - älä riko!!	10.10.11.183:5009	7.9.3 BETA 1	Please select update file
□	6_enkooderit 7.9.2	10.10.11.170:5009	8.1.0 x64	Please select update file
□	5to7	10.10.11.182:5009	7.4.4	Please select update file

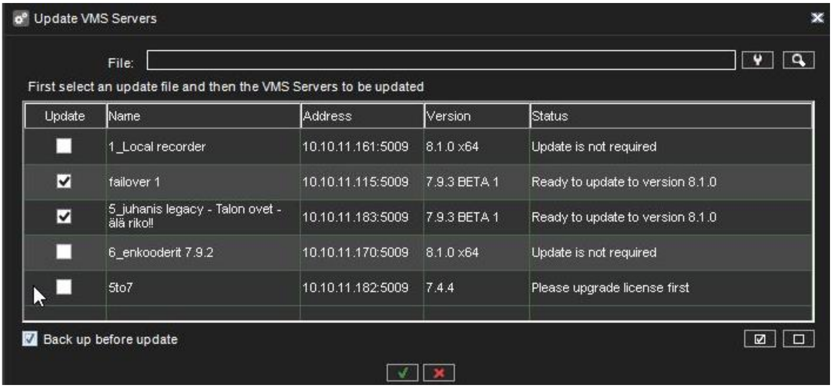
☑ Back up before update

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 EASYVIEW 6.x to 7.x, it is usually necessary to first upgrade the server licenses, and only after this upgrade the EASYVIEW software. The Update EASYVIEW Servers dialog will inform the user if license upgrade is needed before software update.*

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



Update VMS Servers

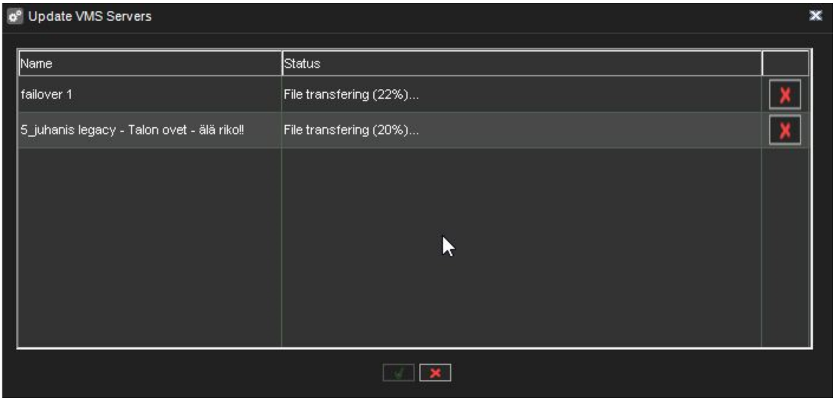
File:

First select an update file and then the VMS Servers to be updated

Update	Name	Address	Version	Status
□	1_Local recorder	10.10.11.161:5009	8.1.0 x64	Update is not required
☑	failover 1	10.10.11.115:5009	7.9.3 BETA 1	Ready to update to version 8.1.0
☑	5_juhanis legacy - Talon ovet - älä riko!!	10.10.11.183:5009	7.9.3 BETA 1	Ready to update to version 8.1.0
□	6_enkooderit 7.9.2	10.10.11.170:5009	8.1.0 x64	Update is not required
□	5to7	10.10.11.182:5009	7.4.4	Please upgrade license first

☑ Back up before update

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



Name	Status	
failover 1	File transfering (22%)...	✗
5_juhanis legacy - Talon ovet - älä riko!!	File transfering (20%)...	✗

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

NOTES:

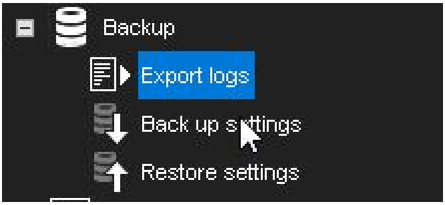
- *If network connection is slow or intermittent, the progress dialog might display no status information for the installation file transfer and update progress. This is no cause for alarm, in most cases the update will be successful, but it might take a long time (20 – 30 minutes). it is recommended to prepare for possibility to have remote access to any such servers.*

- *If a local server was selected to be updated, System manager will be automatically closed soon after this dialog is shown.*

- *In rare cases, some servers require system restart after remote EASYVIEW software update, if connection between the Master Server and EASYVIEW Server is not returning after the update. It is recommended to monitor the connection to EASYVIEW Servers after the update.*

- *Since Version 7.4.3 EASYVIEW has had support for 64-bit servers. The upgrade from 32-bit (x86) to 64-bit can be achieved in exactly same way as installing any DEASYVIEW version. After the update, the control panel of windows will show DEASYVIEW-x64 for 64-bit DEASYVIEW.*

Exporting Log Files

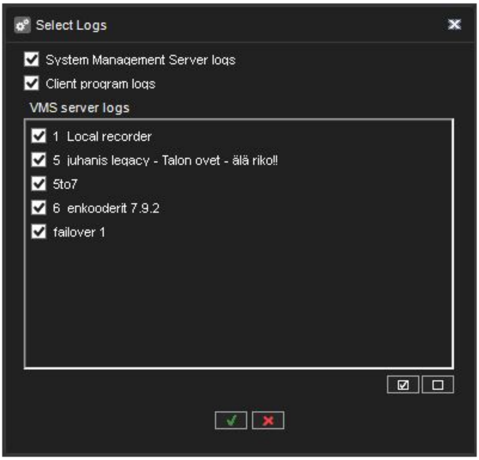


If there are problems with the system, you can export log files and send them to the system supplier.

You can save the log files to a hard disk, floppy disk, or other 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**.



Select Logs

☑ System Management Server logs
☑ Client program logs

VMS server logs

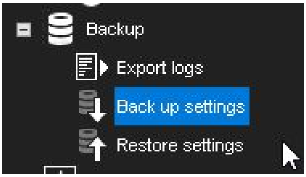
☑ 1 Local recorder
☑ 5 juhanis legacy - Talon ovet - älä riko!!
☑ 5to7
☑ 6 enkooderit 7.9.2
☑ failover 1

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.

Backing Up Settings

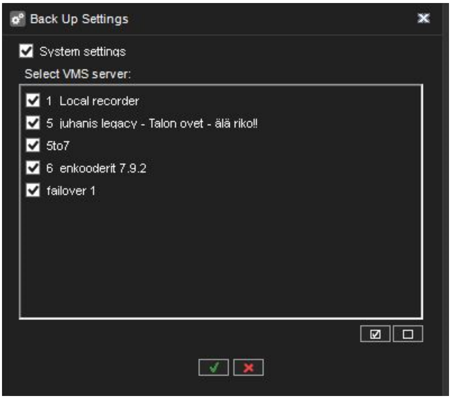


Back up system settings to be able to restore them if the hard disk that contains the settings fails. You can back up system settings and server settings. System settings contain data about the servers, profiles, and user accounts. EASYVIEW Server settings contain data about the devices connected to the servers and their parameters.

You can save the backup copy to a hard disk, network drive, CD/DVD disc, floppy disk, or other removable or non-removable device. Backup files have the file extension ".vbk".

To back up settings:

1. On the **System** tab, open **Backup settings**. The **Backup settings** dialog box is shown.



Back Up Settings

☑ System settings

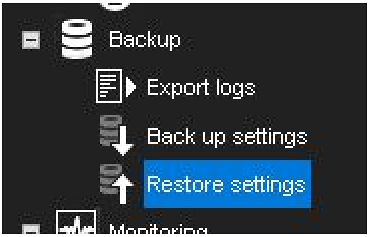
Select VMS server:

☑ 1 Local recorder
☑ 5 juhanis legacy - Talon ovet - älä riko!!
☑ 5to7
☑ 6 enkooderit 7.9.2
☑ failover 1

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.

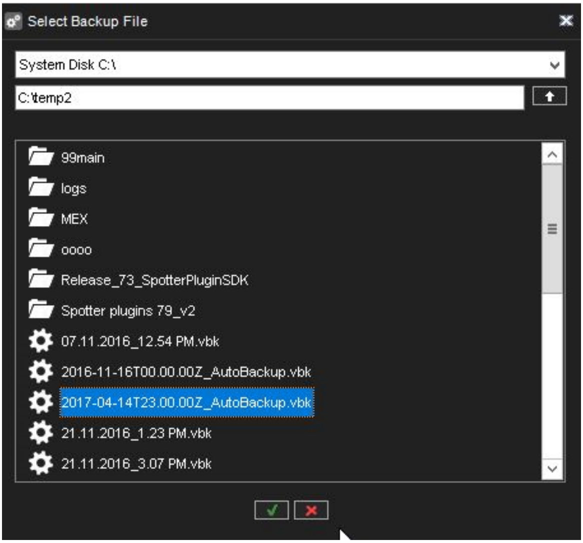
RESTORING SETTINGS



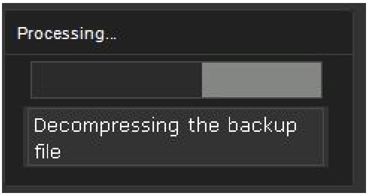
If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs.

To restore settings:

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

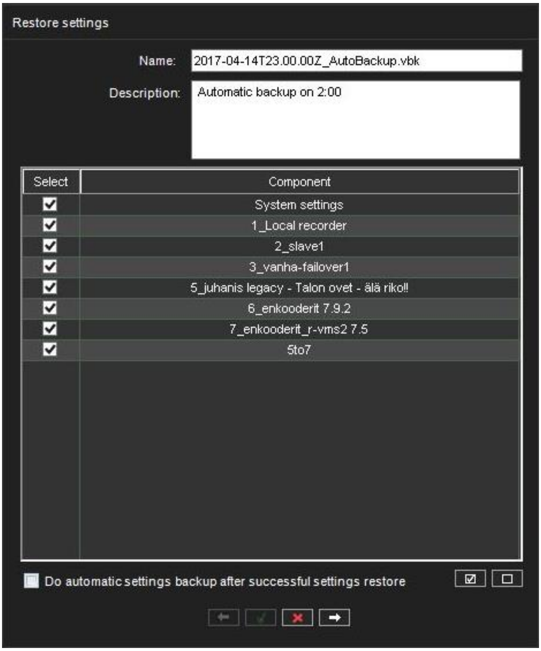


2. Find and select the backup file (.vbk) and click **OK**. The system decompresses the file and then shows the **Restore settings** dialog box. The dialog box also shows a description of the settings.



Processing...

Decompressing the backup file



Restore settings

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

Description: Automatic backup on 2:00

Select	Component
☑	System settings
☑	1_Local recorder
☑	2_slave1
☑	3_vanha-failover1
☑	5_juhanis legacy - Talon ovet - älä riko!!
☑	6_enkooderit 7.9.2
☑	7_enkooderit_r-vms2 7.5
☑	5to7

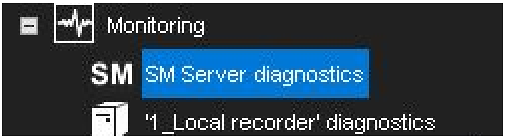
□ Do automatic settings backup after successful settings restore

3. Select the system and server specific settings that you want to restore and click **Start restore**. The settings are restored.

4. Click **OK** to accept the new settings or **Start restore process again** to return to the **Restore settings** dialog.

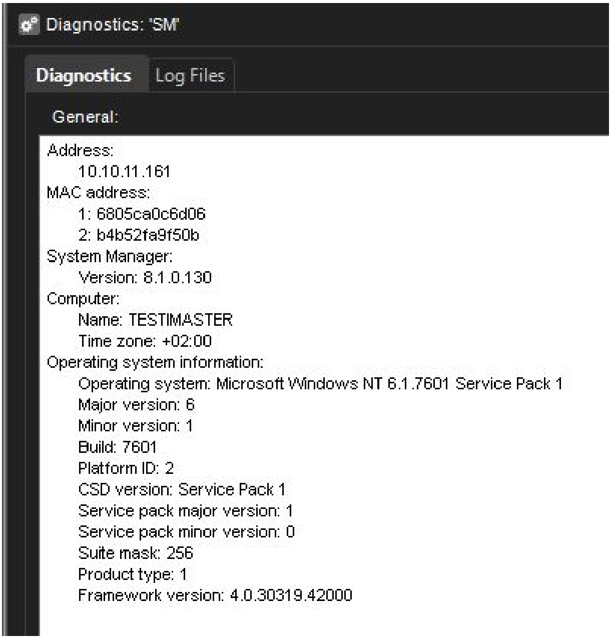
The option **Do automatic settings backup after successful settings restore** is recommended especially when restoring system after failover has happened.

System Management Diagnostics



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

General



```
Address:
      10.10.11.161
MAC address:
      1: 6805ca0c6d06
      2: b4b52fa9f50b
System Manager:
      Version: 8.1.0.130
Computer:
      Name: TESTIMASTER
      Time zone: +02:00
Operating system information:
      Operating system: Microsoft Windows NT 6.1.7601 Service Pack 1
      Major version: 6
      Minor version: 1
      Build: 7601
      Platform ID: 2
      CSD version: Service Pack 1
      Service pack major version: 1
      Service pack minor version: 0
      Suite mask: 256
      Product type: 1
      Framework version: 4.0.30319.42000
```

In SMServer Diagnostics, you can examine this information:

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

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

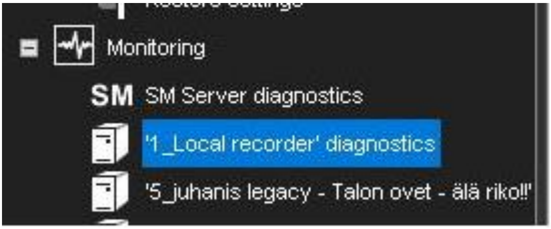
Log Files

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

To examine a log file:

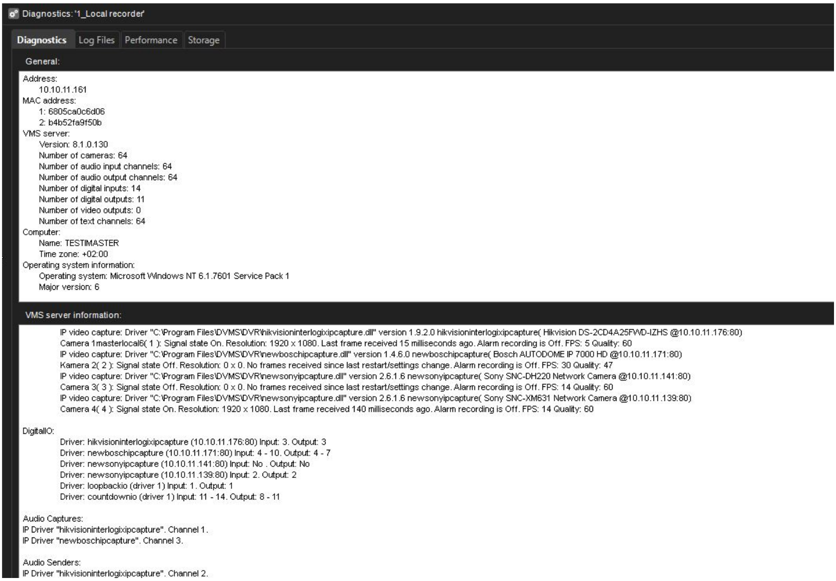
- Select the file from the drop-down list. The contents are shown in **Contents of selected log file.**

Server Diagnostics


Monitoring
SM
SM Server diagnostics
'1_Local recorder' diagnostics
'5_juhanis legacy - Talon ovet - älä riko!!'

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

DIAGNOSTICS



```
General:
Address:
    10.10.11.161
MAC address:
    1: 6805ca0c6d06
    2: b4b52fa9f50b
VMS server:
    Version: 8.1.0.130
    Number of cameras: 64
    Number of audio input channels: 64
    Number of audio output channels: 64
    Number of digital inputs: 14
    Number of digital outputs: 11
    Number of video outputs: 0
    Number of text channels: 64
Computer:
    Name: TESTIMASTER
    Time zone: +02:00
Operating system information:
    Operating system: Microsoft Windows NT 6.1.7601 Service Pack 1
    Major version: 6

VMS server information:
         IP video capture: Driver "C:\Program Files\DVMS\DVR\hikvisioninterlogixipcapture.dll" version 1.9.2.0 hikvisioninterlogixipcapture( Hikvision DS-2CD4A25FWD-IZHS @10.10.11.176:80)
         Camera 1masterlocal6( 1 ): Signal state On. Resolution: 1920 x 1080. Last frame received 15 milliseconds ago. Alarm recording is Off. FPS: 5 Quality: 60
         IP video capture: Driver "C:\Program Files\DVMS\DVR\newboschipcapture.dll" version 1.4.6.0 newboschipcapture( Bosch AUTODOME IP 7000 HD @10.10.11.171:80)
         Kamera 2( 2 ): Signal state Off. Resolution: 0 x 0. No frames received since last restart/settings change. Alarm recording is Off. FPS: 30 Quality: 47
         IP video capture: Driver "C:\Program Files\DVMS\DVR\newsonyipcapture.dll" version 2.6.1.6 newsonyipcapture( Sony SNC-DH220 Network Camera @10.10.11.141:80)
         Camera 3( 3 ): Signal state Off. Resolution: 0 x 0. No frames received since last restart/settings change. Alarm recording is Off. FPS: 14 Quality: 60
         IP video capture: Driver "C:\Program Files\DVMS\DVR\newsonyipcapture.dll" version 2.6.1.6 newsonyipcapture( Sony SNC-XM631 Network Camera @10.10.11.139:80)
         Camera 4( 4 ): Signal state On. Resolution: 1920 x 1080. Last frame received 140 milliseconds ago. Alarm recording is Off. FPS: 14 Quality: 60

DigitalIO:
         Driver: hikvisioninterlogixipcapture (10.10.11.176:80) Input: 3. Output: 3
         Driver: newboschipcapture (10.10.11.171:80) Input: 4 - 10. Output: 4 - 7
         Driver: newsonyipcapture (10.10.11.141:80) Input: No . Output: No
         Driver: newsonyipcapture (10.10.11.139:80) Input: 2. Output: 2
         Driver: loopbackio (driver 1) Input: 1. Output: 1
         Driver: countdownio (driver 1) Input: 11 - 14. Output: 8 - 11

Audio Captures:
IP Driver "hikvisioninterlogixipcapture". Channel 1.
IP Driver "newboschipcapture". Channel 3.

Audio Senders:
IP Driver "hikvisioninterlogixipcapture". Channel 2.
```

The **Diagnostics** tab shows this information:

- Information about the server:
    - Software version
    - Model
    - Number of cameras, audio channels, digital inputs, digital outputs, and video outputs
- The name of the computer and the time zone
- Operating system information
- Processor information
- Installed drivers, for example, capture drivers, video output drivers, digital output drivers, and PTZ drivers.

LOG FILES

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

To see the contents of a log file:

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

PERFORMANCE

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

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

STORAGE

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

EASYVIEW Server up time. 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 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 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 store.

Newest time. The date and time of the newest image in store.

Total no. of images. The total number of images in 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.

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.

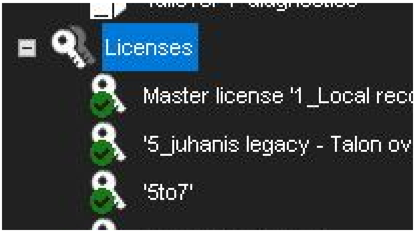
Total number of samples. The total number of text data samples in store.

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.

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.

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 dialog box, copy the MAC address and either:
    - Purchase a license key from your supplier
    - Or send the MAC address to your supplier,

   In return, you will receive the license key as a text file.
3. After getting your license file:

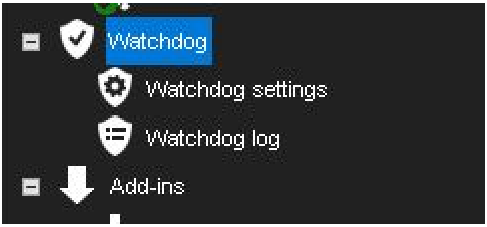
   In the License Information dialog box, click **Import license from file**.
4. Click **OK**. The system is updated immediately.

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 clipboard** to copy the key to 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 clipboard. This allows users to fetch the VCA license without starting the VCA Configurator.

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 EASYVIEW 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 **EASYVIEW Server** drop-down list.

To set a digital output notification:

1. On the **System** tab, select **Watchdog settings**.
2. Select a server from the **EASYVIEW Server** drop-down list. As digital output signals are server-specific, you cannot select **All EASYVIEW 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\DEASYVIEW\DVR\WDEventProviders\

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

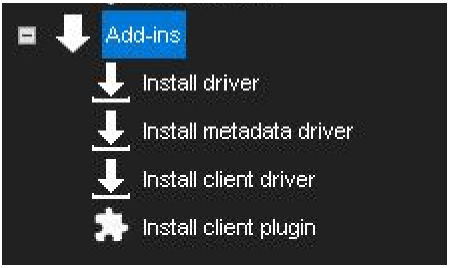
At the moment, these files need to be edited manually. Each XML file contains the documentation regarding the configuration options.

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.

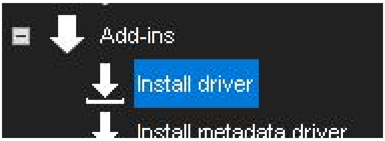
After the files have been edited, Watchdog needs to be restarted for the changes to take effect.

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.*

INSTALLING NEW DRIVERS AND PLUGINS



INSTALLING EXTERNAL DRIVER PACKAGES



To be able to use IP cameras, digital I/O devices or text data in the EASYVIEW 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.

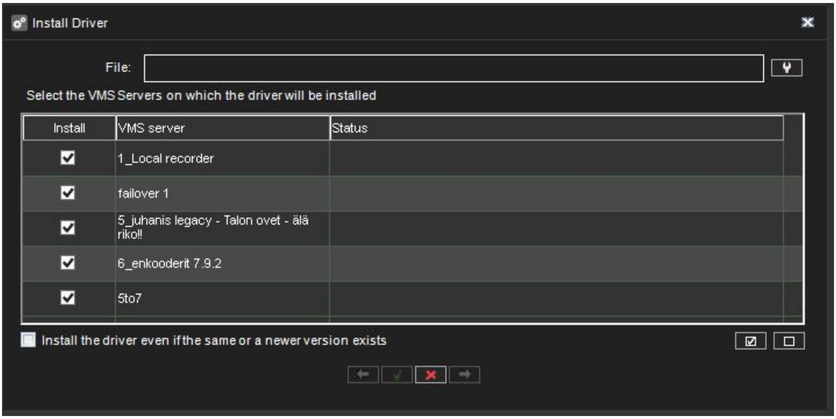
When installing a driver installation package, the system compares the files in the installation package to the existing files on the servers. It usually installs the files only if they do not exist on the servers, or if the files in the installation package are newer than the files on the servers. However, 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, and find and select the driver package (.zip file). The **Install Driver** dialog box is shown.



Install Driver

File:

Select the VMS Servers on which the driver will be installed

Install	VMS server	Status
☑	1_Local recorder	
☑	failover 1	
☑	5_juhanis legacy - Talon ovet - älä rikoI!	
☑	6_enkooderit 7.9.2	
☑	5to7	

☐ Install the driver even if the same or a newer version exists

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 dialog 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.*

Installing Metadata Drivers

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

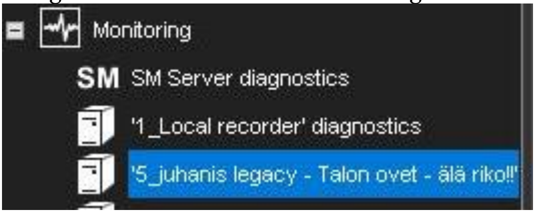
Installing Client Drivers

TruCast (direct streaming from camera to Viewing Client client) requires different type of camera driver. These are called (Managed) TruCast Client drivers.

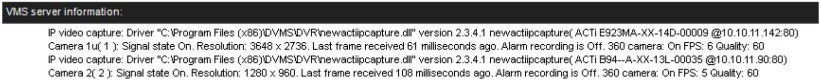
The client camera drivers are installed in similar way as Viewing Client plugins and metadata drivers, using the **Install client driver** option in system manager.

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 EASYVIEW Server* diagnostics


Monitoring
SM
SM Server diagnostics
'1_Local recorder' diagnostics
'5_juhanis legacy - Talon ovet - älä rikol!'

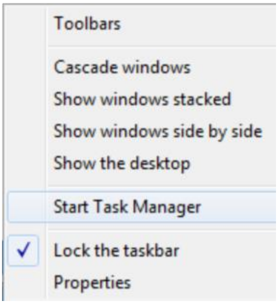
        i. All cameras using the same driver are grouped together in the Diagnostics screen
        ii. Device paths for the driver .DLL files are written in the diagnostic



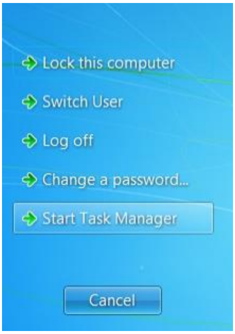
```
VMS server information:
    IP video capture: Driver "C:\Program Files (x86)\DVMS\DVR\newactiipcapture.dll" version 2.3.4.1 newactiipcapture( ACTi E923MA-XX-14D-00009 @10.10.11.142:80)
    Camera 1u( 1 ): Signal state On. Resolution: 3648 x 2736. Last frame received 61 milliseconds ago. Alarm recording is Off. 360 camera: On FPS: 6 Quality: 60
    IP video capture: Driver "C:\Program Files (x86)\DVMS\DVR\newactiipcapture.dll" version 2.3.4.1 newactiipcapture( ACTi B94--A-XX-13L-00035 @10.10.11.90:80)
    Camera 2( 2 ): Signal state On. Resolution: 1280 x 960. Last frame received 108 milliseconds ago. Alarm recording is Off. 360 camera: On FPS: 5 Quality: 60
```

    b) The instructions for camera removal can be found in the chapter *Cameras*, subchapter *Adding and Removing IP Cameras*, page 32
3. Shut down the recording service (DVRServer process)
    a) Open the Task manager

i. Open by right-clicking the taskbar and select Start Task Manager



ii. 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.

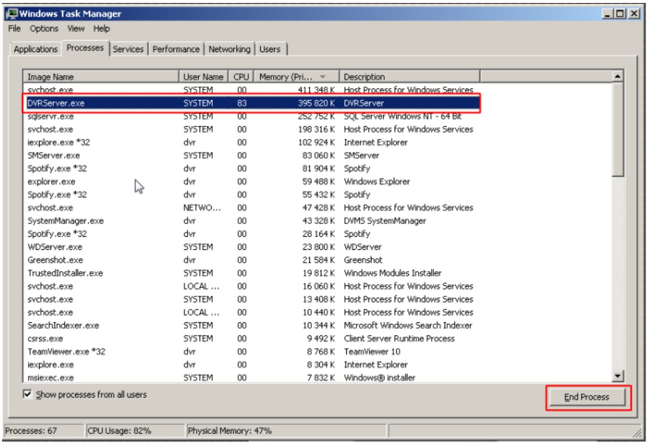

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

Image Name	User Name	CPU	Memory (Pri...	Description
svchost.exe	SYSTEM	00	411 348 K	Host Process for Windows Services
DVRServer.exe	SYSTEM	83	395 820 K	DVRServer
sqlservr.exe	SYSTEM	00	252 752 K	SQL Server Windows NT - 64 Bit
svchost.exe	SYSTEM	00	198 316 K	Host Process for Windows Services
iexplore.exe *32	dvr	00	102 924 K	Internet Explorer
SMServer.exe	SYSTEM	00	83 060 K	SMServer
Spotify.exe *32	dvr	00	81 904 K	Spotify
explorer.exe	dvr	00	59 488 K	Windows Explorer
Spotify.exe *32	dvr	00	55 432 K	Spotify
svchost.exe	NETWO...	00	47 428 K	Host Process for Windows Services
SystemManager.exe	dvr	00	43 328 K	DVMS SystemManager
Spotify.exe *32	dvr	00	28 164 K	Spotify
WDServer.exe	SYSTEM	00	23 800 K	WDServer
Greenshot.exe	dvr	00	21 584 K	Greenshot
TrustedInstaller.exe	SYSTEM	00	19 812 K	Windows Modules Installer
svchost.exe	LOCAL ...	00	16 060 K	Host Process for Windows Services
svchost.exe	SYSTEM	00	13 408 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	10 440 K	Host Process for Windows Services
SearchIndexer.exe	SYSTEM	00	10 344 K	Microsoft Windows Search Indexer
csrss.exe	SYSTEM	00	9 492 K	Client Server Runtime Process
TeamViewer.exe *32	dvr	00	8 768 K	TeamViewer 10
iexplore.exe	dvr	00	8 304 K	Internet Explorer
msiexec.exe	SYSTEM	00	7 832 K	Windows® installer

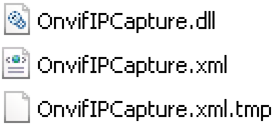
☑ Show processes from all users

Processes: 67 CPU Usage: 82% Physical Memory: 47%

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\DEASYVIEW\DVR\ of the server's main hard drive

b) Drivers create three files, the driver .dll, an .xml file and a temporary file for the .xml

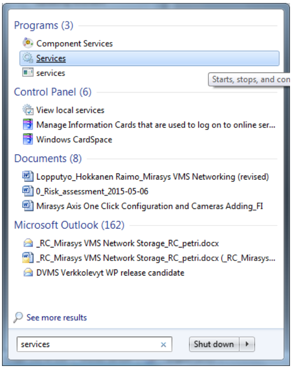


OnvifIPCapture.dll
OnvifIPCapture.xml
OnvifIPCapture.xml.tmp

5. Restart the recording service

a) Open the Services program

i. Open the Start Menu and type in "services" in the search bar



Programs (3)
Component Services
Services
services
Starts, stops, and con

Control Panel (6)
View local services
Manage Information Cards that are used to log on to online ser...
Windows CardSpace

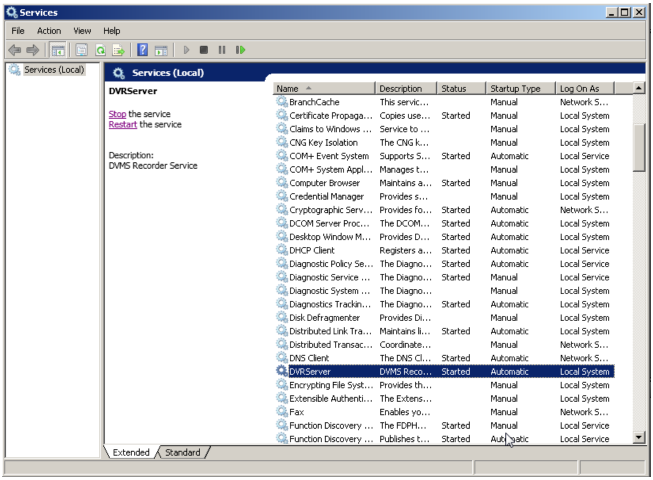
Documents (8)
Lopputyo_Hokkanen Raimo_Mirasys VMS Networking (revised)
0_Risk_assessment_2015-05-06
Mirasys Axis One Click Configuration and Cameras Adding_FI

Microsoft Outlook (162)
_RC_Mirasys VMS Network Storage_RC_petri.docx
_RC_Mirasys VMS Network Storage_RC_petri.docx (_RC_Mirasys...
DVMS Verkkolevyt WP release candidate

See more results

services

b) Browse to the DVRServer service



DVRServer

Stop the service
Restart the service

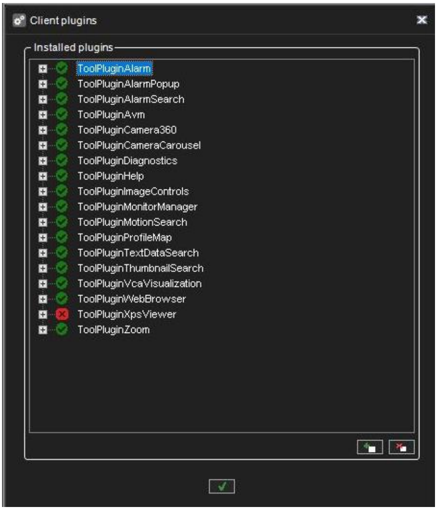
Description:
DVMS Recorder Service

Name	Description	Status	Startup Type	Log On As
BranchCache	This servic...		Manual	Network S...
Certificate Propaga...	Copies use...	Started	Manual	Local System
Claims to Windows ...	Service to ...		Manual	Local System
CNG Key Isolation	The CNG k...		Manual	Local System
COM+ Event System	Supports S...	Started	Automatic	Local Service
COM+ System Appl...	Manages t...		Manual	Local System
Computer Browser	Maintains a...	Started	Manual	Local System
Credential Manager	Provides s...		Manual	Local System
Cryptographic Serv...	Provides fo...	Started	Automatic	Network S...
DCOM Server Proc...	The DCOM...	Started	Automatic	Local System
Desktop Window M...	Provides D...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Local Service
Diagnostic Policy Se...	The Diagno...	Started	Automatic	Local Service
Diagnostic Service ...	The Diagno...	Started	Manual	Local Service
Diagnostic System ...	The Diagno...		Manual	Local System
Diagnostics Trackin...	The Diagno...	Started	Automatic	Local System
Disk Defragmenter	Provides Di...		Manual	Local System
Distributed Link Tra...	Maintains li...	Started	Automatic	Local System
Distributed Transac...	Coordinate...		Manual	Network S...
DNS Client	The DNS Cl...	Started	Automatic	Network S...
DVRServer	DVMS Reco...	Started	Automatic	Local System
Encrypting File Syst...	Provides th...		Manual	Local System
Extensible Authenti...	The Extens...		Manual	Local System
Fax	Enables yo...		Manual	Network S...
Function Discovery ...	The FDPH...	Started	Manual	Local Service
Function Discovery ...	Publishes t...	Started	Automatic	Local Service

c) Right-click the DVRServer service and select "Start"

INSTALLING VIEWING CLIENT PLUGINS

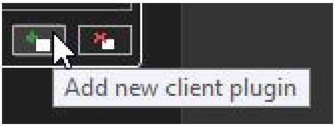
Client plugins for user interfaces such as Viewing Client can be installed through System Manager. Plugin installation can be opened from system tab under Add-ins.



- ToolPluginAlarm
- ToolPluginAlarmPopup
- ToolPluginAlarmSearch
- ToolPluginAvm
- ToolPluginCamera360
- ToolPluginCameraCarousel
- ToolPluginDiagnostics
- ToolPluginHelp
- ToolPluginImageControls
- ToolPluginMonitorManager
- ToolPluginMotionSearch
- ToolPluginProfileMap
- ToolPluginTextDataSearch
- ToolPluginThumbnailSearch
- ToolPluginVcaVisualization
- ToolPluginWebBrowser
- ToolPluginXpsViewer
- ToolPluginZoom

To install a client plugin:

1. On the **System** tab, under **Add-ins**, open **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** dialog 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 Viewing Client user interface.

To remove a client plugin:

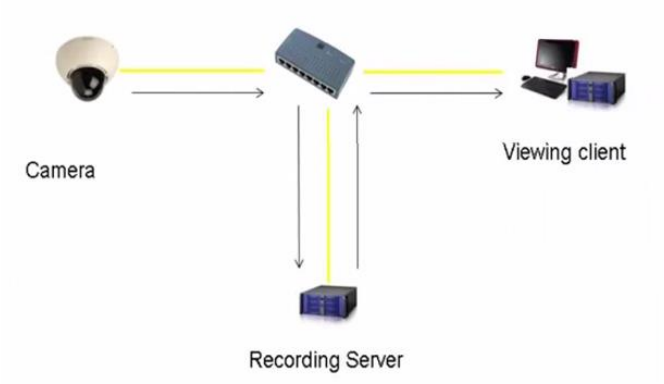
1. On the **System** tab, under Add-ins, open **Install client plugin**.
2. In the plugin installation window, select **Remove client plugin**.

TRUCAST

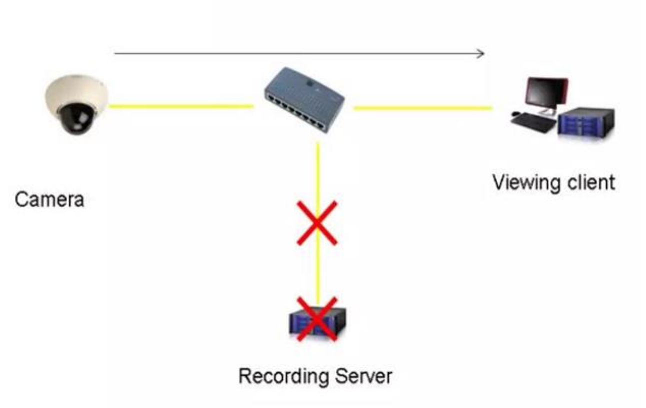
TruCast is the direct camera video streaming feature in EASYVIEW.

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

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



If the connection to the EASYVIEW 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 EASYVIEW Server connection is OK. This can be useful if users want to optimize network utilization.

Supported Cameras

TruCast requires a separate camera capture driver for the client.

Currently, drivers exist for following camera manufacturers:

- ACTi,
- Axis,
- Bosch,
- Dahua,
- Hikvision,
- Lilin,
- Samsung,
- Sony,
- Stanley and
- Ernitec and others via ONVIF

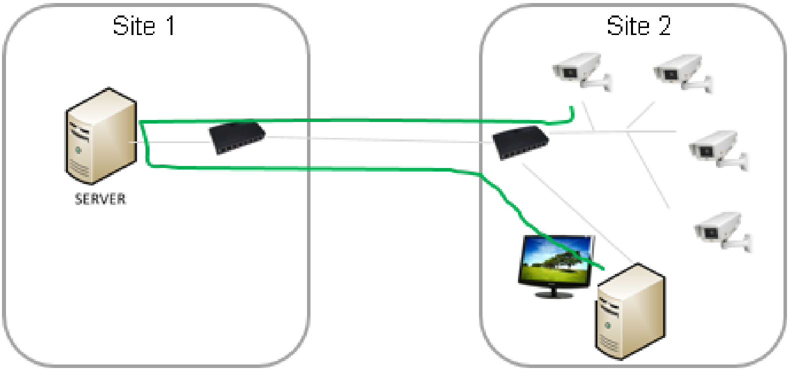
Use the ONVIF TruCast driver for cameras that are not on the supported list.

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

Network Optimization

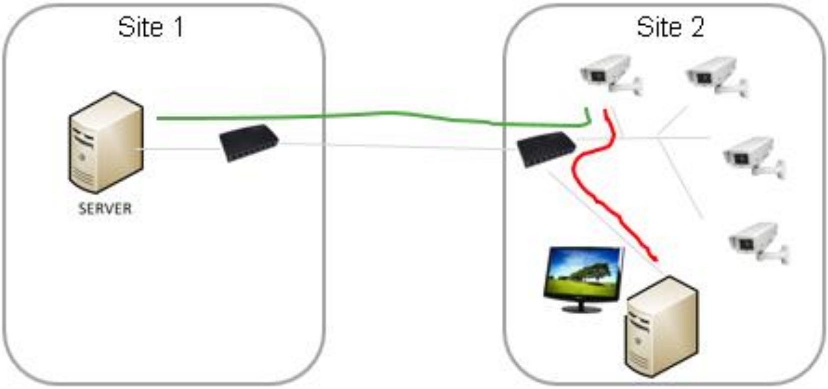
TruCast can be used to reduce network load in specific scenarios. Mainly the load reduction takes place when the server is located off-site (remote), and the viewing client is on-site (local to the cameras).

In the 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.



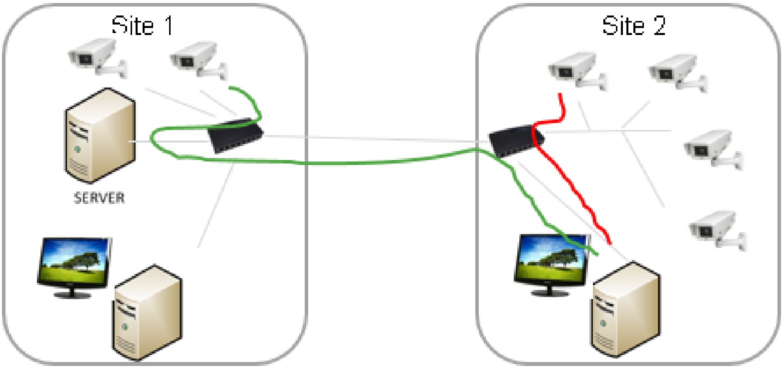
In this solution, the traffic between the two sites is increased.

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

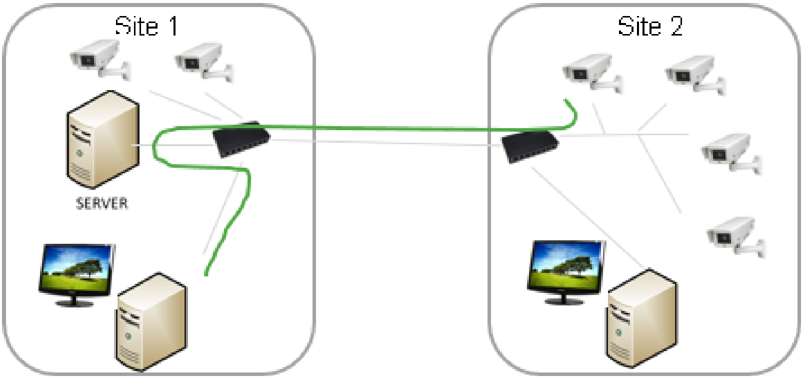


In the example scenario 2, there are cameras on two sites and viewing clients on two sites.

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 on 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 Viewing Client layouts.

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 lower framerate (for example 8 fps). This reduces the storage and network requirements considerably.

OTHER INFORMATION

IMPACT OF TRUCAST TO IMAGE DELAY

Since the TruCast stream does not travel to the EASYVIEW 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 EASYVIEW 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 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.

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. They are named with the ".sdi" file name 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 Viewing Client clients. This is done when Viewing Client is restarted from desktop.

After Viewing Client has downloaded the new drivers, the system is ready for TruCast use.

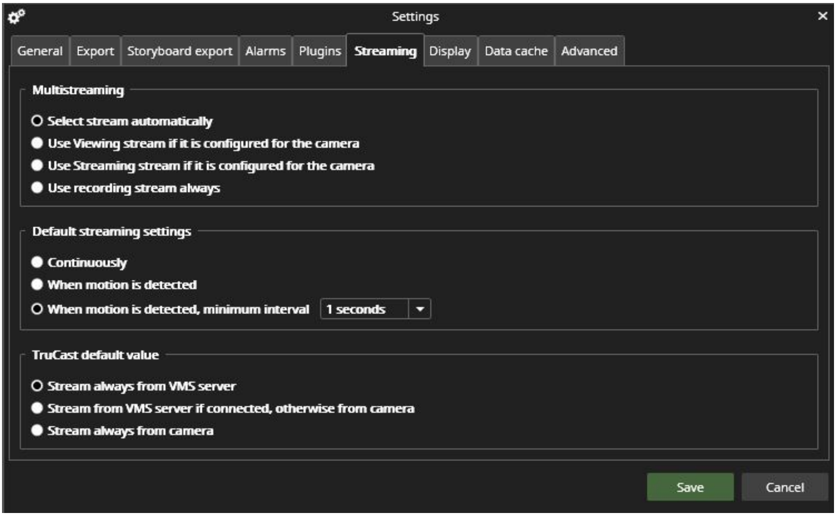
Please note that only those cameras which' client driver was installed will appear as TruCast enabled.

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 Viewing Client 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.



Multistreaming

○ Select stream automatically
● Use Viewing stream if it is configured for the camera
● Use Streaming stream if it is configured for the camera
● Use recording stream always

Default streaming settings

● Continuously
● When motion is detected
○ When motion is detected, minimum interval 1 seconds

TruCast default value

○ Stream always from VMS server
● Stream from VMS server if connected, otherwise from camera
● Stream always from camera

TruCast Default Setting

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

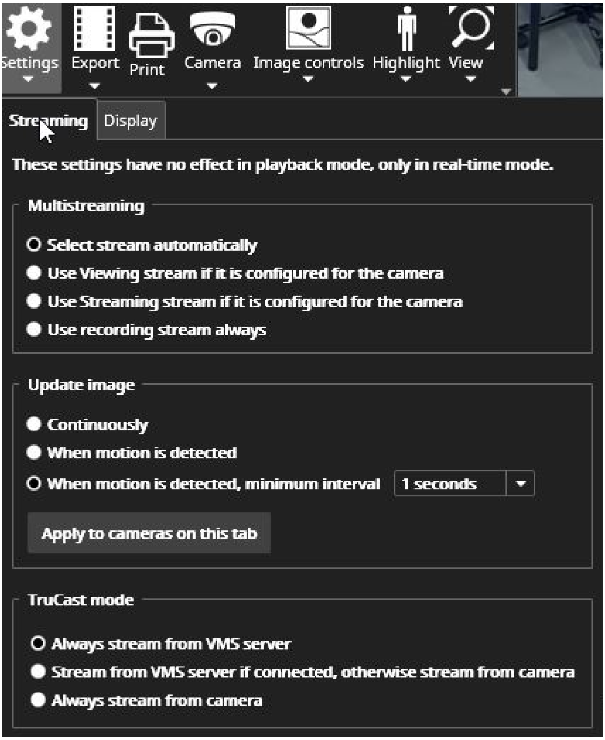
The possible values are

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

Using TruCast

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

For those cameras that have TruCast the setting is available.



These settings have no effect in playback mode, only in real-time mode.

Multistreaming

○ Select stream automatically
● Use Viewing stream if it is configured for the camera
● Use Streaming stream if it is configured for the camera
● Use recording stream always

Update image

● Continuously
● When motion is detected
○ When motion is detected, minimum interval 1 seconds

Apply to cameras on this tab

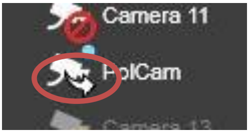
TruCast mode

○ Always stream from VMS server
● Stream from VMS server if connected, otherwise stream from camera
● Always stream from camera

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.


Camera 11
PolCam
Camera 13