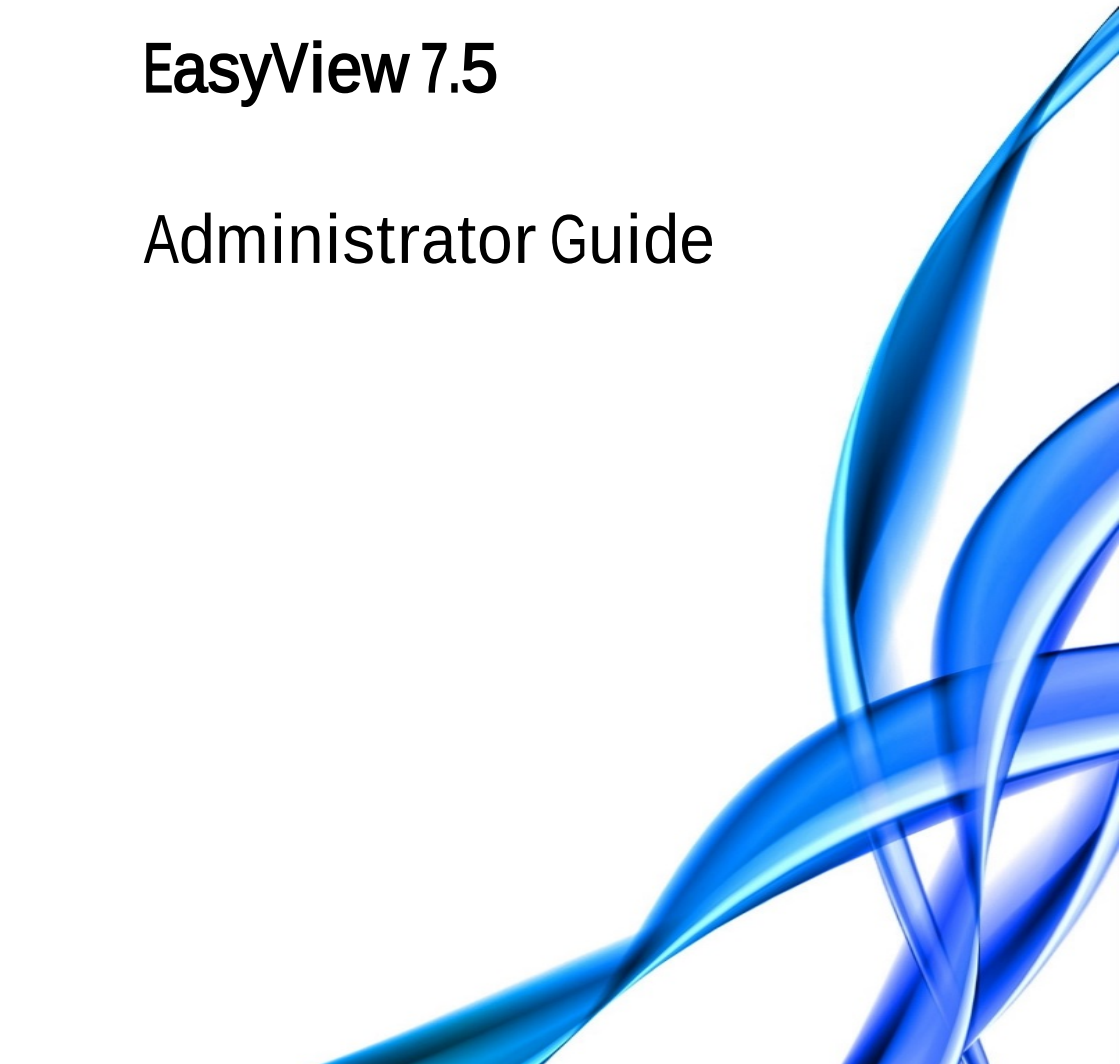
ernitec

EasyView 7.5

Administrator Guide



CONTENTS

Before You Start **6**
Help Documentation 6
Overview of This Guide 6
Technical Support 7
What's New In 7.5 7
About the System **8**
What is Ernitec Software? 8
License Types 11
OS Compatibility 13
Configuring the System **14**
Logging In **16**
Using the System in Dual-Password Mode 18
Locking System Manager 20
Management User Interface **21**
Recorders **23**
Adding and Removing Recorders 23
Configuring Recorders 24
General Settings 25
Failover Servers **27**
Failover Functionality 27
Failover Licensing 28
An Example Redundant Architecture With Failover 29
Recording Servers (Normal, Failover, Broken) 29
Failover Servers in System Manager 30
Adding and Removing Failover Servers 32
Port Forwarding **33**

Automatic Router Configuration 33
Single Recorder Behind Router 34
More Than One Server Behind Router 35
More Than One Server On Multiple Sites 38
Cameras 39
Adding and Removing Analog Cameras 39
Adding and Removing IP Cameras 39
Limiting the Camera Configuration to Certain Camera Drivers 42
Click Remove Selected Editing Camera Settings 43
Motion Detection 47
Video Content Analytics 51
Privacy Zones 53
Scheduler (Video) 55
Multi-Streaming 56
Remote Workstation 57
Edge Storage 58
Multi-Casting 59
Audio 61
Adding, Editing and Removing Audio Devices 61
Audio Settings 62
General Settings 62
Audio Detection 63
Scheduler (Audio) 65
Audio Communication Hardware Settings 66
Audio Communication Settings 67
Digital I/O 68
Digital I/O Settings 68
Logical I/O 70
Video Outputs 77

Video Output Settings 77
Alarms 80
Alarm Settings 80
Accessing the Alarm List 80
Adding a New Alarm 80
Editing an Alarm 83
Deleting an Alarm 83
Action Types and Settings 84
Holiday Schedules 91
Storage 93
Storage Settings 93
Adding Storage Space 93
Storage Settings 95
Automatic Deletion of Video, Audio and Text Data 96
Archiving 97
Text Channels 99
Text Channel Settings 99
Profiles 101
Adding and Editing Profiles 102
Adding Device Groups and Devices to a Profile 103
Editing Profile Specific Alarm Settings 105
Adding Maps to Profiles 107
Users 109
User Roles 109
Adding New User Groups 115
Domain Based User Groups (LDAP) 115
Editing User Groups 116
Deleting User Groups 117
Adding New Users 117

Monitoring Users 118
Logging Users Off 118
Disabling or Activating a User Account 119
System 120
General System Settings 122
E-Mail Settings 123
Managing Recorder Addresses 125
Managing System Addresses (Master Server Addresses) 125
Updating Recording Servers 126
Exporting Log Files 128
Backing Up Settings 129
Restoring Settings 129
System Management Diagnostics 130
Recorder Diagnostics 131
Licenses 133
Software Watchdog 135
Installing New Drivers and Plugins 138
Installing External Driver Packages 138
Installing Metadata Drivers 139
Installing Client Drivers 139
Removing Drivers 139
Installing EasyView Plugins 142
ThruCast 144
Supported cameras 145
Network Optimization 145
Impact of Multistreaming and ThruCast for Network Optimization and Storage 148
Other Information 148
Configuration 149
Using ThruCast 151

BEFORE YOU START

Ernitec VMS software is a distributed, digital video management system (EASYVIEW) 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 dome 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 (DVR), digital (NVR) or hybrid (consisting of both analog and digital) surveillance systems.

HELP DOCUMENTATION

This help documentation, for example, is available:

- *Installation Guide*: Shows how to install the recorders and the client programs. It also shows how to add devices to the system, for example, IP cameras, dome cameras, and video matrices.
- *Administrator's Guide*: Shows how to use the System Manager program for configuring the system.
- *EasyView User Guide*: Complete instruction how to operate all features of Ernitec EasyView program. (Not available in all languages.)
- *VCA Installation and Configuration Guide:* Instructions how to install and configure Ernitec Video Content Analytics.

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

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

OVERVIEW OF THIS GUIDE

This guide is intended for those who set up a Ernitec system. It shows how to add recorders 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 the system supplier.

WHAT'S NEW IN 7.5

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

New features in version 7.5

- Installer installs also SQL Express to 64-bit windows machines
- EasyView user role can be exported and imported

The following new features are documented in the EasyView User Guide

- Storyboard
- Custom camera grids
- Profile Maps can react to alarms by switching view
- Tab plugins can exist in camera grid cell
- Layouts can be loaded from user lock or login
- Camera grid zero bezel border
- Fast bookmarking

ABOUT THE SYSTEM

WHAT IS ERNITEC SOFTWARE?

Ernitec software is a distributed, digital video management system (VMS or EASYVIEW) 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 dome (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 (DVR), digital (NVR) or hybrid (consisting of both analog and digital) surveillance systems.

A centralized surveillance system can consist of up to 150 local or remote recorders.

Ernitec software is sold both separately and as part of Ernitec video management systems consisting of both the software and the recorder hardware. Please contact your Ernitec supplier for information on Ernitec software or hardware.

WHAT DOES A SYSTEM CONTAIN?

The Ernitec system consists of these components:

- 1-150 Recording Servers
    - **Master Recorder** (one of the recorders, or the only recorder in a single-server environment)
    - **Slave Recorders** ("nodes", if the system consists of multiple recorders)
- Client programs:
    - Ernitec VMS System Manager
    - Ernitec VMS EasyView for Windows
    - Ernitec VMS System Monitor
    - Ernitec VMS WebClient (optional)

RECORDERS

The DVRs and NVRs record video and audio from multiple cameras and audio channels and write the data on hard disks. You can access a recorder locally or over a network by using the System Manager and EasyView programs, and monitor recorder functionality through the System Monitor application.

A recorder contains the computer, the operating system, the recorder software, video capture cards (only DVRs), their drivers, and cameras.

An NVR does not have video capture cards. Instead, it records video from IP cameras connected to a network.

In addition, you can connect these devices to a recorder:

- Dome cameras
- Dome camera keyboard
- External devices, such as sensors, to the digital inputs of a DVR
- External devices, such as doors, lights, and gates, to the digital outputs of a DVR
- Video monitors (only DVRs)
- Printer
- Backup unit (NAS, SAN, or RAID, for example)

MASTER SERVER

In a networked, Enterprise system one of the servers must be set as the Master Server. A Master Server is the central recorder of a surveillance system. All other recorders connect to it, and all client applications communicate through the Master Server.

If the system contains only one recorder, that recorder is the Master Server. If there is more than one recorder, 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: *From release 7.3.0 onwards, all Master Servers must have SQL Server Express or other Microsoft SQL Server installed.*

The Master Server does these things:

- It verifies the identity of all programs and users who want to login 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 recorders.
- It generates reports.
- It stores watchdog event
- It stores alarms
- It stores audit trail

CLIENT PROGRAMS

The **System Manager** program is used by the system administrator for the following:

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

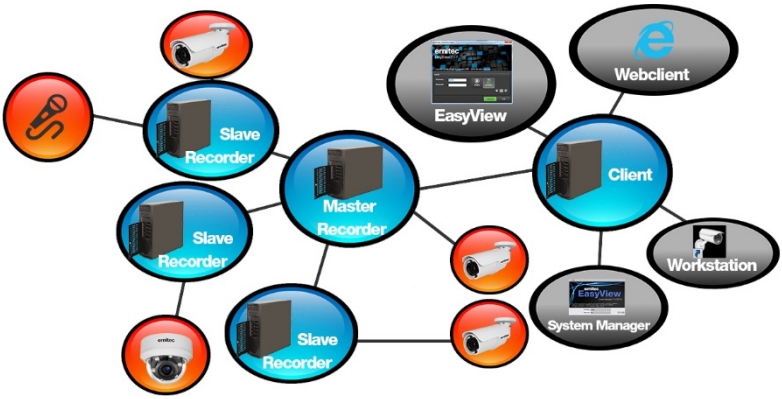
End users use the **EasyView** program, for example, for these tasks:

- Monitor real-time and recorded video and audio
- Control 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 installed by default. Users can install **Workstation** client by choosing it separately from the installer option menu.

In addition, system administrators can use the **System Monitor** application to monitor the status of the recorders.

This figure shows a system with four recorders (three slave and one master), as well as a connected client computer with four client applications:



NETWORK REQUIREMENTS

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

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

LICENSE TYPES

The Ernitec VMS software has two default license types: the single recorder Ernitec VMS Pro license aimed for the retail and small business sector, and the Ernitec VMS Enterprise license aimed for multi-recorder and multi-user surveillance installations.

Ernitec VMS Pro

The Ernitec VMS Pro license type is meant for single recorder systems. The license type is tailored for the needs of the retail sector and small businesses, and as such is constructed to offer services related to their needs.

The Ernitec VMS Pro license contains the basic functionalities needed for small scale video surveillance, including real-time and playback video viewing. The license does not support advanced features such as (but not limited to) the Map Tool, archiving, audio channels or text data channels.

The Ernitec VMS Pro license has the same user interface as the Ernitec VMS Enterprise software with non-included functionalities may be greyed out/disabled.

Ernitec VMS Enterprise

The Ernitec VMS Enterprise license type offers the full functionality of the software for multi-recorder installations.

Unlike the Ernitec VMS Pro license, the Ernitec VMS Enterprise license has a full support for all features supported by the software. The license allows for up to 10 simultaneous users with varying user rights to start with.

The Ernitec VMS Pro license can be updated into a Ernitec VMS Enterprise license by updating the license key. Please refer to *Ernitec VMS Installation Guide* for information on updating the license key.

License Type Comparison

Feature	Pro	Enterprise
Camera channels*	50	128
Max. number of recorders	1	1-150 (6 or above with upgraded license **)
Max. number of users	5 simultaneous	10 simultaneous (11 or above with upgraded license)
WebClient & Gateway***	YES	YES
Network drive data storage (NAS support)	YES	YES
Audio recording	NO	YES
Text data	NO	YES
Map tool	NO	YES
Archiving	NO	YES

** = Amount of cameras that can be added not limited by license, but is limited in practice by the hardware that is being used.*

*** = Upgraded license installations support surveillance systems with up to 150 recorders. Please contact info@Ernitec.com for further information. Systems above 150 slaves are possible on a case by case basis.*

**** = The Gateway Server and the WebClient application are installed with a separate installation file.*

OS COMPATIBILITY

Ernitec VMS 7.5 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	EasyView for Windows client application
Windows 7 Pro / Enterprise	32-bit only	X	X	X	X
Windows 8 Pro & Pro Retail	32-bit only	X	X	X	X
Windows 2008 Server R2 Enterprise	32-bit 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

NOTES:

- *Ernitec VMS has not supported Windows XP since Ernitec VMS version 6.4. If Windows XP support is required, do not install Ernitec VMS 6.4, or any later releases.*
- *Make sure that the "Desktop Experience" feature is activated for Windows server operating systems.*
- *No releases before Ernitec VMS V7.4 has support for Windows 10. Any older versions (V7.3 or older), if used with Windows 10, must be upgraded to the latest V7.4 release (V7.4.5 is the latest/current release at the date of this document) or V7.5.*

CONFIGURING THE SYSTEM

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

To configure the system, perform these steps:

1. Add recorders to the system and configure their settings.
2. Add the correct licenses for the recorders.
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 "EasyView only" installer is provided.*

NOTE*: After configuring the system,* ***back up system settings and all recorder 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`

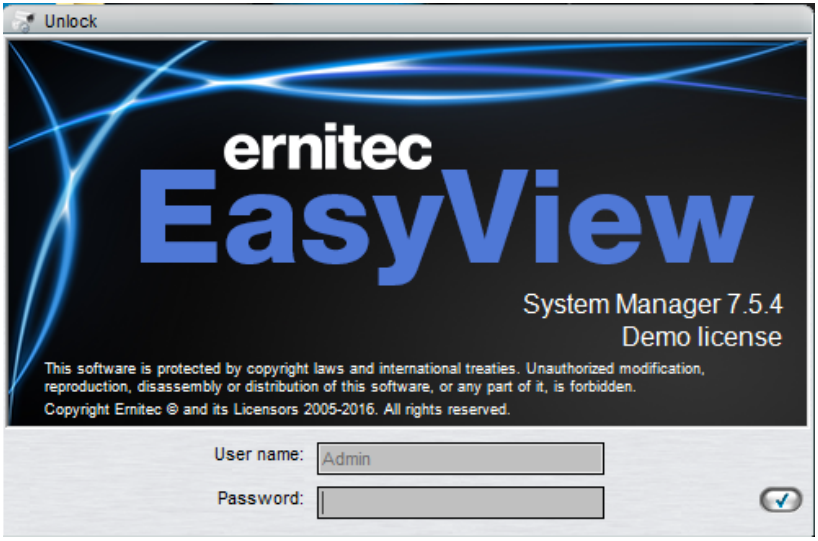
Password: `0308`

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 **VMS System Manager** on the desktop.
   - Click **Start**, point to **Programs** and then to **EASYVIEW**. Click **VMS System Manager**.



2. The login screen is shown. Select the Master Recorder to which you want to connect to from the **System address** pull-down menu.
3. 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.*
4. 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.**

To login another recorder:

1. Do one of the following:
   - Double-click the shortcut icon **VMS System Manager** on the desktop.

- Click **Start**, point to **Programs** and then to **EASYVIEW**. Click **VMS System Manager**.

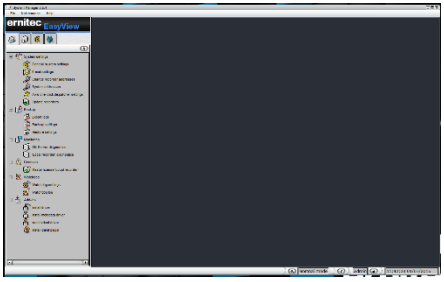
2. The address selection screen is displayed. Click **Details**.
3. Select the desired address from the address list, or click **Add** and type the recorder's IP address.
4. Click **OK** to connect to the selected recorder.
5. The login screen is shown. Type your user name in the **User name** box, and your password in the **Password** box.
   NOTE: *The user name and password are case sensitive.*
6. Click **login**. A progress bar is shown on the screen while the program loads.

After the program starts, the user interface is shown.

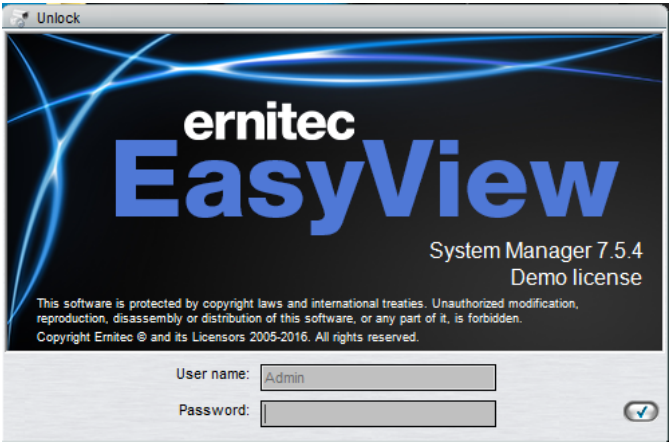
NOTE: *Only one user can be logged in with System Manager administrator rights at any given time. If additional users with administrator rights try to log into System Manager, they are given system monitoring rights, allowing them to view the system settings.*

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.



Also EasyView has two passwords.

Also the EasyView user interface lock query and Workstation application have two password views.

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.

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:

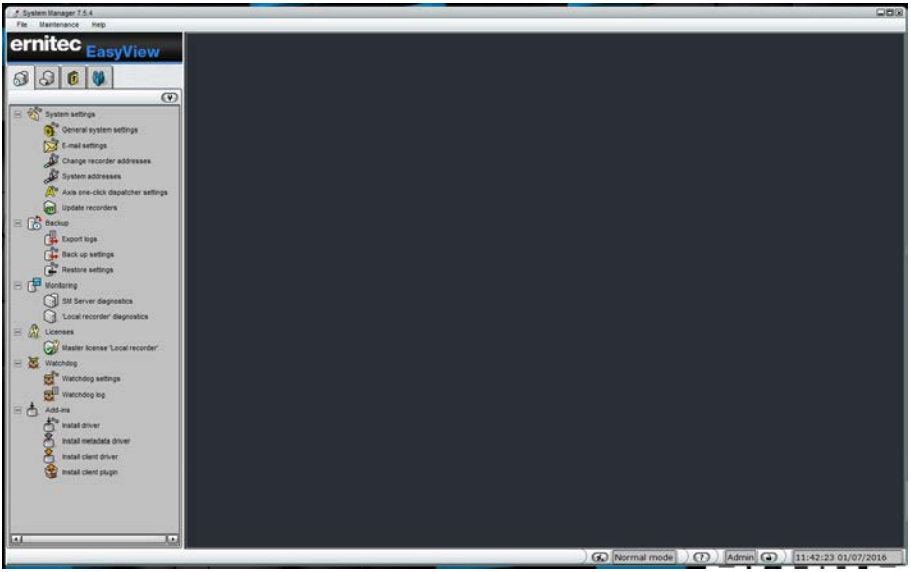
- On the menu bar, click **User** and then **Lock Program**.
- On the status bar, click **Lock program**.

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, Recorders, 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:

- Back up 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 recorders to the system and configure them on the **Recorders** tab.
- Add and edit user profiles on the **Profiles** tab.
- Add and edit user accounts on the **Users** tab.

RECORDERS

These sections describe how to add recorders to the system and how to configure their settings.

ADDING AND REMOVING RECORDERS

You can have (depending on the license) from 1 to 150 recorders in one system. One recorder should not belong to more than one system.

You can specify a password for each recorder. The system will prompt for the password if someone tries to add the recorder to another system.

To add a recorder to the system:

1. Open the **Recorders** tab .
2. Click **Add Recorder** in the lower-left corner of the navigation pane. The **General Settings** dialog box is shown.
3. Do the following:
   - Type a descriptive name for the recorder.
   - Type a description of the recorder. The description is shown only on this tab.
   - Type the IP address or DNS name of the recorder.
   - To specify a password for the recorder or to change the existing password, click **Change Password** and type the password in the **New password** and **Confirm new password** boxes. If the recorder already has a password, you will be prompted for the existing password before the recorder is added to the system and the password changed.
   - If the recorder is used as part of an integrated system or with the Ernitec Remote Monitoring Center system, select **Allow SDK and RMC video services.**
   - If the recorder is to receive alarms from an integrated system, select **Allow SDK alarm control.**

- If the recorder is to be used as failover recorder, select the box. **"use as a failover recorder"**

4. Click **OK**. The recorder and the devices connected to it (for example, cameras and audio channels) are added to the list.
   NOTE: *If the recorder is password protected, the system prompts for the password.*

To remove a recorder from the system:

1. Select the recorder that you want to remove.
2. Click **Remove Recorder** .
3. Click **OK** to confirm.

Connection status:

The connection status of each recorder is shown by the color of the circle adjacent to the recorder's name:

Green. The connection is OK.

Yellow. The system is connecting to the recorder.

Red. No connection. In case the connection to the recorder is lost, the System Manager application will automatically try to connect to the recorder.

CONFIGURING RECORDERS

On the **Recorders** tab, you can configure these settings for each recorder:

Icon	Name	Description
	General	Change the name and the description of the recorder. Here you will also find the IP address of the recorder.
	**Port forwarding**	User can see what the automatic port forwarding has configured as ports for this recorder. The ports can be changed if user wants
	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 recorder 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 **Recorders** tab to the workspace.

GENERAL SETTINGS

In general settings, you can change the name of the recorder and the description of the recorder. You can also specify or change the password that is used to protect the general settings of the recorder. If you specify a

password, the system will prompt for the password if the recorder is added to another system.

NOTE: *The IP address or DNS name of a recorder cannot be changed through the general settings screen.*

FAILOVER SERVERS

Ernitec VMS supports Failover servers as a Ernitec VMS Enterprise option.

Failover servers are servers that are on a passive standby until the system recognizes that one of the active servers (Master or Slave) 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 EasyView plugins (such as ANPR+ or Map Plugins) 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 recording 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 Enterprise 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, one recording server, one failover server.

Failover migration will be triggered in the following conditions:

- The Master server has lost the connection to a recording server and the timeout set by the administrator has been reached
- A recording server has informed the master server that connection to all the material disks (recording storage) on the recording server have failed

- Manual data recovery from recording server hard drives can be attempted, if the disks are still functional
- A recording server's Watchdog service has informed the Master server that it cannot initialize 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 recording 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 recording servers are added to failover queue

Failover queue is handled after the failover restore has been completed.

FAILOVER LICENSING

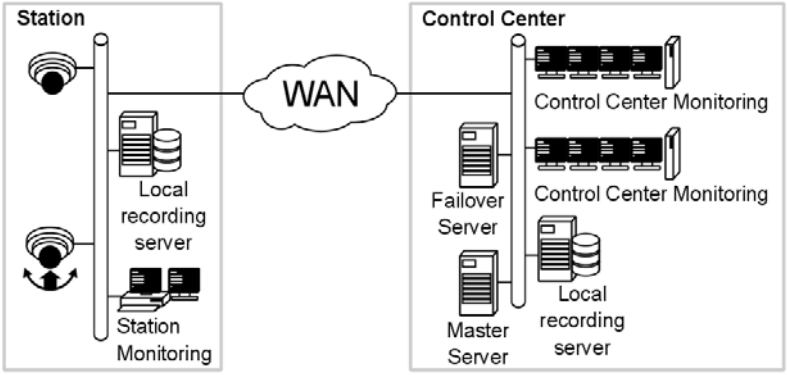
The Failover functionality uses automatic backups generated by the *SMServer* service when doing failover, and therefore the system must have automatic backup option enabled; either as an Automatic Flash backup in Ernitec systems or a non-Flash based backup in hardware provided by another hardware distributor.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

For the failover feature to function, the *SMServer* 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 recording 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 EasyView for Windows client.

The control center houses the system network's failover and Master servers. The failover server can take over when a station's local recording server becomes unusable. The Master 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 recording server and failover server need to be similar in terms of hardware and assigned drive letters. Please note that the master needs to be installed on separate hardware. So the minimum hardware setup consists of three servers: one Master, one recording server, one failover server.

RECORDING SERVERS (NORMAL, FAILOVER, BROKEN)

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

- Recording 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 recording server 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 **Recorders** tab in System Manager shows failover and broken servers in their own groups (under *Failover recorders* and *Broken recorders*). The *Failover recorders* group shows server connection states and server general settings if connection is available. The *Broken recorders* 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 recorder to the system, it can be defined to be a failover recorder. Failover recorder is a backup recorder that shall assume the duties of any recorder that is defined to be under failover protection.

Failover servers must have same file system (same drive letters) as the recording 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 *recorder* list. When any recording server is deemed to be broken or inaccessible, they are moved under the "*broken recorders*" folder and any available failover server shall take the responsibilities of the broken recording server.

Failover settings can be controlled from the general settings of the selected server. The failover transition is done if 1) all material disks are broken or 2) the server is inaccessible longer than a defined time period.

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

Adding a failover server

Failover servers in the recorder *list*

ADDING AND REMOVING FAILOVER SERVERS

To add a failover server to the system:

4. Open the **Recorders** tab 

5. Click **Add Recorder** in the lower-left corner of the navigation pane. The **General Settings** dialog box is shown

6. Do the following:

   - Type in a descriptive name for the server
   - Type in 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
   - **To enable the server as a failover server, check the box. "use as a failover recorder"**

7. Click **OK**. The server is added to the list.
   ***NOTE**: If the recorder is password protected, the system prompts for the password*

To remove a recorder from the system:

8. Select the server that you want to remove

9. Click **Remove Recorder**

10. Click **OK** to confirm

PORT FORWARDING

The basic idea with port forwarding is that it is possible to access one or more recording 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.

AUTOMATIC ROUTER CONFIGURATION

When a recording 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, recorder 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 recording 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 recorder 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).

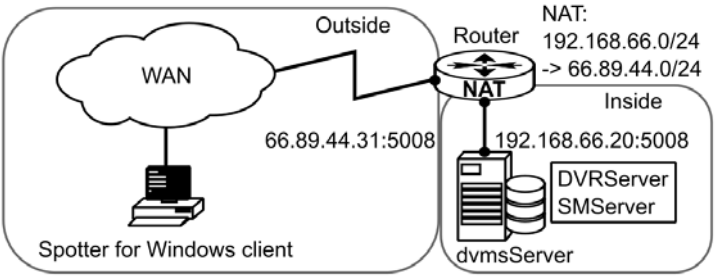
The first port is used for SMServer communication (5008, 5012, 5016...)

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

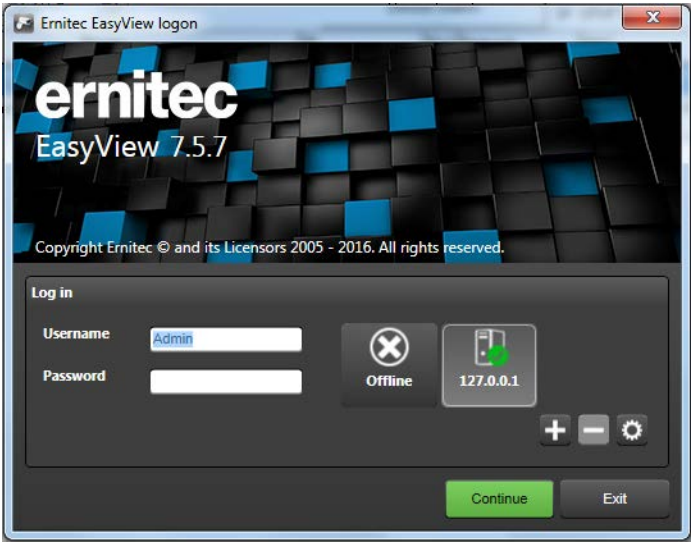
When connecting to a master recorder, therefore the port is typically 5008. When adding new recorders to the master, the port is typically 5009. If there are more than one recorder on site, then the ports are 5009 +4, 5009 + 8 etc.

SINGLE RECORDER BEHIND ROUTER

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

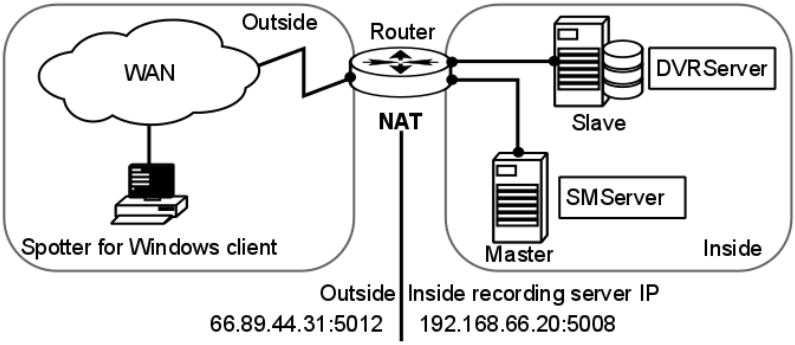


If user is using a single recorder system from WAN, he needs to connect to the VMS server with the outside IP address that the router has translated. The user can check the port forwarding what the port in use is, but it is with high likelihood port 5008.

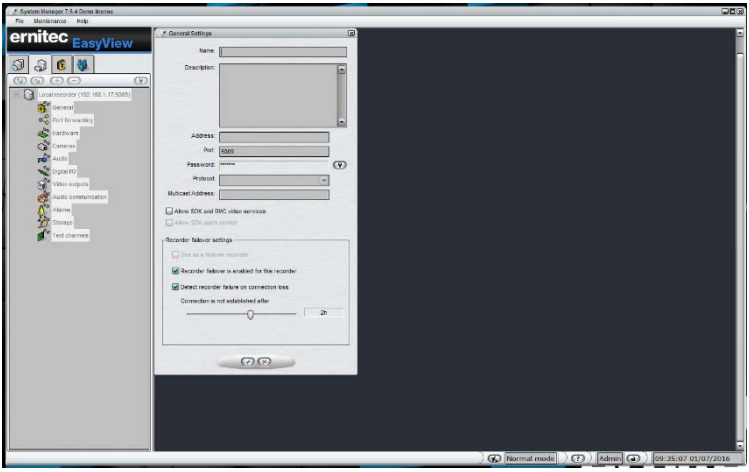


MORE THAN ONE SERVER BEHIND ROUTER

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

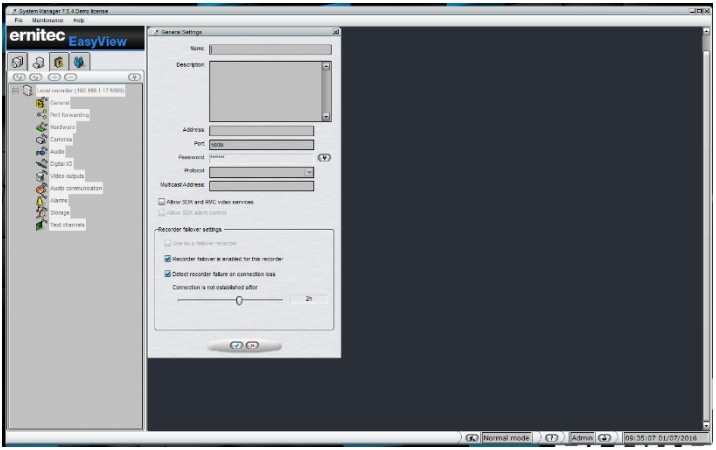


If user is configuring a larger system with multiple recorders on single site, he can add the recorders to the system manager application with the external or internal IP address.

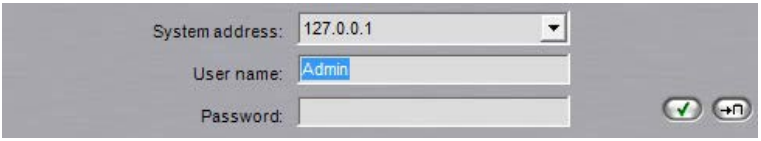


When adding a new slave server, if the slave server has done automatic port forwarding, there will be a note shown to user that he can choose between internal IP address and external IP address. If the recorder is to be used from WAN, then the external IP address should be chosen.

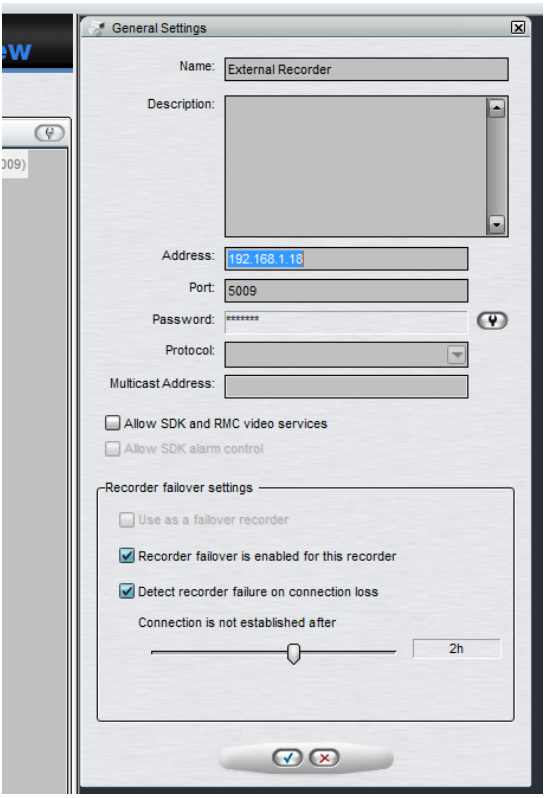
The exact ports that the recorder has done port forwarding to, can be found by



starting the system manager on the local recorder (locally on the slave server, start system manager to 127.0.0.1 and log in with the default password Admin/0308) and check the port forwarding settings.



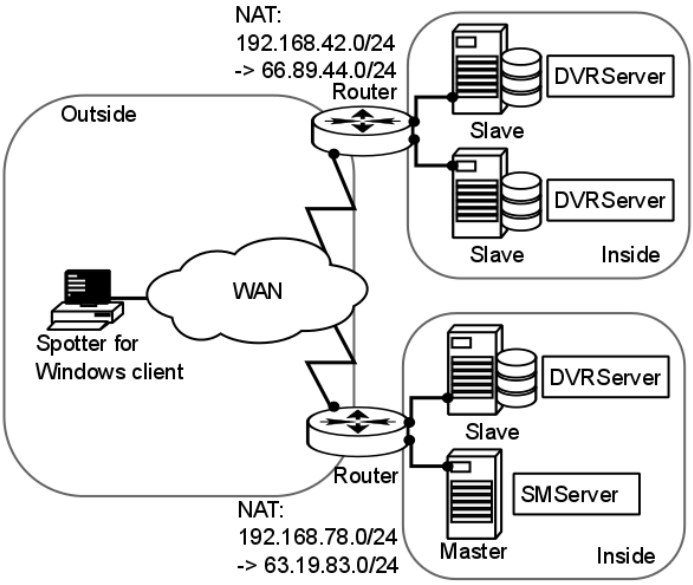
When adding a recorder to a master when not on the local site (cannot use the local IP address) then the user must know the external IP address and either have knowledge of the first port that the port forwarding was done to.



If the recorder that is added is single recorder, the port is most likely 5009. If there are multiple recorders 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 recording servers (Slaves) to the Master from the other site.

CAMERAS

ADDING AND REMOVING ANALOG CAMERAS

Analog camera installation and removal is described in the *Ernitec VMS Installation Guide*.

Analog camera configuration is done in the **System Manager**.

ADDING AND REMOVING IP CAMERAS

IP cameras can be configured through the **Video** tab of **Hardware settings**.

IP cameras and video servers can be configured through the **automated camera search** function or through the **IP camera finder** tool. Manual configuration is required only if the automated search tools fail to find a camera. The automated search tools provide the system with accurate information on the device, while manual configuration lacks some information (such as exact image resolutions).

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 a camera's IP audio inputs and outputs 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.

IP camera addition:

- In automatic configuration, the user selects the **automatic camera search** option from the driver list and provides the camera details, after which the system configures the camera automatically.
- **IP camera finder** can be used to search for cameras in the local area network and to add them to the system automatically without the user having to know the camera's IP address.

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

NOTE: *In most IP dome cameras, the dome functionality is installed simultaneously with the camera driver through* ***automatic camera search*** *or* ***IP camera finder****. In most analog cameras, dome functionality*

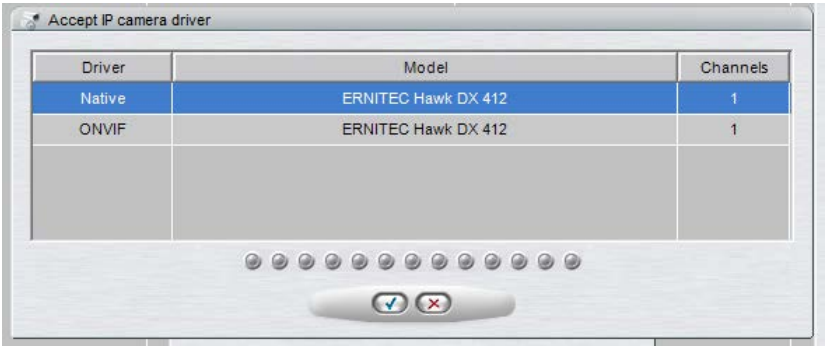
*drivers are installed through separate camera specific installation packages. Please see **Ernitec VMS Installation Guide** for further information.*

To configure an IP camera through automatic camera search:

1. Set an IP address or DNS name, user name and password for the cameras in the camera's internal settings. See the camera manual for details.
2. On the **Video** tab, click **Add Camera** .
3. Type the IP address or DNS name of the camera or video server.
4. Type the port number, which is usually 80.
5. Type the user name and password for the camera.
6. Click **OK**.
7. The **Settings** column shows a link to the camera's internal settings. You can click the link to access the settings.

NOTES:

- *If the automated camera search fails to find a camera in the provided address, you are asked to manually configure the camera and to select the camera model from a drop-down menu before retrying. However, manual configuration is not recommended, as it provides the system with limited information on the camera.*
- *It is possible to choose between native driver and ONVIF driver after entering the camera IP address. The ONVIF driver is also included in the installation package by default. (see image below)*



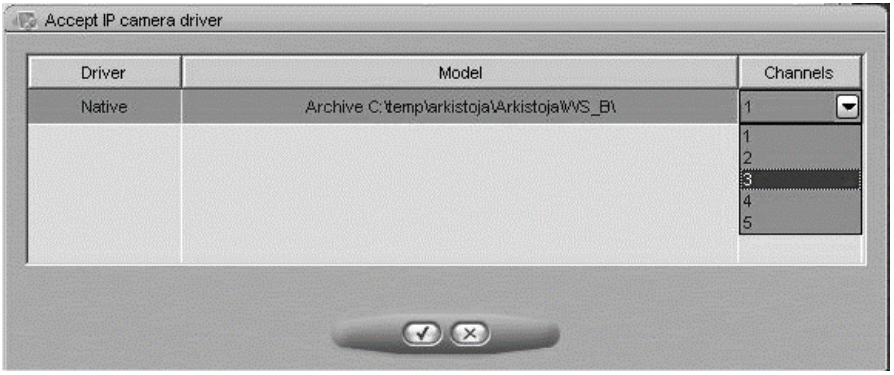
To configure IP cameras through the IP camera finder tool:

1. Set an IP address or DNS name, user name and password for the cameras in the camera's internal settings. See the camera manual for details.
2. On the **Video** tab, click **IP camera finder** .
3. After the IP camera search is complete, select the cameras you want to add to the system.
4. Type the username and password for the cameras.
5. Click **Add Selected Cameras** . The systems add's the selected cameras to the system with the selected username and password.
6. If the system cannot add some of the selected cameras, you can repeat steps 4-5 for the cameras.
7. Click **Close** to exit the **IP camera finder**.

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.*

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**.



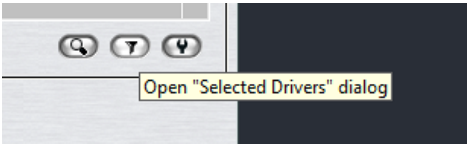
To add a multi-channel device with less than maximum number of channels:

1. When adding the device, there is a dialog asking how many channels the user wants to add
2. to add the device with less than maximum number of channels, use the pull down menu.

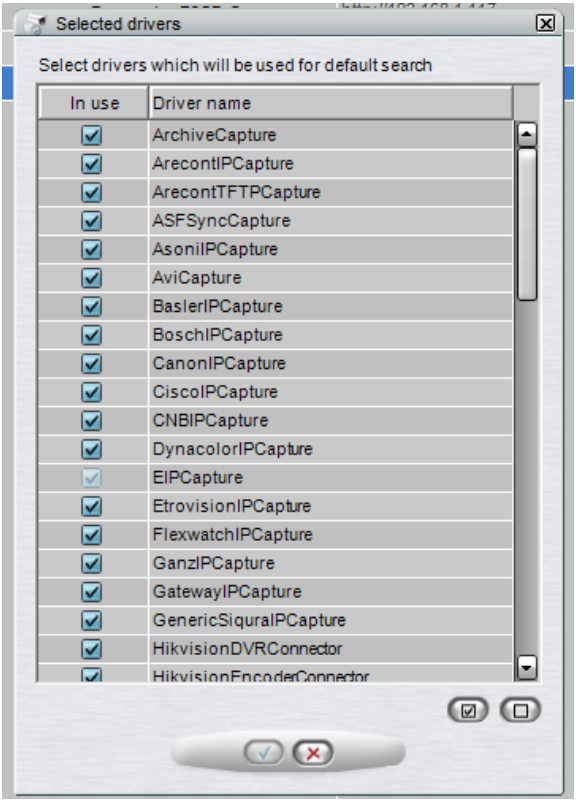
LIMITING THE CAMERA CONFIGURATION TO CERTAIN CAMERA DRIVERS

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.



CLICK REMOVE SELECTED EDITING CAMERA SETTINGS

You can edit the settings for each camera on a recorder on the **Cameras** page in the **Recorder** tab in the **System Manager**.

To edit camera settings:

1. Open the **Recorders** tab.
2. Select the correct recorder and open the **Cameras** page from the recorder menu.

The **General** tab shows a summary of camera parameters in the upper part of the page. You can change the parameters in the lower part of the window.

The screen contains the following parameters:

- **No.** The number of the camera in the system.
- **In Use.** Shows if a camera is enabled (green check mark) or disabled (red cross).
- **360.** This setting should be used if the EasyView 360 plugin is used and the camera is supported. Contact Ernitec for list of supported cameras for on-client-360 image de-warping
- **Name**. The name of the camera. By default, cameras are named *Camera 1*, *Camera 2*, and so on. But you can change the default name.
- **Quality.** The quality with which images are recorded (0-100%).
- **Resolution.** The resolution with which images are recorded. For analog cameras, the options are **Normal**, **High** and **Maximum**. For manually configured IP cameras, three resolution settings (with the highest being the maximum resolution supported by the camera model) are displayed. For automatically configured IP cameras, the exact image resolutions supported by the camera model are displayed.
- **Rate.** Record rate as images per second (ips).
- **Camera Driver Information.** Shows the driver information for the camera.
- **Load.** The load caused on one capture card (or IP camera server) by the record rates. If the load is more than 100%, the program will not let you save the settings.

To edit camera information:

1. On the **General** tab, click on the name of the camera you want to edit.
   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.*
2. Edit the camera information.
3. Click **OK** to save the changes.

NOTE: *Please note that if you select more than one cameras, you cannot set parameters that are not supported by all selected cameras. For example, if*

you select three cameras, and only two of them support the H.264 video codec, you cannot set H.264 as the codec for the selected cameras.

Camera parameters

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 EasyView 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 EasyView client that the camera is a 360 camera, and EasyView will show the image de-warping options in the camera toolbar (if installed)

Codec. The codec used for transmitting the video between the recorder and the client applications, and in the case of IP cameras, for transmitting the video between the IP camera and the recorder. 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 recorder software can be selected. The codecs supported by the recorder software are JPEG, MPEG-4 and H.264.

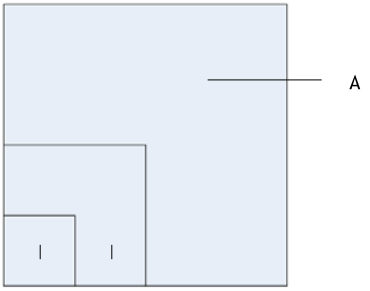
Quality. Set this value between 0%-100%. A higher value means better image quality but also large image data size. To decrease the image data size, set the value lower. However, setting the value lower also decreases the quality of the images. 50% is usually sufficient. For wireless and low bandwidth connections, select 0%.

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

For analog cameras, the options are **Normal**, **High** and **Maximum**. Likewise, for manually configured IP cameras, three resolution settings (with the highest being the maximum resolution supported by the camera model) are displayed.

For both analog and manually configured IP cameras, the highest resolution setting gives the maximum resolution supported by the camera. The second highest resolution usually gives one fourth of the maximum resolution, and the lowest one provides one sixteenth of the maximum resolution.

This figure illustrates the available resolutions for analog and manually configured IP cameras:



Available resolutions for analog and manually configured IP cameras. A. Maximum B. High C. Normal

Record rate. Set the record rate. The maximum rate depends on the video standard and the camera type.

Description. Here you can type a description of the camera that will be shown to all users in the EasyView program.

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

Multiple streaming (multi-streaming).

Reference image. A reference images is an image captured from the camera, which makes it easier to identify the cameras. In addition, in the EasyView 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.

Frame rate optimization

Showing real-time video locally causes a load on the computer processor because the system compresses and de-compresses video. Video recording also requires processing power. If a recorder is used only to record video and not for real-time viewing, it is possible to use the available resources for recording more images.

NOTE*: Local viewing directly from the capture card (viewing raw, uncompressed video) does not cause a load on the computer processor. If*

only direct viewing is used, you can use the default setting **Local use** *50%/***Remote use** *50% for frame rate optimization.*

Follow these guidelines to find a suitable setting:

- If real-time video is viewed primarily on the recorder and the recorder does not support direct viewing, set this value to **Local use** 100%/**Remote** use 0%. This makes it possible to view video from more cameras at the same time.
- If real-time video is viewed only over a network from client computers, set this value to **Local use** 0%/**Remote use** 100%. This gives up to 50% more resources for recording.
- If real-time video is viewed both locally and over a network, you may need to experiment to find a suitable value. The default value is **Local use** 50%/**Remote use** 50%. If there are problems with real-time viewing on the recorder, move the slider to the left to allocate more resources to viewing.

Total load. This is the total load caused on the recorder by the record rates. If the load is more than 100%, you cannot save the settings.

HDD Load. This is the hard disk load caused on the recorder by the record rates. The load rate is an estimate based on the average load of hard disks on the recorder. The rate should be used as an estimation only, and it does not guarantee that the actual load rates will not exceed the estimate.

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 a default motion detection mask. When the default mask is used, the system detects motion in all of the image area.

NOTE*: You cannot edit the default mask.*

In addition to the default mask, you can have four more 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. Open the **Recorders** tab.
2. Select the correct recorder and open the **Cameras** page from the recorder menu.
3. In the **Motion Detection** tab, select the camera from the camera list.
4. Click the mask that you want to edit.
5. To change the name of the mask, click **Change Mask Name** and type a new name for the mask.
6. Paint the areas red where you want the system to detect movement and remove the red from areas where you want to ignore movement. Use the pen tool or the other drawing tools. For example, use the **Eraser** to remove red from areas where you want to ignore movement.
7. Set the detection sensitivity.
8. Set the minimum quantity of movement.
9. Select the motion detection method: comparative, adaptive, or hermeneutic motion detection.
10. 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. Adjust detection sensitivity and the required quantity of movement as necessary. Note that you cannot use the drawing tools in the test mode.

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 required 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.

To use the default motion detection frame rate:

- Mark the **Use default** checkbox.

To change the motion detection frame rate:

- Unmark the **Use default** checkbox.
- Use the slider to define the desired motion detection frame rate.

NOTE: *If there is only one motion detection frame rate available, the Motion detection frame rate slider is disabled.*

Motion detection method

You can use one of these three motion detection algorithms:

- Comparative motion detection
- Adaptive motion detection
- Hermeneutic motion detection

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.

NOTE*: Learning the background image can take some time.*

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.

Counter

You can test the motion detection settings with the counter tool. The counter tool displays the motion detected by the system, listing the number of images containing motion in the **Motion** bar.

To use the counter tool:

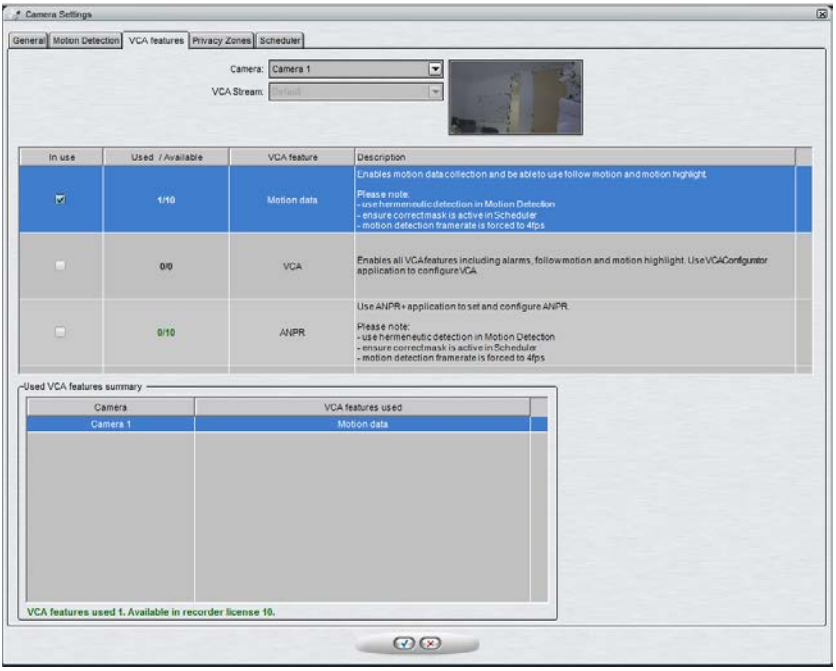
1. Click **Start / Stop Motion Counter**  .
2. Edit the **Sensitivity**, **Quantity** and **Motion detection frame rate** fields to change the motion detection settings as instructed above.
   NOTE: *When the counter tool is active, the* ***Quantity*** *field has an additional value on the right side of the quantity limit. This value contains the actual percentage of changed pixels.*
3. Click **Start / Stop Motion Counter**  to stop the counter.

NOTE: *You can click* ***Reset counter tool*** *to reset the* ***Motion*** *bar.*

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)



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

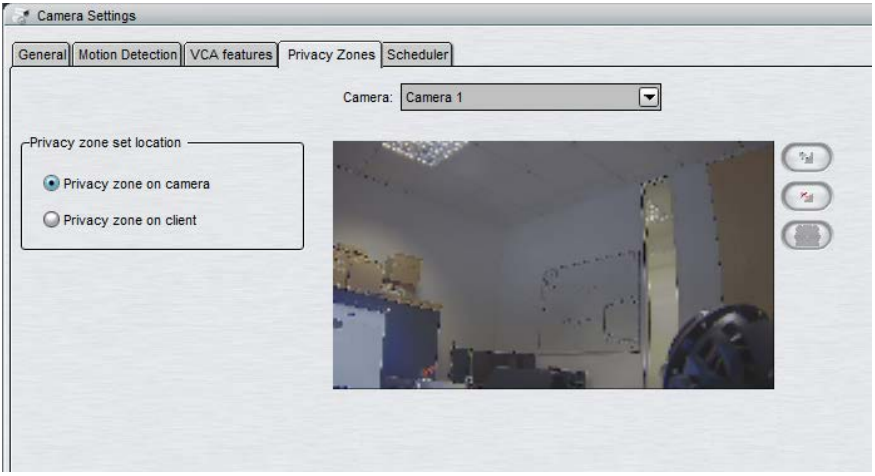
- on the camera: these privacy zones are camera based areas that are not recorded or displayed in the camera view: image data from the areas is not transmitted by the camera to the recorder.
- on the EasyView client: these privacy zones are implemented only on the viewing client. This allows the complete video to be recorded and exported, but the privacy screened areas are only accessible for users who have the rights to do so

Note: *privacy screen on EasyView client requires license upgrade for both the master server and the recorder that the camera is connected to.*

Please refer to the camera manufacturer documentation to see what cameras support the on-camera-screen feature.

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

The Privacy Zones tab



To add a privacy zone:

1. Open the **Recorders** tab.
2. Select the correct recorder and open the **Cameras** page from the recorder menu.
3. In the **Privacy Zones** tab, select the camera from the camera list.
4. Select if you want the privacy zone to be **on the camera** or **on the client** (requires license update)
5. Click **Add privacy zone** .
6. 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.
7. Repeat steps 1-3 to create as many private zones as required.
8. Click **OK**.

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

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

To remove a private zone:

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**  .
4. Click **OK**.

To remove all privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click **Remove all privacy zones** .
3. Click **OK**.

SCHEDULER (VIDEO)

After opening the **Cameras** page as instructed above, you can edit camera specific recording schedules. By default, video is recorded when the system detects motion in the camera scene. 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.

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 set the regular schedule:

1. Open the **Recorders** tab.
2. Select the correct recorder and open the **Cameras** page from the recorder menu.
3. Select the camera from the camera list.
4. On the **Regular Schedule** tab, click the option that you want to apply and then click the hours that you want to change.

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).*

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.

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

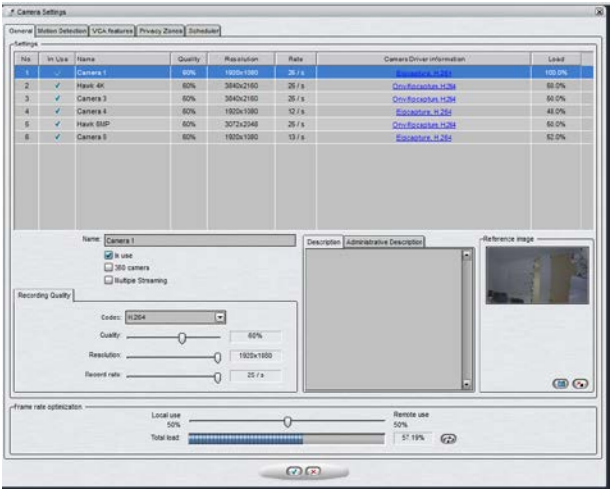
MULTI-STREAMING

Multi-streaming enables separate feeds from a single camera. The feature allows for separate streams to be used for recording and viewing, as well as an additional stream for remote streaming.

Please refer to the camera manufacturer documentation to see what cameras support the feature.

The feature needs to be configured in System Manager.

In Ernitec System Manager, multi-streaming is configured in camera settings:



To configure multi-streaming in System Manager:

1. Select a compatible camera and enter the camera's configuration menu.
2. Click **Multiple Streaming** on.
3. Configure the **Recording quality**, **Viewing Quality**, and **Streaming Quality** tabs. The **Streaming Quality** tab is used only with the **Remote workstation** functionality (see below).

REMOTE WORKSTATION

In some cases, it is necessary to open the same video stream in different locations with different image quality. For example, a separate image quality might be required for security center, and a separate one for off-site use with slow network connections. The remote workstation functionality enables users to open an additional video stream with different image quality in comparison to the "prime" viewing stream.

Please refer to the camera manufacturer documentation to see what cameras support the feature.

The feature needs to be configured in System Manager, and in the EasyView / Gateway XML settings for the computer in which the remote workstation stream is used.

In Ernitec System Manager, remote workstation is configured in camera settings through the **multi-streaming** options.

To configure remote workstation in System Manager:

1. Select a compatible camera and enter the camera's configuration menu.
2. Click **Multiple Streaming** on.
3. Configure the **Streaming Quality** tab to match remote workstation requirements.

To configure remote workstation in the EasyView XML files for the computer in which the remote workstation stream is used:

1. Open the XML file.

   a. For EasyView:
   C:\Users\[USERNAME]\AppData\Roaming\EASYVIEW\EasyView\7.5.0\ EasyView.exe.config

   b. For Gateway:
   C:\Program Files (x86)\EASYVIEW\Gateway\ServiceLauncher.exe.config

2. Find and edit the following string:
   <add key="VideoStreamType" value="Live"/> <!-- Possible values: Live, Remote -->
   In the string, change **Live** to **Remote** to enable the remote stream.
   Note: *The key is case sensitive.*

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. Ernitec takes no responsibility for XML errors caused by editing the files.*

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 a SD card on the camera. Once network connection has been re-established, video is transmitted from the camera's SD card to the recorder.

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.

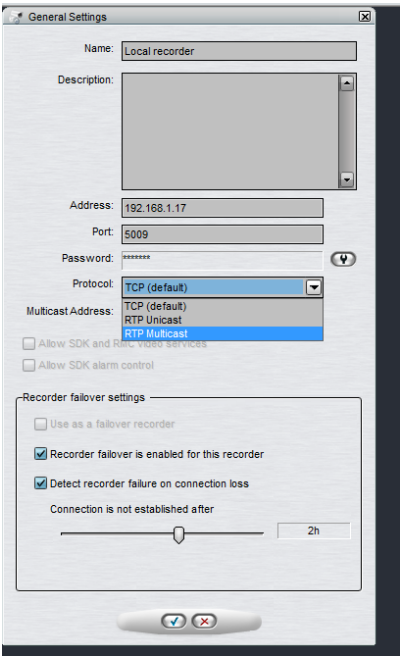
MULTI-CASTING

When a single workstation stream is opened multiple times, the recorder – 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 multicast, stream for each video channel is sent to LAN only once. All applications in LAN can receive the single stream, so network bandwidth usage is much lower than when sending stream for each streaming application separately.

The feature needs to be configured in System Manager, and through network settings. Please refer to the camera's documentation for instructions on enabling multi-streaming. Please refer to your network infrastructure service for information on enabling multi-casting support on the network level.

To configure multi-casting in System Manager:



1. In the recorder'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 recorders 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 **Recorders** tab.
2. Select the correct recorder and open the **Audio** page from the recorder menu.
3. Select the capture driver from the list.
4. Select one of these options:
   - **Mono**. Select to use two mono channels.
   - **Stereo**. Select to combine two mono channels into one stereo channel.
5. 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 **Recorders** tab.
2. Select the correct recorder and open the **Audio** page from the recorder menu.
3. Click **Edit Audio Channel** in the lower right corner of the tab. The **Configure Audio** dialog box is shown.
4. Edit the information fields.
5. Click **OK**.

To remove an audio device:

1. Open the **Recorders** tab.
2. Select the correct recorder and open the **Audio** page from the recorder menu.
3. 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.*
4. The last audio device on the list is removed from the recorder.

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 EasyView client. Only one EasyView 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 recorder, meaning that the communication is not recorded in the system.

GENERAL SETTINGS

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

- **No.** The number of the channel.
- **In Use.** Shows if a channel is enabled or disabled.
- **Name**. The name of the channel.

- **Mono / Stereo**. Shows if a channel is a mono or stereo channel.
- **Compression**. Shows if compression is on or off. A 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 EasyView program.
   - **Administrative Description**. Here you can type a description of the channel that will be shown in the EasyView program to only system administrators.

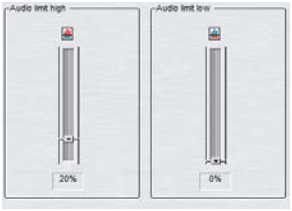
AUDIO DETECTION

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**.



A

Limits for audio detection. **A**. *Audio level* **B**. *Low limit* **C**. *High limit.*

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**).

You can, however, use different recording schedules for each audio channel. First, set the regular week schedule on the **Regular Schedule** tab and then, if necessary, set holidays on the **Holidays** tab.

You can apply different recording options for each hour of the week. These options are available:

- **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.

To set the regular schedule:

1. On the **Regular Schedule** tab, select the audio channel from the drop-down list.
2. Click the option that you want to apply and then click the hours you want to change.

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).*

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

To copy the current schedule for all audio devices:

You can copy the currently selected recording schedule for all audio devices 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.

1. On the **Holidays** tab, select the year and the month.
2. From the list on the left, select the day schedule that you want to apply for the holiday.
3. Then, on the calendar, click the day that you want to apply a special schedule to.

To add a custom schedule:

1. Click **Add Schedule** .
2. Type a name for the schedule.
3. Click the recording option that you want to apply and then click the hours that you want to change. To change more than one hour at a time, keep the SHIFT key pressed.

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.

AUDIO COMMUNICATION HARDWARE SETTINGS

On the **Audio Communication** tab, set the capture and playback devices that are used on the recorder. On the client computers, the system uses the default Windows devices.

To configure audio communication channels:

- On the **Audio Communication** tab, select the capture driver for the audio input device and then the playback device for audio playback.

AUDIO COMMUNICATION SETTINGS

You can connect a call button, a microphone, and a speaker to a recorder and use them as a door or gate phone. Each recorder 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 EasyView 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 recorder.
2. Connect a microphone and a speaker to the recorder and to the user's workstation.

To set up audio communication:

1. Open the **Recorders** tab.
2. Select the correct recorder and open the **Audio Communication** page from the recorder 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

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.

NOTE: *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.*

DRIVERS

In addition to the default digital I/O drivers included in the system, new drivers can be added to the system by installing them as plugins.

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

To take an I/O device driver into use:

5. If necessary, install the device driver package.
6. Open the **Recorders** tab.
7. Select the correct recorder and open the **Digital I/O** page from the recorder menu.
8. Click **Add I/O driver** in the lower right corner of the screen.
9. Select the driver from the **Model** drop-down menu.
10. Configure the device settings in the **Properties** list.
11. 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 **Recorders** tab.
2. Select the correct recorder and open the **Digital I/O** page from the recorder 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 **Recorders** tab.
2. Select the correct recorder and open the **Digital I/O** page from the recorder menu.
3. Click on the I/O device driver you want to delete.
4. Click **Delete I/O driver** in the lower right corner of the screen.
5. Click **Ok** to confirm the deletion.

DIGITAL INPUTS

You can use digital inputs to activate alarms. In digital input settings, set the polarity of the inputs. Set the alarm actions in alarm settings.

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

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

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

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

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

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

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

LOGICAL I/O

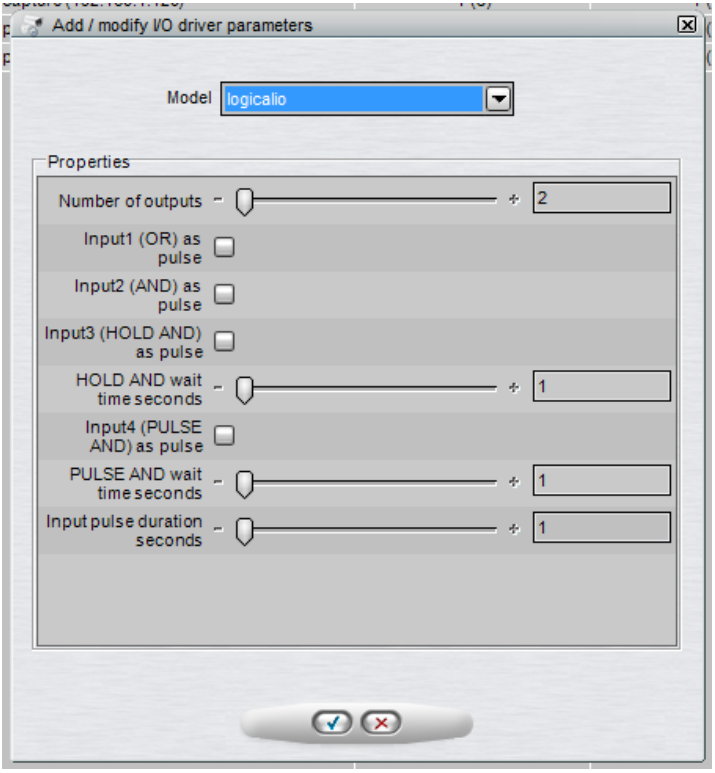
With Logical I/O it is possible to create actions based on the OR and AND operators.

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.

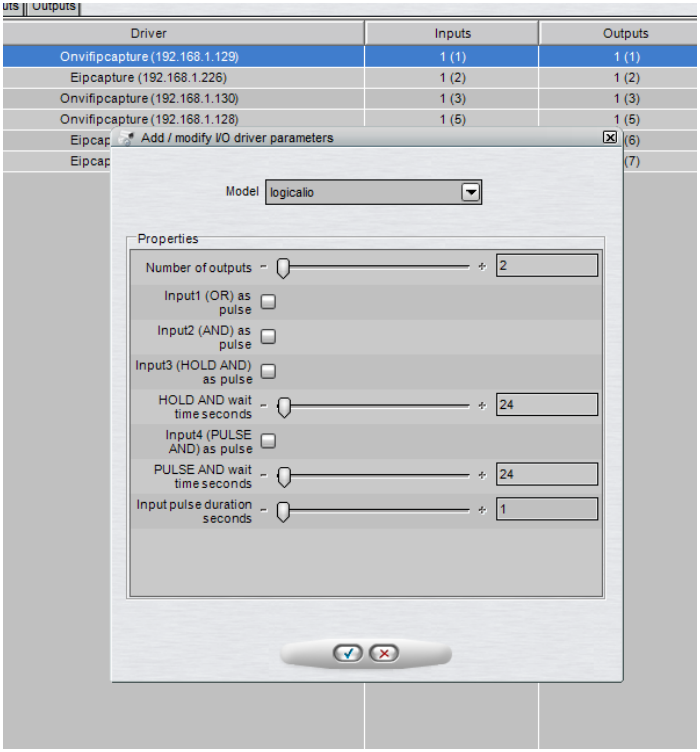
When a new Logical I/O is being added, the first option in the dialog is how many output states are used as operands in the AND/OR decision making. The minimum number is 2 and maximum is 32.



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

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

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

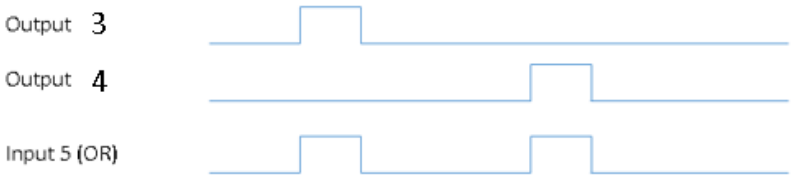


The example has 2 outputs that are the operands. These can be seen in the IO list as outputs 3 and 4.

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

OR INPUT

The first input that the Logical I/O will generate is OR signal. If any of the outputs are on, the OR input will be turned on.

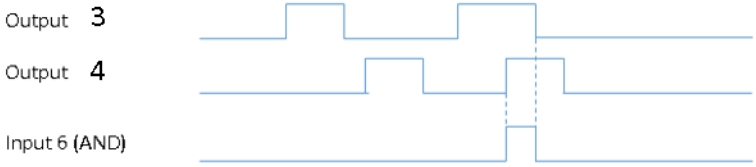


In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, the input 5 will be turned on as a result.

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

AND INPUT

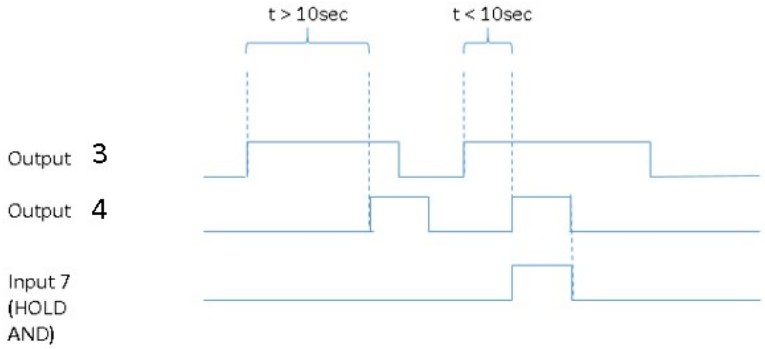
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on at the same time, the input 6 will be turned on.



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.



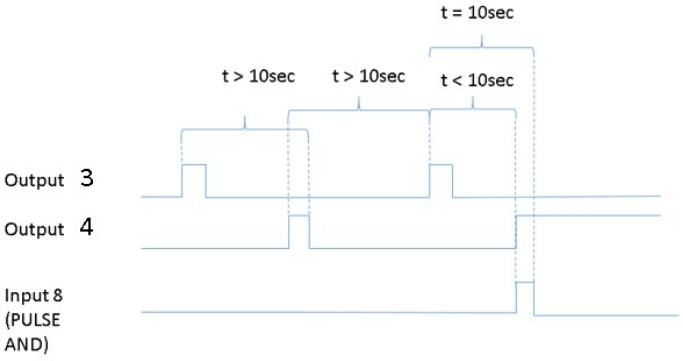
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, the input 7 will become active.

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.

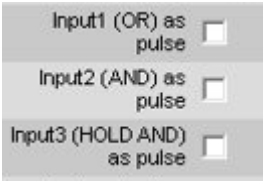
In our example, if output 3 has been active inside 10 seconds, and output 4 becomes active, then the input 8 will be turned on.



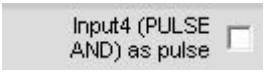
Input 8 remains on until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details). In our example, when 10 seconds has elapsed from output 3 activation, the input 8 will be turned off.

PULSE MODE FOR INPUTS

For each of the four inputs, it is possible to define pulse mode to be in use.



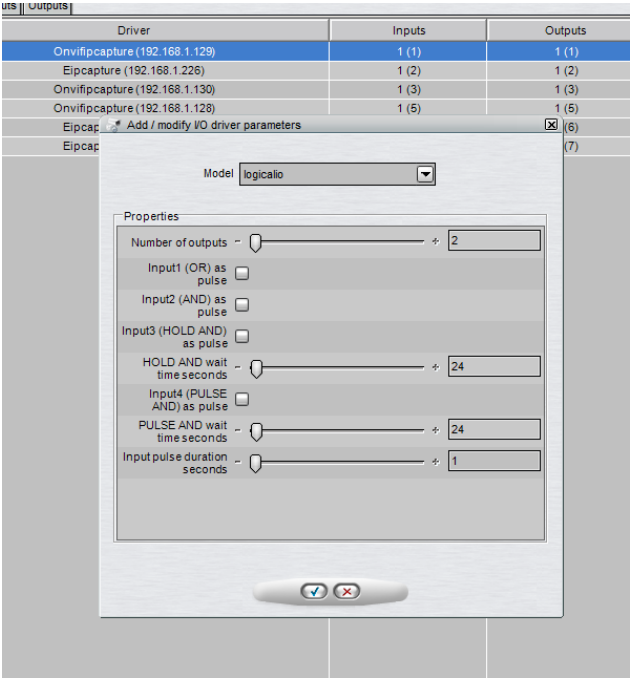
and



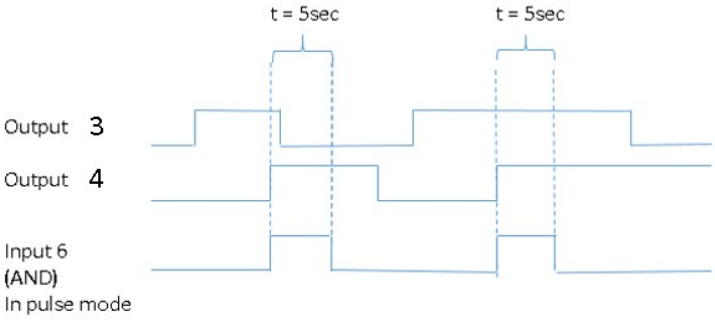
The pulse duration can also be adjusted.

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

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



It would mean behavior like this:



VIDEO OUTPUTS

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 EasyView 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 **Recorders** tab.
2. Select the correct recorder and open the **Video outputs** page from the recorder menu.
3. Click **Edit Camera Tours** . The **Edit Camera Tours** dialog box is shown.
4. Do as follows:

   c. Click **Add Camera Tour** .

   d. Type a name for the tour.

   e. 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.

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

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

.

h. 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 **Recorders** tab.
2. Select the correct recorder and open the **Video outputs** page from the recorder 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 **Recorders** tab.
2. Select the correct recorder and open the **Video outputs** page from the recorder 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 EasyView 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 recorder 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 **Recorders** tab.

ACCESSING THE ALARM LIST

To access the alarm list:

1. On the **Recorders** tab, select the recorder.
2. Double click on **Alarms**.
3. All alarms configured for the recorder 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. On the **Recorders** tab, select the recorder.
2. Double click on **Alarms**.
3. Click **New Alarm** at the lower left corner of the **Alarms** screen.
4. Type the name of the new alarm to the **Name** field.
5. Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.

6. 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.
7. 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 **EasyView** application.
8. 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.*
9. Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.
10. Select the trigger type from the **Type** drop-down menu.
11. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.

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

    - When this option is selected, the list of available metadata events from the driver is shown on the right side of the screen.
    - Contact Ernitec for more information on how to configure VCA metadata based alarms.
12. 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.

13. Open the **Actions** tab. The **Actions** tab is used to define the actions performed by the alarm when it is triggered.
14. Select the action type from the **Type** drop-down menu. The action type defines the basic functionality of the alarm.
15. 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.
16. Click **Add** to add the device to the **In Use** list. The **In Use** 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 **15-17** for each desired action.*
17. After adding an action to the **In Use** list, you can edit its settings by clicking on the arrow sign on the left side of the name of the action in the **In Use** list. The available settings depend on the type of the selected action.
18. After editing all selected actions, open the **Calendar** tab. The calendar tab is used to define the schedule during which the alarm is active.
19. 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.
20. 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.
21. 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 **Recorders** tab, select the recorder.
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 steps 4-21 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 **Recorders** tab, select the recorder.
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

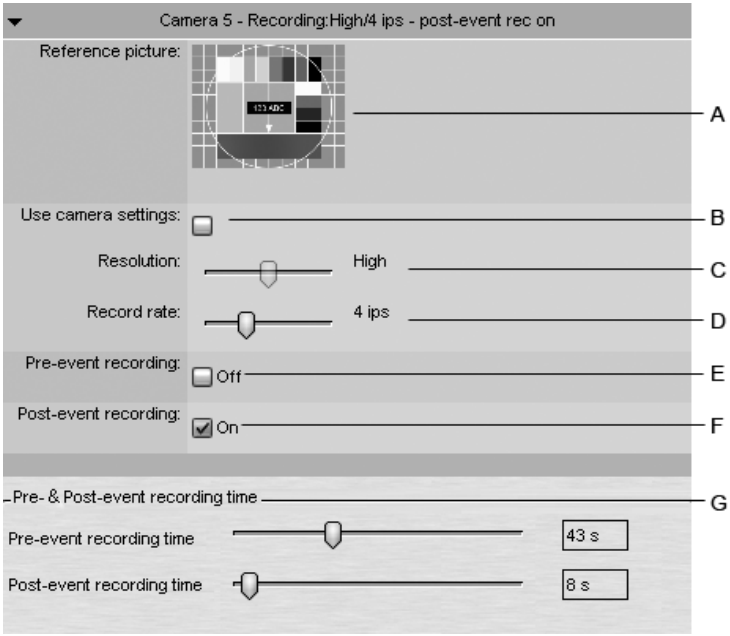
The list below contains the default action types and their parameters. Some of the action types listed above may not be available on all systems.

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 containing this action type is triggered, the recording settings defined by the alarm type will be used instead of the camera's default settings.

In **EasyView**, if alarm pop-up windows are enabled for the user profile, devices used with the **Camera recording** action are displayed in the alarm pop-up view when the alarm is triggered.



The action includes the following fields and parameters:

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

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

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

D) Record rate. Use the slider to change the camera's IPS rate during alarm recording. The slider is inactive if the **Use camera settings** checkbox is marked.

E) Pre-event recording. Mark this checkbox to set 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.

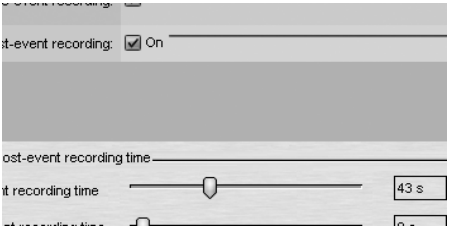
G) Pre- & post-event recording duration. These sliders can be used to set the pre- and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording hasbeen activated.

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 containing this action type is triggered, the recording settings defined by the alarm type will be used instead of the microphone's default settings.

In **EasyView**, if alarm pop-up windows are enabled for the user profile, devices used with the **Audio recording** action are displayed in the alarm pop-up view when the alarm is triggered.



The action includes the following fields and parameters:

A) Pre-event recording. Mark this checkbox to set 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 hasbeen 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 containing 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 containing this action type is triggered, the video feed from the selected camera is displayed on the selected video output.

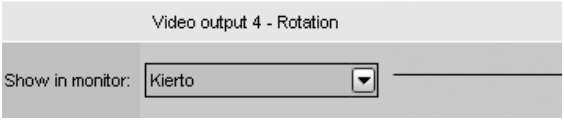
The action includes the following fields and parameters:

A) 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 containing 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:

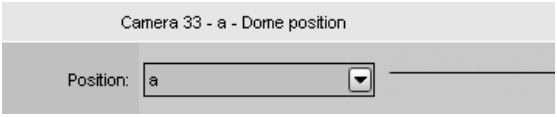
A) Show in monitor. Use the drop-down menu to select the camera tour from which the video feed is displayed in the selected video output during the alarm.

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 PRESET POSITION

The **PTZ/Dome preset position** action can be used to set a PTZ camera to a specified preset position. When an alarm containing this action type is triggered, the dome camera will automatically move to the selected preset position. Please see *Ernitec VMS EasyView User's Guide* for information on setting PTZ camera preset positions.

It should be noted that this action moves the dome camera to a preset position but does not result in the video feed from the dome 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 dome camera.



The action includes the following fields and parameters:

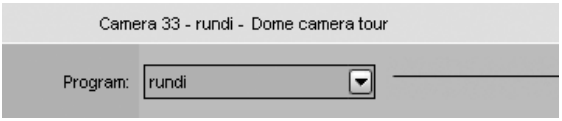
A) Position. Use the drop-down menu to select the preset position to which the dome camera will move during the alarm.

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 CAMERA TOUR

The **PTZ/Dome camera tour** action can be used to set a PTZ camera to start a pre-programmed PTZ camera tour. When an alarm containing this action type is triggered, the selected PTZ camera tour is started. Please see *Ernitec VMS EasyView 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.



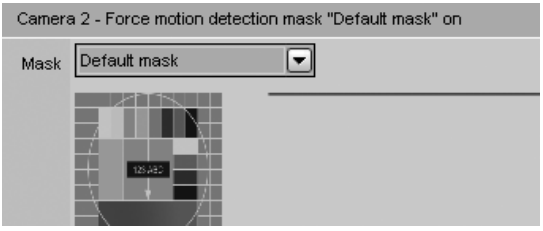
The action includes the following fields and parameters:

A) Program. Use the drop-down menu to select the dome camera tour which will start running when the alarm is triggered.

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

SET MOTION DETECTION MASK

The **Set motion detection mask** action can be used to change the motion detection mask used by a specific camera during the alarm. When the alarm occurs, the motion detection mask used for the designated camera is changed to the alarm specific mask. After the alarm ends, the system restores the default mask.



The action includes the following fields and parameters:

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

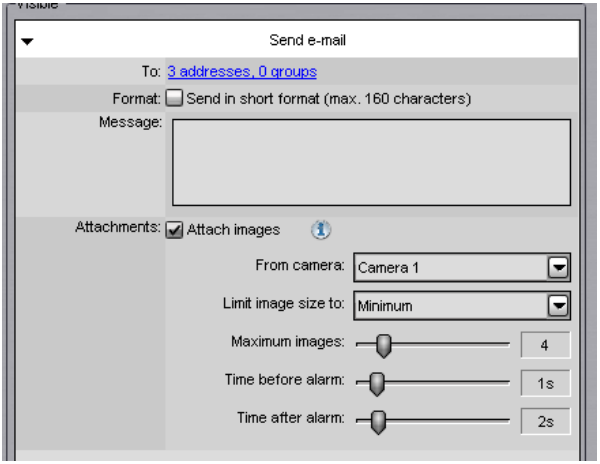
NOTE: *Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

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



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

NOTES:

- *The amount 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:

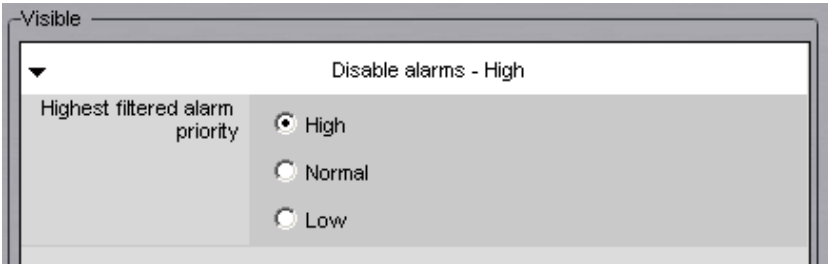
- *Unlike other alarm actions, the **Send e-mail** action can be selected only once for each alarm. Once selected, the action will disappear from the list of available actions.*
- *The message will have alarm name in title.*

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

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 recorder, 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 recorder 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.

When adding a local hard disk for the recorder, make sure that it is of the same capacity than the other disk or disks. This is because the recorder reserves an equal quantity of space on each disk and then writes data on them much like RAID-0. For example, if there are three disks, the recorder writes one second of data on disk 1, one second on disk 2, and one second on disk 3. Then it starts over from disk 1.

The difference to RAID-0 is that the recorder copies the same index data to all disks. Therefore, if one disk fails in a three-disk recorder, only one third of the data is lost.

There is one more advantage from using more than one disk. If one disk fails, the recorder will continue its operation, storing data on the remaining disks.

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. Click **Define network drive** to map the network drive.
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.

NOTE: *Recommended maximum size for a single storage disk is 10 TB.*

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 recorder's hard disks or on a network drive.

The archive files can be opened on any EasyView 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 recorder hard disks or network drives on which they are automatically saved.*

To set an automatic archiving schedule:

1. In the **Data storage** pane, click on the devices that you want to include in the automating archiving process.
   TIP: To select adjacent devices or folders, hold down the SHIFT key and then click the first and last device that you want to select. To add a device to a selection or to remove it from a selection, keep the CTRL key pressed and then click the device that you want to add or remove.
   NOTE: *Selecting a device group (folder) also selects its contents.*
2. Mark the **Archive** checkbox.
3. Click **Modify archive settings** .
4. Set the archive password by clicking **Change archive password** .
5. Select, whether to create the archive on a daily or weekly basis by selecting **Every day** or **Once a week**.
   - 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 recorder) or on a network drive by selecting **Recorder 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 recorders 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*:

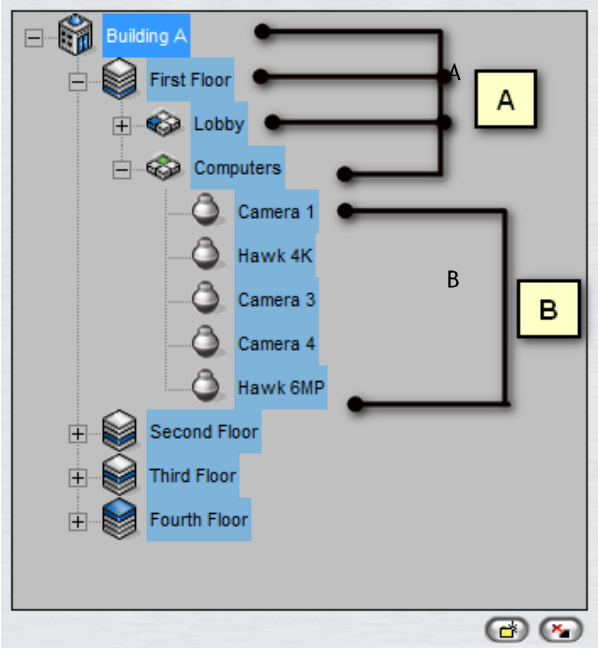
- Cameras (fixed cameras and dome cameras)
- Audio channels
- Audio communication channel
- Digital inputs (alarm inputs)
- Digital outputs (control outputs)
- Video outputs
- Text channels
- Alarms

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 Recorder 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 recorders.

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 EasyView program. The description is shown only in System Manager.
3. On the **Devices** tab, add device groups and devices to the profile. Or remove devices that you do not want the users to access. You can select devices from different recorders or from other profiles and even copy existing profiles.
4. For each device, you can set user rights. Under **Selected devices**, click the device and then select or clear the appropriate check boxes.
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 **Recorders** 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 EasyView 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 options applies to real-time and playback views.
6. Add as many device groups as necessary.

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 recorder 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 EasyView.
6. If the device is a dome camera, you can set the profile specific dome release time by using the **Automatic dome release** slider control. The setting defines the time the user can be idle before dome controls are released and other users can access the controls.
7. Under **User rights**, select the functions that the user can activate.
8. For text channels, you can also select what data is shown in the device window. Click the **Device Window Options** tab to access the settings.

Device window options for text channels

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

Show 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

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 recorder 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):

- **Administrator 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.
- **Archive viewing role:** This role enables the users to use EasyView to open data archives. Users with this role are allowed to login to EasyView but not to System Manager. They can perform all the basic operational functions in the EasyView application.
- **Custom role:** *Custom role* is an auxiliary role that can be set to any user role except for *Administrator role*. *Custom role* can be set for user groups with no roles (see *End user* below). *Custom role* provides the ability to restrict the functionalities the users can view and access in the **EasyView** application.
- **End user:** If no specific roles are selected for a user group, they are treated as end users. End users are allowed to login to EasyView but not to System Manager. They can perform all the basic operational functions in the EasyView application, except for viewing archives. **This is the default role for standard users.**

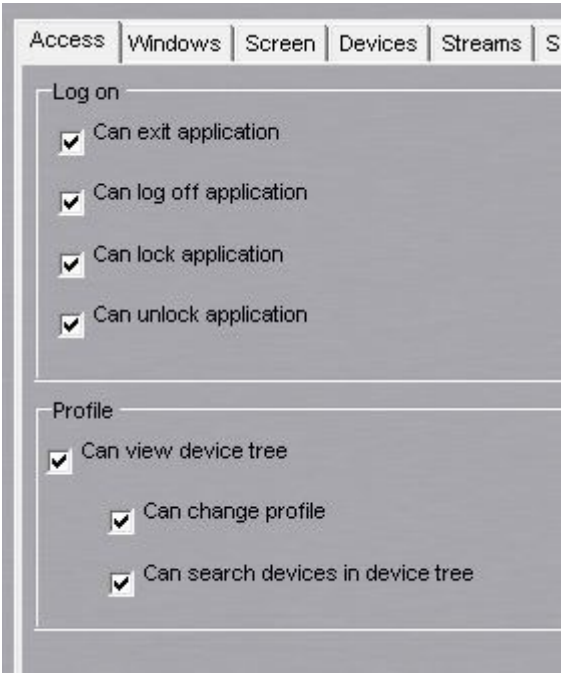
CUSTOM ROLES

Custom role provides the ability to restrict the functionalities the users can view and access in both **EasyView**.

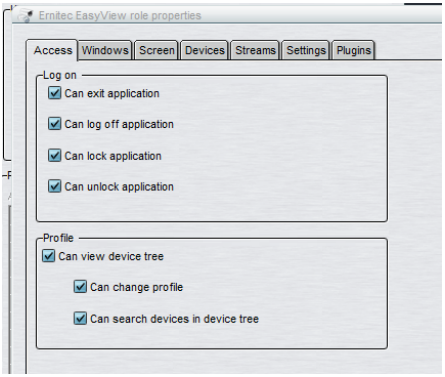
Custom user role properties can be edited by setting *Custom role* on and clicking the custom role properties edit button.

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

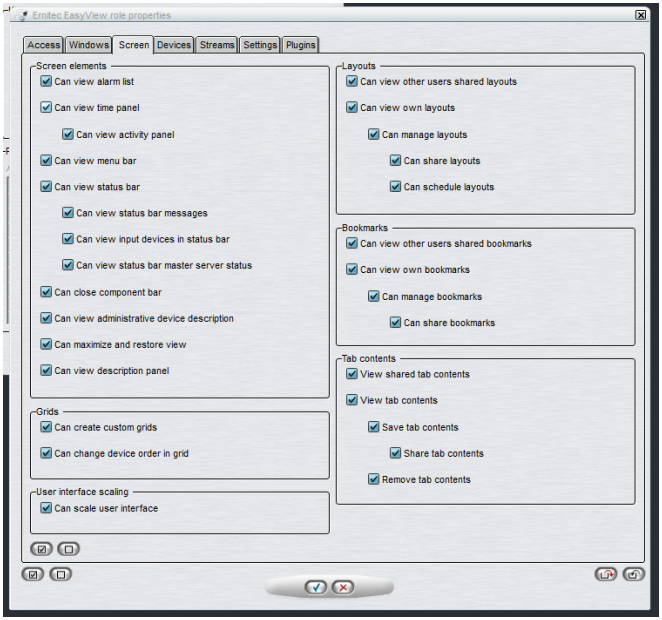
The first tab of the role customization contains options for the application access and the device tree visibility.



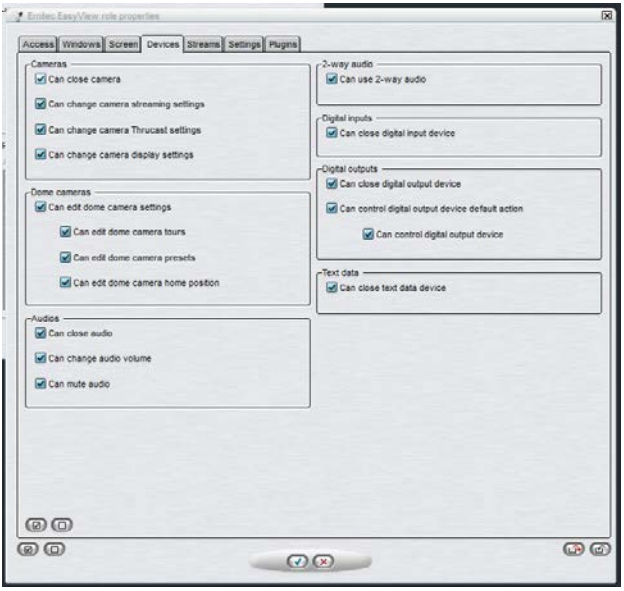
The second tab contains options for EasyView window management and tab management.



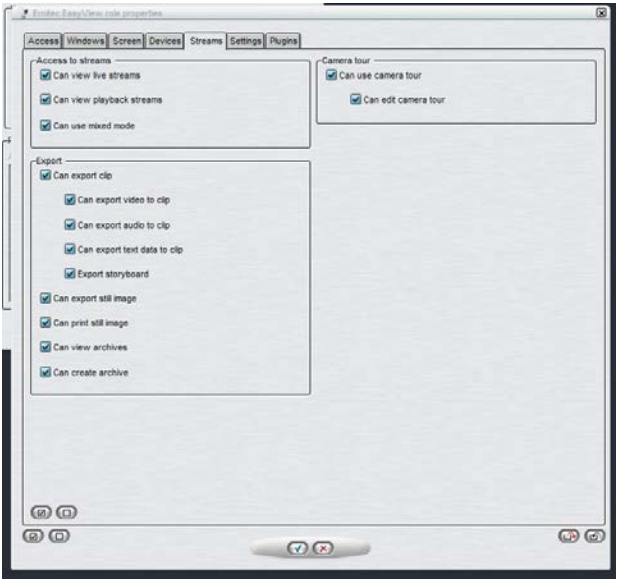
The third tab contains options for different screen element access and layout access, bookmarks and camera grid.



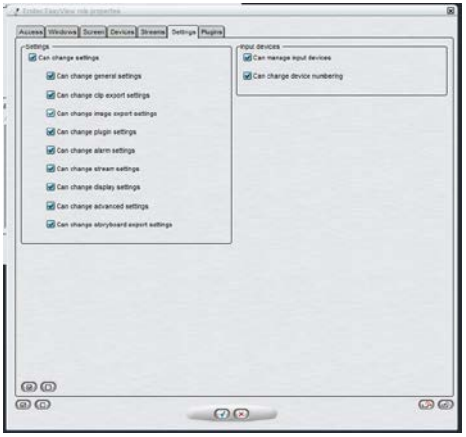
The fourth tab contains options for media control.



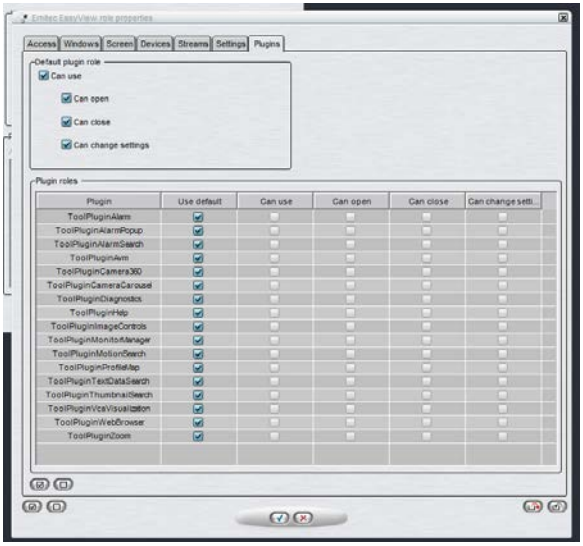
The fifth tab contains options for stream access and exporting.



The sixth tab contains options for EasyView settings.



The final tab contains options for plugins.



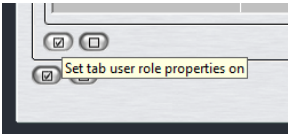
Each plugin behavior can be either default or custom. The default behavior can be controlled from the ”Default plugin role” controls.

EXPORTING AND IMPORTING USER ROLE SETTINGS

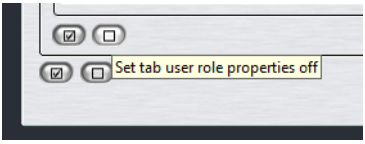
There are six new buttons in the bottom of the EasyView user role settings window:

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” (EasyView 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

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.
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.

DOMAIN BASED USER GROUPS (LDAP)

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

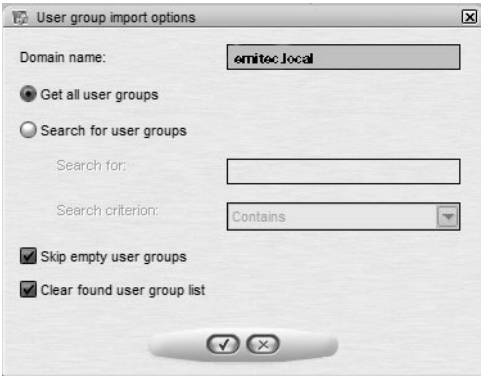
By default, user group rights are synchronized with their parent domain every 30 minutes. Please contact your system supplier if f you need to change the default interval.

This feature requires a license update.

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

1. Click **Import User Groups**  in the upper-left corner of the **Users** tab (next to the **Edit User Group** button). The master recorder needs to be connected to a domain for the button to be displayed. If the recorder is not connected to a domain, the button is not visible.
2. Type the name of the domain into the **User group domain** dialogue box.

3. Select, whether to get all user groups, or to search for specific groups. If you want to search specific groups by name, you can add a search criterion based on the text string 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.*

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 EasyView 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 EasyView program.*

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 EasyView 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 recorders, 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 recorder addresses
  - System addresses
- Update recorders
- Backup
  - Export files
- Exporting log files
- Back up system settings
- Restore system settings
- Diagnostics
  - SM Server diagnostics
  - Recorder diagnostics
- Licenses
- Software Watchdog
- Add-ins (drivers and plugins)

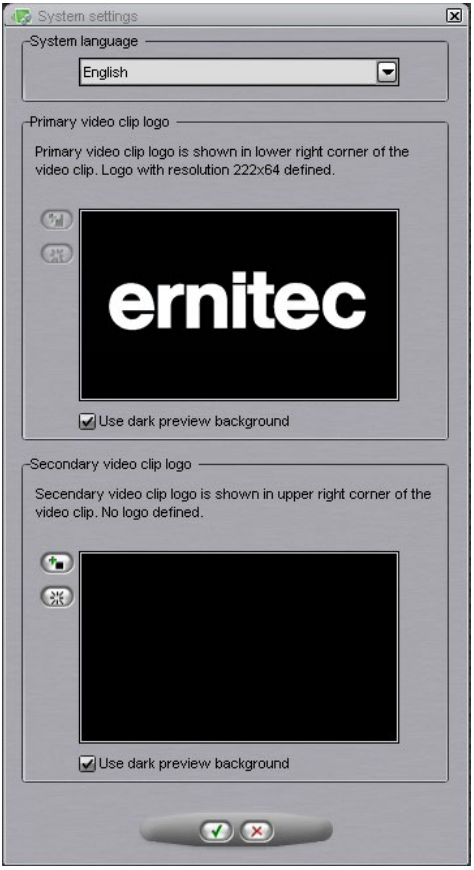
To open a tool, do one of the following:

- Click the tool and then click **Edit** .

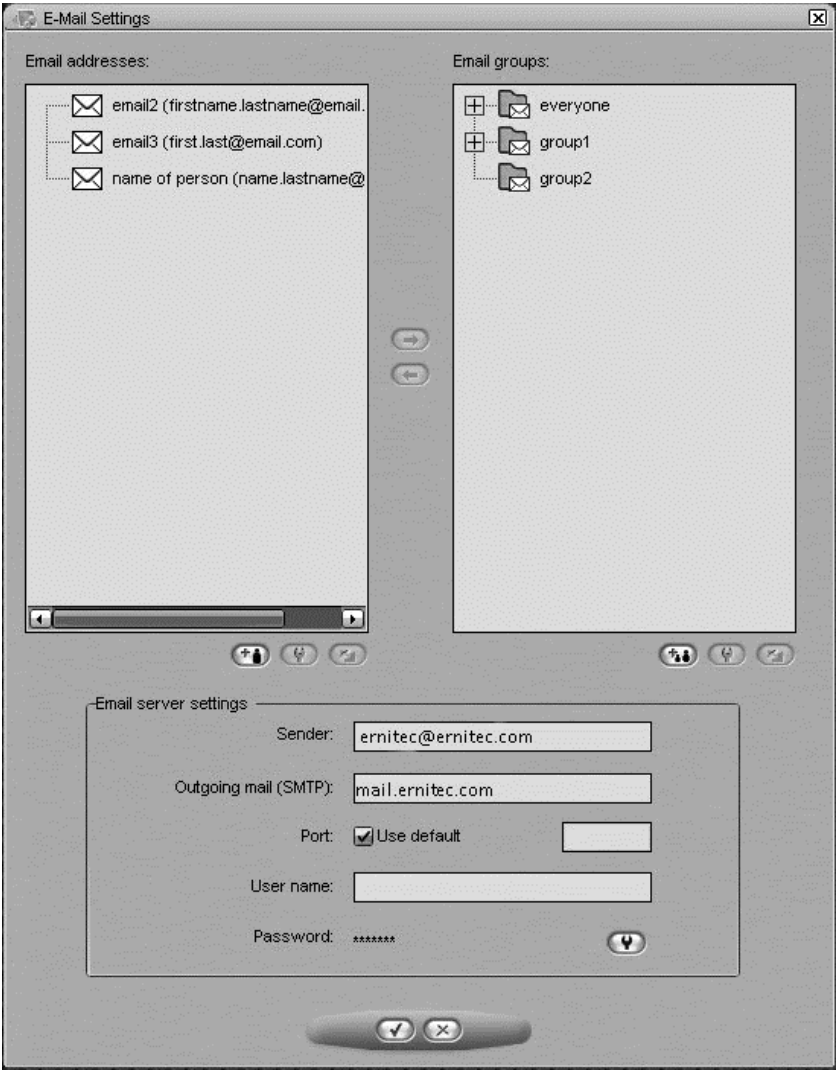
- Double-click the tool**.**
- Drag the tool from **System** tab to the workspace.

GENERAL SYSTEM SETTINGS

In this section you can control system language and the logos that are attached to exported video clips.



E-MAIL SETTINGS



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

To set the e-mail notification settings:

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

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

To add new e-mail addresses to the system:

1. On the **System** tab, open **E-mail settings**.
2. Click **Add new e-mail address**  to add a new address.
3. Type the recipient's name and e-mail address to the **Name** and **Address** fields.
4. Click **OK**.

To add new e-mail group to the system:

1. On the **System** tab, open **E-mail settings**.
2. Click **Add new e-mail address**  to add a new address.
3. Type the group name
4. Click **OK**.

To add one or more recipients to a group:

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

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

Other available actions:

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

MANAGING RECORDER ADDRESSES

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

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

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

MANAGING SYSTEM ADDRESSES (MASTER SERVER ADDRESSES)

A Master Server is the central server of a surveillance system. All other recording servers connect to it, and all client applications communicate through the Master Server. During the login phase, the client applications can select the Master Server they will connect to.

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

NOTE: *Users can connect to any of the defined Master Server addresses provided 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:

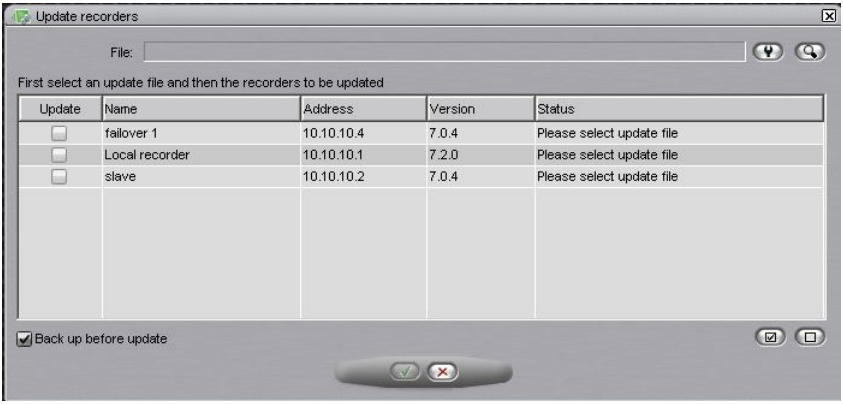
1. On the **System** tab, open **System addresses**.
2. Click on the Master Server address with the changed IP address.
3. Click **Modify system address** .
4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

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 RECORDING SERVERS

It is possible to update the local recorder and all connected recording servers remotely via the **Update recorders** –option



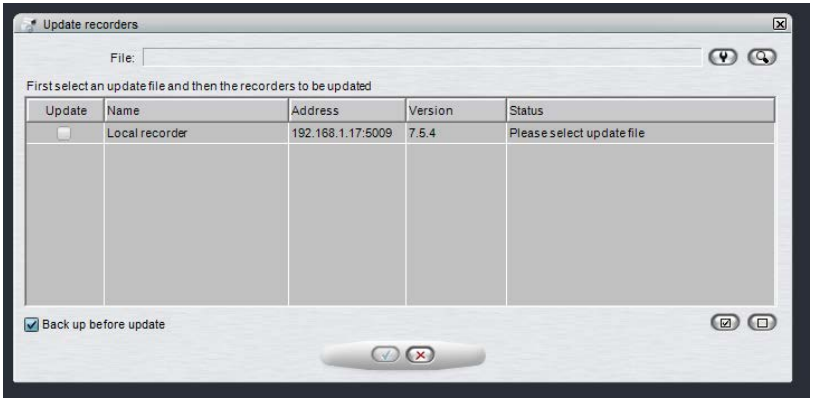
To update recorders, first select the installation file with the button.

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

NOTE: *When performing a major version upgrade, for example from VMS 6.x to 7.x, it is usually necessary to first upgrade the recorder licenses, and only after this upgrade the VMS software. The update recorders dialog will inform the user if license upgrade is needed before software update.*

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

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



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

NOTES:

- *If network connection to slaves 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 recorders.*

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

- *In rare cases, some slave recorders require system restart after remote VMS software update, if connection between master and slave is not returning after the update. It is recommended to monitor the connection to slaves after the update.*

- *Since Version 7.4.3 Ernitec VMS 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 EASYVIEW version. After the update, the control panel of windows will show EASYVIEW-x64 for 64-bit EASYVIEW.*

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**.
2. Select the logs to export and click **OK**.
   If there are problems with a recorder, select that recorder's logs. In addition, select the System Management Server and client program logs.
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 recorder settings. System settings contain data about the recorders, profiles, and user accounts. Recorder settings contain data about the devices connected to the recorders 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.
2. Select the system and recorder 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 recorder 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.
3. Select the system and recorder 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.

SYSTEM MANAGEMENT DIAGNOSTICS

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

GENERAL

In SMServer Diagnostics, you can examine this information:

- 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.**

RECORDER DIAGNOSTICS

Recorder diagnostics shows information about the recorder and the CPU and network usage.

DIAGNOSTICS

The **Diagnostics** tab shows this information:

- Information about the recorder:
  - 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 recorder was last started by the up time.

Recorder up time. Shows the time that the recorder 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 recorder 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.

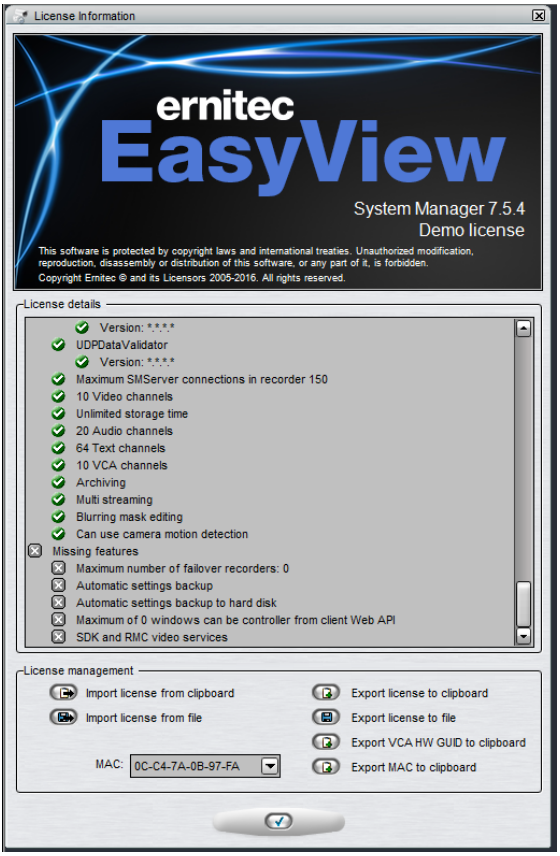
% used. This value shows what percentage of space the text channel has used of the total capacity reserved for the recordings.

LICENSES

The recorder needs a valid license for full functionality. Depending on the installation, you may need to upgrade the license information when adding new functionality or cameras to the system. To get a license key, please contact your supplier and follow the license upgrade procedure as detailed by the supplier. If you have any problems in upgrading the license, please contact *orders@Ernitec.com*.

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

To import a license key:



1. On the **System** tab, under **Licenses**, double-click the recorder that you want to update.

2. In the License Information dialog box, copy the MAC address and either:
    - Purchase a license key from the Ernitec Extranet
    - Or send the MAC address to your supplier, (or, in specific cases *orders@Ernitec.com*)

    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 recorder 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.

AUTOMATICALLY UPDATING SLAVE SERVER LICENSES

You can automatically update slave server licenses (and software) through the System Manager. For more information, please refer to the *Installation Guide*.

SOFTWARE WATCHDOG

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

In the Software 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 recorder. Alternatively, you can select the same events for all recorders by selecting **All recorders** 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 recorder specific; you have to select a specific recorder from the **Recorder** drop-down list.

To set a digital output notification:

1. On the **System** tab, select **Watchdog settings**.
2. Select a recorder from the **Recorder** drop-down list. As digital output signals are recorder specific, you cannot select **All recorders**.
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 recorders. However, you can select one or several recorders 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 (x86)\EASYVIEW\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.

Ernitec provides tailored customization services for Watchdog customization. Please contact *info@Ernitec.com* for information.

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. Ernitec takes no responsibility for XML errors caused by editing the files.*

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 VMS system, the driver for each device must be installed on the recorder. 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 recorders. It usually installs the files only if they do not exist on the recorders, or if the files in the installation package are newer than the files on the recorders. 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.
3. Select the recorders 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

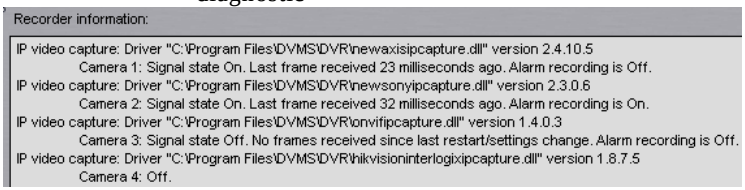
ThruCast (direct streaming from camera to EasyView client) requires different type of camera driver. These are called (Managed) ThruCast Client drivers.

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

REMOVING DRIVERS

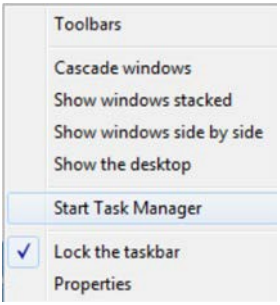
1. Identify driver you wish to remove/disable
2. Remove the cameras using the driver in question using System Manager
    a) Drivers installed on a Recorder can be found through the System Manager's *Local Recorder* diagnostics

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

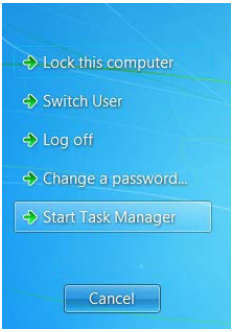


b) The instructions for camera removal can be found in the chapter *Cameras*, subchapter *Adding and Removing IP Cameras*, page 32

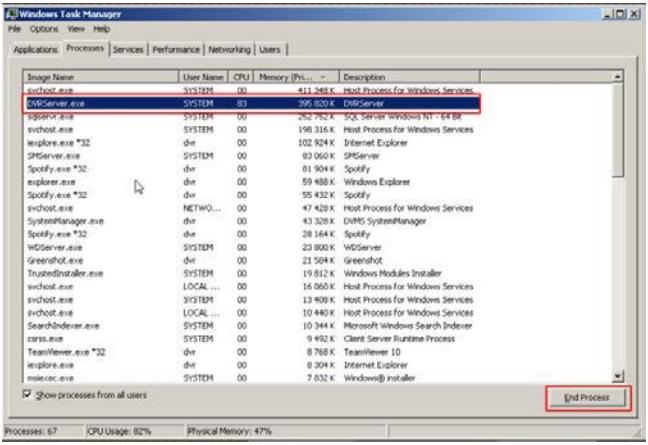
3. Shut down the recording service (DVRServer process)
   a) Open the Task manager
      i. Open by right-clicking the taskbar and select Start Task Manager



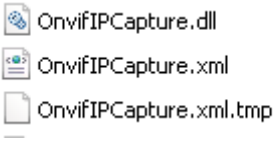
ii. Or open by using the **CTRL-ALT-DEL** key combination and select Start Task Manager



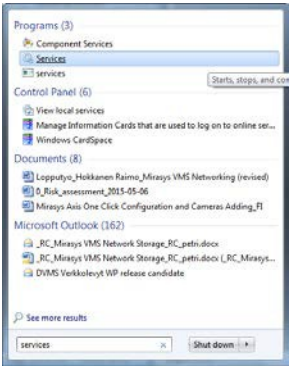
b) In Task Manager, select the *Processes* tab and select DVRServer.exe, then Right-click on the process and select End Process or click the *End Process* button.



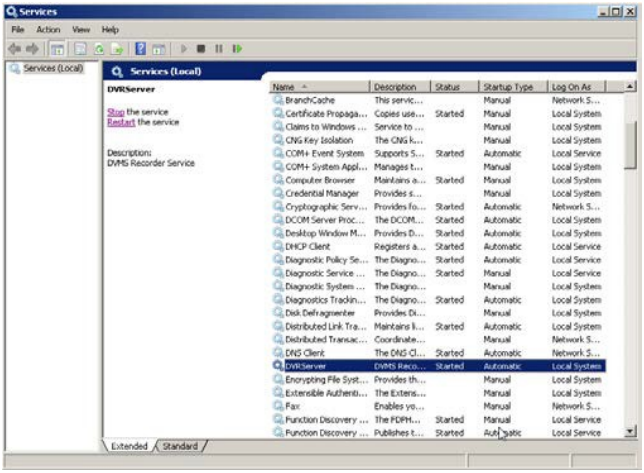
4. Delete the files 'X' from installation folder/directory'Y'
   a) The folder path for the driver files are found in the diagnostics, usually in ~\Program Files\EASYVIEW\DVR\ of the recording server's main hard drive
   b) Drivers create three files, the driver .dll, an .xml file and a temporary file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



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



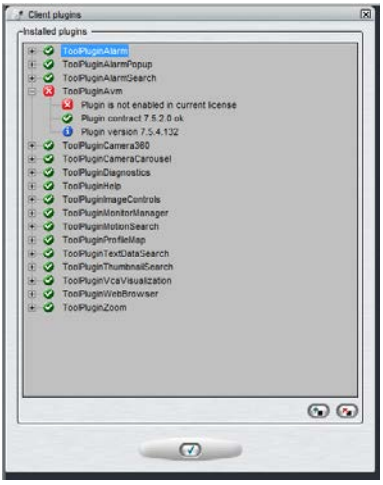
b) Browse to the DVRServer service



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

INSTALLING EASYVIEW PLUGINS

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



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 EasyView user interface.

To remove a client plugin:

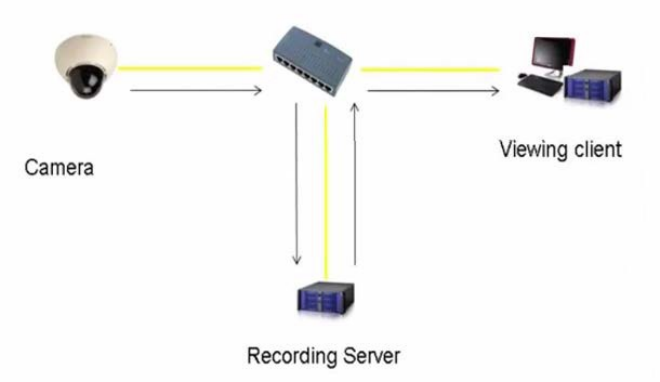
1. On the **System** tab, under Add-ins, open **Install client plugin**.
2. In the plugin installation window, select **Remove client plugin**.

THRUCAST

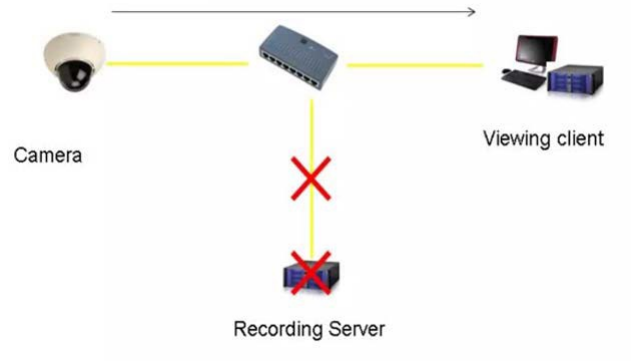
ThruCast is the direct camera video streaming feature in Ernitec VMS.

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

In a normal streaming scenario, the stream to the client comes from the recording server.



If the connection to the recording server is lost, with ThruCast 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 recording server connection is OK. This can be useful if users want to optimize network utilization.

SUPPORTED CAMERAS

ThruCast requires a separate camera capture driver for the client.

Currently, drivers exist for following camera manufacturers:

- ACTi,
- Axis,
- Bosch,
- Hikvision,
- Lilin
- Samsung,
- Sony,
- Stanley and
- ONVIF

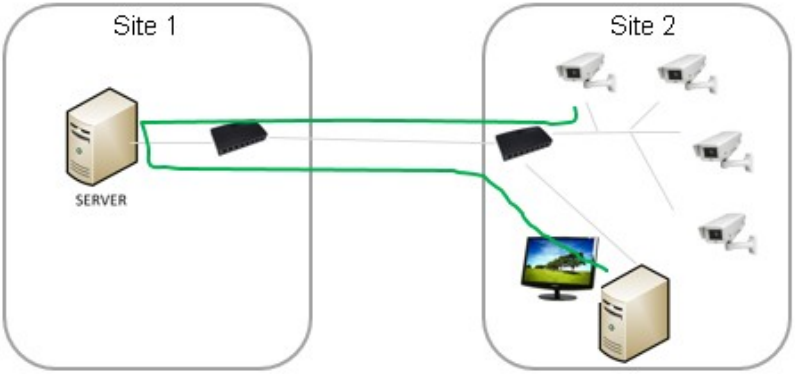
Use the ONVIF ThruCast driver for cameras that are not on the supported list.

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

NETWORK OPTIMIZATION

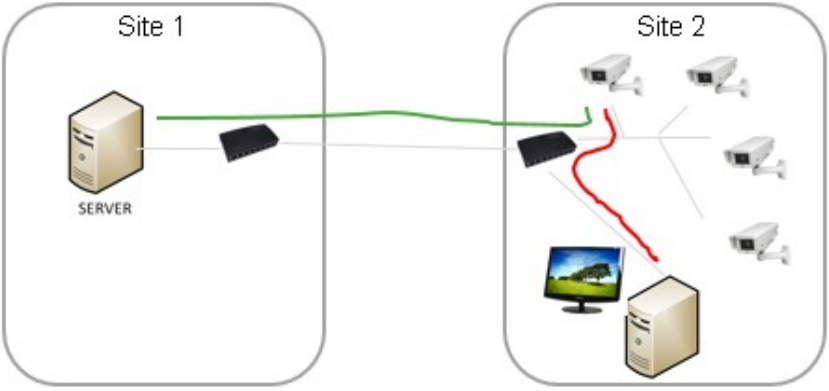
ThruCast can be used to reduce network load in specific scenarios. Mainly the load reduction takes place when the recording server is located off-site (remote), and the viewing client is on-site (local to the cameras).

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



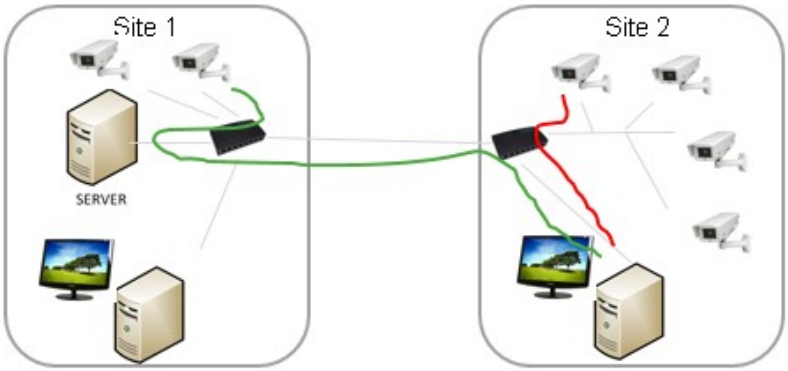
In this solution, the traffic between the two sites is increased.

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

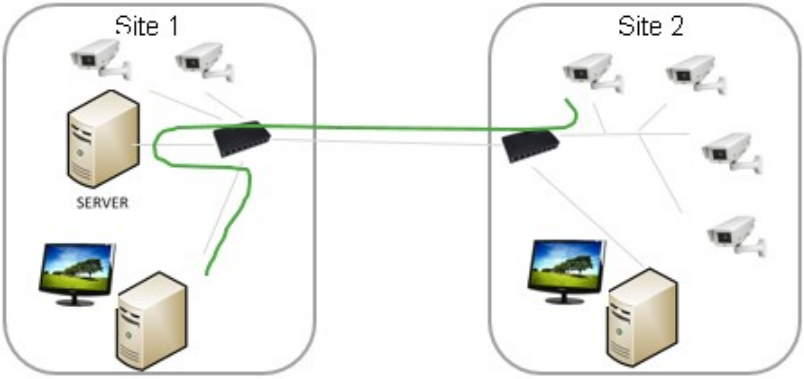


In the example scenario 2, there are cameras on two sites and viewing clients on two sites.

For the Site 2 user, the use of ThruCast makes more sense for the on-site cameras. The user can choose to use ThruCast for all cameras or only for the on-site cameras.



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



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

IMPACT OF MULTISTREAMING AND THRUCAST FOR NETWORK OPTIMIZATION AND STORAGE

Since it is also possible to use a different stream for ThruCast than the recording stream, this should be taken into consideration when planning the network capacity.

For example, users can choose to view live images with ThruCast at a higher framerate (for example 25 fps) and always record at lower framerate (for example 8 fps). This reduces the storage and network requirements considerably.

OTHER INFORMATION

IMPACT OF THRUCAST TO IMAGE DELAY

Since the ThruCast stream does not travel to the recording server and back, the delay from the camera to the client is slightly smaller, but the difference to the stream received from the recording 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 THRUCAST STREAMING

ThruCast does not support PTZ control or Audio

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

LICENSES

ThruCast requires the VMS license to have the “ThruCast” feature and the ThruCast client driver identifiers that are being used.

These ThruCast driver licenses, and the ThruCast feature, are always enabled in the Ernitec Enterprise product version.

MULTIPLE VIEWERS

Since each ThruCast –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

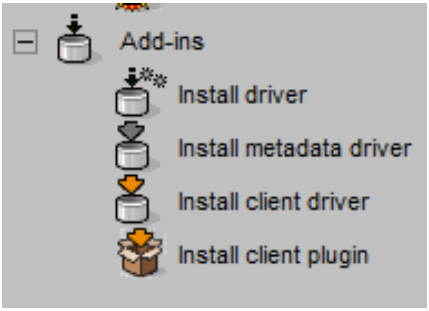
INSTALLING CLIENT DRIVERS

Before starting to use ThruCast, the necessary client drivers need to be installed with the System Manager application, if they have not been installed with the original system installation.

The client driver packages are available in the full setup package from Ernitec. 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 EasyView clients. This is done when EasyView is restarted from desktop.

After EasyView has downloaded the new drivers, the system is ready for ThruCast use.

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

CONFIGURING MULTI-STREAMING

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

The multi-streaming is enabled and configured normally in System Manager – cameras.

In the EasyView 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 ThruCast viewing.

THRUCAST DEFAULT SETTING

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

The possible values are

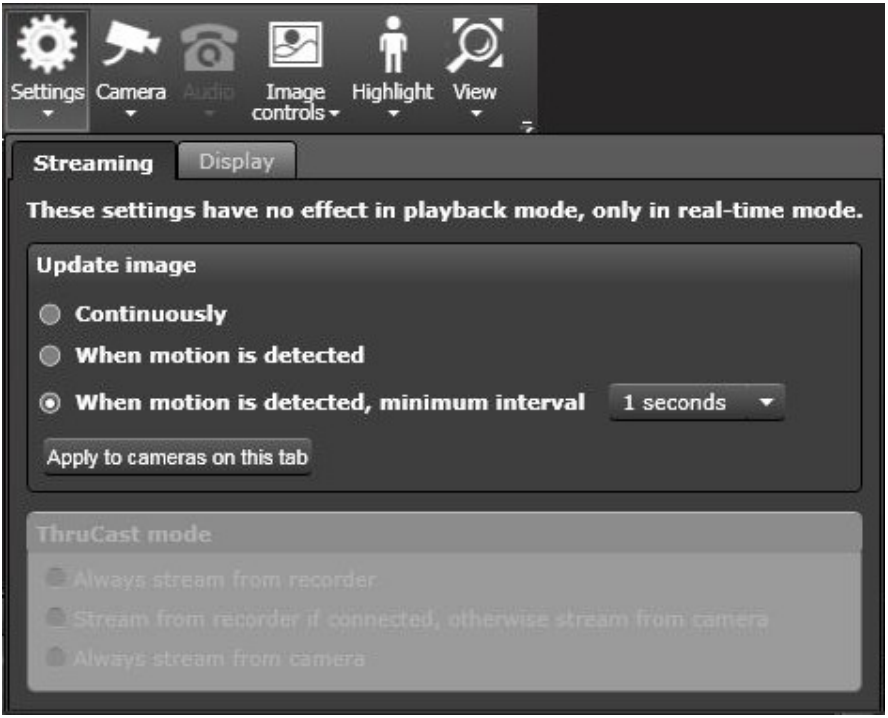
- Always stream from the recording server
- Stream from the recording server normally, but switch to ThruCast if the connection to the recording server is lost
- Always stream using ThruCast

USING THRUCAST

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

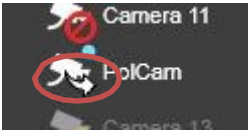
For those cameras that have ThruCast the setting is available.

For cameras that do not have ThruCast, the lower part of the dialog is disabled.



The setting is memorized for each camera separately.

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



COPYRIGHTS