SONY

Network Video Management System
Enterprise Edition 2016 R3

Administrator Manual

Contents

Copyright, trademarks and disclaimer

Copyright© 2016 Sony Corporation.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Sony Corporation reserve the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file **3rd_party_software_terms_and_conditions.txt** located in your surveillance system installation folder.

Before you start

Introduction to the help

The help is divided into sections that each serves a targeted purpose. The sections are structured in a logical flow:

System overview (on page 12)
Provides an introduction to your video surveillance system, system components, and concepts. This is useful if you are new to the system. The system overview also provides a comparison chart that lists the most significant differences between the products.

Installation (on page 22)
Provides installation preconditions and step by step procedures that help you install and upgrade your system.

First time use (on page 47)
Provides an overview of the Management Client and information about best practices to follow to have your system running smoothly. This overview is useful if you are new to the system.

Management Client elements (on page 54)
Provides a thorough walk through of each of the nodes in the **Site Navigation** pane of the Management Client. This section contains conceptual and procedural information about the basic elements of your system.

Feature configuration (on page 205)
Provides self-contained, detailed information about the additional features and add-on products that your system supports.

System maintenance (on page 235)
Provides an overview of the ports used in the system and step-by-step procedures for, for example, backing up your system and monitoring system performance. This section is useful after installation and configuration in order to maintain, expand and optimize your system.

Navigate the built-in help system

Press F1 to access a related help topic or select **Help** > **Contents** from the Management Client toolbar to launch the complete help.

You can navigate between the help window's three tabs: **Contents**, **Index**, and **Search** or use the links inside the help topics.

Tab	Description
Contents	Navigate the help system based on a tree structure.
Index	Select the first letter of the term you are interested in and scroll until you find it. Click a help topic title in the search results list to open the required topic.

Tab	Description
Search	Search for help topics that contain particular terms of interest. For example, search for the term **zoom** and receive a list in the search result of all help topics that contains the term **zoom**. Click a help topic title in the search results list to open the required topic.

To print a help topic, navigate to the required topic and click the browser's **Print** button.

System overview

Product overview

This Network Video Management System is a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance, with support for devices from different vendors. The solution offers centralized management of all devices, servers, and users, and empowers an extremely flexible rule system driven by schedules and events.

Your system consists of the following main elements:

- The **management server** - the center of your installation, consists of multiple servers.

- One or more **recording servers**.

- One or more **Network Video Management System Management Clients**.

- **Network Video Management System Download Manager**.

- One or more **Network Video Management System Smart Clients**.

- One or more **Network Video Management System Web Clients** and/or **NVMS Mobile clients** if needed.

Your system also includes fully integrated Matrix functionality for distributed viewing of video from any camera on your surveillance system to any computer with Network Video Management System Smart Client installed.

You can install your system on virtualized servers or on multiple physical servers in a distributed setup.

The system also offers the possibility of including the standalone Network Video Management System Smart Client – Player when you export video evidence from the Network Video Management System Smart Client. Network Video Management System Smart Client – Player allows recipients of video evidence (such as police officers, internal or external investigators and more) to browse and play back the exported recordings without having to install any software on their computers.

Your system can handle an unlimited number of cameras, servers, and users and across multiple sites if required. Your system can handle IPv4 as well as IPv6.

A distributed system setup
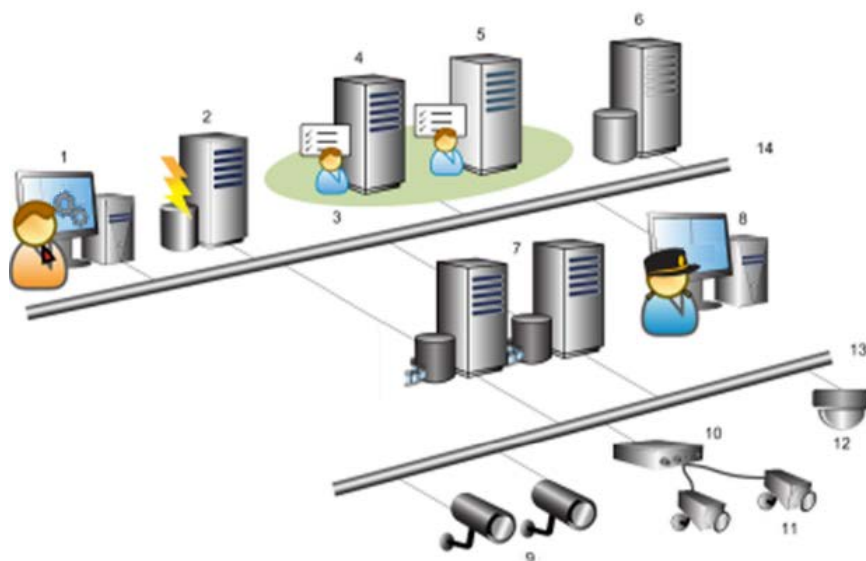
Example of a system setup. The number of cameras, recording servers, and connected clients, can be as high as you require.

Legend:

1. Management Client(s)
2. Event server
3. Microsoft cluster
4. Management server
5. Failover management server
6. SQL server
7. Recording server(s)
8. Network Video Management System Smart Client(s)
9. IP video cameras
10. Video server
11. Analog cameras
12. PTZ IP camera
13. Camera network
14. Server network

System components

Management server

The management server is the central component of the VMS system. It stores the configuration of the surveillance system in a relational database, either on the management server computer itself or on a separate SQL server on the network. It also handles user authentication, user rights, the

rule system and more. The management server runs as a service, and is typically installed on a dedicated server.

Users connect to the management server for initial authentication, then transparently to the recording servers for access to for video recordings, etc.

Failover management server

Failover support on the management server is achieved by installing the management server in a Microsoft Windows Cluster. The cluster will then ensure that another server take over the management server function should the first server fail.

Recording server

The recording server is responsible for communicating with the network cameras and video encoders, recording the retrieved audio and video as well as providing client access to both live and recorded audio and video.

Device Drivers

- Communication with the network cameras and video encoders are done through a device driver developed specifically for individual devices or a series of similar devices from the same manufacture.

- The device drivers are by default installed when the recording server is installed, but can later be updated by downloading and installing a newer version of the device pack.

Media Database

- The retrieved audio and video data is stored in the tailor-made high performance media database optimized for recording and storing audio and video data.

Event server

The event server handles various tasks related to events, alarms, maps and 3rd party integrations via the MIP Software Development Kit (SDK).

Events:

- All system events are consolidated in the event server so there are one place and interface for partners to make integrations that utilize system events.

- Furthermore, the event server offers 3rd party access to sending events to the system via the Generic events or Analytics events interface.

Alarms:

- The event server hosts the alarm feature, alarm logic, alarm state as well as handling the alarm database. The alarm database is stored in the same SQL server the management server uses.

Maps:

- The event server also hosts the maps that are configured and used in Network Video Management System Smart Client.

MIP SDK:

- Finally, third-party-developed plug-ins can be installed on the event server and utilize access to system events.

Log server

The log server is responsible for storing all log messages for the entire system. The log server uses the same SQL server as the management server and is typically installed on the same server as the management server, but can be installed on a separate server if needed to increase performance of the management and log servers.

SQL server

The management server, event server and log server uses an SQL server to store, for example, the configuration, alarms, events and log messaged.

The system installer includes Microsoft SQL Server Express that can be used freely for systems up to 300 cameras.

For larger systems over 300 cameras it is recommended to use the SQL Server 2008 R2 Standard or Enterprise edition on a dedicated server as these editions can handle larger databases and offer backup functionality.

Active Directory

Active Directory is a distributed directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. It identifies resources on a network in order for users or applications to access them.

With the Active Directory installed, you can add Windows users from Active Directory, but you also have the option of adding basic users without Active Directory. Note that there are certain system limitations related to basic users.

Virtual servers

You can run all system components on virtualized Windows® servers, such as VMware® and Microsoft® Hyper-V®.

Virtualization is often preferred to better utilize hardware resources. Normally, virtual servers running on the hardware host server do not load the virtual server to a great extent, and often not at the same time. However, recording servers record all cameras and video streams. This puts high load on CPU, memory, network, and storage system. So, when run on a virtual server, the normal gain of virtualization disappears to a large extent, since - in many cases - it uses all available resources.

If run in a virtual environment, it is important that the hardware host has the same amount of physical memory as allocated for the virtual servers and that the virtual server running the recording server is allocated enough CPU and memory - which it is not by default. Typically, the recording server needs 2-4 GB depending on configuration. Another bottleneck is network adapter allocation and hard disk performance. Consider allocating a physical network adapter on the host server of the virtual server running the recording server. This makes it easier to ensure that the network adapter is not overloaded with traffic to other virtual servers. If the network adapter is used for several virtual servers, the network traffic might result in the recording server not retrieving and recording the configured amount of images.

Clients

About the Management Client

Feature-rich administration client for configuration and day-to-day management of the system. Available in several languages.

Typically installed on the surveillance system administrator's workstation or similar.

For a detailed overview of the Management Client, see Management Client overview (on page 49).

About Network Video Management System Smart Client

Designed for Sony Network Video Management System IP video management software, the Network Video Management System Smart Client is an easy-to-use client application that provides intuitive control over security installations. Manage security installations with Network Video Management System Smart Client which gives users access to live and recorded video, instant control of cameras and connected security devices, and an overview of recordings. Available in multiple local languages, Network Video Management System Smart Client has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.

The interface allows you to tailor your viewing experience to specific working environments by selecting a light or dark theme, depending on room lighting or brightness of the video. It also features work-optimized tabs and an integrated video timeline for easy surveillance operation. Using the MIP SDK, users can integrate various types of security and business systems and video analytics applications, which you manage through Network Video Management System Smart Client.

Network Video Management System Smart Client must be installed on users' computers. Surveillance system administrators manage clients' access to the surveillance system through the Management Client. Recordings viewed by clients are provided by your Network Video Management System's Image Server service. The service runs in the background on the surveillance system server. Separate hardware is not required.

To download Network Video Management System Smart Client, you must connect to the surveillance system server which presents you with a welcome page that lists available clients and language versions. System administrators can use Network Video Management System Download Manager to control what clients and language versions should be available to users on the welcome page of the Network Video Management System Download Manager.

About NVMS Mobile client

NVMS Mobile client is a mobile surveillance solution closely integrated with the rest of your Network Video Management System. It runs on your Android tablet or smartphone, your Apple® tablet, smartphone or portable music player and gives you access to cameras, views and other functionality set up in the management clients.

Use the NVMS Mobile client to view and play back live and recorded video from one or multiple cameras, control pan-tilt-zoom (PTZ) cameras, trigger output and events and use the Video push functionality to send video from your device to your Network Video Management System.

If you want to use NVMS Mobile client with your system, you must add a Mobile server to establish the connection between the NVMS Mobile client and your system. Once the Mobile server is set up, download the NVMS Mobile client for free from Google Play or App Store to start using NVMS Mobile.

You need one hardware device license per device that should be able to push video to your Network Video Management System.

About Network Video Management System Web Client

Network Video Management System Web Client is a web-based client application for viewing, playing back and sharing video. It provides instant access to the most commonly used surveillance functions, such as viewing live video, play back recorded video, print and export evidence. Access to features depends on individual user rights which are set up in the management client.
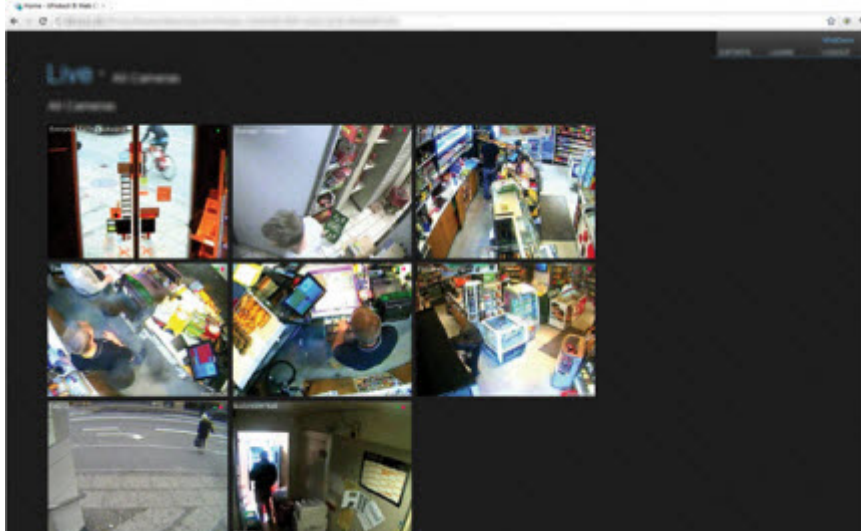
To enable access to the Network Video Management System Web Client, you must install a Mobile server to establish the connection between the Network Video Management System Web Client and your system. The Network Video Management System Web Client itself does not require any installation itself and works with most Internet browsers. Once you have set up the Mobile server, you can monitor your Network Video Management System anywhere from any computer or tablet with Internet access (provided you know the right external/Internet address, user name and password).

About licenses

In the navigation tree, you can also see your SLC if you select **Basics** > **License Information**.

You have purchased at least two types of licenses:

Base licenses: As a minimum, you have a base license for one of the Network Video Management System products. You may also have one or more base licenses for Network Video Management System add-on products.

Hardware device licenses: Every hardware device that you add to your Network Video Management System requires a hardware device license. You do not need hardware device licenses for speakers, microphones or input and output devices attached to your cameras. You need only one hardware device license per video encoder IP address even if you connect several cameras to the video encoder. A video encoder can have one or more IP addresses.

For more information, see the list of supported hardware on the Sony website http://www.sony.net/CameraSystem/NVMS/Technical-documents. If you want to use the video push feature in NVMS Mobile, you also need one hardware device license per mobile device or tablet that should be able to push video to your system.

About IPv6 and IPv4

Your system supports IPv6 as well as IPv4. So does Network Video Management System Smart Client.

IPv6 is the latest version of the Internet Protocol (IP). The Internet protocol determines the format and use of IP addresses. IPv6 coexists with the still much more widely used IP version IPv4. IPv6 was developed in order to solve the address exhaustion of IPv4. IPv6 addresses are 128-bit long, whereas IPv4 addresses are only 32-bit long.

It meant the the Internet's address book grew from 4.3 billion unique addresses to 340 undecillion (340 trillion trillion trillion) addresses. A growth factor of 79 octillion (billion billion billion).

More and more organizations are implementing IPv6 on their networks. For example, all US federal agency infrastructures are required to be IPv6 compliant. Examples and illustrations in this manual reflect use of IPv4 because this is still the most widely used IP version. IPv6 works equally well with the system.

About using the system with IPv6

The following conditions apply when using the system with IPv6:

Servers

Servers can often use IPv4 as well as IPv6. However, if just one server in your system (for example, a management server or recording server) requires a particular IP version, all other servers in your system must communicate using the same IP version.

> **Example**: All of the servers in your system except one can use IPv4 as well as IPv6. The exception is a server which is only capable of using IPv6. This means that all servers must communicate with each other using IPv6.

Devices

You can use devices (cameras, inputs, outputs, microphones, speakers) with a different IP version than that being used for server communication provided your network equipment and the recording servers also support the devices' IP version. See also the illustration below.

Clients

If your system uses IPv6, users should connect with the Network Video Management System Smart Client. The Network Video Management System Smart Client supports IPv6 as well as IPv4.

If one or more servers in your system can **only** use IPv6, Network Video Management System Smart Client users **must** use IPv6 for their communication with those servers. In this context, it is important to remember that Network Video Management System Smart Clients technically connect to a management server for initial authentication, and then to the required recording servers for access to recordings.

However, the Network Video Management System Smart Client users do not have to be on an IPv6 network themselves, provided your network equipment supports communication between different IP versions, and they have installed the IPv6 protocol on their computers. See also illustration. To install IPv6 on a client computer, open a command prompt, type *Ipv6 install*, and press **ENTER**.

Example illustration
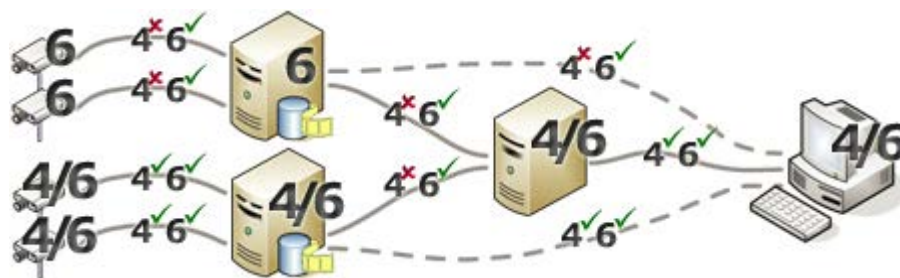
Example: Since one server in the system can only use IPv6, all communication with that server must use IPv6. However, that server also determines the IP version for communication between all other servers in the system.

No Matrix Monitor compatibility

If using IPv6, you cannot use the Matrix Monitor application with your system. Matrix functionality in Network Video Management System Smart Client is not affected.

About writing IPv6 addresses

An IPv6 address is usually written as eight blocks of four hexadecimal digits, with each block separated by a colon.

> **Example:** *2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

You may shorten addresses by eliminating leading zeros in a block. Also note that some of the four-digit blocks may consist of zeros only. If any number of such 0000 blocks are consecutive, you may shorten addresses by replacing the 0000 blocks with two colons as long as there is only one such double colon in the address.

> **Example:**
> *2001:0B80:0000:0000:0000:0F80:3FA8:18AB* can be shortened to
>
> *2001:B80:0000:0000:0000:F80:3FA8:18AB* if removing the leading zeros, or to
>
> *2001:0B80::0F80:3FA8:18AB* if removing the 0000 blocks, or even to
>
> *2001:B80::F80:3FA8:18AB* if removing the leading zeros as well as the 0000 blocks.

Using IPv6 Addresses in URLs

IPv6 addresses contain colons. Colons, however, are also used in other types of network addressing syntax. For example, IPv4 uses a colon to separate IP address and port number when both are used in a URL. IPv6 has inherited this principle. Therefore, to avoid confusion, square brackets are put around IPv6 addresses when they are used in URLs.

> **Example** of a URL with an IPv6 address:
> http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB*]*, which may of course be shortened to, for example, http://[2001:B80::F80:3FA8:18AB*]*

> **Example** of a URL with an IPv6 address and a port number:
> http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, which may of course be shortened to, for example, http://[2001:B80::F80:3FA8:18AB]:1234

For more information about IPv6, see, for example, the IANA website http://www.iana.org/numbers/. IANA, the Internet Assigned Numbers Authority, is the organization responsible for the global coordination of IP addressing.

System requirements

For information about the **minimum** system requirements to the various components of your system, go to the Sony website http://www.sony.net/CameraSystem/Product-info.

Installation

Before you start installation

Go through all these mandatory and important prerequisites before you start the actual installation.

Prepare Active Directory

If you want to add users to your system through the Active Directory service, you must have a server with Active Directory installed and acting as domain controller available on your network.

For easy user and group management, Sony recommends that you have Microsoft Active Directory® installed and configured before you install your Network Video Management System. If you add the management server to the Active Directory after installing your system, you must reinstall the management server, and replace users with new Windows users defined in the Active Directory.

Installation method

As part of the installation wizard, you must decide which installation method to use. You should base your selection on your organization's needs, but it is very likely that you already decided on the method when you purchased the system.

Options	Description
Single Server	Installs all management server components, recording server, and Network Video Management System Smart Client on the current computer. You only need to make a minimum of selections and all components are preselected in the un-editable component list. Depending on hardware and configuration, smaller systems with up to 50-100 cameras can run on a single server. The SQL server is not in the list, but is also installed on the current computer.
Distributed	Installs only the management server components on the current computer. This means that the recording server and Network Video Management System Smart Client are not visible in the component list. You cannot edit anything in the component list.

You must install the recording server, Network Video Management System Smart Client, and SQL server on other computers afterwards. |

Options	Description
Custom	The management server is always selected in the system component list and is always installed, but you can select freely what to install on the current computer, such as the other management server components, the recording server and Network Video Management System Smart Client. By default, the recording server is cleared in the component list, but you can change this. Depending on your selections, you must install the cleared components and the SQL server on other computers afterwards.

Single Server
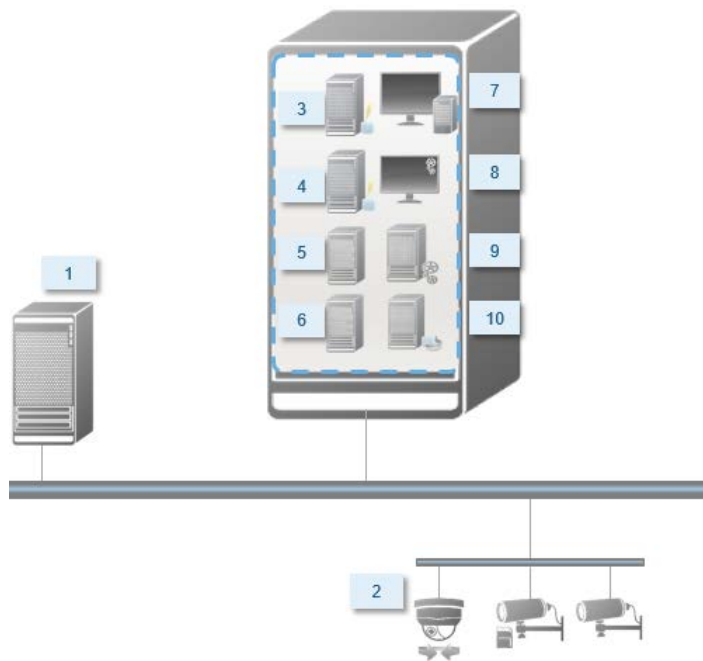
Typical system components in a system:

1. **Active Directory**
2. **Devices**
3. **SQL server**
4. **Event server**
5. **Log server**
6. **Service channel**
7. **Network Video Management System Smart Client**
8. **Management Client**
9. **Management server**
10. **Recording server**
11. **NVMS Mobile server**
12. **Network Video Management System Web Client**

13. **NVMS Mobile client**

14. **Network Video Management System Smart Client with Network Video Management System Smart Wall**

Distributed
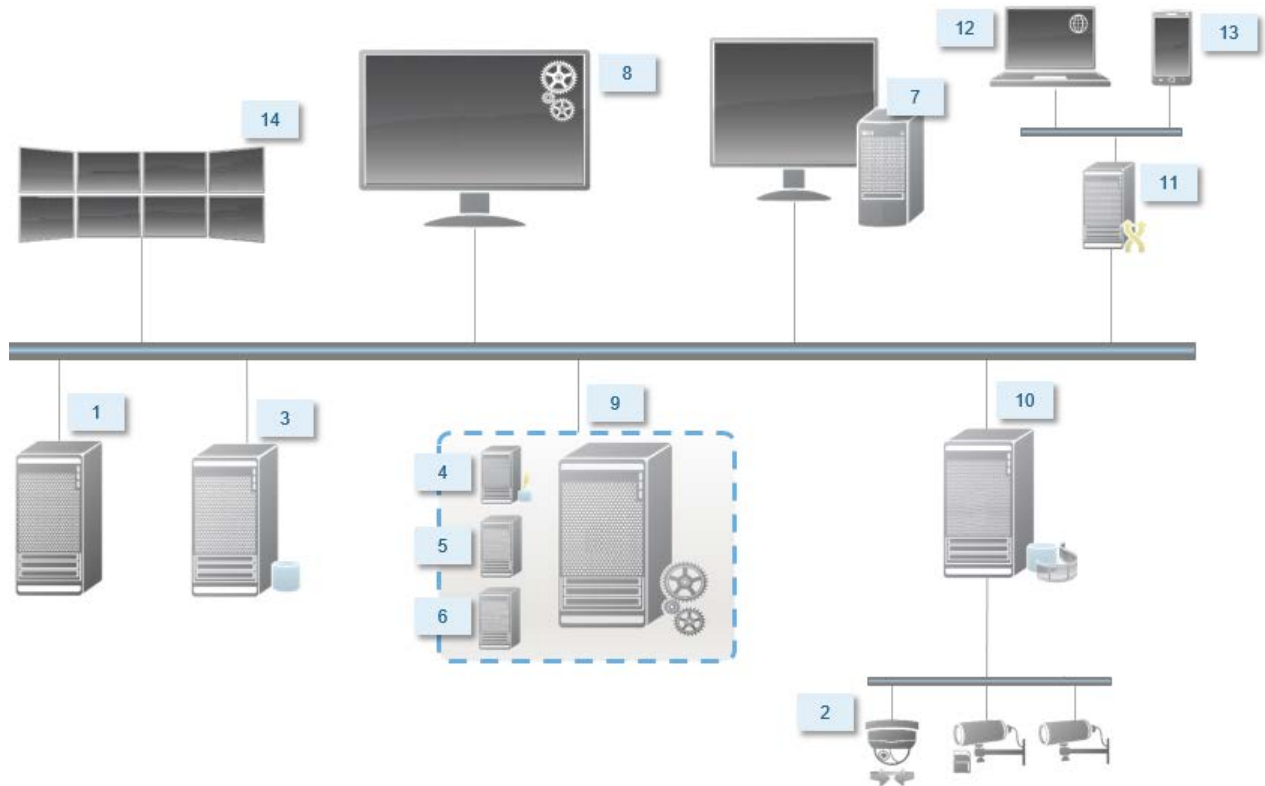
Determine SQL server type

The Microsoft SQL Server Express Edition is a "lightweight" version of a full SQL server. It is easy to install and prepare for use, and is often a good choice for systems with less than 300 cameras. This version of the SQL Server is included in the single server installation.

For large installations with more than 300 cameras, Sony recommends that you use a dedicated existing SQL server on a dedicated computer on the network. You must have administrator rights on the SQL server.

Sony recommends that you install the database on a dedicated hard disk drive that is not used for other purposes. Installing the database on its own drive improves the entire system performance.

When you select **Distributed** or **Custom** as part of the installation wizard, you must decide what to do regarding the SQL server.

If you do not have an SQL server installed, the options are:

- **Install SQL Server Express on this computer**.

- **Use an existing SQL Server on the network:** When you use a dedicated computer for the SQL database on the network, the list of SQL servers that your account can access appears.

If you have an SQL server installed, the options are:

- **Use the installed Microsoft SQL Server Express database on this computer**.

- **Use an existing SQL Server on the network:** When you use a dedicated computer for the SQL database on the network, the list of SQL servers that your account can access appears.

  You are also asked whether you want to create a new database, use an existing database, or overwrite an existing database.

  - **Create new database**: For a new installation.

  - **Use existing database**: If you are installing the database as part of an upgrade of the system, and you want to use your existing database.

Select service account

As part of the installation, you are asked to specify an account to run the Sony services on this computer. The services always run on this account no matter which user is logged in. Make sure that the account has all necessary user rights, for example, the proper rights to perform tasks, proper network and file access, and access to network shared folders.

You can select either a predefined account, or a user account. Base your decision on the environment that you want to install your system in:

Domain environment

In a domain environment:

- Sony recommends that you use the built-in Network Service account. It is easier to use even if you need to expand the system to multiple computers.

- You can also use domain user accounts, but they are potentially more difficult to configure.

Workgroup environment

In a workgroup environment, Sony recommends that you use a local user account that has all necessary rights. This is often the administrator account.

Important: If you have installed your system components on multiple computers, the selected user account must be configured on all computers in your installations with identical user name, password, and access rights.

About Kerberos authentication

Kerberos is a ticket-based network authentication protocol. It is designed to provide strong authentication for client/server or server/server applications.

Use Kerberos authentication as an alternative to the older Microsoft NT LAN (NTLM) authentication protocol.

Kerberos authentication requires mutual authentication, where the client authenticates to the service and the service authenticates to the client. This way you can authenticate more securely from Network Video Management System clients to Network Video Management System servers without exposing your password.

To make mutual authentication possible in your Network Video Management System video management software you must register Service Principal Names (SPN) in the active directory. An SPN is an alias that uniquely identifies an entity such as a Network Video Management System

server service. Every service that uses mutual authentication must have an SPN registered so that clients can identify the service on the network. Without correctly registered SPNs, mutual authentication is not possible.

The table below lists the different Sony services with corresponding port numbers you need to register:

Service	Port number
Management server - IIS	80 - Configurable
Management server - Internal	8080
Recording server - Data Collector	7609
Event Server	22331

The number of services you need to register in the active directory depends on your current installation. Data Collector is installed automatically when installing Management Server, Recording Server, or Event Server.

You must register two SPNs for the user running the service: one with the hostname and one with the fully qualified domain name.

If you are running the service under a network user service account, you must register the two SPNs for each computer running this service.

This is the Sony SPN naming scheme:
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]

The following is an example of SPNs for the recording server service running on a computer with the following details:
Hostname: Record-Server1
Domain: Surveillance.com

SPNs to register:
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609

About virus scanning

As is the case with any other database software, if an antivirus program is installed on a computer running Network Video Management System software, it is important that you exclude specific file types and folders, as well as certain network traffic. Without implementing these exceptions, virus scanning uses a considerable amount of system resources. On top of that, the scanning process can temporarily lock files, which could result in a disruption in the recording process or even corruption of databases.

When you need to perform virus scanning, do not scan Recording Server folders that contain recording databases (by default C:\mediadatabase\, as well as all subfolders). Also, avoid performing virus scanning on archive storage directories.

Create the following additional exclusions:

- File types: .blk, .idx, .pic

- Folders and subfolders:

  - C:\Program Files\Sony or C:\Program Files (x86)\Sony

  - C:\ProgramData\Sony\MIPSDK

  - C:\ProgramData\Sony\NVMS Mobile Server\Logs

  - C:\ProgramData\Sony\- Network VMS Data Collector Server\Logs

  - C:\ProgramData\Sony\- Network VMS Event Server\logs

  - C:\ProgramData\Sony\- Network VMS Log Server

  - C:\ProgramData\Sony\- Network VMS Management Server\Logs

  - C:\ProgramData\Sony\- Network VMS Recording Server\Logs

  - C:\ProgramData\Sony\- Network VMS Report Web Server\Logs

  - C:\ProgramData\Sony\- Network VMS Service Channel\Logs

- Exclude network scanning on the following TCP ports:

Product	TCP ports
Network Video Management System Enterprise Edition	80, 8080, 7563, 25, 21, 9993
NVMS Mobile	8081

or

- Exclude network scanning of the following processes:

Product	Processes
Network Video Management System Enterprise Edition	VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
NVMS Mobile	VideoOS.MobileServer.Service.exe

Your organization may have strict guidelines regarding virus scanning, but it is important that you exclude the above folders and files from virus scanning.

Register Software License Code

Before you install, you must have the name and location of the software license file that you received from Sony.

Sony recommends that you register your SLC before installation. See the license guide on our website http://www.sony.net/CameraSystem/NVMS/Manuals.

Install the system

Select one of the installation options:

- Install your system - Single Server option (on page 28)

- Install your system - Distributed option (on page 29)

- Install your system - Custom option (on page 30)

Install your system - Single Server option

The **Single Server** option installs all management server components, recording server, and Network Video Management System Smart Client on the current computer. Depending on hardware and configuration, smaller systems with up to 50-100 cameras can run on a single server. You only need to make a minimum of selections and all components are preselected in the un-editable component list. The SQL server is not in the list, but is also installed on the current computer.

1. If you are installing a version downloaded from the Internet, run the `Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe` file from the location where you saved it.

   Alternatively, insert the software DVD. If the dialog box does not open automatically, run the `Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe` file from the DVD.

2. The installation files unpack. Depending on your security settings, one or more Windows® security warnings appear. Accept these and the unpacking continues.

3. When done, the **Sony Network Video Management System Enterprise Edition** dialog box appears,

   a) Select the **Language** to use during the installation (this is **not** the language your system uses once installed, this is selected later). Click **Continue**.

   b) In **Type the location of the license file**, enter your license file from your Network Video Management System provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.

   c) Read the *Sony End-user License Agreement*. Select the **I accept the terms in the license agreement** check box.

4. Select **Single Server**. A list of components to install appears (you cannot edit this list). Click **Continue**.

5. Select **File location** for the program file. In **Product language**, select the language in which your Network Video Management System product should be installed. Click **Install**.

6. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

   Microsoft® IIS is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security settings, one or more Windows security warnings may appear. Accept these and the installation completes.

7. When done, your installation completes and you can continue with configuration, see Configuration process (see "Configure the system in the Management Client" on page 37).

Install your system - Distributed option

The **Distributed** option installs only the management server components on the current computer. This means that the recording server and Network Video Management System Smart Client are not visible in the un-editable component list. You must install the recording server, Network Video Management System Smart Client, and SQL server on other computers.

1. If you are installing a version downloaded from the Internet, run the `Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe` file from the location where you saved it.

   Alternatively, insert the software DVD. If the dialog box does not open automatically, run the `Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe` file from the DVD.

2. The installation files unpack. Depending on your security settings, one or more Windows® security warnings appear. Accept these and the unpacking continues.

3. When done, the **Sony Network Video Management System Enterprise Edition** dialog box appears,

   a) Select the **Language** to use during the installation (this is **not** the language your system uses once installed, this is selected later). Click **Continue**.

   b) In **Type the location of the license file**, enter your license file from your Network Video Management System provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.

   c) Read the *Sony End-user License Agreement*. Select the **I accept the terms in the license agreement** check box.

4. Select **Distributed**. A non-editable list of components to be installed appears. Click **Continue**.

5. Select the type of SQL server database you want. Also specify the name of the SQL server. Click **Continue**.

6. Select either **Create new database** or **Use existing database** and name the database. If you choose the latter, select to **Keep** or **Overwrite** existing data. Click **Continue**.

7. Select **File location** for the program file. In **Product language**, select the language in which your Network Video Management System product should be installed. Click **Install**.

8. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

   Microsoft® IIS is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security settings, one or more Windows security warnings may appear. Accept these and the installation completes.

9. Install at least one recording server and Network Video Management System Smart Client on another computer.

See also

Install the recording server (on page 31)

Install your system - Custom option

The **Custom** option installs the management server always, but you can select freely among the other management server components, recording server, and Network Video Management System Smart Client to install on the current computer. By default, the recording server is unselected in the component list, but you can edit this. Depending on your selections you must install the unselected components afterwards on other computers plus the SQL server.

1. If you are installing a version downloaded from the Internet, run the `Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe` file from the location where you saved it.

   Alternatively, insert the software DVD. If the dialog box does not open automatically, run the `Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe` file from the DVD.

2. The installation files unpack. Depending on your security settings, one or more Windows® security warnings appear. Accept these and the unpacking continues.

3. When done, the **Sony Network Video Management System Enterprise Edition** dialog box appears,

   a) Select the **Language** to use during the installation (this is **not** the language your system uses once installed, this is selected later). Click **Continue**.

   b) In **Type the location of the license file**, enter your license file from your Network Video Management System provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.

   c) Read the *Sony End-user License Agreement*. Select the **I accept the terms in the license agreement** check box.

4. Select **Custom**. A list of components to be installed appears. Apart from the management server, all elements in the list are optional. The recording server is by default deselected, but you can change this if needed. Click **Continue**.

5. Select the type of SQL server database you want. If relevant, also specify the name of the SQL server. Click **Continue**.

6. Select either **Create new database** or **Use existing database** and name the database. If you choose the latter, select to **Keep** or **Overwrite** existing data. Click **Continue**.

7. Select either **This predefined account** or **This account** to select the service account. If needed, enter a password and confirm this. Click **Continue**.

8. If you have more than one available IIS website, you can select any of these. However, if any of your websites have HTTPS binding, select one of these. Click **Continue**.

9. Select **File location** for the program file. In **Product language**, select the language in which your Network Video Management System product should be installed. Click **Install**.

10. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

    Microsoft® IIS is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security

settings, one or more Windows security warnings may appear. Accept these and the installation completes.

11. Depending on your selections, install the remaining servers on other computers:

a) Go to the Management server's download web page from Windows' **Start** menu.

b) Select **Programs** > **Sony** > **Administrative Installation Page** and copy the Internet address.

c) Log into each of the computers to install:

- Log server.

- Event server.

- Management Client.

d) Open an Internet browser, paste the address of the Management server's download web page into the address field and download the relevant installer.

e) Run the installer.

12. Install the recording server on a separate computer, see Install the recording server (on page 31).

Install the recording server

Once you have installed the management server, download the separate recording server installer from the management server's web page.

1. On the management server, go to the Management server's download web page from Windows' **Start** menu.

2. Select **Programs** > **Sony** > **Administrative Installation Page** and copy the Internet address.

3. Log into the computer where you want to install the recording server.

4. Open an Internet browser, paste the address of the Management server's download web page into the address field and select the Recording Server installer. Save the installer somewhere appropriate and run it from here or run it directly from the web page.

5. Select the **Language** you want to use during the installation. Click **Continue**.

6. Select:

   Typical: to install a recording server with default values, or

   Custom: to install a recording server with custom values.

7. Specify the recording server settings:

- Name.

- Management server address.

- Path to save recordings, and click **Continue**.

8. If you selected **Custom**:

    a) Specify the number of recording servers you want to install on this computer. Click **Continue**.

    b) Specify the service account. If needed, enter a password and confirm this. Click **Continue**.

9. Select **Files location** for the program file. In **Product language**, select the language in which to install your system. Click **Install**.

10. The software is now installed. Once it is completed, you see a list of successfully installed components. Click **Close**.

    When you have installed the recording server, you can check its state from the **Recording Server service** icon.

11. When done, your installation completes and you can continue with configuration, see Configuration process (see "Configure the system in the Management Client" on page 37).

Install a recording server silently

The advantage of a silent install is that you can do it remotely. Follow the steps below:

1. Locate the recording server installation file: *Sony-NetworkVMSRecordingServerInstaller_x64.exe*.

    1. Log into the management server.

    2. Open an internet browser and type the address: http://localhost/Installation/Admin/

    3. Save the recording server installation file on the server where you want to install the new recording server.

        Or you can browse to the file. The path is typically:
        C:\Program Files\Sony\- Network VMS Management Server\IIS\httpdocs\Admin\Recording Server Installer\[version number] [bit-version]\All Languages\en-US

2. Run a silent installation using these options:

    *   Run with default parameter settings:

    To run a silent installation using the default values for all parameters, start a command prompt (cmd.exe) in the directory where the installation program is located and perform following command:

    >Sony-NetworkVMSRecordingServerInstaller_x64.exe --quiet

    *   To do customized installation you need to specify the list of parameters that you want to overwrite:

    For example, to change the path to Management Server of the installation, run:

    ><Sony-NetworkVMSRecordingServerInstaller_x64.exe --quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

These are the parameters that you may use through command line parameters:

- To change name of the recording server:

RECORDERNAME – name of the recorder that will appear in Management Client.

   --quiet --parameters=RECORDERNAME:NewRecorderName

- To change Management Server:

SERVERHOSTNAME – hostname of the Management Server where Recording Server will connect to

SERVERPORT – port of the Management Server (80 by default)

   --quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

- To install Recording Server as different user than NT AUTHORITY\NETWORK SERVICE:

RECUSERACCOUNT – flag that determines if user account is used or one of the predefined accounts

RECSERVICEACCOUNT – name of the used user or predefined service account

RECPASSWORD – encrypted! password for the user. Leave empty for predefined accounts.

To find out the encrypted version of the password you can run installer in usual mode. Open c:\ProgramData\Sony\Installer\Sony - Network VMS Recording Server (64_bit)I.log (there could be number added in the end of the name if more than one installation was ran on the computer)

Find string 'Command Line'. This would be full list of parameters that was used during installation. The one marked with ENCRYPTEDPASSWORD will have encrypted password.

   --quiet --parameters=RECUSERACCOUNT:true:RECSERVICEACCOUNT:Sony\okr:RECPASSWORD:encryptedpasswork

- In order to change the location of the installation from default you must first perform:

><Sony-NetworkVMSRecordingServerInstaller_x64.exe --generateargsfile=C:\temp

In the specified location you will find .xml file with the parameters. So you would need to change parameters in this file and run your installation with the newly modified file.

- To change location of the installation:

INSTALLDIR - path where Recording Server should be installed to

TARGETDIR – should be the same as INSTALLDIR

INSTALLLOCATION – should be the same as INSTALLDIR

- To change location of recordings:

MEDIADBPATH – path to the Media database with all recordings

E.g. modifications in my Argements_.xml were. My new location of the installation will be %ProgramFiles(x86)%\Sony\bla and new location for recordings is C:\MD

<KeyValueParametersOfStringString>

*<Value>***%ProgramFiles(x86)%\Sony\bla***</Value>*

<Key>INSTALLDIR</Key>

</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>

  *<Value>***%ProgramFiles(x86)%\Sony\bla***</Value>*

  <Key>TARGETDIR</Key>

</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>

  *<Value>***%ProgramFiles(x86)%\Sony\bla***</Value>*

  <Key>INSTALLLOCATION</Key>

</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>

  *<Value>***C:\MD***</Value>*

  *<Key>***MEDIADBPATH***</Key>*

</KeyValueParametersOfStringString>

Run the:

><Sony-NetworkVMSRecordingServerInstaller_x64.exe --quiet --arguments=C:\temp\Arguments_.xml

Troubleshooting

Where can I find the log files of the installation?

The log files of the installation are located under **C:\ProgramData\Sony\Installer**

How do I see a list of default parameters that will be used during a single server installation?

To see a list of parameters with all default values you can run **Sony-NetworkVMSRecordingServerInstaller_x64.exe --generateargsfile=C:\temp**

It will generate a file called Arguments.xml in the specified folder.

How do I see the parameters that were used during my customized installation?

The full list of parameters used to run the installation are in **C:\ProgramData\Sony\Installer\Sony Network Video Management System Recording Server (64_bit)I.log** + search for 'Command line'

How do I see a full list of possible parameters?

Run **Sony-NetworkVMSRecordingServerInstaller_x64.exe --help**
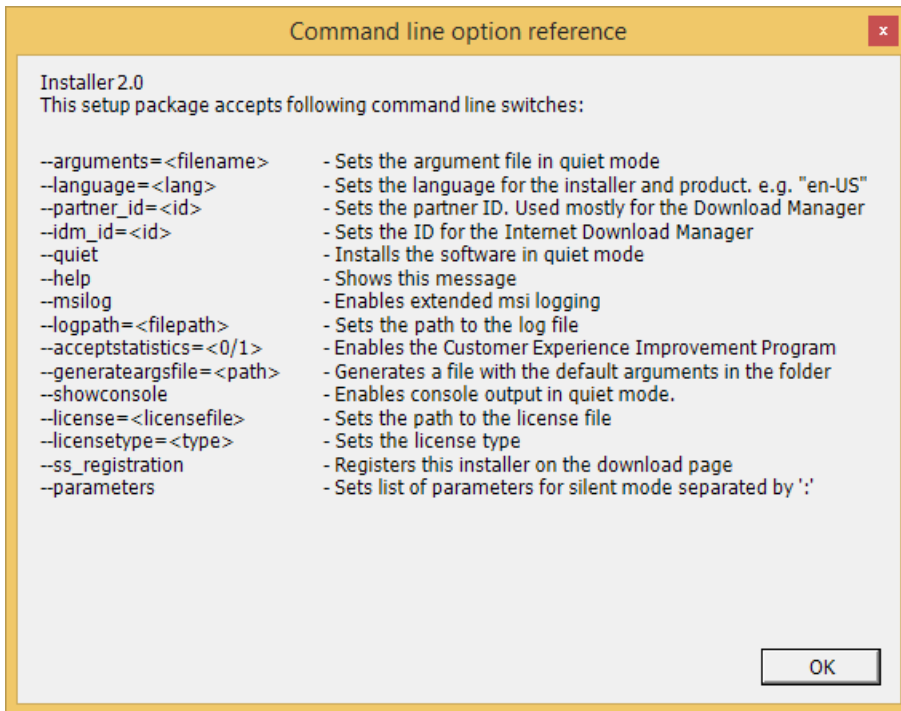
Set up Kerberos authentication

Use Kerberos authentication as an alternative to the older Microsoft NT LAN (NTLM) authentication protocol.

See About Kerberos authentication (on page 25) for more information.

Installation for workgroups

If you do not use a domain setup with an Active Directory server, but a workgroup setup, do the following when you install:

1. Log in to Windows using a common administrator account.

   Make sure to use the same account on all computers in the system.

2. Depending on your needs, start the management or recording server installation and click **Custom**.

3. Depending on what you selected in step 2, select to install the Management or Recording Server service using a common administrator account.

4. Finish the installation.

5. Repeat steps 1-4 to install any other systems you want to connect. They must all be installed using a common administrator account.

You cannot use this approach when you **upgrade** workgroup installations. See instead Alternative upgrade for workgroup (on page 46).

Installation troubleshooting

The following issues may occur during or upon installation of the management server or recording servers. For each issue, one or more solutions are available.

Issue: Recording server startup fails due to port conflict

This issue can only appear if the Simple Mail Transfer Protocol (SMTP) service is running as it uses port 25. If port 25 is already in use for, it may not be possible to start the Recording Server service. It is important that port number 25 is available for the recording server's SMTP service.

SMTP Service: Verification and solutions

To verify whether SMTP Service is installed:

1. From Windows' **Start** menu, select **Control Panel**.

2. In the **Control Panel**, double-click **Add or Remove Programs**.

3. In the left side of the **Add or Remove Programs** window, click **Add/Remove Windows Components**.

4. In the **Windows Components** wizard, select **Internet Information Services (IIS)**, and click **Details**.

5. In the **Internet Information Services (IIS)** window, verify whether the **SMTP Service** check box is selected. If so, SMTP Service is installed.

If SMTP Service is installed, select one of the following solutions:

Solution 1: Disable SMTP Service, or set it to manual startup

This solution lets you start the recording server without having to stop the SMTP Service every time:

1. From Windows' **Start** menu, select **Control Panel**.

2. In the **Control Panel**, double-click **Administrative Tools**.

3. In the **Administrative Tools** window, double-click **Services**.

4. In the **Services** window, double-click **Simple Mail Transfer Protocol (SMTP)**.

5. In the **SMTP Properties** window, click **Stop**, then set **Startup type** to either **Manual** or **Disabled**.

   When set to **Manual**, the SMTP Service can be started manually from the **Services** window, or from a command prompt using the command *net start SMTPSVC*.

6. Click **OK**.

Solution 2: Remove SMTP service

Removing the SMTP Service may affect other applications using the SMTP Service.

1. From Windows' **Start** menu, select **Control Panel**.

2. In the **Control Panel** window, double-click **Add or Remove Programs**.

3. In the left side of the **Add or Remove Programs** window, click **Add/Remove Windows Components**.

4. In the **Windows Components** wizard, select the **Internet Information Services (IIS)** item, and click **Details**.

5. In the **Internet Information Services (IIS)** window, clear the **SMTP Service** check box.

6. Click **OK**, **Next**, and **Finish**.

Issue: Changes to SQL server location prevents database access

This is an issue if the location of the SQL Server is changed, for example by changing the host name of the computer running the SQL Server. The result of this issue is that the access to the database is lost.

Solution: Use the update SQL address tool found at the tray icon.

Configure the system in the Management Client

In the following, you see a list of the typical tasks for configuring your system.

Even if the tasks are listed as a checklist, a completed checklist does not in itself guarantee that the system matches the exact requirements of your organization. To make the system match the needs of your organization, Sony recommends that you monitor and adjust the system continuously.

For example, it is a good idea to test and adjust the motion detection sensitivity settings of individual cameras under different physical conditions, including day/night and windy calm weather, once the system is running.

The setup of rules, which determine most of the actions your system performs, including when to record video, is another example of configuration that you can change according to your organization's needs.

☑	You have finished the initial installation of your system. See Install the system (on page 28).
☑	Change the trial SLC to a permanent SLC (if required). See Change Software License Code (on page 38).
☑	Log in to the Management Client.
☐	Authorize use of your system's recording servers. See Authorize a recording server (on page 59).
☐	Verify that each recording server's storage settings meet your needs. See About storage and archiving (on page 62).
☐	Verify that each recording server's archiving settings meet your needs. See Archive settings properties (on page 69).

☐	Detect the hardware, cameras or video encoders to add to each recording server. See Add hardware (on page 74).
☐	Configure each recording server's individual cameras. See About camera devices (on page 85).
☐	Enable storage and archiving for individual cameras or for a group of cameras. This is done from the individual cameras or from the device group. See Attach a device or group of devices to a storage (on page 65).
☐	Enable and configure devices. See Working with devices (on page 84).
☐	Rules determine the system's behavior to a large extent. You create rules to define when cameras should record, when pan-tilt-zoom (PTZ) cameras should patrol, and when notifications should be sent, for example. Create rules. See About rules and events (on page 130).
☐	Add roles to the system. See About roles (on page 164).
☐	Add users and/or groups of users to each of the roles. See Assign/remove users and groups to/from roles (on page 167).
☐	Activate licenses. See Activate licenses offline (on page 56).

Change Software License Code

If you run your installation on a trial Software License Code (SLC) during the first period, you can change it into a permanent SLC without any un- or reinstallation actions when you have received your new software license file.

Important: This must be done locally on the management server. You **cannot** do this from the Management Client.

1. On the management server, go to the notification area of the taskbar.

2. Right-click the **Management Server** icon and select **Change License**.

3. Click **Import License**.

4. Next, select the software license file saved for this purpose. When done, the selected software license file location is added just below the **Import License** button.

5. Click **OK** and you are now ready to register SLC. See Register Software License Code (on page 27).

About local IP address ranges

When a client, such as Network Video Management System Smart Client, connects to a surveillance system, an amount of initial data communication, including the exchange of contact addresses goes on in the background. This happens automatically, and is transparent to users.

Clients may connect from the local network as well as from the Internet, and in each case the surveillance system should be able to provide suitable addresses so the clients can get access to live and recorded video from the recording servers:

- When clients connect locally, the surveillance system should reply with local addresses and port numbers.

- When clients connect from the Internet, the surveillance system should reply with the recording servers' public addresses, that is the address of the firewall or NAT (Network Address Translation) router, and often also a different port number (which is then forwarded to recording servers).

The surveillance system must therefore be able to determine whether a client belongs on a local IP range or on the Internet. For this purpose, you can define a list of IP ranges which the surveillance system should recognize as coming from a local network.

Install clients

Install Network Video Management System Smart Client silently

You can deploy Network Video Management System Smart Client or your surveillance software to users' computers using tools such as Microsoft Systems Management Server (SMS). Such tools let you build up databases of hardware and software on local networks. The databases can then, among other things, be used for distributing and installing software applications, such as Network Video Management System Smart Client, over local networks.

1. Locate the Smart Client installation program (.exe) file - *Sony - Network VMS Smart Client 2016 R3 Installer.exe* or *Sony - Network VMS Smart Client 2016 R3 Installer x64.exe* for 32-bit and 64-bit versions respectively. You find the file in a subfolder under the folder **httpdocs**. The **httpdocs** folder is located under the folder in which your Sony surveillance software is installed.

    The path is typically:
    C:\Program Files\Sony\- Network VMS Management Server\IIS\httpdocs\- Network VMS Smart Client Installer\[version number] [bit-version]\All Languages\en-US

    For example:
    C:\Program Files\Sony\- Network VMS Management Server\IIS\httpdocs\- Network VMS Smart Client Installer\2016 (32-bit)\All Languages\en-US

2. Run a silent installation using one of the following two options:

    a Run with default parameter settings:

To run a silent installation using the default values for all parameters, start a command prompt (cmd.exe) in the directory where the installation program is located and perform following command:

>*Sony - Network VMS Smart Client 2016 R3 Installer.exe -–quiet*

This performs a quiet installation of the Network Video Management System Smart Client using default values for parameters such as target directory and so on. To change the default settings, see below.

b Customize default parameters using an xml argument file as input:

To customize the default installation settings, provide an xml file with modified values as input. To generate the xml file with default values, open a command prompt in the directory where the installation program is located and perform the following command:

>*Sony - Network VMS Smart Client 2016 R3 Installer.exe --generateargsfile=[path]*

Open the generated Arguments.xml file, using for example Windows Notepad, and perform any changes needed. Then, to run silent installation using these modified values, perform the following command in the same directory.

>*Sony - Network VMS Smart Client 2016 R3 Installer.exe --arguments=args.xml --quiet*

Install NVMS Mobile server

Once you have installed the NVMS Mobile server, you can use NVMS Mobile client and Network Video Management System Web Client with your system. To reduce the overall use of system resources on the computer running the management server, install the NVMS Mobile server on a separate computer.

The management server has a built-in public installation webpage. From this webpage, administrators and end-users can download and install the required Network Video Management System components from the management server or any other computer in the system.

To access the installation webpage:

1. Enter the following URL in your browser: http://[management *server address]/installation/admin*

   [management server address] is the IP address or host name of the management server.

2. Click **All Languages** for the NVMS Mobile server installer.

3. Run the downloaded file. Click **Yes** to all warnings. Unpacking starts.

4. Select language for the installer. Click **Continue**.

5. Read and accept the license agreement. Click **Continue**.

6. Select the installation type. Click **Typical** to install with the default selections.

7. Specify the primary surveillance system server:

   • Management server URL

   • Log in

   • User name and password. Click **Continue**.

8. Select the file location and product language. Click **Install**. When the installation is complete, a list of successfully installed components is displayed. Click **Close**.

You are ready for configuration of NVMS Mobile (see "NVMS Mobile configuration" on page 216).

Download Manager/download web page

The management server has a built-in web page. This web page enables administrators and end users to download and install required Network Video Management System components from any location, locally or remotely.

The web page is capable of displaying two sets of content, both in a language version that by default matches the language of the system installation:

- One web page is targeted at **administrators**, enabling them to download and install key system components. Most often the web page is automatically loaded at the end of the management server installation and the default content is displayed. On the management server, you can access the web page from Windows' **Start** menu, select **Programs** > **Sony** > **Administrative Installation Page**. Otherwise you can enter the URL:

    http://[management *server address]:[port]/installation/admin/*

    [management server address] is the IP address or host name of the management server, and [port] is the port number which you have configured IIS to use on the management server. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.

- One web page is targeted at end **users**, providing them access to client applications with default configuration. On the management server, you can access the web page from Windows' **Start** menu, select **Programs** > **Sony** > **Public Installation Page**. Otherwise you can enter the URL:

    http://[management *server address]:[port]/installation/*

    [management server address] is the IP address or host name of the management server, and [port] is the port number which you have configured IIS to use on the management server.

The two web pages have some default content so you can use them straight away after installation. As administrator however, by using the Download Manager, you can customize what should be displayed on the web pages. You can also move components between the two versions of the web page. To move a component, right-click it, and select the web page version you want to move the component to.

Even though you can control which components users can download and install in Download Manager, you cannot use it as a users' rights management tool. Such rights are determined by roles defined in the Management Client.

On the management server, you can access the Network Video Management System Download Manager from Windows' **Start** menu, select **Programs** > **Sony** > **Network Video Management System Download Manager**.

Download Manager's default configuration

The Download Manager has a default configuration. This ensures that your organization's users can access standard components from the start.

The default configuration provides you a default setup with access to downloading extra or optional components. Usually you access the web page from the management server computer, but you can also access the web page from other computers.

- The first level: Refers to your Network Video Management System product.

- The second level: Refers to the two targeted versions of the web page. **Default** refers to the web page version viewed by end users. **Administration** refers to the web page version viewed by system administrators.

- The third level: Refers to the languages in which the web page is available.

- The fourth level: Refers to the components which are - or can be made - available to users.

- The fifth level: Refers to particular versions of each component, which are - or can be made - available to users.

- The sixth level: Refers to the language versions of the components which are - or can be made - available to users.

The fact that only standard components are initially available - and only in the same language version as the system itself - helps reduce installation time and save space on the server. There is no need to have a component or language version available on the server if nobody uses it.

You can make more components or languages available as required and you can hide or remove unwanted components or languages.

Download Manager's standard installers (user)

By default, the following components are available for separate installation from the management server's download web page targeted at users (controlled by the Download Manager):

- Recording servers.

- Management Client

- Network Video Management System Smart Client

- Event server, used in connection with map functionality

- Log server, used for providing the necessary functionality for logging system information

- Service channel, enables automatic and transparent configuration communication between servers and clients

- NVMS Mobile server - **only available here**

- More options may be available in your organization.

For installation of **device packs**, see Device pack installer - must be downloaded (on page 44).

Add/publish Download Manager installer components

You must complete two procedures to make non-standard components and new versions available on the management server's download page.

First you **add new and/or non-standard components to the Download Manager**. Then you use it to **fine-tune which components should be available** in the various language versions of the web page.

If the Download Manager is open, close it before installing new components.

Adding new/non-standard files to the Download Manager:

1. On the computer where you downloaded the component(s), go to Window's **Start**, enter a *Command Prompt*

2. In the *Command Prompt*, execute the name of the file (*.exe*) with: [space] *--ss_registration*

   Example: *RecordingServer_setup_x64.exe --ss_registration*

   The file is now added to the Download Manager, but **not** installed on the current computer.

To get an overview of installer commands, in the *Command Prompt,* type [space] *--help* and the following window appears:
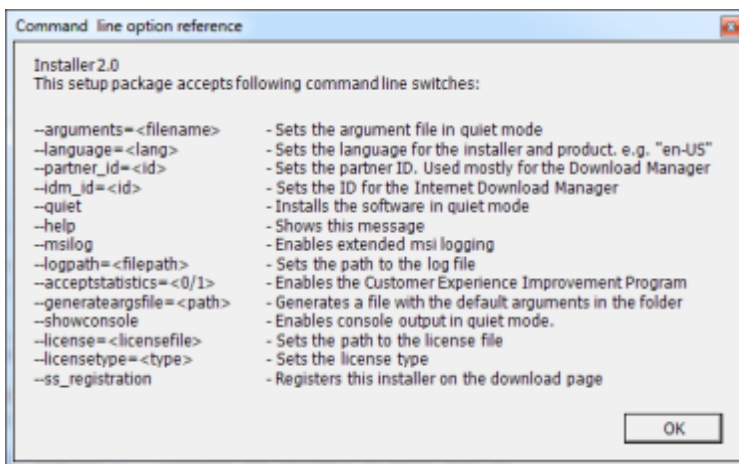
When you have installed new components they are by default selected in the Download Manager and are immediately available to users via the web page. You can always show or hide features on the web page by selecting or clearing check boxes in the Download Manager's tree structure.

You can change the sequence in which components are displayed on the web page. In the Download Manager's tree structure, drag component items and drop them at the required position.

Hide/remove Download Manager installer components

You have three options:

- **Hide components** from the web page by clearing check boxes in the Download Manager's tree structure. The components are still installed on the management server, and by selecting check boxes in the Download Manager's tree structure you can quickly make the components available again.

- **Remove the installation of components** on the management server. The components disappear from the Download Manager, but installation files for the components are kept at *C:\Program Files (x86)\Sony\- Network VMS Download Manager*, so you can re-install them later if required.

1. In the Download Manager, click **Remove features**.

Network Video Management System Enterprise Edition 2016 R3 - Administrator Manual

2. In the **Remove Features** window, select the feature(s) you want to remove.
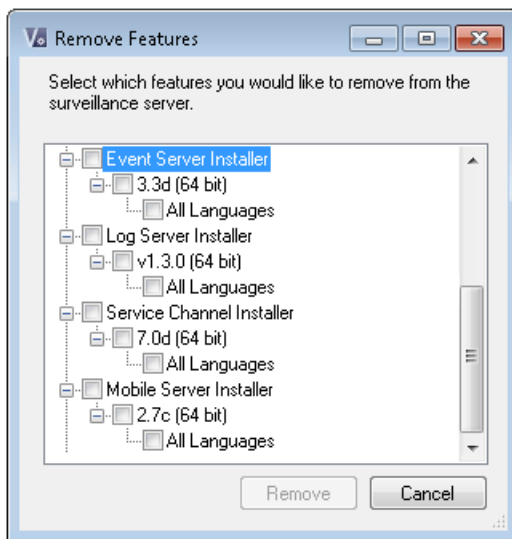
3. Click **OK** and **Yes**.

- **Remove installation files for non-required features** from the management server.
This can help save disk space on the server if you know that your organization is not going to use certain features.

Device pack installer - must be downloaded

The device pack (containing device drivers) included in your original installation is not included on the download website. So, if you need to reinstall the device pack or make the device pack installer available, you must first add or publish the latest device pack installer to the Download Manager:

1. Get the newest device pack from the download page on the Sony website
http://www.sony.net/CameraSystem/NVMS/Software.

2. Add/publish it to the Download Manager by calling it with the *--ss_registration* command.

If you do not have a network connection, you can reinstall the entire recording server from the Download Manager. The installation files for the recording server is placed locally on your computer and in this way you automatically get a reinstall of the device pack.

Upgrade

About upgrade

This information is only relevant if you are upgrading a previous Network Video Management System installation.

Important: Your Network Video Management System no longer supports Microsoft Windows XP.

When you upgrade, all components, except the management server database, are automatically removed and replaced. This includes the drivers of your device pack.

The management server database contains the entire system configuration (recording server configurations, camera configurations, rules, and so on). As long as you do not remove the management server database, no reconfiguration of your system configuration is needed, even if you may want to configure some of the new features in the new version.

Backward compatibility with recording servers from Network Video Management System versions older than this current version is limited. You can still access recordings on such older recording servers, but to be able to change their configuration, they must be of the same version as this current one. Sony recommends that you upgrade all recording servers in your system.

When you do an upgrade including your recording servers, you are asked whether you want to **update** or **keep** your video device drivers. If you choose to update, it might take a few minutes for your hardware devices to make contact with the new video device drivers after restarting your system. This is due to several internal checks being performed on the newly installed drivers.

Upgrade prerequisites

- Have your **software license file (see "About licenses" on page 18)** (.lic) ready.

    - **Service pack upgrade**: During the installation of the management server, the wizard may ask you to specify the location of the software license file. You can use both the software license file you got after your purchase of your system (or latest upgrade) and the activated software license file you got after your last license activation.

    - **Version upgrade:** After you purchased the new version, you receive a new software license file. During the installation of the management server, the wizard asks you to specify the location of the new software license file.

    The system verifies the software license file before you can continue. Already added hardware devices and other devices, which require licenses go into a grace period. If you do not have your software license file, contact your Network Video Management System reseller.

- Have your **new product version** software ready. If you have not purchased the software on a DVD, you can download it from the download page on the Sony website http://www.sony.net/CameraSystem/NVMS/Software.

- Make sure that you have backed up your system configuration (see "About backing up and restoring your system configuration" on page 237).

    The management server stores your system's configuration in a database. The system configuration database can be stored in two different ways:

1. In a SQL Server Express Edition database on the management server itself.

2. In a database on an existing SQL Server on your network.

    If using 2), you must have **Administrator rights on the SQL Server** whenever you want to create, move or upgrade the management server's system configuration database on the SQL Server. Once you are done creating, moving or updating, it is sufficient to be the database owner of the management server's system configuration database on the SQL Server.

When you are ready to start the upgrade, follow the procedures in Upgrade best practices (on page 46).

Upgrade best practices

Read about upgrade prerequisites (on page 45) including SQL database backup before you start the actual upgrade.

If your system is a single server system, you can simply install the new Network Video Management System Enterprise Edition software on top of the existing installation.

Perform the upgrade in this order:

1. Upgrade the management server with the **Distributed** option in the installer.

   1. On the wizard page where you choose components, all management servers components are preselected.

   2. Specify your SQL server, and choose to keep the database.

2. Upgrade the recording servers. You can install recording servers using the installation wizard (see "Install the recording server" on page 31) or silently (see "Install a recording server silently" on page 32). The advantage of a silent install is that you can do it remotely.

3. Upgrade the event server. From your management server's download web page, install the Event Server.

Continue these steps for the other sites in your system.

Alternative upgrade for workgroup

If you do not use a domain setup, but a workgroup setup, you must do the following when you upgrade:

1. On the recording server, create a local Windows user.

2. From the Windows **Control Panel**, find the **Sony Network Video Management System Data Collector service**. Right-click it, select **Properties**, and select the **Log on** tab. Set the Data Collector service to run as the local windows user you just created on the recording server.

3. On the management server, create the same local Windows user (with the same user name and password).

4. In the Management Client, add this local Windows user to the **Administrator**'s group.

For installing with workgroups, see Installation for workgroups (on page 35).

First time use

Best practices

Protect recording databases from corruption

You can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While it is good to have such options, Sony recommends that you take steps to ensure that your camera databases do not become corrupted.

Hard disk failure: protect your drives

Hard disk drives are mechanical devices and are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

- Vibration (make sure the surveillance system server and its surroundings are stable)

- Strong heat (make sure the server has adequate ventilation)

- Strong magnetic fields (avoid)

- Power outages (make sure you use an Uninterruptible Power Supply (UPS))

- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).

- Fire, water, etc. (avoid)

Windows Task Manager: be careful when you end processes

When you work in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking **End Process** in the Windows Task Manager, the process is not given the chance to save its state or data before it is terminated. This may lead to corrupt camera databases.

Windows Task Manager typically displays a warning if you attempt to end a process. Unless you are absolutely sure that ending the process is not going to affect the surveillance system, click **No** when the warning message asks you if you really want to terminate the process.

Power outages: use a UPS

The single-most common reason for corrupt databases is the recording server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your recording servers from being shut down abruptly is to equip each of your recording servers with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs

vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When you assess your needs, however, bear in mind the amount of runtime you require the UPS to be able to provide if the power fails. Saving open files and shutting down an operating system properly may take several minutes.

About daylight saving time

Daylight saving time (DST) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. The use of DST varies between countries/regions.

When you work with a surveillance system, which is inherently time-sensitive, it is important that you know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward.

Example:

The clock jumps forward from 02:00 standard time to 03:00 DST, and the day has 23 hours. In that case, there is no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back.

Example:

The clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day has 25 hours. You reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of 01:30 would be overwritten by the second instance of 01:30.

To solve such an issue from happening, your system archives the current video in the event the system time changes by more than five minutes. You cannot view the first instance of the 01:00 hour directly in any clients, but the data is recorded and safe. You can browse this video in Network Video Management System Smart Client by opening the archived database directly.

About time servers

Once your system receives images, they are instantly time-stamped. Since cameras are separate units which may have separate timing devices, camera time and your system time may not correspond fully. This may occasionally lead to confusion. If your cameras support timestamps, Sony recommends that you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about how to configure a time server, search the Microsoft website http://www.microsoft.com/ for **'time server'**, **'time service'**, or similar terms.

Management Client overview

Login overview

When you launch the Management Client, you must first enter your login information to connect to a system.

About login authorization

The system allows administrators to set up users so they can only log into a system if a second user with sufficient rights authorizes their login. In this case, Network Video Management System Smart Client or the Management Client asks for the second authorization during login.

A user associated with the built-in **Administrators** role has always permission to authorize and is not asked for a second login, unless the user is associated with another role that requires a second login.

To associate login authorization with a role:

- Set **Login authorization required** for the selected role on the **Info** tab (see "Info tab (roles)" on page 168) under **Roles**, so that the user is asked for additional authorization during login.

- Set **Authorize users** for the selected role on the **Overall Security** tab (see "Overall Security tab (roles)" on page 169) under **Roles**, so that the user can authorize other users' logins.

You can choose both options for the same user. This means that the user is asked for additional authorization during login, but can also authorize other users' logins, except for his/her own.
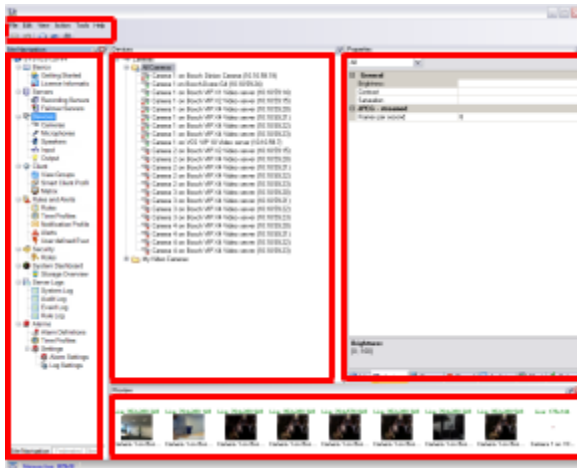
Management Client window overview

The Management Client window is divided into panes. The number of panes and layout depend on your:

- system configuration

- task

- available functions.

Below are some examples of typical layouts:

- When you work with recording servers and devices:

- When you work with rules, time and notification profiles, users, roles:
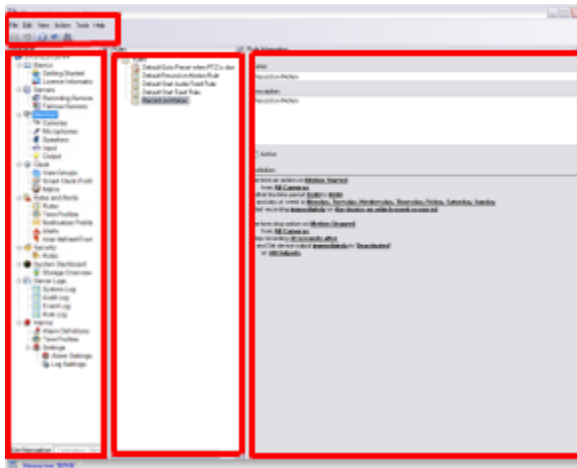
- When you view logs:
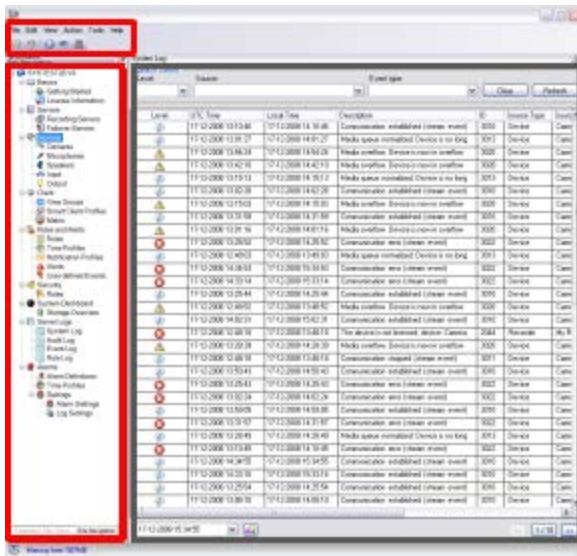
Panes overview

The illustration outlines a typical window layout. You can customize the layout so it may look different on your computer.
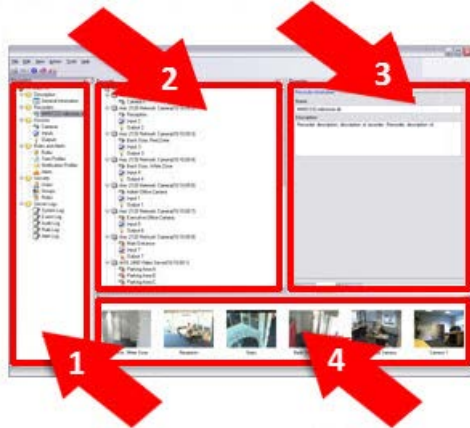
1. Site Navigation pane
2. Overview pane
3. Properties pane
4. Preview pane

Site Navigation pane: This is your main navigation element in the Management Client. It reflects the name, settings and configurations of the site that you have logged into. The site name is visible at the top of the pane. The features are grouped into categories that reflect the functionality of the software.

Overview pane: Provides an overview of the element you have selected in the **Site Navigation** pane, for example as a detailed list. When you select an element in the **Overview** pane, it typically displays the properties in the **Properties** pane. When you right-click elements in the **Overview** pane you get access to the management features.

Properties pane: Displays the properties of the element selected in the **Overview** pane. The properties appear on several dedicated tabs:

Example of properties displayed on tabs

Preview pane: The **Preview** pane appears when you work with recording servers and devices. It shows preview images from the selected cameras or displays information about the state of the device. The example shows a camera preview image with information about the resolution and data rate of the camera's live stream:

By default, the information shown with the camera preview images concerns live streams. This is displayed in green text above the preview. If you want recording stream information instead (red text), select **View** > **Show Recording Streams** in the menu.

Performance can be affected if the **Preview** pane displays preview images from many cameras at a high frame rate. To control the number of preview images, and their frame rate, select **Options** > **General** in the menu.

Menu overview
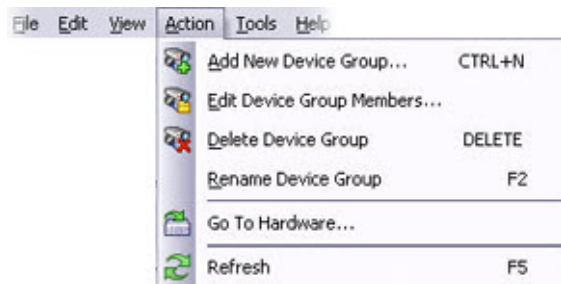
Example only - some menus change depending on context.

File menu

You can save changes to the configuration and exit the application. You can also back up your configuration, see About backing up and restoring your system configuration (on page 237).

Edit menu

You can undo changes.

View menu

Name	Description
Reset Application Layout	Reset the layout of the different panes in the Management Client to their default settings.
Preview Window	Toggle the **Preview** pane on and off when working with recording servers and devices.
Show Recording Streams	By default, the information shown with preview images in the **Preview** pane concerns live streams of the cameras. If you want information about recording streams instead, select **Show Recording Streams**.

Action menu

The content of the **Action** menu differs depending on the element you have selected in the **Site Navigation** pane. The actions you can choose from are the same as when you right-click the element. The elements are described in Management Client elements (on page 54).

Name	Description
Refresh	Is always available and reloads the requested information from the management server.

Tools menu

Name	Description
Registered Services	Manage registered services. See About the service channel (on page 255).
Effective Roles	View all roles of a selected user or group. Only relevant if you run Network Video Management System Enterprise Edition.
Options	Opens the Options dialog box, which lets you define and edit global system settings. Only relevant if you run Network Video Management System Enterprise Edition.

Help menu

You can access the help system and information about the version of the Management Client.

Management Client elements

Basics

License information

You can keep track of all licenses that share the same software license file both on this site and on all other sites, your SUP subscriptions and decide how you want to activate your licenses. For basic information about the different Network Video Management System licenses, see About licenses (on page 18).

Software Upgrade Plan

Here you can find a link to the end user license agreement, which you accepted prior to the installation.

Installed Products

Lists the following information about all your installed base licenses for Network Video Management System VMS and add-on products that share the same software license file:

- Products and versions

- The products' software license code (SLC).

- The expiration date of your SLC. Typically unlimited.

- The expiration date of your SUP subscription.

License Overview - All sites

Lists the number of activated hardware device licenses or other licenses in your software license file and the total amount of available licenses on your system. Here you can easily see if you can still grow your system without purchasing additional licenses.

If you have licenses for add-on products, you can see additional details about these under the add-on product specific nodes in the **Site Navigation Pane**.

License Details - Current Site

The **Activated** column lists the number of activated hardware device licenses or other licenses on this site.

You can also see the number of used device changes without activation (see "About device changes without activation" on page 55) and how many you have available per year in the **Changes without activation** column.

If you have licenses that you have not yet activated and that therefore run in a grace period, these are listed in the **In Grace Period** column. The expiration date of the first license which expires, appears in red below the table.

If you forget to activate licenses before the grace period expires, they will stop sending video to the system. These licenses are shown in the **Grace Period Expired** column. See also Activate licenses after grace period (on page 57).

If you have used more licenses than you have available, these are listed in the **Without License** column and cannot be used in your system. See also Get additional licenses (on page 57).

If you have licenses in a grace period, with an expired grace period or without license, a message will pop up to remind you every time you log into your Management Client.

Hardware devices without licenses are identified by an exclamation mark in the Management Client. Note that the exclamation mark is also used for other purposes. Place your mouse over the exclamation mark to see the purpose.

Features for activating licenses

Below the three tables are

- A drop-down list for manually activating licenses. For more information see Activate licenses offline (on page 56).

- In the lower right corner of the page, you can see when your licenses were activated last (automatically or manually) and when the information on the page were refreshed. The time stamps are from the server and not from the local computer.
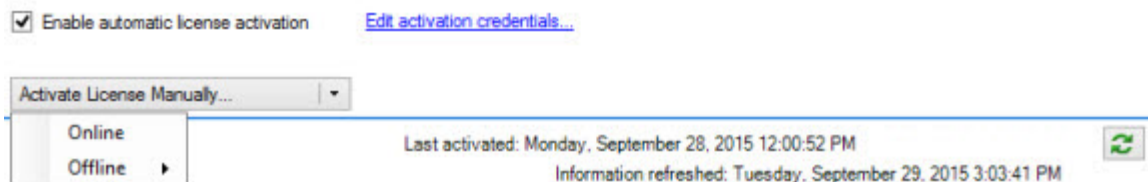
About device changes without activation

On the **Basics** > **License Information** page, the column **Changes without activation** shows the number of hardware devices you can replace or add without having to activate your hardware device licenses and how many changes you have already made since the last activation. Hardware devices added within your device changes without activation run as fully activated hardware device licenses.

How the number of device changes without activation is calculated

The device changes without activation are calculated based on three variables. If you have several installations of the Sony software, the variables apply to each of them separately. The variables are:

- **C%** that is a fixed percentage of the total amount of activated licenses.

- **Cmin** that is a fixed minimum value of the number of device changes without activation.

- **Cmax** that is a fixed maximum value of the number of devices changes without activation.

The number of device changes without activation can never be lower than the **Cmin** value or higher than the **Cmax** value. The calculated value based on the **C%** variable changes according to how many activated devices you have on each installation in your system. Devices added with device changes without activation are not counted as activated by the **C%** variable.

Sony defines the values of all three variables and the values are subject to change without notification. The values of the variables differ depending on the product.

Examples based on C% = 15%, Cmin = 10 and Cmax =100

A customer buys 100 hardware device licenses. He adds 100 cameras to his system. He activates his licenses and he now has 15 device changes without activation.

A customer buys 100 hardware device licenses. He adds 100 cameras to his system and activates his licenses. His device changes without activation is now 15. The customer decides to delete a hardware device from his system. He has now 99 activated devices and his number of device changes without activation drops to 14.

A customer buys 1000 hardware device licenses. He adds 1000 cameras and activates his licenses. His device changes without activation is now 100. According to the **C%** variable, he should now have had 150 devices changes without activation, but the **Cmax** variable only allows him to have 100 devices changes without activation.

A customer buys 10 hardware device licenses. He adds 10 cameras to his system and activates his licenses. His number of device changes without activation is now 10 because of the **Cmin** variable. If the number was only calculated based on the **C%** variable, he would only have had 1 (15% of 10 = 1.5 rounded off to 1).

A customer buys 115 hardware device licenses. He adds 100 cameras to his system and activates his licenses. His device changes without activation is now 15. He adds another 15 cameras without activating them, using 15 out of 15 of his device changes without activation. He removes 50 of the cameras from the system and his device changes without activation goes down to 7. This means that 8 of the cameras previously added within the 15 device changes without activation go into a grace period. The customer now adds 50 new cameras. Because the customer activated 100 cameras on his system last time he activated his licenses, the device changes without activation goes back to 15 and the 8 cameras, which were moved into a grace period, moves back as device changes without activation. The 50 new cameras go into a grace period.

Activate licenses offline

If the computer that runs the management server does not have Internet access, you can activate licenses offline.

1. On the **License Information** node, select **Activate License Manually** -> **Offline** -> **Export License for Activation** to export a license request file (.lrq) with information about your added hardware devices.

2. The license request file (.lrq) is automatically given the same name as your SLC. If you have several sites, remember to make the name unique so you easily can identify which file belong to which site.

3. Copy the license request file to a computer with Internet access and log into our website to obtain the activated software license file (.lic).   See the license guide on our website http://www.sony.net/CameraSystem/NVMS/Manuals.

4. Copy the .lic file that has the same name as your license request file to your computer with Management Client.

5. In Management Client on the **License Information** page, select **Activate License Offline** > **Import Activated License**, and select the activated software license file to import it and thereby activate your licenses.

6. Click **Finish** to end the activation process.

Activate licenses after grace period

If you do not activate a license within the grace period, the device becomes unavailable and cannot send data to the surveillance system.

- The device itself, its configuration and other settings are not removed from the system configuration.

- To be able to receive data from the expired device again, simply activate the license. For more information, see Activate licenses offline (on page 56).

Get additional licenses

If you want to add or if you have already added more hardware devices than you currently have licenses for, you must buy additional licenses to enable the devices to send data to your system.

- To get additional licenses for your system, contact your Network Video Management System product reseller.

New licenses to your existing surveillance system version:

- Simply activate your licenses manually to get access to the new licenses. For more information, see Activate licenses offline (on page 56).

New licenses and an upgraded surveillance system version:

- You receive an updated software license file (.**lic**) (see "About licenses" on page 18) with the new licenses and the new version. You must use the new software license file during the installation of the new version. For more information, see Upgrade prerequisites (on page 45).

Licenses and hardware device replacement

You can replace a hardware device, such as a camera, licensed in your system with a new hardware device, and have the new hardware device activated and licensed instead.

If you remove a hardware device from a recording server, you free a hardware device license.

If you replace a camera with a similar camera (manufacturer, brand, and model), and give the new camera the same IP address, you maintain full access to all the camera's databases. In this case, you move the network cable from the old camera to the new one without changing any settings in the Management Client.

If you replace a hardware device with a different model, you must use the **Replace Hardware** wizard (see Replace hardware (on page 245)) to map all relevant databases of cameras, microphones, inputs, outputs, and settings.

Site information

You can add additional information to a site for an easier identification of each site, for example, in a large setup. Apart from the site name, you can describe:

- Address/location

- Administrator(s)

- Additional information

Update site information

To update site information:

1. Select **Edit**.

2. Select a tag.

3. Enter information in the **Value** field.

4. Click **OK**.

Servers and hardware

Recording servers

About recording servers

You use recording servers for recording of video feeds, and for communicating with cameras and other devices. A surveillance system typically consists of several recording servers.

Recording servers are computers where you have installed the recording server software, and configured it to communicate with a management server. You can see your recording servers in the **Overview** pane when you expand the **Servers** folder and then select **Recording Servers**.
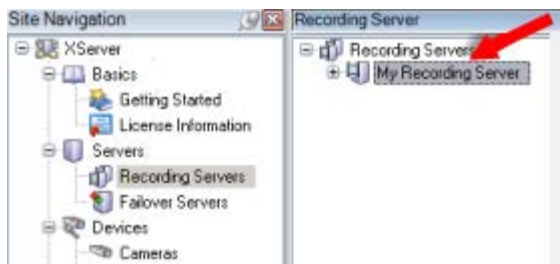
Recording server listed in Overview pane

Backward compatibility with recording server versions older than this version of the management server is limited. You can still access recordings on recording servers with older versions, but if you want to change their configuration, make sure they match this version of the management server. Sony recommends that you upgrade all recording servers in your system to the same version as your management server.

You have several options related to management of your recording servers:

-   Authorize a recording server (on page 59)

-   Add hardware (on page 74)

-   Move hardware (on page 76)

-   Delete all hardware (see "Delete all hardware on a recording server" on page 74)

-   Remove a recording server (on page 73)

Important: When the Recording Server service is running, it is very important that Windows Explorer or other programs do not access Media Database files or folders associated with your system setup. If they do, it is likely that the recording server cannot rename or move relevant media files. This might bring the recording server to a halt. To restart a stopped recording server, stop the Recording Server service, close the program accessing the relevant media file(s) or folder(s), and restart the Recording Server service.

Authorize a recording server

When you first use the system, or when you have added new recording servers to the system, you must authorize the new recording servers.

When you authorize a recording server, you configure it to connect to your management server.

1. Right-click the required recording server in the **Overview** pane.

2. Select **Authorize Recording Server**:

3. After a moment, the recording server is authorized and ready for further configuration via the tabs. You can also Add hardware (on page 74).

Change/verify the basic configuration of a recording server

If your Management Client does not list all the recording servers you have installed, the most likely reason is that you have configured the setup parameters (for example, the IP address or host name of the management server) incorrectly during installation.

You do not need to re-install recording servers to specify the parameters of the management servers, but you can change/verify its basic configuration:

1. On the computer that runs the recording server, right-click the **Recording Server** icon in the notification area.

2. Select **Stop Recording Server service**.

3. Right-click the **Recording Server** icon again and select **Change Settings**.

   The **Recording Server Settings** window appears.

4. Verify/change the following settings:

   - **Management server hostname/IP address**: Specify the IP address or host name of the management server to which the recording server should be connected.

- **Management server port**: Specify the port number to be used when communicating with the management server. Default is port 9993. You can change this if required, but the port number must always match the port number set up on the management server.

5. Click **OK**.

6. To start the Recording Server service again, right-click the **Recording Server** icon, and select **Start Recording Server service**.

Important: Stopping the Recording Server service means that you cannot record and view live video while you verify/change the recording server's basic configuration.

Recording server status icons

The Management Client uses the following icons to indicate the state of individual recording servers:

Icon	Description
	Recording server is running
	Recording server is communicating
	Recording server requires attention: This icon typically appears because the Recording Server service is stopped. 1) Right-click the recording server icon in the notification area. 2) Start/stop the Recording Server service and view recording server status messages.
	Recording server must be authorized: Appears when you load the recording server for the first time. When you first use a recording server, you must authorize it: 1) Right-click the required recording server icon. 2) Select **Authorize Recording Server**. After a moment, the recording server is authorized and ready for further configuration.
	Ongoing database repair: Appears when databases are corrupted, for example due to a power failure, and the recording server is repairing them. The repair process may take some time if the databases are large. See Protect recording databases from corruption (on page 47) for information about how to avoid corrupt databases. **Important:** During a database repair at startup, you cannot record video from cameras connected to the recording server. Only live viewing is available. A database repair at normal operation does not affect any recordings.

Info tab (recording server)

You can verify or edit the name and description of a selected recording server on the **Info** tab.

Info tab, displaying information about a recording server.

Info tab properties

Name	Description
Name	Used when the recording server is listed in the system and clients. The name does not have to be unique. When you rename a recording server, the name is changed globally in the Management Client.
Description	The description appears in a number of listings within the system. A description is not mandatory.
Host name	Displays the recording server's host name.
Web server URL	Displays the URL of the recording server's web server. You use the web server, for example, for handling PTZ camera control commands, and for handling browse and live requests from Network Video Management System Smart Client. The URL includes the port number used for web server communication (typically port 7563).
Time zone	Displays the time zone in which the recording server is located.

Storage tab (recording server)

On the **Storage** tab, you can set up, manage and view storages for a selected recording server.
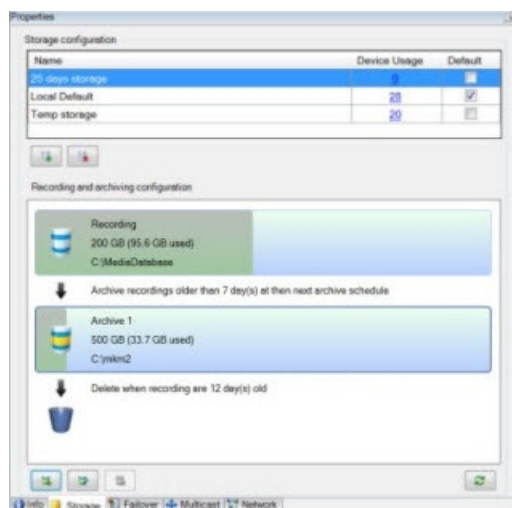
About storage and archiving

When a camera records video or audio, all specified recordings are by default stored in the storage defined for the device. Each storage saves recordings in the recording database **Recording**. A storage has no default archive(s), but you can create these.

To avoid that the recording database runs full, you can create additional storages (see "Add a new recording storage" on page 64). You can also create archives (see "Create an archive within a storage" on page 64) within each storage and start an archiving process to store data.

Archiving is the automatic transfer of recordings from, for example, a camera's recording database to another location. In this way, the amount of recordings that you can store is not limited to the size of the recording database. With archiving you can also back up your recordings to another media.

You configure storage and archiving on a per-recording server basis.

As long as you store archived recordings locally or on accessible network drives, you can use Network Video Management System Smart Client to view them. This is also how you view recordings stored in a cameras' regular databases.

The following mostly mentions cameras and video, but speakers, microphones, audio and sound also apply.

Important: Sony recommends that you use a dedicated hard disk drive for the recording server database to prevent low disk performance. When you format the hard disk, it is important to change its **Allocation unit size** setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help on the Microsoft website http://support.microsoft.com/kb/140365/en-us.

Important: The oldest data in a database is always auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit because data is not deleted fast enough, no more data is written to the database until you free up enough space. The actual maximum size of your database becomes the amount of gigabytes that you specify, minus 5GB.

Attaching devices to a storage

Once you have configured the storage and archiving settings for a recording server, you can enable storage and archiving for individual cameras or a group of cameras. This is done from the individual devices or from the device group. See Attach a device or group of devices to a storage (on page 65).

Effective archiving

When you enable archiving for a camera or a group of cameras, the content of the camera database is automatically moved to an archive at intervals that you define.

Depending on your requirements, you can configure one or more archives for each of your databases. Archives can be located either on the recording server computer itself, or at another location which can be reached by the system, for example on a network drive.

By setting up your archiving in an effective way, you can prune and groom your database storage usage if needed. Often, you want to make archived recordings take up as little space as possible especially on a long-term basis, where it is perhaps even possible to slacken image quality a bit. You can handle effective pruning from the **Storage** tab of a recording server by adjusting several interdependent settings:

- Recording database retention

- Recording database size

- Archive retention

- Archive size

- Archive schedule

- Frames Per Second (FPS).

The size fields define the size of the camera's database, exemplified by the cylinder, and its archive(s) respectively:
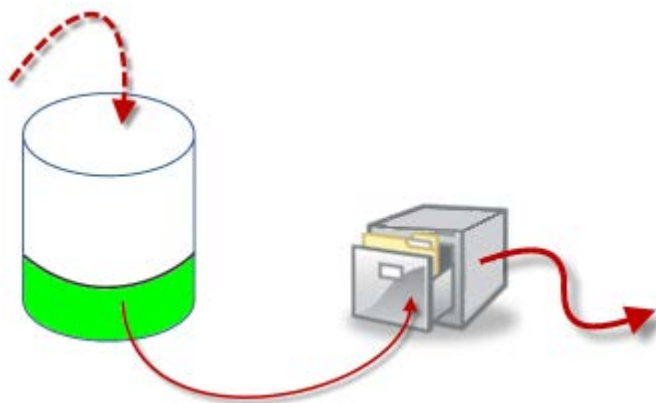
Recordings' way from recording database to archive to deletion

By means of retention time and size setting for the recording database, exemplified by the white area in the cylinder, you define how old recordings must be before they are archived. In our illustrated example, you archive the recordings when they are old enough to be archived.

The retention time and size setting for archives define how long the recordings remain in the archive. Recordings remain in the archive for the time specified, or until the archive has reached the specified size limit. When these settings are met, the system begins to overwrite old recordings in the archive.

The archiving schedule defines how often and at what times archiving takes place.

FPS determines the size of the data in the databases.

To archive your recordings, you must set all these parameters up in accordance with each other. This means that the retention period of a next coming archive must always be longer than the retention period of a current archive or recording database. This is because the number of retention days stated for an archive includes all retention stated earlier in the process. Archiving must also always take place more frequently than the retention period, otherwise you risk losing data. If you have a retention time of 24 hours, any data older than 24 hours is deleted. Therefore, to get your data safely moved to the next archive, it is important to run archiving more often than every 24 hours.

> **Example**: These storages (image to the left) have a retention time of 4 days and the following archive (image to the right) a retention time of 10 days. Archiving is set to occur every day at 10:30, ensuring a much more frequent archiving than retention time.
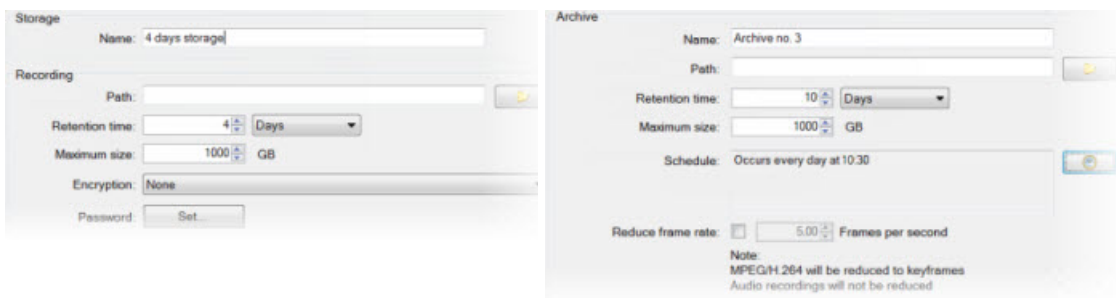
You can also control archiving by use of rules and events.

Add a new recording storage

You always create one storage with a predefined recording database named **Recording**. You cannot rename it. Apart from a recording database, a storage can contain a number of archives.

1. To add an extra storage to a selected recording server, click the ⬇ button located below the **Storage configuration** list. This opens the **Storage and Recording Settings** dialog box.

2. Specify the relevant settings (see "Storage and Recording Settings properties" on page 68).

3. Click **OK**.

If needed, you are now ready to create archive(s) within your new storage. See Create an archive within a storage (on page 64).

Create an archive within a storage

A storage has no default archive when it is created.

1. To create an archive, select the relevant storage in the **Recording and archiving configuration** list.

2. Click the ⬇ button below the **Recording and archiving configuration** list.

3. In the **Archive Settings** dialog box, specify the required settings (see Archive settings properties (on page 69)).

4. Click **OK**.

Attach a device or group of devices to a storage

Once a storage area is configured for a recording server, you can enable it for individual devices such as cameras, microphones or speakers or a group of devices. You can also select which of a recording server's storage areas you want to use for the individual device or the group.

1. Expand **Devices** and select either **Cameras**, **Microphones** or **Speakers** as required.

2. Select the device or a device group.

3. Select the **Record** tab.

4. In the **Storage** area, select **Select**.

5. In the dialog box that appears, select the database that should store the recordings of the device and then click **OK**.

6. In the toolbar, click **Save**.

When you click the device usage number for the storage area on the Storage tab of the recording server, the device is visible in the message report that appears.

Edit settings for a selected storage or archive

1. To edit a storage, select its recording database in the **Recording and archiving configuration** list. To edit an archive, select the archive database.

2. Click the **Edit Recording Storage** button [icon] located below the **Recording and archiving configuration** list.

3. Either edit a recording database or edit an archive.

If you change the maximum size of a database, the system auto-archives recordings that exceed the new limit. It auto-archives the recordings to the next archive or deletes them depending on archiving settings.

Back up archived recordings

Many organizations want to back up their recordings by using tape drives or similar. Exactly how you do this is highly individual and depends on the backup media used in your organization. However, the following is worth bearing in mind:

Back up archives rather than camera databases

Always create backups based on the content of archives, not based on individual camera databases. If you create backups based on the content of individual camera databases, you may cause sharing violations or other malfunctions.

When scheduling a backup, make sure the backup job does not overlap with your specified archiving times. To view each recording server's archiving schedule in each of a recording server's storage areas, see the Storage tab.

Know your archive structure so that you can target backups

When you archive recordings, you store them in a certain sub-directory structure within the archive.

During all regular use of your system, the sub-directory structure is completely transparent to the system's users when they browse all recordings with the Network Video Management System Smart Client. This is true both with archived and non-archived recordings. It is relevant to know the sub-directory structure if you want to back up your archived recordings. See About archive

structure (on page 66) and Backing up and restoring configuration (see "Backing up and restoring system configuration" on page 237).

About archive structure

When you archive recordings, they are stored in a certain sub-directory structure within the archive.

During all regular use of your system, the sub-directory structure is completely transparent to the system's users, as they browse all recordings with the Network Video Management System Smart Client regardless of whether the recordings are archived or not. Knowing the sub-directory structure is primarily interesting if you want to back up your archived recordings.

In each of the recording server's archive directories, the system automatically creates separate sub-directories. These sub-directories are named after the name of the device and the archive database.

Because you can store recordings from different cameras in the same archive, and since archiving for each camera is likely to be performed at regular intervals, further sub-directories are also automatically added.

These sub-directories each represent approximately an hour's worth of recordings. The one-hour split makes it possible to remove only relatively small parts of an archive's data if you reach the maximum allowed size of the archive.

The sub-directories are named after the device, followed by an indication of where the recordings came from (edge camera or via SMTP), **plus** the date and time of the most recent database record contained in the sub-directory.

Naming structure:

> `...[Storage Path]\[Storage name]\[device-name] – plus date and time of most recent recording]\`

If from edge camera:

> `...[Storage Path]\[Storage name]\[device-name] (Edge) – plus date and time of most recent recording]\`

If from SMTP:

> `...[Storage Path]\[Storage name]\[device-name] (SMTP) – plus date and time of most recent recording]\`

> **Real life example:**

> `...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137) – 2011–10–05T11:23:47+02:00\`

Sub-directories:

Even further sub-directories are automatically added. The amount and nature of these sub-directories depend on the nature of the actual recordings. For example, several different sub-directories are added if the recordings are technically divided into sequences. This is often the case if you have used motion detection to trigger recordings.

- **Media**: This folder contains the actual media that is either video or audio (not both).

- **MotionLevel**: This folder contains motion level grids generated from the video data using our motion detection algorithm. This data allows the Smart Search feature in Network Video Management System Smart Client to do very fast searches.

- **Motion**: In this folder the system stores motion sequences. A motion sequence is a time slice for which motion has been detected in the video data. This information is, for example, used in the time line in Network Video Management System Smart Client.

- **Recording**: In this folder the system stores recording sequences. A recording sequence is a time slice for which there are coherent recordings of media data. This information is, for example, used to draw the time line in Network Video Management System Smart Client.

If you want to back up your archives, you can target your backups if you know the basics of the sub-directory structure.

Examples of backup:

To back up the content of an entire archive, back up the required archive directory and all of its content. For example everything under:

        ...F:\OurArchive\

To back up the recordings from a particular camera from a particular period of time, back up the contents of the relevant sub-directories only. For example everything under:

        ...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137) -
        2011-10-05T11:23:47+02:00\

Delete an archive from a storage

1. Select the archive from the **Recording and archiving configuration** list.

    It is only possible to delete the last archive in the list. The archive does not have to be empty.

2. Click the ⬛ button located below the **Recording and archiving configuration** list.

3. Click **Yes**.

Delete a storage
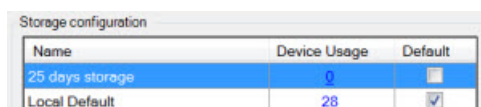
You cannot delete the default storage or storages that devices use as the recording storage for live recordings.
This means that you may need to move devices (see "Move hardware" on page 76) and any not yet archived recordings to another storage before you delete the storage.

1. To see the list of devices that use this storage, click the device usage number.

    If the storage has data from devices that have been moved to another recording server, a warning appears. Click the link to see the list of devices.

2. Follow the steps in Move non-archived recordings from one storage to another (on page 68).

3. Continue until you have moved all devices.

4. Select the storage that you want to delete.

Storage configuration		
Name	Device Usage	Default
25 days storage	0	☐
Local Default	28	☑

5. Click the ⬛ button located below the **Storage configuration** list.

6. Click **Yes**.

Move non-archived recordings from one storage to another

You move recordings from one live recording database to another from the **Record** tab of the device.

1. Select the device type. In the **Overview** pane, select the device.

2. Click the **Record** tab. In the upper part of the **Storage** area, click **Select**.

3. In the **Select Storage** dialog box, select the database.

4. Click **OK**.

5. In the **Recordings Action** dialog box, select if you want to remove already existing - but **non-archived** - recordings to the new storage or if you want to delete them.

6. Click **OK**.

Storage and Recording Settings properties

In the **Storage and Recording Settings** dialog box, specify the following:

Name	Description
Name	Rename the storage if needed. Names must be unique.
Path	Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer.
	If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\server\volume\directory\.
Retention time	Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings).
	The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process.
Maximum size	Select the maximum number of gigabytes of recording data to save in the recording database.
	Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted.
	Important: When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.

Name	Description
Password	Enter a password.

Archive Settings properties

In the **Archive Settings** dialog box, specify the following:

Name	Description
Name	Rename the storage if needed. Names must be unique.
Path	Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer. If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\server\volume\directory\.
Retention time	Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings). The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process.
Maximum size	Select the maximum number of gigabytes of recording data to save in the recording database. Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted. **Important**: When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.
Schedule	Specify an archiving schedule that outlines the intervals with which the archiving process should start. You can archive very frequently (in principle every hour all year round), or very infrequently (for example, every first Monday of every 36 months).

Name	Description
Reduce frame rate	To reduce FPS when archiving, select the **Reduce frame rate** check box and set a frame per second (FPS). Reduction of frame rates by a selected number of FPS makes your recordings take up less space in the archive, but it also reduces the quality of your archive. MPEG-4/H.264/H.265 reduces automatically to key-frames as a minimum. 0.1 = 1 frame per 10 seconds.

Multicast tab (recording server)

Your system supports multicasting of live streams from recording servers. If multiple Network Video Management System Smart Client users want to view live video from the same camera, multicasting helps saving considerable system resources. Multicasting is particularly useful if you use the Matrix functionality, where multiple clients require live video from the same camera.

Multicasting is only possible for live streams, not for recorded video/audio.

If a recording server has more than one network interface card, it is only possible to use multicast on one of them. Through the Management Client you can specify which one to use.

The successful implementation of multicasting also requires that you have set up your network equipment to relay multicast data packets to the required group of recipients only. If not, multicasting may not be different from broadcasting, which can significantly slow down network communication.

About multicasting

In regular network communication, each data packet is sent from a single sender to a single recipient - a process known as unicasting. But with multicasting you can send a single data packet (from a server) to multiple recipients (clients) within a group. Multicasting can help save bandwidth.

- When you use **unicasting**, the source must transmit one data stream for each recipient.

- When you use **multicasting**, only a single data stream is required on each network segment.

Multicasting as described here is **not** streaming of video from camera to servers, but from servers to clients.

With multicasting, you work with a defined group of recipients, based on options such as IP address ranges, the ability to enable/disable multicast for individual cameras, the ability to define largest acceptable data packet size (MTU), the maximum number of routers a data packet must be forwarded between (TTL), and so on.

Multicasting should not be confused with **broadcasting**, which sends data to everyone connected to the network, even if the data is perhaps not relevant for everyone:

Name	Description
Unicasting	Sends data from a single source to a single recipient.

Name	Description
Multicasting	Sends data from a single source to multiple recipients within a clearly defined group.
Broadcasting	Sends data from a single source to everyone on a network. Broadcasting can therefore significantly slow down network communication.

Enable multicasting

To use multicasting, your network infrastructure must support the IP multicasting standard IGMP (Internet Group Management Protocol).

- On the **Multicast** tab, select the **Multicast** check box.

If the entire IP address range for multicast is already in use on one or more recording servers, you first release some multicast IP addresses before you can enable multicasting on additional recording servers.

Assign IP address range

Specify the range you want to assign as addresses for multicast streams from the selected recording server. The clients connect to these addresses when the users view multicast video from the recording server.

For each multicast camera feed, the IP address and port combination must be unique (IPv4 example: 232.0.1.0:6000). You can either use one IP address and many ports, or many IP addresses and fewer ports. By default, the system suggests a single IP address and a range of 1000 ports, but you can change this as required.

IP addresses for multicasting must be within the range defined for dynamic host allocation by IANA. IANA is the authority overseeing global IP address allocation.

Name	Description
IP address	In the **Start** field, specify the first IP address in the required range. Then specify the last IP address in the range in the **End** field.
Port	In the **Start** field, specify the first port number in the required range. Then specify the last port number in the range in the **End** field.

Name	Description
Source IP address for all multicast streams	You can only multicast on one network interface card, so this field is relevant if your recording server has more than one network interface card or if it has a network interface card with more than one IP address.
	To use the recording server's default interface, leave the value 0.0.0.0 (IPv4) or :: (IPv6) in the field. If you want to use another network interface card, or a different IP address on the same network interface card, specify the IP address of the required interface.
	• IPv4: 224.0.0.0 to 239.255.255.255.
	• IPv6, the range is described on the IANA website http://www.iana.org.

Specify datagram options

Specify the settings for data packets (datagrams) transmitted through multicasting.

Name	Description
MTU	Maximum Transmission Unit, the largest allowed physical data packet size (measured in bytes). Messages larger than the specified MTU are split into smaller packets before they are sent. The default value is 1500, which is also the default on most Windows computers and Ethernet networks.
TTL	Time To Live, the largest allowed number of hops a data packet should be able to travel before it is discarded or returned. A hop is a point between two network devices, typically a router. Default value is 128.

Enable multicasting for individual cameras

Multicasting only works when you enable it for the required cameras:

1. Select the recording server and select the required camera in the **Overview** pane.

2. On the **Client** tab, select the **Live multicast** check box. Repeat for all required cameras.

Network tab (recording server)

You define a recording server's public IP address on the **Network** tab.

Why use a public address?

When an access client, such as Network Video Management System Smart Client, connects to a surveillance system, an amount of initial data communication, including the exchange of contact addresses, is shared in the background. This happens automatically, and is completely transparent to the users.

Clients may connect from the local network as well as from the Internet, and in both cases the surveillance system must provide suitable addresses so the clients can get access to live and recorded video from the recording servers:

- When clients connect locally, the surveillance system should reply with local addresses and port numbers.

- When clients connect from the Internet, the surveillance system should reply with the recording server's public address. This is the address of the firewall or NAT (Network Address Translation) router, and often also a different port number. The address and the port can then be forwarded to the server's local address and port.

  To provide access to the surveillance system from outside a NAT (Network Address Translation) firewall, you can use public addresses and port forwarding. This allows clients from outside the firewall to connect to recording servers without using VPN (Virtual Private Network). Each recording server can be mapped to a specific port and the port can be forwarded through the firewall to the server's internal address.

Define public address and port

1. To enable public access, select the **Enable public access** check box.

2. Define the recording server's public address. Enter the address of the firewall or NAT router so clients that access the surveillance system from the Internet can connect to the recording servers.

3. Specify a public port number. It is always a good idea that port numbers used on the firewall or NAT router are different from the ones used locally.

If you use public access, configure the firewall or NAT router so requests sent to the public address and port are forwarded to the local address and port of relevant recording servers.

Assign local IP ranges

You define a list of local IP ranges which the surveillance system should recognize as coming from a local network.

- On the **Network** tab, click **Configure**.

Remove a recording server

Important: If you remove a recording server, all configuration specified in the Management Client is removed for the recording server, including **all** of the recording server's associated hardware (cameras, input devices, and so on).

1. Right-click the recording server you want to remove in the **Overview** pane.

2. Select **Remove Recording Server**.

3. If you are sure, click **Yes**.

4. The recording server and all of its associated hardware are removed.

Delete all hardware on a recording server

Important: When you delete hardware, all recorded data related to the hardware is deleted permanently.

1. Right-click the recording server on which you want to delete all hardware.

2. Select **Delete All Hardware**.

3. Confirm the deletion.

Hardware

About hardware_no MIL Int

Hardware represents:

- The physical unit that connects directly to the recording server of the surveillance system via IP, for example a camera, a video encoder, or an I/O module.

See Add hardware (on page 74) to read about how to add hardware to your system.

Add hardware

You have several options for adding hardware for each recording server you have authorized on your system.

Important: If your hardware is located behind a NAT-enabled router or a firewall, you may need to specify a different port number and configure the router/firewall so it maps the port and IP addresses that the hardware uses.

The **Add Hardware** wizard helps you detect hardware like cameras and video encoders on your network and add them to the recording servers on your system. Only add hardware to **one recording server** at a time.

1. To access **Add Hardware**, right-click the required recording server and select **Add Hardware**.

2. Select one of the wizard options (see below) and follow the instruction on the screen.

3. After installation, you can see the hardware and it's devices in the **Overview** pane.

Name	Description
Express (Recommended)	The system scans automatically for new hardware on the recording server's local network. Select the **Show hardware running on other recording servers** check box to see if detected hardware is running on other recording servers. You can select this option every time you add new hardware to your network and want to use it in your system. You cannot use this option to add remote systems in setups.

Name	Description
Address range scanning	The system scans your network for relevant hardware and remote systems based on your specifications of: • hardware user names and passwords. Not needed if your hardware uses the factory default user names and passwords. • drivers • IP ranges (IPv4 only) • port number (default = 80) You can select this option when you only want to scan a part of your network, for example, when you expand your system.
Manual	Specify details about each hardware separately. This can be a good choice if you want to add only a few pieces of hardware, and you know their IP addresses, relevant user names and passwords or if a camera does not support the automatic discovery function.

Disable/enable hardware

Added hardware is by default **enabled**.

You can see if hardware is enabled or disabled in this way:

Enabled
Disabled

To disable added hardware, for example, for licensing or performance purposes:

1. Expand the recording server, right-click the hardware you want to disable.

2. Select **Enabled** to clear or select it.

Edit hardware

You can edit basic settings, such as IP address/host name, for added hardware:

1. Expand the recording server, right-click the hardware you want to edit.

2. Select **Edit Hardware**. This opens the **Edit Hardware** window, where you can edit relevant properties.

3. Click **OK**.

Enable/disable individual devices

Cameras are by default **enabled**.

Microphones, speakers, metadata, inputs and **outputs** are by default **disabled**.

This means that microphones, speakers, metadata, inputs and outputs must be individually enabled before you can use them in the system. The reason for this is that surveillance systems rely on cameras, whereas the use of microphones and so on is highly individual depending on the needs of each organization.

You can see if devices are enabled or disabled (the examples show an output):

Disabled

Enabled

The same method for enabling/disabling is used for cameras, microphones, speakers, metadata, inputs, and outputs.

1. Expand the recording server and the device. Right-click the device you want to enable.

2. Select **Enabled** to clear or select it.

Set up a secure connection to the hardware

You can set up a secure HTTPS connection using SSL (Secure Sockets Layer) between the hardware and the recording server.

Consult your camera vendor to get a certificate for your hardware and upload it to the hardware, before you continue with the steps below:

1. In the **Overview** pane, right-click the recording server and select the hardware.

Selecting hardware under a recording server

2. On the **Settings** tab, enable HTTPS. This is not enabled by default.

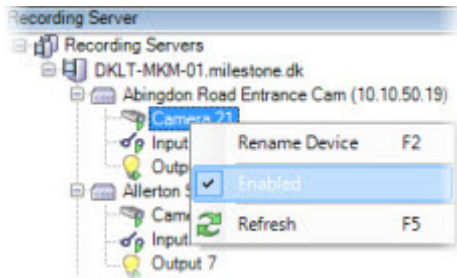3. Enter the port on the recording server to which the HTTPS connection is connected. The port number must correspond with the port set up on the device's homepage.

4. Make changes as needed and save.

Move hardware

About moving hardware

You can move hardware between recording servers that belong to the same site. After a move, the hardware and its devices run on the new recording server and new recordings are stored on this server. The move is transparent to the client users.

The recordings on the old recording server remain there until:

- You delete them from each device's new recording server on the **Record** tab.

If you try to remove a recording server that still contains recordings, you receive a warning.

If you move hardware to a recording server that currently has no hardware added to it, the client users must log out and log in to receive data from the devices.

You can use the move hardware feature to:

- **Load balance**: If, for example, the disk on a recording server is overloaded, you can add a new recording server and move some of your hardware.

- **Upgrade**: If you, for example, have to replace the server that hosts the recording server with a newer model, you can install a new recording server and move the hardware from the old server to the new server.

- **Replace a defective recording server**: If, for example, the server is offline and will never come online again, you can move the hardware to other recording servers and thereby keep the system running. You cannot access the old recordings. See also Replace a recording server (on page 247).

Remote recordings

When you move hardware to another recording server, the system cancels ongoing or scheduled retrievals from edge storages on cameras. The recordings are not deleted, but the data is not retrieved and saved in the databases as expected. You receive a warning if this is the case. For the Network Video Management System Smart Client user, who has started a retrieval when you initiate moving the hardware, the retrieval fails. The Network Video Management System Smart Client user is notified and can try again later.

If someone has moved hardware on a remote site, you must manually synchronize the central site with the **Update hardware** option to reflect the new configuration of the remote site. If you do not synchronize, the moved cameras remain disconnected on the central site.

See also

Move hardware (wizard) (on page 77)

Move hardware (wizard)

To move hardware from one recording server to another, run the **Move hardware** wizard. The wizard takes you through the necessary steps to complete a move for one or more hardware devices.

Prerequisites
Before you start the wizard:

- Make sure that the new recording server can access the physical camera via the network.

- Install the recording server (on page 31) that you want to move hardware to.

- Authorize it (see "Authorize a recording server" on page 59) and verified that it is online.

- Install the same device pack version (see "About video device drivers" on page 248) on the new recording server that you run on the existing server.

To run the wizard:

1. In the **Site Navigation** pane, select **Recording Servers**.

2. In the **Overview** pane, right-click the recording server you want to move hardware from or right-click a specific hardware device.

3. Select **Move Hardware**.

   If the recording server that you move hardware from is disconnected, an error message appears. You should only choose to move hardware from a disconnected recording server if you are sure that it will never come online again. If you move hardware anyway and the server comes back online, you risk an unexpected behavior from the system due to having the same hardware running on two recording servers for a period. Possible issues are, for example, license errors or events that are not sent to the correct recording server.

4. If you started the wizard from the recording server level, the **Select the hardware you want to move** page appears. Select the hardware devices you want to move.

5. On the **Select the recording server you want to move the hardware to** page, select from the list of recording servers installed on this site.

6. On the **Select the storage you want to use for future recordings** page, the storage usage bar indicates the free space in the recording database for live recordings only, not the archives. The total retention time is the retention period for both the recording database and the archives.

7. The system processes your request.

8. If the move was successful, click **Close**. If you select the new recording server in the Management Client, you can see the moved hardware and now recordings are stored on this server.

   If the move failed, you can troubleshoot the issue below.

Move hardware troubleshooting

If a move did not succeed, one of the following reasons can be the cause:

Error type	Troubleshooting
The recording server is not connected.	Make sure that the recording server is online. You may need to authorize it.
The recording server is not the latest version.	Update the recording server so it runs the same version as the management server.
The recording server could not be found in the configuration.	Make sure that you have authorized the recording server or that it has not been removed.
Updating the configuration or communication with the configuration database failed.	Make sure that your SQL server is connected and running.

Error type	Troubleshooting
Stopping the hardware on the current recording server failed	Maybe another process has locked the recording server or the recording server is in error mode. Make sure that the recording server is running and try again.
The hardware does not exist.	Make sure that the hardware you try to move has not simultaneously been removed from the system by another user. The scenario is quit unlikely.
The recording server that hardware was moved from is back online, but you chose to ignore it when it was offline.	Most likely, you have accepted that the old recording server will never get online again when you started the **Move Hardware** wizard, but during the move, the server came online. Start the wizard again, and select **No** when you are asked to confirm if the server comes online again.

Manage hardware

Info tab (hardware)

For information about the **Info** tab for remote servers, see Info tab (remote server).

Info tab (hardware)

Name	Description
Name	Enter a name. The system uses the name whenever the hardware is listed in the system and in the clients. The name does not have to be unique. When you rename hardware, the name is changed globally in the Management Client.
Description	Enter a description of the hardware (optional). The description appears in a number of listings within the system. For example, when pausing the mouse pointer over the hardware name in the **Overview** pane: Executive Office Reception Stairs Camera covering reception area. Example from a camera.
Model	Identifies the hardware model.
Version	Displays the firmware version of the system as specified by the manufacturer.

Name	Description
Serial number	Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
Driver	Identifies the driver that handles the connection to the hardware.
IE	Opens the default home page of the hardware vendor. You can use this page for administration of the hardware.
Address	The host name or IP address of the hardware.
MAC address	Specifies the Media Access Control (MAC) address of the system hardware. A MAC address is a 12-character hexadecimal number uniquely identifying each piece of hardware on a network.

Settings tab (hardware)

On the **Settings** tab, you can verify or edit settings for the hardware.

The content of the **Settings** tab is determined by the selected hardware, and varies depending on the type of hardware. For some types of hardware, the **Settings** tab displays no content at all or read-only content.

PTZ tab (video encoders)

On the **PTZ** tab, you can enable PTZ (pan-tilt-zoom) for video encoders. The tab is available if the selected device is a video encoder or if the driver supports both non-PTZ and PTZ cameras.

You must enable the use of PTZ separately for each of the video encoder's channels on the **PTZ** tab before you can use the PTZ features of the PTZ cameras attached to the video encoder.

Not all video encoders support the use of PTZ cameras. Even video encoders that support the use of PTZ cameras may require configuration before the PTZ cameras can be used. It is typically the installation of additional drivers through a browser-based configuration interface on the device's IP address.
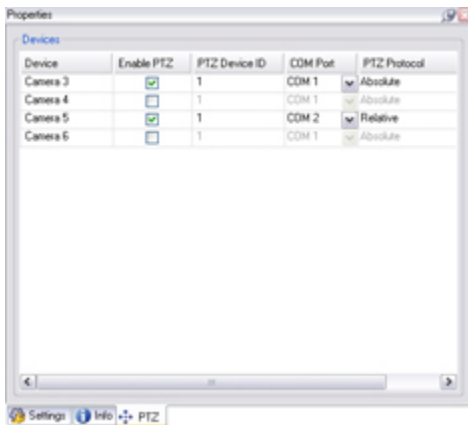
PTZ tab, with PTZ enabled for two channels on a video encoder

Enable PTZ on a video encoder

To enable the use of PTZ cameras on a video encoder, do the following on the **PTZ** tab:

1. In the list of devices connected to the video encoder, select the **Enable PTZ** box for the relevant cameras:

2. In the **PTZ Device ID** column, verify the ID of each camera.

3. In the **COM Port** column, select which video encoder's COM (serial communications) ports to use for control of the PTZ functionality:
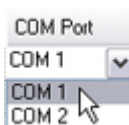
4. In the **PTZ Protocol** column, select which positioning scheme you want to use:
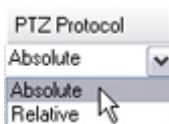
   - **Absolute:** When operators use PTZ controls for the camera, the camera is adjusted relative to a fixed position, often referred to as the camera's home position

   - **Relative:** When operators use PTZ controls for the camera, the camera is adjusted relative to its current position

   The content of the **PTZ protocol** column varies a lot depending on the hardware. Some have 5 to 8 different protocols. See also the camera documentation.

5. In the toolbar, click **Save**.

   You are ready to configure preset positions and patrolling for each PTZ camera:

   - Add a preset position (type 1) (on page 102)

   - Add a patrolling profile (on page 108)

Devices

The devices appear in the Management Client when you add hardware with the **Add Hardware** wizard.

You can manage devices via the device groups if they have the same properties, see About device groups (on page 82).

You can also manage the devices individually:

- Cameras

- Microphones

- Speakers

- Metadata

- Inputs

- Outputs

See About devices (on page 84).

Working with device groups

About device groups

Grouping of devices into device groups is part of the **Add Hardware** wizard, but you can always modify the groups and add more groups if needed.

You can benefit from grouping different types of devices (cameras, microphones, speakers, metadata, inputs, and outputs) on your system:

- Device groups help you maintain an intuitive overview of devices on your system.

- Devices can exist in several groups.

- You can create subgroups and subgroups in subgroups.

- You can specify common properties for all devices within a device group in one go.

- Device properties set via the group are not stored for the group but on the individual devices.

- When dealing with roles, you can specify common security settings for all devices within a device group in one go.

- When dealing with rules, you can apply a rule for all devices within a device group in one go.

You can add as many device groups as required, but you cannot mix different types of devices (for example cameras and speakers) in a device group.
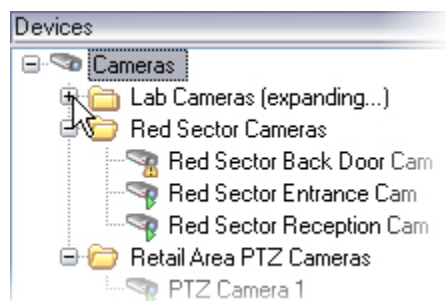
Example: cameras grouped into device groups

Create device groups with **less** than 400 devices so you can view and edit all properties.

If you delete a device group, you only delete the device group itself. If you want to delete a device, for example a camera, from your system, do it on the recording server level.

The following examples are based on grouping cameras into device groups, but the principles apply for all devices:

Add a device group (on page 83)

Add a device group

1. In the **Overview** pane, right-click the device type under which you want to create a device group.

2. Select **Add Device Group**.

3. In the **Add Device Group** dialog box, specify a name and description of the new device group:

   The description appears when you pause the mouse pointer over the device group in the device group list.

4. Click **OK**. A folder representing the new device group appears in the list.

5. Continue with Specify which devices to include in a device group (on page 83).

Specify which devices to include in a device group

1. In the **Overview** pane, right-click the relevant device group folder.

2. Select **Edit Device Group Members**.

3. In the **Select Group Members** window, select one of the tabs to locate the device.

   A device can be a member of more than one device group.

4. Select the devices you want to include, and click **Add** or double-click the device:
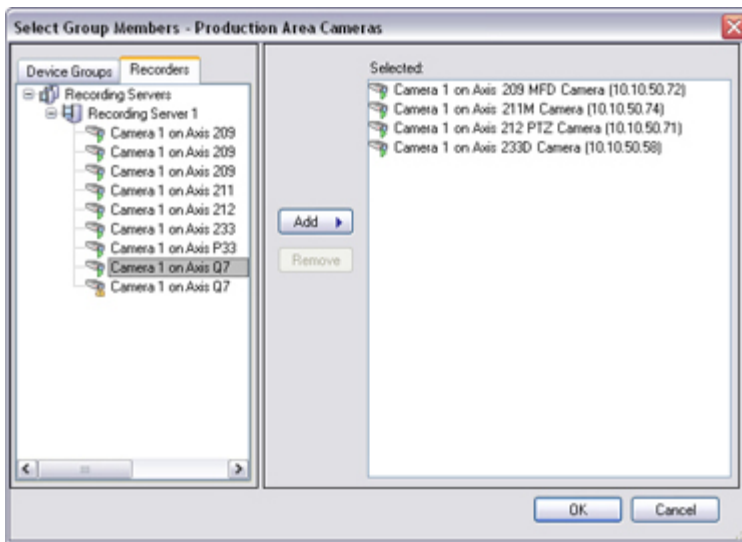
5. Click **OK**.

6. If you exceed the limit of 400 devices in one group, you can add device groups as subgroups under other device groups:

Specify common properties for all devices in a device group

With device groups, you can specify common properties for all devices within a given device group:

1. In the **Overview** pane, click the device group.

   In the **Properties** pane, all properties **which are available on all of the device group's devices** are listed and grouped on tabs.

2. Specify the relevant common properties.

   On the **Settings** tab, you can switch between settings for **all** devices and settings for individual devices.

3. In the toolbar, click **Save**. The settings are saved on the individual devices, not in the device group.

Working with devices

About devices

Hardware has a number of devices that you can manage individually, for example:

- A physical camera has devices that represent the camera part (lenses) as well as microphones, speakers, metadata, input and output either attached or built-in.

- A video encoder has multiple analog cameras connected that appear in one list of devices that represent the camera part (lenses) as well as microphones, speakers, metadata, input and output either attached or built-in.

- An I/O module has devices that represent the input and output channels for, for example, lights.

- A dedicated audio module has devices that represent microphones and speaker inputs and outputs.

The system automatically adds the hardware's devices when you add hardware.

The following sections describe each of the device types with links to the tabs you can use to manage them.

About camera devices

Camera devices are added automatically when you add hardware to the system and are by default enabled.

Camera devices deliver video streams to the system that the client users can use to view live video or that the system can record for later playback by the client users. Roles determine the users' right to view video.

The system comes with a default start feed rule which ensures that video feeds from all connected cameras are automatically fed to the system. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 89).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Cameras**. In the Overview pane, you group your cameras for an easy overview of your cameras. Initial grouping is done as part of the **Add hardware** wizard.

Follow this configuration order to complete the most typical tasks related to configuration of a camera device:

1. Configure camera settings (see Settings tab (see "Settings tab (devices)" on page 92)).

2. Configure streams (see Streams tab (see "Streams tab (devices)" on page 93)).

3. Configure motion (see Motion tab (see "Motion tab (devices)" on page 117)).

4. Configure recording (see Record tab (see "Record tab (devices)" on page 95)).

5. Configure the remaining settings as needed.

About microphone devices

On many devices you can attach external microphones. Some devices have built-in microphones.

Microphone devices are added automatically when you add hardware to the system. They are by default disabled, so you must enable them before use, either as part of the **Add Hardware** wizard or afterwards. Microphones do not require separate licenses. You can use as many microphones as required on your system.

You can use microphones completely independently of cameras.

Microphone devices deliver audio streams to the system that the client users can listen to live or the system can record for later playback by the client users. You can set up the system to receive microphone specific events that trigger relevant actions.

Roles determine the users' right to listen to microphones. You cannot listen to microphones from the Management Client.

The system comes with a default start audio feed rule which ensures that audio feeds from all connected microphones are automatically fed to the system. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 89).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Microphones**. In the Overview pane, you group your microphones for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure microphone devices on these tabs:

- Info tab (see "Info tab (devices)" on page 91)

- Settings tab (see "Settings tab (devices)" on page 92)

- Record tab (see "Record tab (devices)" on page 95)

- Events tab (see "Events tab (devices)" on page 112)

About speaker devices

On many devices you can attach external speakers. Some devices have built-in speakers.

Speaker devices are added automatically when you add hardware to the system. They are by default disabled, so you must enable them before use, either as part of the **Add Hardware** wizard or afterwards. Speakers do not require separate licenses. You can use as many speakers as required on your system.

You can use speakers completely independently of cameras.

The system sends an audio stream to the speakers when a user presses the talk button in Network Video Management System Smart Client. Speaker audio is only recorded when talked to by a user. Roles determine users' right to talk through speakers. You cannot talk through speakers from the Management Client.

If two users want to speak at the same time, the roles determine users' right to talk through speakers. As part of the roles definition, you can specify a speaker priority from very high to very low. If two users want to speak at the same time, the user whose role has the highest priority wins the ability to speak. If two users with the same role want to speak at the same time, the first-come first-served principle applies.

The system comes with a default start audio feed rule that starts the device so the device is ready to send user activated audio to the speakers. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 89).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Speakers**. In the Overview pane, you group your speakers for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure speaker devices on these tabs:

- Info tab (see "Info tab (devices)" on page 91)

- Settings tab (see "Settings tab (devices)" on page 92)

- Record tab (see "Record tab (devices)" on page 95)

About metadata devices

Metadata devices deliver data streams to the system that the client users can use to view data about data, for example, data that describes the video image, the content or objects in the image, or the location of where the image was recorded. Metadata can be attached to cameras, microphones, or speakers.

Metadata can be generated by:

- The device itself delivering the data, for example the camera delivering video.

- A third party system or integration via a generic metadata driver.

The device-generated metadata is automatically linked to one or more devices on the same hardware.

Roles determine the users' right to view metadata.

The system comes with a default start feed rule which ensures that metadata feeds from all connected hardware that supports metadata, are automatically fed to the system. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 89).

For all other configuration and management of metadata devices, expand **Devices** in the Site Navigation pane, then select **Metadata**. In the Overview pane, you group your metadata devices for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure metadata devices on these tabs:

- Info tab (see "Info tab (devices)" on page 91)

- Settings tab (see "Settings tab (devices)" on page 92)

- Record tab (see "Record tab (devices)" on page 95)

About input devices

On many devices you can attach external units to input ports on the device. Input units are typically external sensors. You can use such external sensors, for example, for detecting if doors, windows, or gates are opened. Input from such external input units is treated as events by the system.

You can use such events in rules. For example, you could create a rule specifying that a camera should begin recording when an input is activated, and stop recording 30 seconds after the input is deactivated.

You can use input devices completely independently of cameras.

Before you specify use of external input units on a device, verify that the device itself recognize the sensor operation. Most devices can show this in their configuration interfaces, or via Common Gateway Interface (CGI) script commands.

Input devices are added automatically when you add hardware to the system. They are by default disabled, so you must enable them before use, either as part of the **Add Hardware** wizard or

afterwards. Input devices do not require separate licenses. You can use as many input devices as required on your system.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 89).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Input**. In the Overview pane, you group your input devices for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure input devices on these tabs:

- Info tab (see "Info tab (devices)" on page 91)

- Settings tab (see "Settings tab (devices)" on page 92)

- Events tab (see "Events tab (devices)" on page 112)

Activate input manually for test

With the rules feature, you define rules that automatically activate or deactivate input or you can activate them manually and check the result in the Management Client:

1. In the **Overview** pane, select the relevant input device.

2. Activate the input on the physical device.

3. In the **Preview** pane, see if the indicator lights up green. Then the input device works.
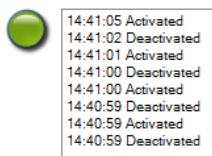
About output devices

On many devices you can attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through the system.

You can use output when creating rules. You can create rules that automatically activate or deactivate outputs, and rules that trigger actions when the state of an output is changed.

Output can be triggered manually from the Management Client and Network Video Management System Smart Client.

Before you specify use of external output units on a device, verify that the device itself can control the device attached to the output. Most devices can show this in their configuration interfaces, or via Common Gateway Interface (CGI) script commands.

Output devices are added automatically when you add hardware to the system. They are by default disabled, so you must enable them before use, either as part of the **Add Hardware** wizard or afterwards. Output devices do not require separate licenses. You can use as many output devices as required on your system.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 89).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Output**. In the Overview pane, you group your input devices for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure output devices on these tabs:

- Info tab (see "Info tab (devices)" on page 91)

- Settings tab (see "Settings tab (devices)" on page 92)

Activate output manually for test

With the rules feature, you define rules that automatically activate or deactivate output or you can activate them manually from a client.

You can activate an output manually from the Management Client to test the functionality:

1. In the **Overview pan**e, select the relevant output device.

2. Typically, the following elements are shown for each output in the **Preview** pane:

3. Select/clear the check box ☑ 🟢 to activate/deactivate the selected output. When an output is activated, the indicator lights up green:

4. Alternatively, click the rectangular button ⬜ to activate the output for the duration defined in the **Output Trigger Time** setting on the **Settings** tab (this feature/setting may not be available for all outputs). After the defined duration, the output is automatically deactivated.

Enable/disable devices via device groups

You can enable/disable devices only via the configured hardware. Unless manually enabled/disabled in the add hardware wizard, camera devices are by default enabled and all other devices are by default disabled.

To locate a device via the device groups to enable or disable:

1. In the **Site Navigation** pane, select the device.

2. In the **Overview** pane expand the relevant group and find the device.

3. Right-click the device, and select **Go To Hardware**.

4. Click the plus node to see all devices on the hardware.

5. Right-click the device you want to enable/disable, and select **Enabled**.

Status icons of devices

When you select a device, information about the current status appears in the **Preview** pane.
The following icons indicate the status of the devices:

Cam-era	Micro-phone	Spea-ker	Meta-data	In-put	Out-put	Description
						Device enabled and retrieving data: The device is enabled and you retrieve a live stream.
						Device recording: The device is recording data on the system.
						Device temporarily stopped or has no feed: When stopped, no information is transferred to the system. If it is a camera, you cannot view live video. A stopped device can still communicate with the recording server for retrieving events, setting settings etc., as opposed to when a device is disabled.
						Devices disabled: Cannot be started automatically through a rule and cannot communicate with the recording server. If a camera is disabled, you cannot view live or recorded video.
						Device database being repaired.
						Device requires attention: The device does not function correctly. Pause the mouse pointer over the device icon to get a description of the problem in the tooltip.
						Status unknown: Status of the device is unknown, for example, if the recording server is offline.
						Note that some icons can be combined, as in this example where **Device enabled and retrieving data** is combined with **Device recording**.

Info tab (devices)

About the Info tab

On the **Info** tab, you can view and edit basic information about a device in a number of fields. All devices have an **Info** tab.

Example of **Info** tab from a camera.

Info tab properties

Name	Description
Name	The name is used whenever the device is listed in the system and clients. When you rename a device, the name is changed globally in the Management Client.
Description	Enter a description of the device (optional). The description appears in a number of listings within the system. For example, when you pause the mouse pointer over the name in the **Overview** pane.
Hardware name	Displays the name of the hardware, with which the device is connected. The field is non-editable from here, but you can change it by clicking **Go To** next to it. This takes you to hardware information where you can change the name.
Port number	Displays the port on which the device is attached on the hardware. For single-device hardware, the port number is typically **1**. For multi-device hardware, such as video servers with several channels, the port number typically indicates the channel on which the device is attached, for example **3**.

Settings tab (devices)
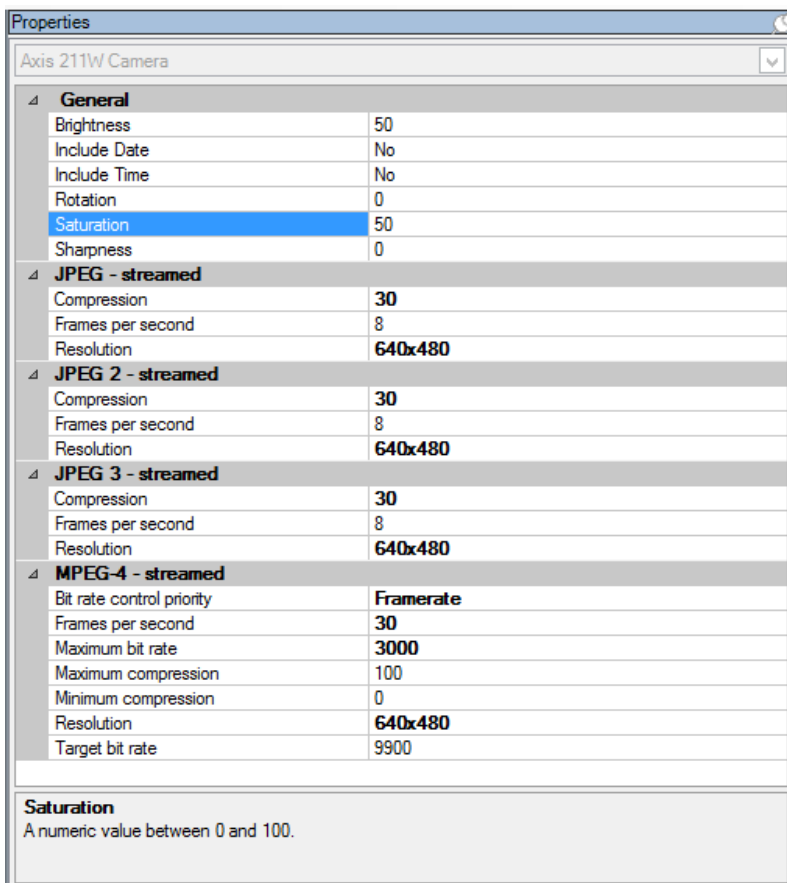
About the Settings tab

On the **Settings** tab, you can view and edit settings for a device in a number of fields. All devices have a **Settings** tab.

The values appear in a table as changeable or read-only. When you change a setting to a non-default value, the value appears **in bold**.

The content of the table depends on the device driver.

Allowed ranges appear in the information box below the settings table:

Settings tab, example from **camera**.

About camera settings

You can view or edit settings, such as:

- default frame rate

- resolution

- compression

- the maximum number of frames between keyframes

- on-screen date/time/text display for a selected camera, or for all cameras within a device group.

The drivers for the cameras determine the content of the **Settings** tab. The drivers vary depending on the type of camera.

For cameras that support more than one type of stream, for example MJPEG and MPEG-4/H.264/H.265, you can use multi-streaming, see About multi-streaming (on page 94).

When you change a setting, you can quickly verify the effect of your change if you have the **Preview** pane enabled. You cannot use the **Preview** pane to judge the effect of frame rate changes because the **Preview** pane's thumbnail images use another frame rate defined in the **Options** dialog box.

If you change the settings for **Max. frames between keyframes** and **Max. frames between keyframes mode**, it may lower the performance of some functionalities in Network Video Management System Smart Client. For example, Network Video Management System Smart Client requires a keyframe to start up showing video, so a longer period between keyframes, prolongs the Network Video Management System Smart Client start up.

Streams tab (devices)

About the Streams tab

The following devices have a **Streams** tab:

- Cameras

The **Streams** tab lists by default a single stream. It is the selected camera's default stream, used for live and recorded video.

For live streaming, you can set up and use as many live streams as the camera supports, but you can only select one stream for recording at a time. To change which stream to use for recording, select the **Record** box for the stream to be recorded.
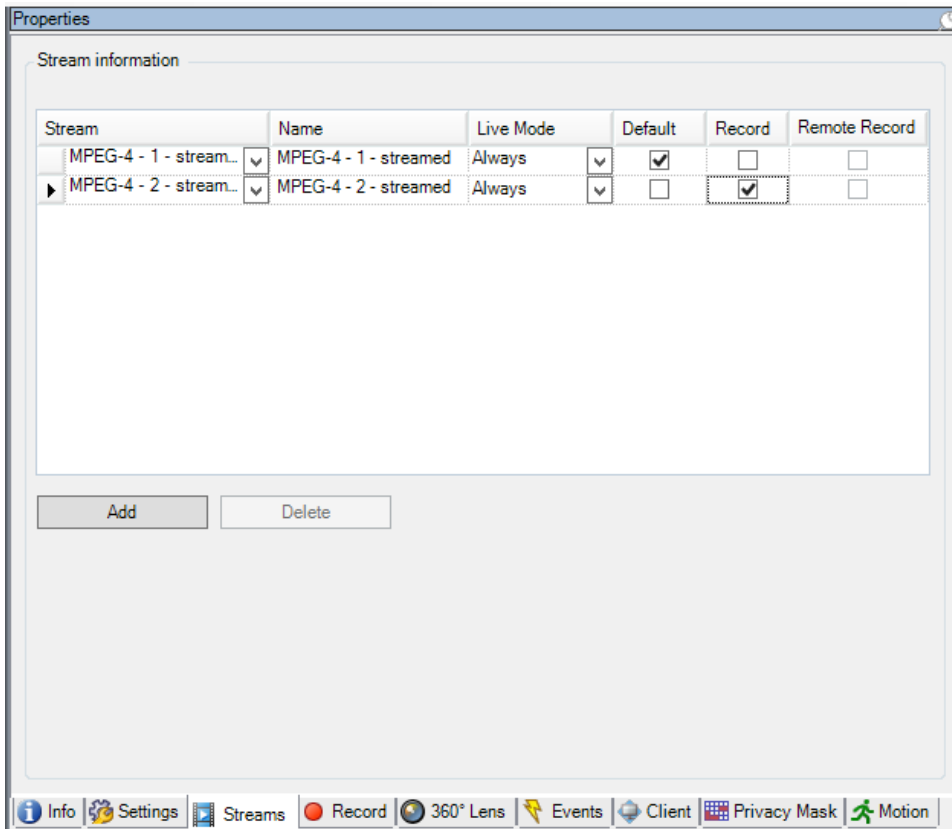
About multi-streaming

Playback of recorded video and viewing live video do not necessarily require the same video quality and frame rate to achieve the best result. You can have **either** one stream for live viewing and another stream for playback purposes **or** multiple separate live streams with different resolution, encoding, and frame rate.

Example 1, live and recorded video:

- For viewing **live** video, your organization may prefer MPEG4 at a high frame rate.

- For playing back **recorded** video, your organization may prefer MJPEG at a lower frame rate because this preserves disk space.

Example 2, multiple live videos:

- For viewing **live video from a local operating point**, your organization may prefer MPEG4 at a high frame rate to have the highest quality of video available.

- For viewing **live video from a remotely connected operating point**, your organization may prefer MJPEG at a lower frame rate and quality in order to preserve network bandwidth.

Even when cameras support multi-streaming, individual multi-streaming capabilities may vary between different cameras. See the camera's documentation for more information.

To see if a camera offers different types of streams, see the **Settings** tab.

Add a stream

1. On the **Streams** tab, click **Add**. This adds a second stream to the list.

2. In the **Name** column, edit the name of the stream. The name appears in Network Video Management System Smart Client.

3. In the **Live Mode** column, select when live streaming is needed.

   - **Always**: the stream runs even if no Network Video Management System Smart Client users request the stream.

   - **Never**: the stream is off. Only use this for recording streams, for example, if you want recordings in high quality and need the bandwidth.

   - **When needed**: the stream starts when a user of Network Video Management System Smart Client requests for it.

4. In the **Default** column, select which stream is default.

5. In the **Record** column, select the check box if you want to record this stream or leave it cleared if you only want to use it for live video.

6. In the **Remote Recording** column, select the check box if you want to use this recording stream for retrieving remote- and edge recordings.

7. Click **Save**.

Important: If you set a stream to **Default** or **Record**, the stream is always running independent of the **Live Mode** setting. Selecting **When needed** and **Always** have the same effect in the system and if you select **Never**, the stream is running, but cannot be viewed live.

If you do not want the streams to run at all unless someone is viewing live video, you can modify the **Default Start Feed Rule** to start on request with the predefined **Live Client Feed Requested** event.

Record tab (devices)

About the Record tab

The following devices have a **Record** tab:

- Cameras

- Microphones

- Speakers

- Metadata

Recordings from a device are only saved in the database when you have enabled recording and the recording-related rule criteria are met.

Parameters that cannot be configured for a device are grayed out.
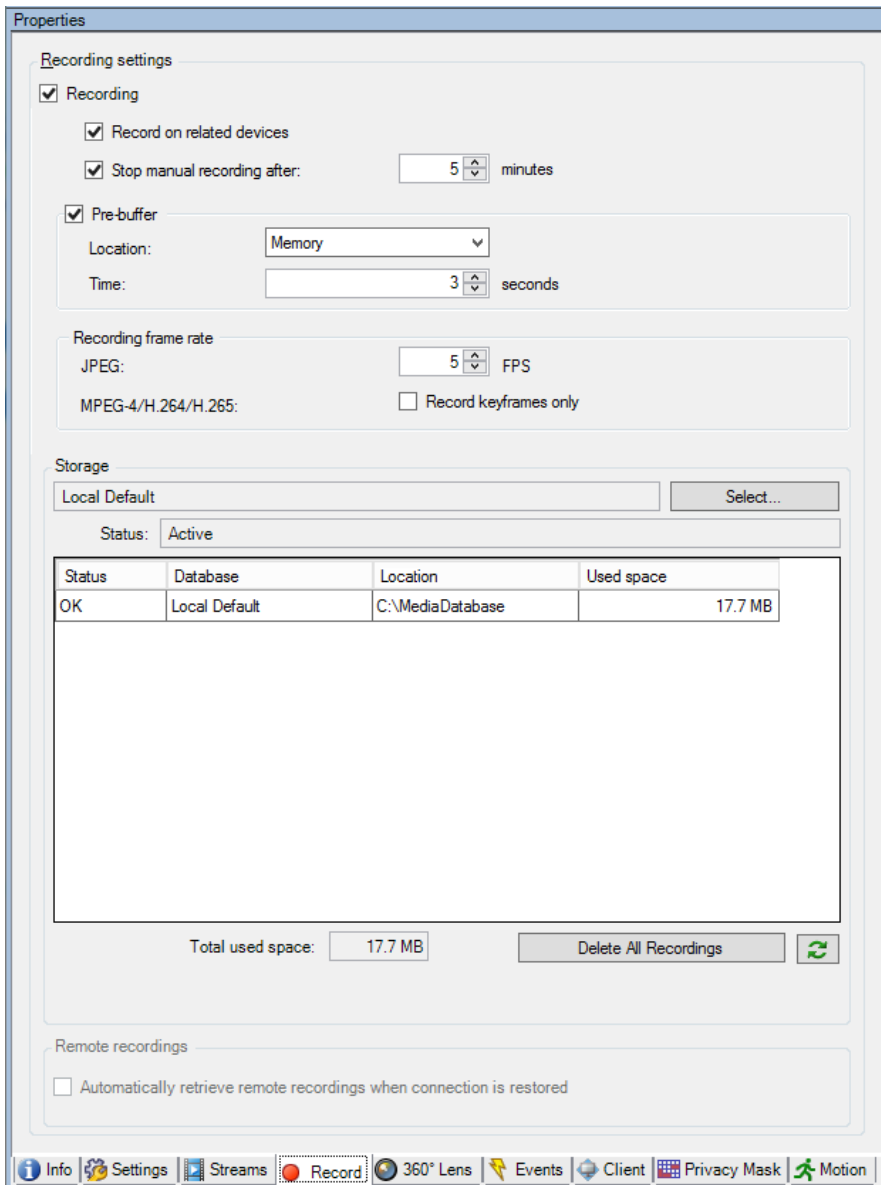
Record tab, example from **camera**

Enable/disable recording

Recording is by default enabled. To enable/disable recording:

1. In the **Site Navigation** pane, select **Recording Servers**.

2. Select the relevant device in the **Overview** pane.

3. On the **Record** tab, select or clear the **Recording** check box.

You must enable recording for the device before you can record data from the camera. A rule that specifies the circumstances for a device to record does not work if you have disabled recording for the device.

Enable recording on related devices

For camera devices, you can enable recording for related devices, for example, microphones that are connected to the same recording server. It means that the related devices record when the camera records.

Recording on related devices are enabled by default for new camera devices, but you can disable and enable as you want. For existing camera devices in the system, the check box is cleared by default.

1. In the **Site Navigation** pane, select **Recording Servers**.

2. Select the relevant camera device in the **Overview** pane.

3. On the **Record** tab, select or clear the **Record on related devices** box.

4. On the **Client** tab, specify the devices that relate to this camera.

If you want to enable recording on related devices that are connected to another recording server, you must create a rule.

About pre-buffering

Pre-buffering is the ability to record audio and video before the actual triggering event occurs. This is useful when you want to record the audio or video that leads up to an event that triggers recording, for example, opening a door.

Pre-buffering is possible because the system continuously receives audio and video streams from the connected devices and temporarily stores them for the defined pre-buffer period.

- If a recording rule is triggered, the temporary recordings are made permanent for the rule's configured pre-recording time.

- If no recording rule is triggered, the temporary recordings in the pre-buffer are automatically deleted after the defined pre-buffer time.

To use the pre-buffer function, the devices must be enabled and sending a stream to the system.

Storage of the temporary pre-buffer recordings

You can choose the storage location of the temporary pre-buffer recordings:

- In the memory; the pre-buffer period is limited to 15 seconds.

- On the disk (in the media database); you can choose all values.

Storage to the memory instead of to disk improves system performance, but is only possible for shorter pre-buffer periods.

When recordings are stored in the memory, and you make some of the temporary recordings permanent, the remaining temporary recordings are deleted and cannot be restored. If you need to be able to keep the remaining recordings, store the recordings on the disk.

Devices that support pre-buffering

Cameras, microphones and speakers support pre-buffering. For speakers, the streams are only sent when the Network Video Management System Smart Client user uses the **Talk to speaker** function. This means that depending on how your speaker streams are triggered to be recorded there is little or no pre-buffering available.

In most cases you set up speakers to record when the Network Video Management System Smart Client user uses the **Talk to speaker** function. In such cases, no speaker pre-buffer is available.

Manage pre-buffering

Enable and disable pre-buffering:

Pre-buffering is enabled by default with a pre-buffer size of three seconds and storage to the memory.

1. To enable/disable pre-buffering, select/clear the **Pre-buffer** check box.

Specify storage location and pre-buffer period:

Temporary pre-buffer recordings are stored either in the memory or on the disk:

1. For **Location**, select **Memory** or **Disk** and specify the number of seconds.

   The number of seconds you specify must be sufficiently large to accommodate your requirements in the various recording rules you define.
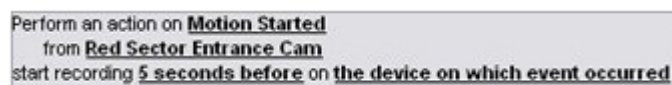
   If you require a pre-buffer period of more than 15 seconds, select **Disk**.

2. If you change the location to **Memory**, the system reduced the period to 15 seconds automatically.

Use pre-buffer in rules:

When you create rules that trigger recording, you can select that recordings should start some time before the actual event (pre-buffer).

> **Example:** The below rule specifies that recording should start on the camera 5 seconds before motion is detected on the camera.

Detail from a rule relying on pre-buffering

To use the pre-buffer recording function in the rule, you must enable pre-buffering on the device being recorded and you must set the pre-buffer length to at least the same length as specified in the rule.

Manage manual recording

Stop manual recording after is enabled by default with a recording time of five minutes. This is to ensure that the system automatically stops all recordings started by the Network Video Management System Smart Client users.

1. To enable and disable manual recording to be stopped automatically by the system, select/clear the **Stop manual recording after** check box.

2. When you enable it, specify a recording time. The number of minutes you specify must be sufficiently large to accommodate the requirements of the various manual recordings without overloading the system.

Add to roles:

You must grant the right to start and stop manual recording to the client users on each camera in **Roles** on the **Device** tab.

Use in rules:

The events you can use when you create rules related to manual recording are:

- **Manual Recording Started**

- **Manual Recording Stopped**

Specify recording frame rate

You can specify the recording frame rate for JPEG.

- Select or type the recording frame rate (in FPS, frames per second) in the **Recording frame rate: (JPEG)** box.

Recording frame rate:

JPEG: 5   FPS

Specifying a specific recording frame rate

Enable keyframe recording

You can enable keyframe recording for MPEG-4/H.264/H.265 streams. It means that the system switches between recording keyframes only and recording all frames depending on your rule settings.

You can, for example, let the system record keyframes when there is no motion in the view and switch to all frames only in case of motion detection to save storage.

1. Select the **Record keyframes only** box.

Recording frame rate

JPEG: 5   FPS

MPEG-4/H.264/H.265:   ☑ Record keyframes only
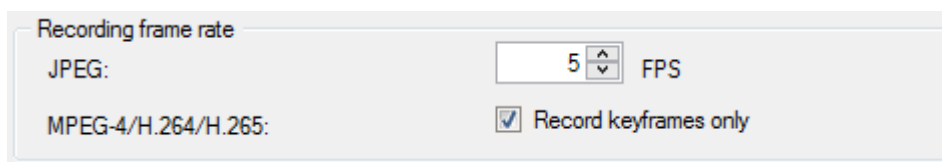
Enabling keyframe recording

2. Set up a rule that activates the function, see About actions and stop actions (on page 131).

About storage

Under **Storage**, you can monitor and manage the databases for a device or a group of devices added to the same recording server.

Above the table, you can see the selected database and its status. In this example, the selected database is the default **Local Default** and the status is **Recordings also located on other recording servers**. The other server is the recording server in building A.

Possible statuses for selected database:

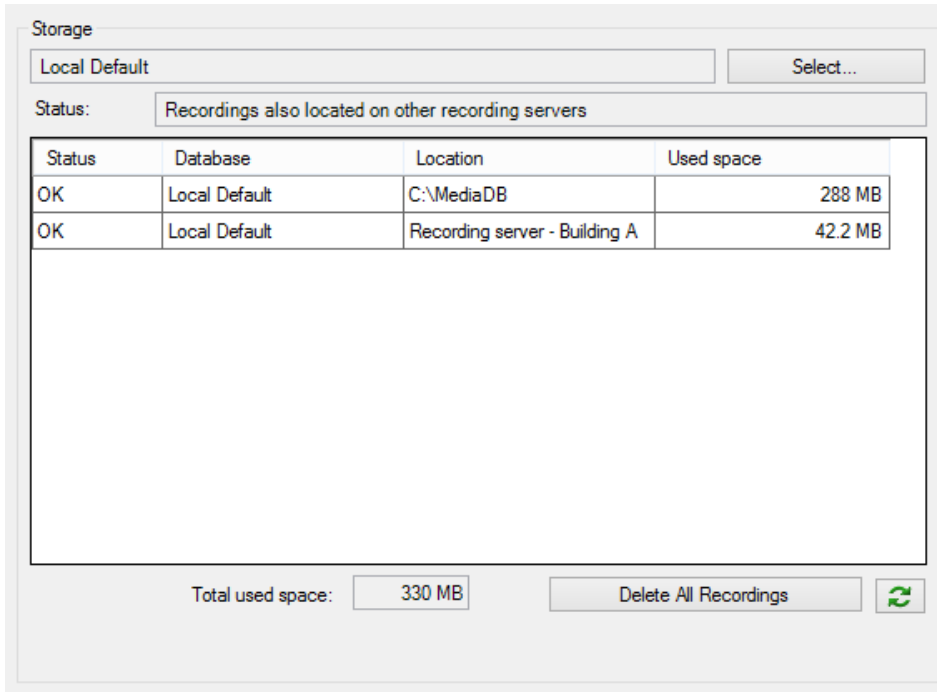| Name	Description
Recordings also located on other recording servers	The database is active and running and has recordings located in storages on other recording servers as well.
Archives also located in old storage	The database is active and running and has archives located in other storages as well.
Active	The database is active and running.
Data for some of the devices chosen is currently moving to another location	The database is active and running and the system is moving data for one or more selected devices in a group from one location to another.
Data for the device is currently moving to another location	The database is active and running and the system is moving data for the selected device from one location to another.

Further down in the window, you can see the status of each database (**OK**, **Offline** or **Old Storage**), the location of each database and how much space each database uses.

If all servers are online, you can see the total spaced used for the entire storage in the **Total used space** field.

With the **Delete All Recordings** button, you can delete all recordings for the device or device group if you have added all devices in the group to the same server. Protected data is not deleted.

For information about configuration of storage, see About storage and archiving (on page 62).

About remote recording

To ensure that all recordings are saved in case of network issues, select **Automatically retrieve remote recordings when connections are restored**. This enables automatic retrieval of recordings once connection is re-established.

The type of hardware selected determines where recordings are retrieved from:

- For a camera with local recording storage, recordings are retrieved from the camera's local recording storage.

You can use the following functionality independently of the automatic retrieval:

- Manual recording.

- The **Retrieve and store remote recordings from <devices>** rule.

- The **Retrieve and store remote recordings between <start and end time> from <devices>** rule.

Presets tab (devices)

About the Presets tab

The following devices have a **Presets** tab:

- PTZ cameras that support preset positions

On the **Presets** tab, you can create or import preset positions, for example:

- In rules for making a PTZ (pan-tilt-zoom) camera move to a specific preset position when an event occurs.

- In patrolling, for the automatic movement of a PTZ camera between a number of preset positions.

- For manual activation by the Network Video Management System Smart Client users.

You can lock a preset position if you want to prevent users in Network Video Management System Smart Client or users with limited security rights from updating this preset. Locked presets are indicated with this icon .

You assign PTZ permission to roles on the Overall Security tab (see "Overall Security tab (roles)" on page 169) or the PTZ tab (see "PTZ tab (roles)" on page 177).

You can monitor if the system is currently patrolling or a user has taken control, in the **PTZ session** area. (see "PTZ session properties" on page 107)

You also change the PTZ session timeouts for the camera.
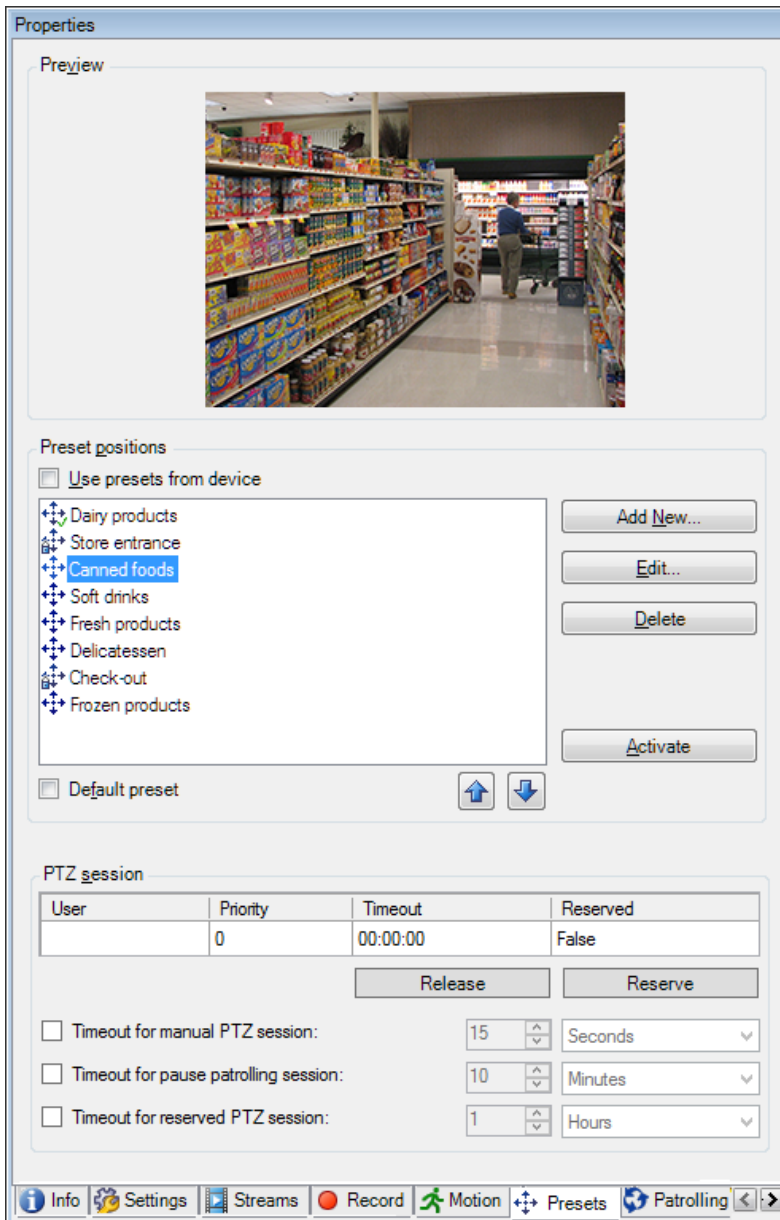
Presets tab, with preset positions defined

Add a preset position (type 1)

To add a preset position for the camera:

1. Click **Add New**. The **Add Preset** window appears:
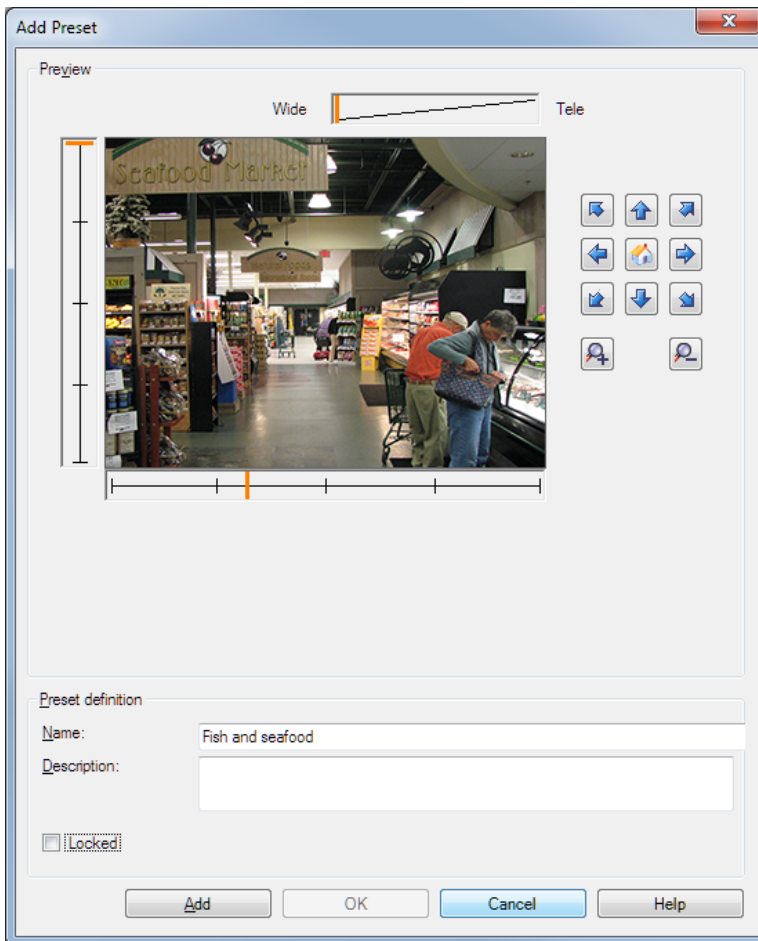
2. The **Add Preset** window displays a live preview image from the camera. Use the navigation buttons and/or sliders to move the camera to the required position.

3. Specify a name for the preset position in the **Name** field.

4. Optionally, type a description of the preset position in the **Description** field.

5. Select **Locked** if you want to lock the preset position. Only users with sufficient rights can unlock the position afterwards.

6. Click **Add** to specify presets. Keep adding until you have the presets you want.

7. Click **OK**. The **Add Preset** window closes, and adds the position to the **Presets** tab's list of available preset positions for the camera.

Use preset positions from the camera (type 2)

As an alternative to specifying preset positions in the system, you can specify preset positions for some PTZ cameras on the camera itself. You can typically do this by accessing a product-specific configuration web page.

1. Import the presets into the system by selecting **Use presets from device**.

Any presets you have previously defined for the camera are deleted and affect any defined rules and patrolling schedules as well as remove the presets available for the Network Video Management System Smart Client users.

2. Click **Delete** to delete presets that your users do not need.

3. Click **Edit** if you want to change the display name of the preset (see "Edit a preset position name (type 2 only)" on page 105).

4. If you later want to edit such device-defined presets, edit on the camera and then re-import.

Assign a default preset position

If required, you can assign one of a PTZ camera's preset positions as the camera's default preset position.

It can be useful to have a default preset position because it allows you to define rules that specify that the PTZ camera should go to the default preset position under particular circumstances, for example after you have operated the PTZ camera manually.

1. To assign a preset position as the default, select the preset in your list of defined preset positions.

2. Select the **Default preset** check box below the list.

You can only define one preset position as the default preset position.

Edit a preset position (type 1 only)

To edit an existing preset position defined in the system:

1. Select the preset position in the **Presets** tab's list of available preset positions for the camera.

2. Click **Edit**. This opens the **Edit Preset** window:
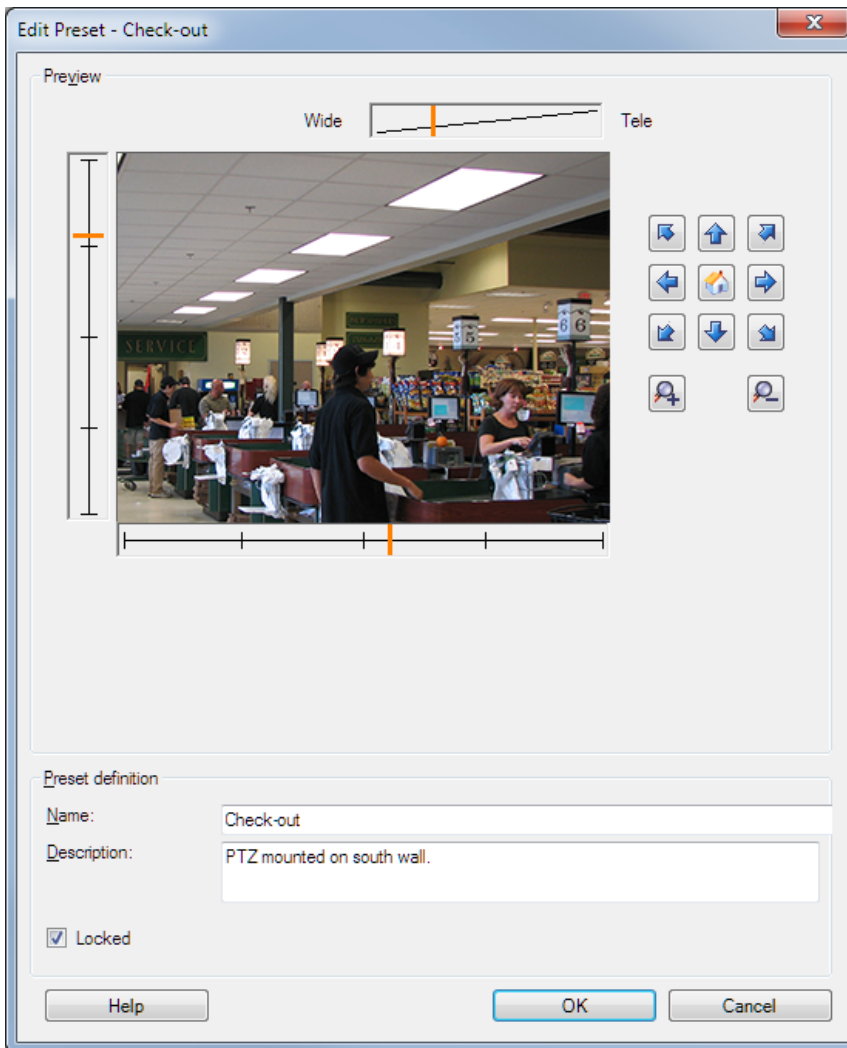
Example only. Features are camera-dependent

3. The **Edit Preset** window displays live video from the preset position. Use the navigation buttons and/or sliders to change the preset position as required.

4. Change the name/number and description of the preset position if needed.

5. Select **Locked** if you want to lock the preset position. Only users with sufficient rights can unlock the position afterwards.

6. Click **OK**.

Edit a preset position name (type 2 only)

To edit the name of a preset position defined in the camera:

1. Select the preset position in the **Presets** tab's list of available presets for the camera.

2. Click **Edit**. This opens the **Edit Preset** window:
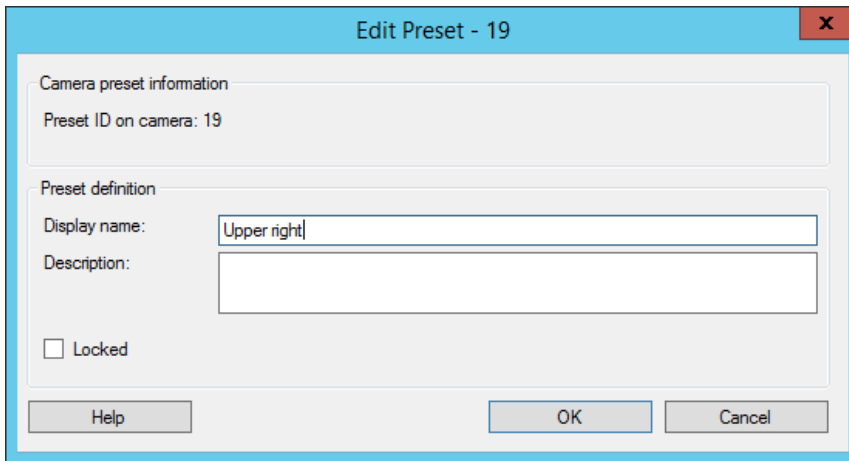
Example of a preset defined in the camera

3. Change the name and add a description of the preset position if needed.

4. Select **Locked** if you want to lock the preset name. You can lock a preset name if you want to prevent users in Network Video Management System Smart Client or users with limited security rights from updating the preset name or deleting the preset. Locked presets are indicated with this icon 🖼️. Only users with sufficient rights can unlock the preset name afterwards.

5. Click **OK**.

Lock a preset position

You can lock a preset position if you want to prevent users in Network Video Management System Smart Client or users with limited security rights from updating or deleting a preset. Locked presets are indicated with this icon 🖼️.

You lock presets as part of adding (see "Add a preset position (type 1)" on page 102) and editing (see "Edit a preset position (type 1 only)" on page 104).

Test a preset position (type 1 only)

1. Select the preset position in the **Presets** tab's list of available preset positions for the camera.

2. Click **Activate**.

3. The camera moves to the selected preset position.

Specify PTZ session timeouts

Management Client and Network Video Management System Smart Client users with the necessary user rights can manually interrupt the patrolling of PTZ cameras.

You can specify how much time should pass before regular patrolling is resumed for all PTZ cameras on your system:

1. Select **Tools** > **Options**.

2. On the **Options** window's **General** tab, select the amount of time in the:

- **Timeout for manual PTZ sessions** list (default is 15 seconds).

- **Timeout for pause patrolling sessions** list (default is 10 minutes).

The settings apply for all PTZ cameras on your system.

You can change the timeouts individually for each camera.

1. In the **Site Navigation** pane, click **Camera**.

2. In the Overview pane, select the camera.

3. On the **Presets** tab, select the amount of time in the:

- **Timeout for manual PTZ session** list (default is 15 seconds).

- **Timeout for pause patrolling session** list (default is 10 minutes).

The settings apply for this camera only.

PTZ session properties

The **PTZ session** table shows the current status of the PTZ camera.

Name	Description
User	Displays the user that has pressed the **Reserved** button and currently controls the PTZ camera. If a patrolling session is activated by the system, it displays **Patrolling**.
Priority	Displays the user's PTZ priority. You can only take over PTZ sessions from users with a lower priority than you.
Timeout	Displays the remaining time of the current PTZ session.

You can change the following timeouts for each PTZ camera.

Name	Description
Timeout for manual PTZ session	Specify the timeout period for manual PTZ sessions on this camera if you want the timeout to be different from the default period. You specify the default period in the **Tools** menu under **Options**.
Timeout for pause patrolling PTZ session	Specify the timeout period for pause patrolling PTZ sessions on this camera if you want the timeout to be different from the default period. You specify the default period in the **Tools** menu under **Options**.

Patrolling tab (devices)

About the Patrolling tab

The following devices have a **Patrolling** tab:

- PTZ cameras

On the **Patrolling** tab, you can create patrolling profiles - the automatic movement of a PTZ (pan-tilt-zoom) camera between a number of preset positions.
Before you can work with patrolling, you must specify at least two preset positions for the camera in the **Presets** tab.

Patrolling profiles are the definitions of how patrolling should take place. This includes the order in which the camera should move between preset positions and how long it should remain at each position. You can create an unlimited number of patrolling profiles and use them in your rules. For example, you may create a rule specifying that one patrolling profile should be used during daytime opening hours and another during nights.
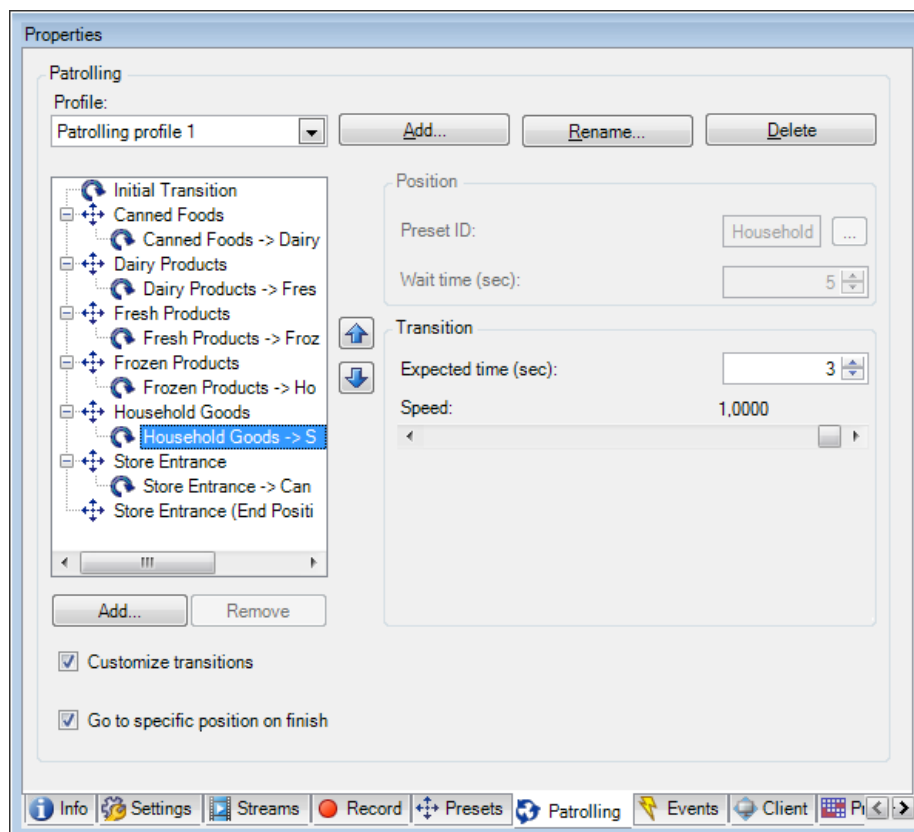
Patrolling tab, displaying a patrolling profile with customized transitions

Add a patrolling profile

Add a profile that you want to use in a rule:

1. Click **Add**. The **Add Profile** dialog box appears.

2. In the **Add Profile** dialog box, specify a name for the patrolling profile.

3. Click **OK**. The button is disabled if the name is not unique.

   The new patrolling profile is added to the **Profile** list. You can now specify the preset positions and other settings for the patrolling profile.

Specify preset positions in a patrolling profile

1. Select the patrolling profile in the **Profile** list:

2. Click **Add**.

3. In the **Select Preset** dialog box, select the preset positions for your patrolling profile:

4. Click **OK**. The selected preset positions are added to the list of preset positions for the patrolling profile:
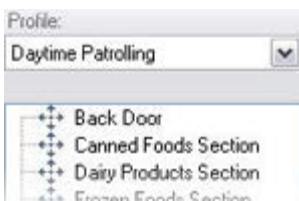
5. The camera uses the preset position at the top of the list as the first stop when it patrols according to the patrolling profile. The preset position in the second position from the top is the second stop, and so forth.

Specify the time at each preset position

When patrolling, the PTZ camera by default remains for 5 seconds at each preset position specified in the patrolling profile.

To change the number of seconds:

1. Select the patrolling profile in the **Profile** list.

2. Select the preset position for which you want to change the time:

3. Specify the time in the **Time on position (sec)** field:

4. If required, repeat for other preset positions.

Customize transitions

By default, the time required for moving the camera from one preset position to another, known as **transition**, is estimated to be three seconds. During this time, motion detection is by default disabled on the camera, because irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions.

You can only customize speed for transitions if your camera supports PTZ scanning and is of the type where preset positions are configured and stored on your system's server (type 1 PTZ camera). Otherwise the **Speed** slider is grayed out.

You can customize the following:

- The estimated transition time.

- The speed with which the camera moves during a transition.

To customize transitions between the different preset positions:

1. Select the patrolling profile in the **Profile** list.

2. Select the **Customize transitions** check box:

Transition indications are added to the list of preset positions.

3. In the list, select the transition:

4. Specify the estimated transition time (in number of seconds) in the **Expected time (sec)** field:
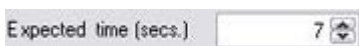
5. Use the **Speed** slider to specify the transition speed. When the slider is in its rightmost position, the camera moves with its default speed. The more you move the slider to the left, the slower the camera moves during the selected transition.

6. Repeat as required for other transitions.

Specify an end position

You can specify that the camera should move to a specific preset position when patrolling according to the selected patrolling profile ends.

1. Select the patrolling profile in the **Profile** list.

2. Select the **Go to specific position on finish** check box. This opens the **Select preset** dialog box.

3. Select the end position, and click **OK**.

   You can select any of the camera's preset positions as the end position, you are not limited to the preset positions used in the patrolling profile.

4. The selected end position is added to the profile list.

   When patrolling according to the selected patrolling profile ends, the camera moves to the specified end position.

Fisheye lens tab (devices)

About the Fisheye Lens tab

The following devices have a **Fisheye Lens** tab:

- Fixed cameras with a fisheye lens

On the **Fisheye Lens** tab, you can enable and configure fisheye lens support for the selected camera.
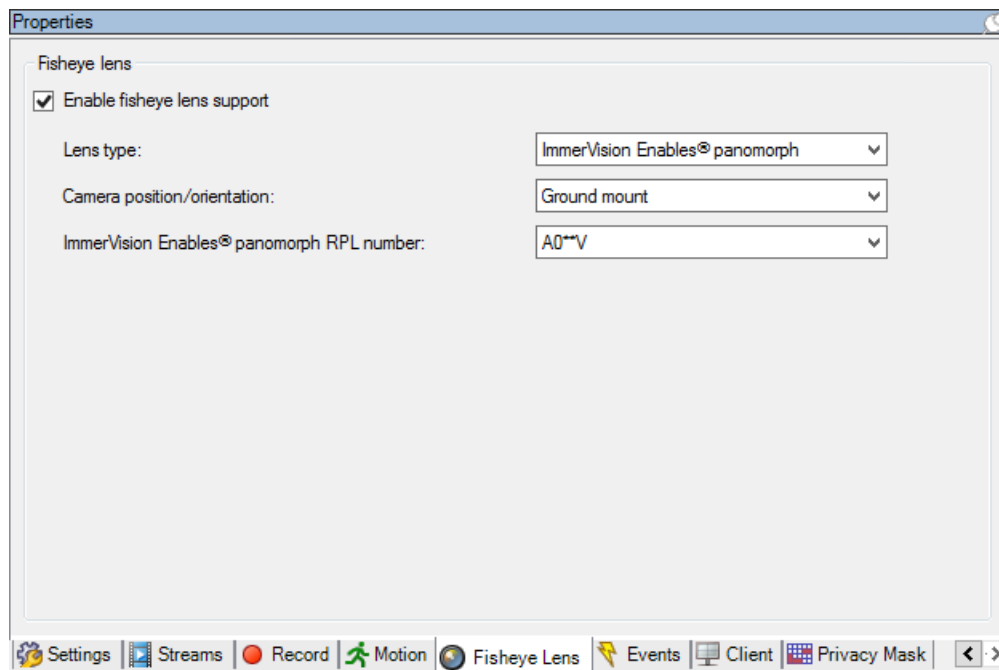
Enable and disable fisheye lens support

The fisheye lens support is disabled by default.

To enable or disable it, select or clear the **Fisheye Lens** tab's **Enable fisheye lens support** check box.

Specify fisheye lens settings

When you enable the fisheye lens support:

1. Select the lens type.

2. Specify the physical position/orientation of the camera from the **Camera position/orientation** list.

3. Select a Registered Panomorph Lens (RPL) number from the **ImmerVision Enables® panomorph RPL number** list.

   This ensures the identification and correct configuration of the lens used with the camera. You usually find the RPL number on the lens itself or on the box it came in. For details of ImmerVision, panomorph lenses, and RPLs, see the Immervision website https://www.immervisionenables.com/**.**

Events tab (devices)

About the Events tab

The following devices have an **Events** tab:

- Cameras

- Microphones

- Inputs

In addition to the system's event, some devices can be configured to trigger events. You can use these events when creating event-based rules in the system. Technically, they occur on the actual hardware/device rather than on the surveillance system.
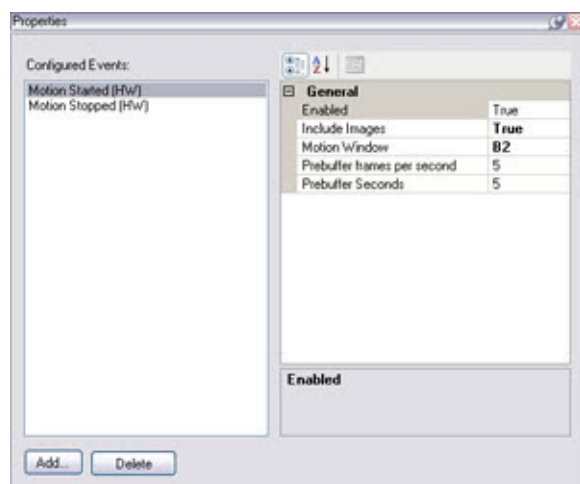
Event tab, example from **camera**

When you delete an event, it affects all rules that use the event.

- Add an event (on page 113)

- Specify event properties (on page 113)

- Use several instances of an event (on page 113)

Add an event

1. In the **Overview** pane, select a device.

2. Select the **Events** tab and click **Add**. This opens the **Select Driver Event** window.

3. Select an event. You can only select one event at a time.

4. Click **OK**.

5. In the toolbar, click **Save**.

Specify event properties

You can specify properties for each event you have added. The number of properties depends on the device and the event. In order for the event to work as intended, you must specify some or all of the properties identically on the device as well as on this tab.

Use several instances of an event

To be able to specify different properties for different instances of an event, you can add an event more than once.

The following example is specific to **cameras**.

Example: You have configured the camera with two motion windows, called A1, and A2. You have added two instances of the **Motion Started (HW)** event. In the properties of one instance, you have specified the use of motion window A1. In the properties of the other instance, you have specified the use of motion window A2.

When you use the event in a rule, you can specify that the event should be based on motion detected in a specific motion window for the rule to be triggered:
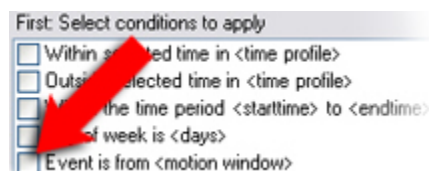
Example: Specifying specific motion window
as part of a rule's conditions

Event tab (properties)

Name	Description
Configured events	Which events you may select and add in the **Configured events** list is determined entirely by the device and its configuration. For some types of devices, the list is empty.
General	The list of properties depends on the device and the event. In order for the event to work as intended, you must specify some or all of the properties identically on the device as well as on this tab.

Client tab (devices)

About the Client tab

The following devices have a **Client** tab:

- Cameras

On the **Client** tab you can specify which other devices are viewed and heard when you use the camera in Network Video Management System Smart Client.

The related devices also record when the camera records, see Enable recording on related devices (on page 97).

Client tab properties

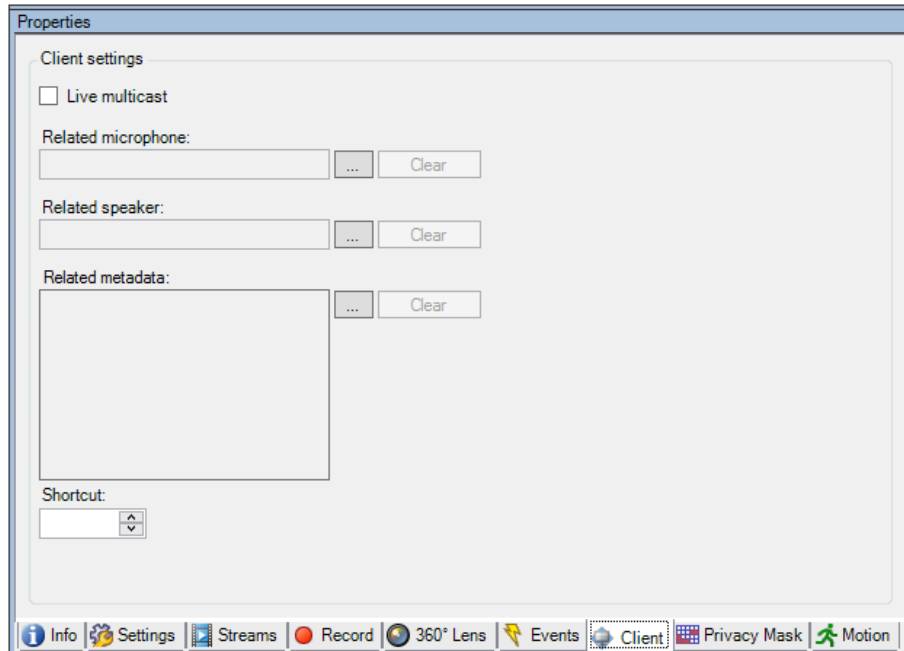| Name	Description
Live multicast	The system supports multicast of live streams from the recording server to Network Video Management System Smart Client. To enable multicast of live streams from the selected camera, select the check box. You must also configure multicasting for the recording server. See About multicasting (on page 70). If multicast streams do not work, for example due to restrictions on the network or on individual clients, the system reverts to unicast.
Related microphone	Specify from which microphone on the camera, that Network Video Management System Smart Client users by default receive audio. The Network Video Management System Smart Client user can manually select to listen to another microphone if needed. The related microphones record when the camera records.
Related speaker	Specify through which speakers on the camera, that Network Video Management System Smart Client users speak by default. The Network Video Management System Smart Client user can manually select another speaker if needed. The related speakers record when the camera records.
Related metadata	Specify one or more metadata devices on the camera, that Network Video Management System Smart Client users receive data from. The related metadata devices record when the camera records.
Shortcut	To ease the selection of cameras for the Network Video Management System Smart Client users, define keyboard shortcuts to the cameras. • Create each shortcut so it uniquely identifies the cameras. • A camera shortcut number cannot be longer than four digits.

Privacy mask tab (devices)

About the Privacy Mask tab

The following devices have a **Privacy Mask** tab:

• Cameras

On the **Privacy Mask** tab, you can enable and configure privacy masking for the selected camera. You can define which areas of the image to mask before distribution. For example, if a surveillance camera covers a street, in order to protect residents' privacy, you can mask certain areas of a building (could be windows and doors) with privacy masking.

When viewed via Network Video Management System Smart Client or any other media, privacy masked areas appear as black areas which no one can remove.
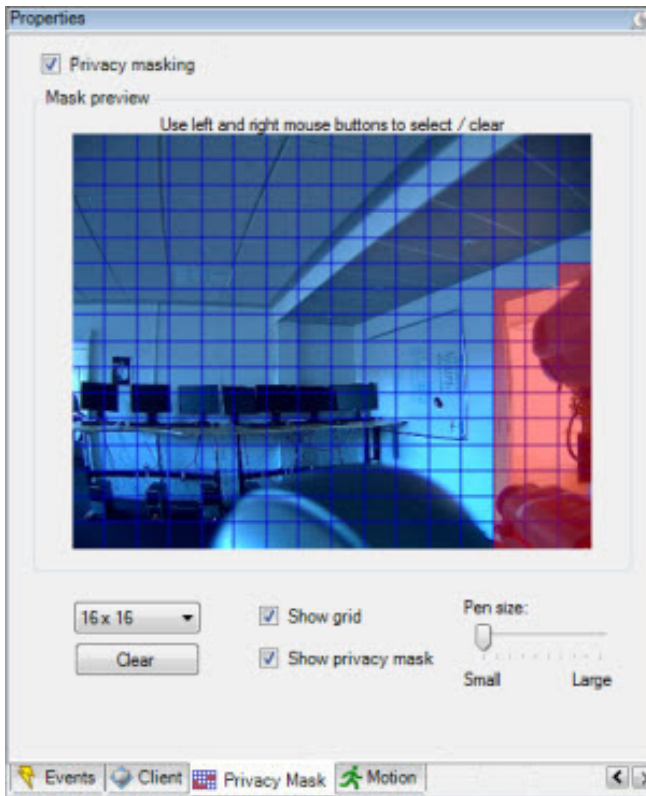
Red areas indicate the areas masked for privacy.

When you use privacy masks with PTZ cameras and you pan-tilt-zoom the camera, the selected area masked for privacy does **not** move accordingly because the masked area is locked to the camera image. As an alternative, some PTZ cameras support enabling of a position based privacy mask in the camera itself.

In a   setup, the central site disregards privacy masking defined in a remote site. If you want to apply the same privacy masking, you must redefine it on the central site.

Enable/disable privacy masking

The privacy masking feature is disabled by default.

To enable/disable the privacy masking feature for a camera:

- Select/clear the **Privacy Mask** tab's **Privacy masking** check box.

Specify privacy mask settings

When you enable privacy masking, the preview image is divided into selectable sections by a grid.

1. To define privacy mask regions, drag the mouse pointer over the required areas in the preview image. Press down the left mouse button to select a grid section. Right mouse button clears a grid section.

2. You can define as many privacy mask regions as needed. Privacy mask regions are shown in red.
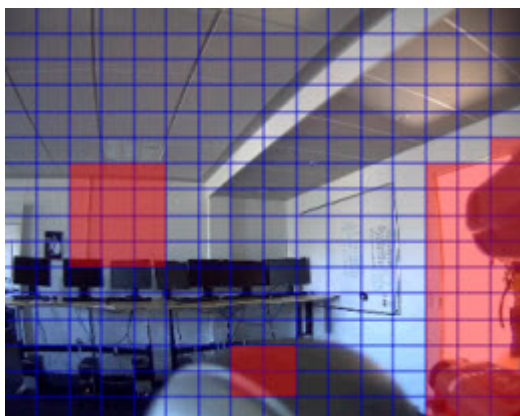
Three privacy mask regions defined in the preview window. In this case, the grid is visible.

The red privacy mask indications also appear in the preview image on the **Motion** tab.

Privacy mask tab (properties)

Name	Description
Grid Size	The value you selected in the **Grid size** list determines the density of the grid, regardless whether the grid is shown or not. Select between the values 8×8, 16×16, 32×32 or 64×64.
Show Grid	Select the **Show grid** check box to make the grid visible.
Show Privacy Mask	When you select the **Show privacy mask** check box (default), selected regions are highlighted in red in the preview image. Hiding regions may provide a less obscured view of the preview image. Sony recommends that you keep the **Show privacy mask** box selected to avoid that regions exist without you or your colleagues being aware of it.
Pen size	Use the **Pen size** slider to indicate the size of the selections you wish to make when you click and drag the grid to select regions. Default is set to small, which is equivalent to one square in the grid.

Motion tab (devices)

About the Motion tab

The following devices have a **Motion** tab:

- Cameras

On the **Motion** tab, you can enable and configure motion detection for the selected camera. Motion detection configuration is a key element in your system: Your motion detection configuration determines when the system generates motion events and typically also when video is recorded.

Time spent on finding the best possible motion detection configuration for each camera helps you later avoid, for example, unnecessary recordings. Depending on the physical location of the camera, it may be a good idea to test motion detection settings under different physical conditions such as day/night and windy/calm weather.

Before you configure motion detection for a camera, Sony recommends that you have configured the camera's image quality settings, for example resolution, video codec and stream settings on the **Settings** tab. If you later change image quality settings, you should always test any motion detection configuration afterwards.
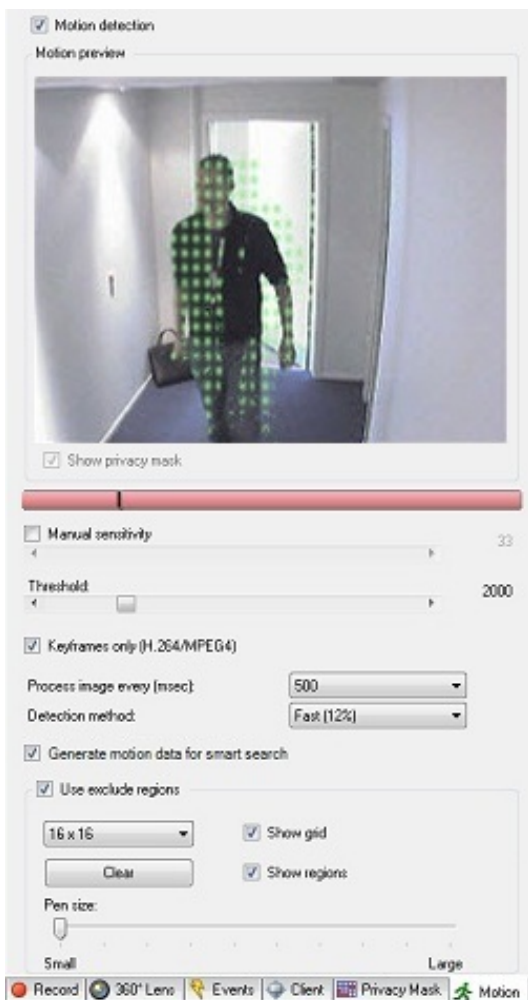
Camera properties: **Motion** tab with red deflection on the motion indication bar

You can configure all the settings for a group of cameras, but you would typically set the exclude regions per camera.

- Enable and disable motion detection (on page 119)

- Specify motion detection settings (on page 119)

Enable and disable motion detection

You specify the default setting of motion detection for cameras on the **Tools** > **Options** > **General** tab.

To enable or disable motion detection afterwards for a camera:

- Select or clear the **Motion** tab's **Motion detection** check box.

Important: When you disable motion detection for a camera, motion detection-related rules for the camera do not work.

Specify motion detection settings

You can specify settings related to the amount of changes required in a camera's view in order for the change to be regarded as motion. You can for example specify intervals between motion detection analysis and areas of a view in which motion should be ignored.

About dynamic sensitivity

Motion detection is by default set up for dynamic sensitivity. To adjust the sensitivity level manually, see Enable manual sensitivity (on page 119).

Sony recommends that you do not enable manual sensitivity because:

- With dynamic sensitivity, the system calculates and optimizes the sensitivity level automatically and suppresses the motion detections that come from noise in the images.

- Dynamic sensitivity improves motion detection at nighttime, where the noise in the images often triggers false motion.

- The system is not overloaded from too much recording.

- The users are not missing results from too little recording.

Enable manual sensitivity

The sensitivity setting determines **how much each pixel** in the image must change before it is regarded as motion.

1. Select the **Motion** tab's **Manual Sensitivity** check box.

2. Drag the slider to the left for a higher sensitivity level, and to the right for a lower sensitivity level.

   The **higher** the sensitivity level, the less change is allowed in each pixel before it is regarded as motion.

   The **lower** the sensitivity level, the more change in each pixel is allowed before it is regarded as motion.

   Pixels in which motion is detected are highlighted in green in the preview image.

3. Select a slider position in which only detections you consider motion are highlighted.

Highlighted motion in the preview image

You can compare and set the exact sensitivity setting between cameras by the number in the right side of the slider.

Specify threshold

The motion detection threshold determines **how many pixels** in the image must change before it is regarded as motion.

1. Drag the slider to the left for a higher motion level, and to the right for a lower motion level.

2. Select a slider position in which only detections that you consider motion are detected.

The black vertical line in the motion indication bar shows the motion detection threshold: When detected motion is above the selected detection threshold level, the bar changes color from green to red, indicating a positive detection.

Motion indication bar: changes color from green to red when above the threshold, indicating a positive motion detection

Select keyframes settings

Determines if motion detection is done on keyframes only instead of on the entire video stream. Only applies to MPEG-4/H.264/H.265.

Motion detection on keyframes reduces the amount of processing power used to carry out the analysis.

Select **Keyframes only (MPEG-4/H.264/H.265)** box to do motion detection on keyframes only.

Select image processing interval

You can select how often the system performs the motion detection analysis.

From the **Process image every (msec)** list:

- Select the interval. For example, every 1000 milliseconds are once every second. Default value is every 500 milliseconds.

  The interval is applied if the actual frame rate is higher than the interval you set here.

Specify detection method

Lets you optimize motion detection performance by analyzing only a selected percentage of the image, for example 25%. By analyzing 25%, only every fourth pixel in the image is analyzed instead of all pixels.

Using optimized detection reduces the amount of processing power used to carry out the analysis, but also means a less accurate motion detection.

- In the **Detection method** list, select the wanted detection method.

About generate motion data for smart search

With **Generate motion data for smart search** enabled, the system generates motion data for the images used for motion detection. For example, if you select motion detection on keyframes only, the motion data is also produced for keyframes only.

The extra motion data enables the client user, via the smart search function, to quickly search for relevant recordings based on motion in the selected area of the image. The motion data is not generated for areas with privacy masks.

Motion detection threshold and exclude regions do not influence the generated motion data.

You specify the default setting of generating smart search data for cameras on the **Tools** > **Options** > **General** tab.

Specify exclude regions

You can disable motion detection in specific areas of a camera view.

Disabling motion detection in specific areas helps you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

When you use exclude regions with PTZ cameras and you pan-tilt-zoom the camera, the excluded area does **not** move accordingly because the area is locked to the camera image, and not the object.

1. To use exclude regions, select the **Use exclude regions** check box.

   A grid divides the preview image into selectable sections.

2. To define exclude regions, drag the mouse pointer over the required areas in the preview image while you press the left mouse button. Right mouse button clears a grid section.

You can define as many exclude regions as needed. Excluded regions appear in blue.
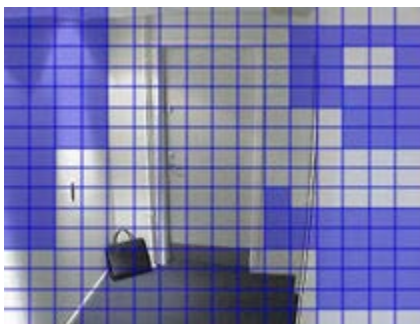
Three exclude regions defined in the preview window. In this case, the grid is visible.

The blue exclude areas only appear in the preview image on the **Motion** tab, not in any other preview images in the Management Client or access clients.

Client

About clients

The Client section of the Management Client consists of:

Name	Description
Network Video Management System Smart Wall	Network Video Management System Smart Wall is an add-on that allows you to send view content from Network Video Management System Smart Client to dedicated video wall.
	For more detailed information about Network Video Management System Smart Wall, see About Network Video Management System Smart Wall (on page 208).
View groups	The way in which video from cameras is presented is called a view. To control who can see what in Network Video Management System Smart Client, you can create view groups to group views in logical entities. You can assign access to these view groups through roles and limit who can access individual view groups to specific roles. Select **View Groups** to design and work with view groups to fit your surveillance needs.
Smart Client profiles	To differentiate Network Video Management System Smart Client users, you can create Smart Client profiles, prioritize these and customize their profiles as needed for the different tasks at hand.
Matrix	Matrix is a feature for distributing video remotely. If you use Matrix, you can push video from any camera on your system's network to any running Network Video Management System Smart Client.

View groups

About view groups

The way in which the system presents video from one or more cameras in clients is called a view. A view group is a container for one or more logical groups of such views. In clients, a view group is presented as an expandable folder from which users can select the group and the view they want to see:

Example from Network Video Management System Smart Client: Arrow indicates a view group, which contains a logical group (called Amenities), which in turn contains 3 views.

About view groups and roles

By default, each role you define in the Management Client is also created as a view group. When you add a role in the Management Client, the role by default appears as a view group for use in clients.

- You can assign a view group based on a role to users/groups assigned to the relevant role. You may change these view group rights by setting this up in the role afterwards.

- A view group based on a role carries the role's name.

  Example: If you create a role with the name **Building A Security Staff**, it appears in Network Video Management System Smart Client as a view group called **Building A Security Staff**.

  In addition to the view groups you get when adding roles, you may create as many other view groups as you like. You can also delete view groups, including those automatically created when adding roles.

- Even if a view group is created each time you add a role, view groups do not have to correspond to roles. You can add, rename or remove any of your view groups if required.

Note that if you rename a View group, client users already connected must log out and log in again before the name change is visible.

Add a view group

1. Right-click **View Groups**, and select **Add View Group**. This opens the **Add View Group** dialog box.

2. Type the name and an optional description of the new view group and click **OK**.

Note: No roles have the right to use the newly added view group until you have specified such rights. If you have specified which roles that can use the newly added view group, already connected client users with the relevant roles must log out and log in again before they can see the view group.

Smart Client profiles

About Smart Client profiles

Smart Client profiles allows system administrators to control how Network Video Management System Smart Client should look and behave and what features and panes Network Video Management System Smart Client users have access to. You can set up user rights for: panes and options, minimize/maximize options, inactivity time-control, remember password or not, view shown after log in, layout of print reports, export path, and more.

To manage Smart Client profiles in the system, expand **Client** and select **Smart Client Profiles**. You can also learn about the relationship between Smart Client profiles, roles and time profiles and how to use these together (see "Create and set up Smart Client profiles, roles and time profiles" on page 124).

Add and configure a Smart Client profile

You must create a Smart Client profile before you can configure it.

1. Right-click **Smart Client Profiles**.

2. Select **Add Smart Client Profile**.

3. In the **Add Smart Client Profile** dialog box, type a name and description of the new profile and click **OK**.

4. In the **Overview** pane, click the profile you created to configure it.

5. Adjust settings on one, more or all of the available tabs and click **OK**.

Copy a Smart Client profile

If you have a Smart Client profile with complicated settings or rights and need a similar profile, it might be easier to copy an already existing profile and make minor adjustments to the copy than to creating a new profile from scratch.

1. Click **Smart Client Profiles**, right-click the profile in the **Overview** pane, select **Copy Smart Client Profile**.

2. In the dialog box that appears, give the copied profile a new unique name and description. Click **OK**.

3. In the **Overview** pane, click the profile you just created to configure it. This is done by adjusting settings on one, more or all of the available tabs. Click **OK**.

Create and set up Smart Client profiles, roles and time profiles

When you work with Smart Client profiles, it is important to understand the interaction between Smart Client profiles, roles and time profiles.

- Smart Client profiles deal with user right settings in Network Video Management System Smart Client

- Roles deal with security settings in clients, MIP SDK and more

- Time profiles deal with time aspects of the two profiles-types

Together these three features provide unique control and customizing possibilities with regards to Network Video Management System Smart Client user rights.

Example: You need a user in your Network Video Management System Smart Client setup who should only be allowed to view live video (no playback) from selected cameras, and only during normal working hours (8.00 to 16.00). One way of setting this up could be as follows:

1. Create a Smart Client profile, and name it, for example, **Live only**.

2. Specify the needed live/playback settings on **Live only**.

3. Create a time profile, and name it, for example, **Daytime only**.

4. Specify the needed time period on **Daytime only**.

5. Create a new role and name it, for example, **Guard (Selected cameras)**.

6. Specify which cameras **Guard (Selected cameras)** can use.

7. Assign the **Live only** Smart Client profile and the **Daytime only** time profile to the **Guard (Selected cameras)** role to connect the three elements.

You now have a mix of the three features creating the wanted result and allowing you room for easy fine-tuning and adjustments. Note also that you can do the setup in a different order, for example, creating the role first and then the Smart Client profile and the time profile, or any other order you prefer.

Set simplified mode as the default mode

Through the Smart Client profiles, you can configure your system to automatically open Network Video Management System Smart Client in simplified mode with a limited set of features and tabs. By default, Network Video Management System Smart Client opens in advanced mode with the complete set of features and tabs.

If the Network Video Management System Smart Client operator at some point decides to switch to a different mode than the default mode, Network Video Management System Smart Client remembers this setting the next time the operator opens the program.

1. In Management Client, expand the **Client** node.

2. Select the relevant Smart Client profile.

3. Click the **General** tab.
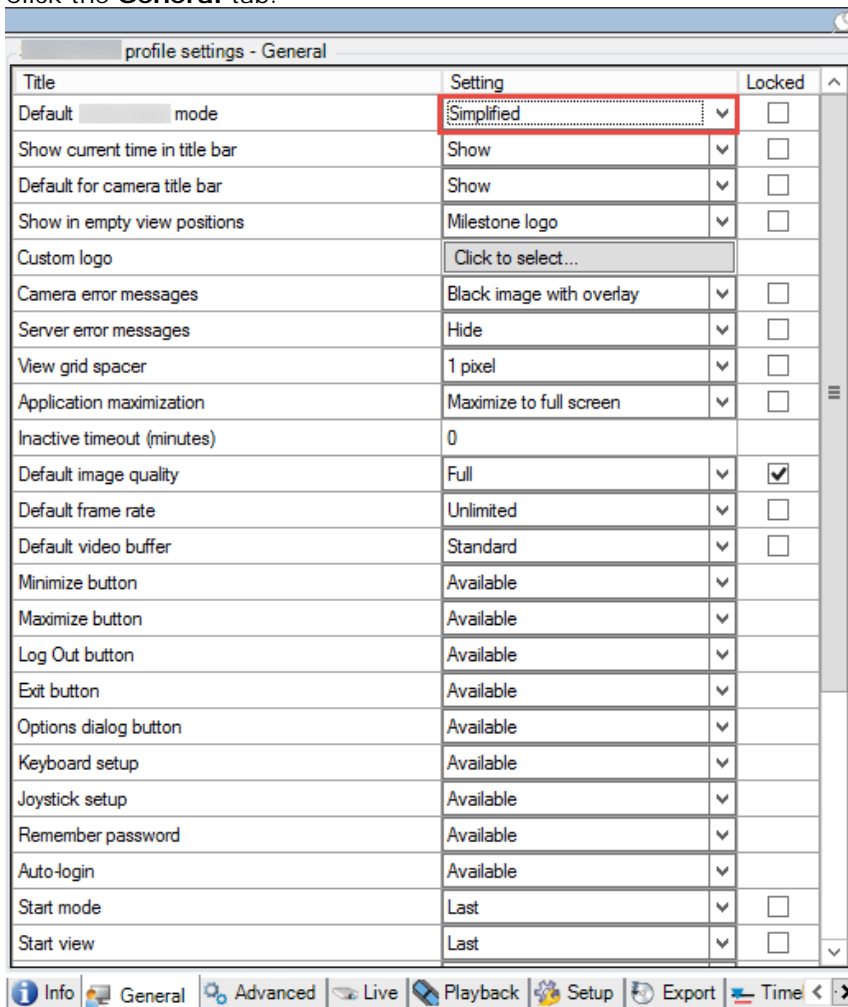
4. In the **Default Smart Client mode** list, select **Simplified**. Network Video Management System Smart Client now opens in simplified mode for those users associated with the current Smart Client profile.

See also

Prevent operators from switching between simple and advanced mode

In Network Video Management System Smart Client, operators can switch between simple and advanced mode. However, you can prevent the Network Video Management System Smart Client operators from switching between modes. Technically, you must lock the setting that determines whether Network Video Management System Smart Client opens in simple mode or advanced mode.

1. In Management Client, expand the **Client** node.

2. Select the relevant Smart Client profile.

3. Click the **General** tab.

Title	Setting	Locked
Default _____ mode	Simplified	☐
Show current time in title bar	Show	☐
Default for camera title bar	Show	☐
Show in empty view positions	Milestone logo	☐
Custom logo	Click to select...	
Camera error messages	Black image with overlay	☐
Server error messages	Hide	☐
View grid spacer	1 pixel	☐
Application maximization	Maximize to full screen	☐
Inactive timeout (minutes)	0	
Default image quality	Full	☑
Default frame rate	Unlimited	☐
Default video buffer	Standard	☐
Minimize button	Available	
Maximize button	Available	
Log Out button	Available	
Exit button	Available	
Options dialog button	Available	
Keyboard setup	Available	
Joystick setup	Available	
Remember password	Available	
Auto-login	Available	
Start mode	Last	☐
Start view	Last	☐

Info | General | Advanced | Live | Playback | Setup | Export | Time

4. Verify that the **Default Smart Client mode** list has the proper value. If **Enabled**, Network Video Management System Smart Client opens in simple mode.

5. Select the **Locked** check box. The mode toggling button in Network Video Management System Smart Client is hidden.

See also

Set simple mode as the default mode (see "Set simplified mode as the default mode" on page 125)

Smart Client profile properties

The following tabs allow you to specify the properties of each Smart Client profile. You can lock the settings in the Management Client if required, so the users of Network Video Management System Smart Client cannot change them:

Tab	Description
Info	Name and description, priority of existing profiles and an overview of which roles use the profile.
	If a user is a member of more than one role, each with their individual Smart Client profile, the user gets the Smart Client profile with the highest priority.
General	Settings such as show/hide and mini- and maximize menu settings, login/-out, startup, timeout, info and messaging options, and Sequence Explorer settings.
Advanced	Advanced settings such as maximum decoding threads, deinterlacing and time zone settings.
	Maximum decoding threads controls how many decoding threads are used to decode video streams. It can help improve performance on multi-core computers in live as well as playback mode. The exact performance improvement depends on the video stream. It is mainly relevant if using heavily coded high-resolution video streams like H.264/H.265, for which the performance improvement potential can be significant, and less relevant if using, for example, JPEG or MPEG-4.
	With **deinterlacing**, you convert video into a non-interlaced format. Interlacing determines how an image is refreshed on a screen. The image is refreshed by first scanning the odd lines in the image, then scanning the even lines. This allows a faster refresh rate because less information is processed during each scan. However, interlacing may cause flickering, or the changes in half of the image's lines may be noticeable.
Live	Availability of live tabs/panes, camera playback and overlay buttons, bounding boxes, and live-related MIP plug-ins.
Playback	Availability of playback tabs/panes, layout of print reports, independent playback, bounding boxes, and playback-related MIP plug-ins.
Setup	Availability of general setup/panes/buttons, setup-related MIP plug-in and rights to edit a map and to edit live video buffering.
Exports	Paths, privacy masks, video and still image formats and what to include when exporting these, export formats for Network Video Management System Smart Client – Player and much more.
Timeline	Whether to include audio or not, visibility of indication of time and motion, and finally how to handle playback gaps.

Matrix

About Matrix

With Matrix, you can send video from any camera on a network operating your system to Matrix-recipients. A Matrix recipient is a computer that can display Matrix-triggered video. There are two kinds of Matrix recipients:

- computers running a dedicated Matrix application and

- computers running Network Video Management System Smart Client.

To see a list of Matrix recipients configured in the Management Client, expand **Client** in the **Site Navigation** pane, then select **Matrix**. A list of Matrix configurations is displayed in the **Properties** pane.

Each Matrix recipient, regardless whether it is a computer with the Matrix Monitor or the Network Video Management System Smart Client, must be configured to receive Matrix-triggered video. See the Matrix Monitor and Network Video Management System Smart Client documentation for more information.

Add Matrix recipients

To add an existing Matrix recipient, for example an existing Matrix Monitor or Network Video Management System Smart Client installation, through the Management Client:

1. Expand **Clients**, then select **Matrix**.

2. Right-click **Matrix Configurations** and select **Add Matrix**.

3. Fill out the fields in the **Add Matrix** dialog box.

4. In the **Address** field enter the IP address or the host name of the required Matrix recipient.

5. In the **Port** field enter the port number used by the Matrix recipient installation. You can find the port number and password in this way: For a Matrix Monitor application, go to the Matrix Monitor **Configuration** dialog box. For Network Video Management System Smart Client, see the Network Video Management System Smart Client documentation.

6. Click **OK**.

You can now use the Matrix recipient in rules.

Note: Your system does not verify that the specified port number or password is correct or that the specified port number, password, or type corresponds with the actual Matrix recipient. Make sure that you enter the correct information.

Define rules sending video to Matrix-recipients

To send video to Matrix-recipients you must include the Matrix recipient in a rule that triggers the video transmission to the related Matrix-recipient. To do so:

1. In the **Site Navigation** pane, Expand **Rules and Events** > **Rules**. Right-click **Rules** to open the **Manage Rule** wizard. In the first step, select a rule type and in the second step, a condition.

2. In **Manage Rule**'s step 3 (**Step 3: Actions**) select the **Set Matrix to view <devices>** action.

3. Click the Matrix link in the initial rule description.

4. In the **Select Matrix Configuration** dialog box, select the relevant Matrix-recipient, and click **OK**.

5. Click the **devices** link in the initial rule description, and select from which cameras you would like to send video to the Matrix-recipient, then click **OK** to confirm your selection.

6. Click **Finish** if the rule is complete or define if required additional actions and/or a stop action.

If you delete a Matrix-recipient, any rule that includes the Matrix-recipient stops working.

Send the same video to several Network Video Management System Smart Client views

If the Matrix-recipient is Network Video Management System Smart Client, you can send the same video to Matrix positions in several of Network Video Management System Smart Client's views, provided the views' Matrix positions share the same port number and password:

1. In Network Video Management System Smart Client, create the relevant views and Matrix positions that share the same port number and password.

2. In the Management Client, add the relevant Network Video Management System Smart Client as a Matrix-recipient.

3. You may include the Matrix-recipient in a rule.

Rules and events

About rules and events

Rules are a central element in your system. Rules determine highly important settings, such as when cameras should record, when PTZ cameras should patrol, when notifications should be sent, etc.

Example: A rule specifying that a particular camera should begin recording when it detects motion.

Events are central elements when using the **Manage Rule** wizard. In the wizard, events are primarily used for triggering actions. For example, you can create a rule which specifies that in the **event** of detected motion, the surveillance system should take the **action** of starting recording of video from a particular camera.

Two types of conditions can trigger rules:

| Name	Description
Events	When events occur on the surveillance system, for example when motion is detected, when the system receives input from external sensors.
Time	When you enter specific periods of time, for example: `Thursday 16th August 2007 from 07.00 to 07.59` or `every Saturday and Sunday.`

You can work with the following under **Rules and Events**:

- **Rules:** Rules are a central element in the system. The behavior of your surveillance system is to a very large extent determined by rules. When creating a rule, you can work with all types of events.

- **Time profiles:** Time profiles are periods of time defined in the Management Client. You use them when you create rules in the Management Client, for example to create a rule which specifies that a certain action should take place within a certain time profile.

- **Notification profiles:** You can use notification profiles to set up ready-made email notifications, which can automatically be triggered by a rule, for example when a particular event occurs.

- **User-defined events:** User-defined events are custom-made events that makes it possible for users to manually trigger events in the system or react to inputs from the system.

- **Analytics events**: Analytics events are data received from an external third-party video content analysis (VCA) providers. You can use analytics events as basis for alarms.

- **Generic events:** Generic events allow you to trigger actions in the Network Video Management System event server by sending simple strings via the IP network to your system.

See Events overview (on page 137) for a list of events.

About actions and stop actions

When you add rules (see "Add a rule" on page 146) in the **Manage Rule** wizard, you can select between different actions:
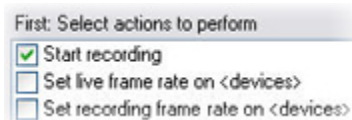
Example: Selecting actions

Some of the actions require a stop action. **Example**: If you select the action **Start recording**, recording starts and potentially continues indefinitely. As a result, the action **Start recording** has a mandatory stop action called **Stop recording**.

The **Manage Rule** wizard makes sure you specify stop actions when necessary:
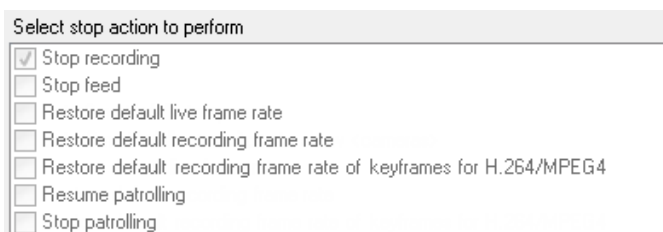
Selecting stop actions. In the example, note the mandatory stop action (selected, dimmed), the non-relevant stop actions (dimmed) and the optional stop actions (selectable).

Each type of action from your Network Video Management System is described. You may have more actions available if your system installation uses add-on products or vendor-specific plug-ins. For each type of action, stop action information is listed if relevant:

Action	Description
Start recording on <devices>	Start recording and saving data in the database from the selected devices.
	When your select this type of action, the **Manage Rule** wizard prompts you to specify:
	When recording should start. This happens either immediately or a number of seconds before the triggering event/beginning of the triggering time interval and on which devices the action should take place.
	This type of action requires that you have enabled recording on the devices to which the action are linked. You can only save data from before an event or time interval if you have enabled pre-buffering for the relevant devices. You enable recording and specify pre-buffering settings for a device on the **Record** tab.
	Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Stop recording**.
	Without this stop action, recording would potentially continue indefinitely. You also have the option of specifying further stop actions.
Start feed on <devices>	Begin data feed from devices to the system. When the feed from a device is started, data is transferred from the device to the system, in which case you may view and record, depending on the data type.
	When you select this type of action, the **Manage Rule** wizard prompts you to specify on which devices to start the feeds. Your system includes a default rule which ensures that feeds are always started on all cameras.
	Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Stop feed**.
	You can also specify further stop actions.
	Note that using the mandatory stop action **Stop feed** to stop the feed from a device means that data is no longer transferred from the device to the system, in which case live viewing and recording of video, for example, is no longer possible. However, a device on which you have stopped the feed can still communicate with the recording server, and you can start the feed again automatically through a rule, as opposed to when you manually have disabled the device.
	Important: While this type of action enables access to selected devices' data feeds, it does not guarantee that data is recorded, as you must specify recording settings separately.
Set <Smart Wall> to <preset>	Sets the Network Video Management System Smart Wall to a selected preset. Specify the preset on the **Smart Wall Presets** tab.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Set <Smart Wall> <monitor> to show cameras	Sets a specific Network Video Management System Smart Wall monitor to display live video from the selected cameras on this site.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.

Action	Description
Set <Smart Wall> <monitor> to show text <messages>	Sets a specific Network Video Management System Smart Wall monitor to display a user-defined text message of up to 200 characters. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Remove cameras from <Smart Wall> monitor <monitor>	Stop displaying video from a specific camera. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Set live frame rate on <devices>	Sets a particular frame rate to use when the system displays live video from the selected cameras that substitutes the cameras' default frame rate. Specify this on the **Settings** tab. When you select this type of action, the **Manage Rule** wizard prompts you to specify which frame rate to set, and on which devices. Always verify that the frame rate you specify is available on the relevant cameras. **Stop action required**: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Restore default live frame rate**. Without this stop action, the default frame rate would potentially never be restored. You also have the option of specifying further stop actions.
Set recording frame rate on <devices>	Sets a particular frame rate to use when the system saves recorded video from the selected cameras in the database, instead of the cameras' default recording frame rate. When you select this type of action, the **Manage Rule** wizard prompts you to specify which recording frame rate to set, and on which cameras. You can only specify a recording frame rate for JPEG, a video codec with which each frame is separately compressed into a JPEG image. This type of action also requires that you have enabled recording on the cameras to which the action is linked. You enable recording for a camera on the **Record** tab. The maximum frame rate you can specify depends on the relevant camera types, and on their selected image resolution. **Stop action required**: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Restore default recording frame rate**. Without this stop action, the default recording frame rate would potentially never be restored. You also have the option of specifying further stop actions.
Set recording frame rate to all frames for MPEG4/H.264/H.265 on <devices>	Sets the frame rate to record all frames when the system saves recorded video from the selected cameras in the database, instead of keyframes only. Enable the recording keyframes only function on the **Record** tab. When you select this type of action, the **Manage Rule** wizard prompts you to select which devices the action should apply for. You can only enable keyframe recording for H.264/H.265 and MPEG4. This type of action also requires that you have enabled recording on the cameras to which the action is linked. You enable recording for a camera on the **Record** tab.

Action	Description
	Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Restore default recording frame rate of keyframes for MPEG4/H.264/H.265** Without this stop action, the default setting would potentially never be restored. You also have the option of specifying further stop actions.
Start patrolling on <device> using <profile> with PTZ priority <priority>	Begins PTZ patrolling according to a particular patrolling profile for a particular PTZ camera with a particular priority. This is an exact definition of how patrolling should be carried out, including the sequence of preset positions, timing settings, and more. When you select this type of action, the **Manage Rule** wizard prompts you to select a patrolling profile. You can only select one patrolling profile on one device and you cannot select several patrolling profiles. This type of action requires that the devices to which the action is linked are PTZ devices. You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the **Patrolling** tab. **Stop action required**: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Stop patrolling** Without this stop action, patrolling would potentially never stop. You can also specify further stop actions.
Pause patrolling on <devices>	Pauses PTZ patrolling. When you select this type of action, the **Manage Rule** wizard prompts you to specify the devices on which to pause patrolling. This type of action requires that the devices to which the action is linked are PTZ devices. You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the **Patrolling** tab. **Stop action required**: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: **Resume patrolling** Without this stop action, patrolling would potentially pause indefinitely. You have also the option of specifying further stop actions.
Move <device> to <preset> position with PTZ priority <priority>	Moves a particular camera to a particular preset position - however always according to priority. When selecting this type of action, the **Manage Rule** wizard prompts you to select a preset position. Only one preset position on one camera can be selected. It is not possible to select several preset positions. This type of action requires that the devices to which the action is linked are PTZ devices. This action requires that you have defined at least one preset position for those devices. You define preset positions for a PTZ camera on the **Presets**

Action	Description
	tab.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Move to default preset on \<devices\> with PTZ priority \<priority\>	Moves one or more particular cameras to their respective default preset positions - however always according to priority. When you select this type of action, the **Manage Rule** wizard prompts you to select which devices the action should apply for.
	This type of action requires that the devices to which the action is linked are PTZ devices. This action requires that you have defined at least one preset position for those devices. You define preset positions for a PTZ camera on the **Presets** tab.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Set device output to \<state\>	Sets an output on a device to a particular state (activated or deactivated). When you select this type of action, the **Manage Rule** wizard prompts you to specify which state to set, and on which devices.
	This type of action requires that the devices to which the action is linked each have at least one external output unit connected to an output port.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Send notification to \<profile\>	Sends a notification, using a particular notification profile. When you select this type of action, the **Manage Rule** wizard prompts you to select a notification profile, and which devices to include pre-alarm images from. You can only select one notification profile and you cannot select several notification profiles. Note that a single notification profile may contain several recipients.
	You can also create more rules to the same event and send different notifications to each of the notification profiles. You can copy and re-use the content of rules by right-clicking a rule in the **Rules** list.
	This type of action requires that you have defined at least one notification profile. Pre-alarm images are only included if you have enabled the **Include images** option for the relevant notification profile.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Make new \<log entry\>	Generates an entry in the rule log. When selecting this type of action, the **Manage Rule** wizard prompts you to specify a text for the log entry. When you specify the log text, you can insert variables, such as **$DeviceName$**, **$EventName$**, into the log message.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.

Action	Description
Start plug-in on <devices>	Starts one or more plug-ins. When you select this type of action, the **Manage Rule** wizard prompts you to select required plug-ins, and on which devices to start the plug-ins.
	This type of action requires that you have at least one or more plug-ins installed on your system.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Stop plug-in on <devices>	Stops one or more plug-ins. When you select this type of action, the **Manage Rule** wizard prompts you to select required plug-ins, and on which devices to stop the plug-ins.
	This type of action requires that you have at least one or more plug-ins installed on your system.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Apply new settings on <devices>	Changes device settings on one or more devices. When you select this type of action, the **Manage Rule** wizard prompts you to select relevant devices, and you can define the relevant settings on the devices you have specified.
	If you define settings for more than one device, you can only change settings that are available for all of the specified devices.
	Example: You specify that the action should be linked to Device 1 and Device 2. Device 1 has the settings A, B and C, and Device 2 has the settings B, C and D. In this case, you can only change the settings that are available for both devices, namely settings B and C.
	No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Set Matrix to view <devices>	Makes video from the selected cameras appear on a computer capable of displaying Matrix-triggered video such as a computer on which you have installed either Network Video Management System Smart Client or the Matrix Monitor application.
	When you select this type of action, the **Manage Rule** wizard prompts you to select a Matrix recipient, and one or more devices from which to display video on the selected Matrix recipient.
	This type of action allows you to select only a single Matrix recipient at a time. If you want to make video from the selected devices appear on more than one Matrix recipient, you should create a rule for each required Matrix recipient or use the Network Video Management System Smart Wall feature. By right-clicking a rule in the **Rules** list, you can copy and re-use the content of rules. This way, you can avoid having to create near-identical rules from scratch.
	As part of the configuration on the Matrix recipients themselves, users must specify the port number and password required for the Matrix communication. Make sure that the users have access to this information. The users must typically also define the IP addresses of allowed hosts from which commands regarding display of Matrix-triggered video is accepted. In that case, the users must also know the IP address of

Action	Description
	the management server, or any router or firewall used.
Send SNMP trap	Generates a small message which logs events on selected devices. The text of SNMP traps are auto-generated and cannot be customized. It can contain the source type and name of the device on which the event occurred. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Retrieve and store remote recordings from <devices>	Retrieves and stores remote recordings from selected devices (that support edge recording) in a specified period before and after the triggering event. Note that this rule is independent of the **Automatically retrieve remote recordings when connection is restored** setting. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Retrieve and store remote recordings between <start and end time> from <devices>	Retrieves and stores remote recordings in a specified period from selected devices (that support edge recording). Note that this rule is independent of the **Automatically retrieve remote recordings when connection is restored** setting. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Save attached image	Ensures that when an image is received from the Images Received event (sent via SMTP email from a camera), it is saved for future usage. In future, other events can possibly also trigger this action. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Activate archiving on <archives>	Starts archiving. When you select this type of action, the **Manage Rule** wizard prompts you to select relevant archives. **No mandatory stop action**: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.

Events overview

When you add an event-based rule in the **Manage Rule** wizard, you can select between a number of different event types. In order for you to get a good overview, events you can select are listed in groups according to whether they are:

Hardware:

Some hardware is capable of creating events themselves, for example to detect motion. You can use these as events but you must configure them on the hardware before you can use them in the

system. You may only be able to use the events listed on some hardware as not all types of cameras can detect tampering or temperature changes.

Hardware - Configurable events:

Configurable events from hardware are automatically imported from device drivers. This means that they vary from hardware to hardware and are not documented here. Configurable events are not triggered until you have added them to the system and configured them on the **Event** tab for hardware. Some of the configurable events also require that you configure the camera (hardware) itself.

Hardware - Predefined events:

Event	Description
Communication Error (Hardware)	Occurs when a connection to the hardware is lost.
Communication Started (Hardware)	Occurs when communication with the hardware is successfully established.
Communication Stopped (Hardware)	Occurs when communication with the hardware is successfully stopped.

Devices - Configurable events:

Configurable events from devices are automatically imported from device drivers. This means that they vary from device to device and are not documented here. Configurable events are not triggered until you have added them to the system and configured them on the **Event** tab on a device.

Devices - Predefined events:

Event	Description
Communication Error (Device)	Occurs when a connection to a device is lost, or when an attempt is made to communicate with a device, and the attempt is unsuccessful.
Communication Started (Device)	Occurs when communication with a device is successfully established.
Communication Stopped (Device)	Occurs when communication with a device is successfully stopped.

Event	Description
Feed Overflow Started	Feed overflow (media overflow) occurs when a recording server cannot process received data as quickly as specified in the configuration and therefore is forced to discard some recordings. If the server is healthy, feed overflow usually happens because of slow disk writes. You can resolve this either by reducing the amount of data written, or by improving the storage system's performance. Reduce the amount of written data by reducing frame rates, resolution or image quality on your cameras, but this may degrade recording quality. If you are not interested in that, instead improve your storage system's performance by installing extra drives to share the load or by installing faster disks or controllers. You can use this event to trigger actions that helps you avoid the problem, for example, to lower the recording frame rate.
Feed Overflow Stopped	Occurs when feed overflow (see description of the **Feed Overflow Started** event) ends.
Live Client Feed Requested	Occurs when client users request a live stream from a device. The event occurs upon the request even if the client user's request later turns out to be unsuccessful, for example because the client user does not have the rights required for viewing the requested live feed or because the feed is for some reason stopped.
Live Client Feed Terminated	Occurs when client users no longer request a live stream from a device.
Manual Recording Started	Occurs when a client user starts a recording session for a camera. The event is triggered even if the device already is being recorded via rule actions.
Manual Recording Stopped	Occurs when a client user stops a recording session for a camera. If the rule system also have started a recording session it continues recording even after the manual recording is stopped.
Motion Started	Occurs when the system detects motion in video received from cameras. This type of event requires that the system's motion detection is enabled for the cameras to which the event is linked. In addition to the system's motion detection, some cameras can detect motion themselves and trigger the **Motion Started (HW)** event, but it depends on the configuration of the camera hardware and in the system. See **Hardware - Configurable events** above.

Event	Description
Motion Stopped	Occurs when motion is no longer detected in received video. See also the description of the **Motion Started** event. This type of event requires that the system's motion detection is enabled for the cameras to which the event is linked. In addition to the system's motion detection, some cameras can detect motion themselves and trigger the Motion Stopped (HW) event, but it depends on the configuration of the camera hardware and in the system. See **Hardware - Configurable events** above.
Output Activated	Occurs when an external output port on a device is activated. This type of event requires that at least one device on your system supports output ports.
Output Changed	Occurs when the state of an external output port on a device is changed. This type of event requires that at least one device on your system supports output ports.
Output Deactivated	Occurs when an external output port on a device is deactivated. This type of event requires that at least one device on your system supports output ports.
PTZ Manual Session Started	Occurs when a manually operated PTZ session (as opposed to a PTZ session based on scheduled patrolling or automatically triggered by an event) is started on a camera. This type of event requires that the cameras to which the event is linked are PTZ cameras.
PTZ Manual Session Stopped	Occurs when a manually operated PTZ session (as opposed to a PTZ session based on scheduled patrolling or automatically triggered by an event) is stopped on a camera. This type of event requires that the cameras to which the event is linked are PTZ cameras.
Recording Started	Occurs whenever recording is started. There is a separate event for manual recording started.
Recording Stopped	Occurs whenever recording is stopped. There is a separate event for manual recording stopped.
Settings Changed	Occurs when settings on a device are successfully changed.
Settings Changed Error	Occurs when an attempt is made to change settings on a device, and the attempt is unsuccessful.

External events - Predefined events:

Event	Description
Request Start Recording	Activated when start recordings are requested via the MIP Software Development Kit (SDK). Through the MIP SDK a third party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) for your system.
Request Stop Recording	Activated when stop recordings are requested via the MIP SDK. Through the MIP SDK a third party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) for your system.

External events - Generic events:

Generic events allow you to trigger actions in the system by sending simple strings via the IP network to the system. The purpose of generic events is to allow as many external sources as possible to interact with the system.

External events - User-defined events:

A number of events custom made to suit your system may also be selectable. You can use such user-defined events for:

- Making it possible for client users to manually trigger events while viewing live video in the clients.

- Countless other purposes. For example, you may create user-defined events which occur if a particular type of data is received from a device.

  See About user-defined events (on page 155) for more information.

Recording servers:

Event	Description
Archive Available	Occurs when an archive for a recording server becomes available after having been unavailable (see **Archive Unavailable**).
Archive Unavailable	Occurs when an archive for a recording server becomes unavailable, for example if the connection to an archive located on a network drive is lost. In such cases, you cannot archive recordings. You can use the event to, for example, trigger an alarm or a notification profile so that an email notification is automatically sent to relevant people in your organization.
Archive Not Finished	Occurs when an archive for a recording server is not finished with the last archiving round when the next is scheduled to start.

Event	Description
Database Disk Full	Occurs when a database disk is full. A database disk is considered to be full when there is less than 5GB of space is left on the disk: The oldest data in a database is always auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data is deleted even if a next archive is defined. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data is written to the database until enough space has been freed. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.
Database Full - Auto Archive	Occurs when an archive for a recording server is full and needs to auto-archive to an archive in the storage.
Database Repair	Occurs if a database becomes corrupted, in which case the system automatically attempts two different database repair methods: a fast repair and a thorough repair.
Database Storage Available	Occurs when a storage for a recording server becomes available after having been unavailable (see **Database Storage Unavailable**). You can, for example, use the event to start recording if it has been stopped by a **Database Storage Unavailable** event.
Database Storage Unavailable	Occurs when a storage for a recording server becomes unavailable, for example if the connection to a storage located on a network drive is lost. In such cases, you cannot archive recordings. You can use the event to, for example, stop recording, trigger an alarm or a notification profile so an e-mail notification is automatically sent to relevant people in your organization.

Events from add-on products and integrations:

Events from add-on products and integrations can be used in the rule system, for example:

- Analytics events can also be used in the rule system.

Rules

About rules

Rules specify actions to carry out under particular conditions. Example: When motion is detected (condition), a camera should begin recording (action).

The following are **examples** of what you can do with rules:

- Start and stop recording

- Set non-default live frame rate

- Set non-default recording frame rate

- Start and stop PTZ patrolling

- Pause and resume PTZ patrolling

- Move PTZ cameras to specific positions

- Set output to activated/deactivated state

- Send notifications via e-mail

- Generate log entries

- Generate events

- Apply new device settings, for example a different resolution on a camera

- Make video appear in Matrix recipients

- Start and stop plug-ins

- Start and stop feeds from devices

Stopping a device means that video is no longer transferred from the device to the system, in which case you cannot view live video nor record video. In contrast, a device on which you have stopped the feed can still communicate with the recording server, and you can start the feed from the device automatically through a rule, as opposed to when the device is manually disabled in the Management Client.

Important: Some rule content may require that certain features are enabled for the relevant devices. For example, a rule specifying that a camera should record does not work as intended if recording is not enabled for the relevant camera. Before creating a rule, Sony recommends that you verify that the devices involved can perform as intended.

About default rules

Your system includes a number of default rules that you can use basic features without needing to set anything up. You can deactivate or modify the default rules as you need. If you modify or deactivate the default rules, your system may not work as desired nor guarantee that video feeds or audio feeds are automatically fed to the system.

Default rule	Description
Goto Preset when PTZ is done	Ensures that PTZ cameras go to their respective default preset positions after you have operated them manually. This rule is not enabled by default.
	Even when you have enabled the rule, you must have defined default preset positions for the relevant PTZ cameras in order for the rule to work. You do this on the **Presets** tab.
Record on Motion	Ensures that as long as motion is detected in video from cameras, the video is recorded, provided recording is enabled for the relevant cameras. Recording is by default enabled.
	While the default rule specifies recording based on detected motion, it does not guarantee that the system records video, as you may have disabled individual cameras' recording for one or more cameras. Even when you have enabled recording, remember that the quality of recordings may be affected by individual camera's recording settings.

Default rule	Description
Record on Request	Ensures that video is recorded automatically when an external request occurs, provided recording is enabled for the relevant cameras. Recording is enabled by default.
	The request is always triggered by a system integrating externally with your system, and the rule is primarily used by integrators of external systems or plug-ins.
Start Audio Feed	Ensures that audio feeds from all connected microphones and speakers are automatically fed to the system.
	While the default rule enables access to connected microphones' and speakers' audio feeds immediately upon installing the system, it does not guarantee that audio is recorded, as you must specify recording settings separately.
Start Feed	Ensures that video feeds from all connected cameras are automatically fed to the system.
	While the default rule enables access to connected cameras' video feeds immediately upon installing the system, it does not guarantee that video is recorded, as cameras' recording settings must be specified separately.
Start Metadata Feed	Ensures that data feeds from all connected cameras are automatically fed to the system.
	While the default rule enables access to connected cameras' data feeds immediately upon installing the system, it does not guarantee that data is recorded, as cameras' recording settings must be specified separately.

Recreate default rules

If you accidentally delete any of the default rules, you can recreate them by typing the following content:

Default rule	Text to type
Goto preset when PTZ is done	Perform an action on PTZ Manual Session Stopped from All Cameras
	Move immediately to default preset on the device on which event occurred
Record on Motion	Perform an action on Motion Started from All Cameras start recording three seconds before on the device on which event occurred
	Perform stop action on Motion Stopped from All Cameras stop recording three seconds after
Record on Request	Perform an action on Request Start Recording from External start recording immediately on the devices from metadata
	Perform stop action on Request Stop Recording from External stop recording immediately

Default rule	Text to type
Start Audio Feed	Perform an action in a time interval always start feed on All Microphones, All Speakers Perform an action when time interval ends stop feed immediately
Start Feed	Perform an action in a time interval always start feed on All Cameras Perform an action when time interval ends stop feed immediately
Start Metadata Feed	Perform an action in a time interval always start feed on All Metadata Perform an action when time interval ends stop feed immediately

About validating rules

You can validate the content of an individual rule or all rules in one go. When you create a rule, the **Manage Rule** wizard ensures that all of the rule's elements make sense. When a rule has existed for some time, one or more of the rule's elements may have been affected by other configuration, and the rule may no longer work. For example, if a rule is triggered by a particular time profile, the rule does not work if you have deleted that time profile or if you no longer have permissions to it. Such unintended effects of configuration may be hard to keep an overview of.

Rule validation helps you keep track of which rules have been affected. Validation takes place on a per-rule basis and each rule is validated by themselves. You cannot validate rules against each other, for example in order to see whether one rule conflicts with another rule, not even if you use the **Validate All Rules** feature.

Note that you cannot validate whether configuration of prerequisites outside the rule itself may prevent the rule from working. For example, a rule specifying that recording should take place when motion is detected by a particular camera validates OK if the elements in the rule itself are correct, even if motion detection, which is enabled on a camera level, not through rules, has not been enabled for the relevant camera.

You validate an individual rule or all rules in one go by right-clicking the rule you want to validate and select **Validate Rule** or **Validate All Rules**. A dialog box informs you whether the rule(s) validated successfully or not. If you chose to validated more than one rule and one or more rules did not succeed, the dialog box lists the names of the affected rules.

About rule complexity

You exact number of options depends on the type of rule you want to create, and on the number of devices available on your system. Rules provide a high degree of flexibility: you can combine event and time conditions, specify several actions in a single rule, and very often create rules covering several or all of the devices on your system.

You can make your rules as simple or complex as required. For example, you can create very simple time-based rules:

Example	Explanation
Very Simple Time-Based Rule	On Mondays between 08.30 and 11.30 (time condition), Camera 1 and Camera 2 should start recording (action) when the time period begins and stop recording (stop action) when the time period ends.
Very Simple Event-Based Rule	When motion is detected (event condition) on Camera 1, Camera 1 should start recording (action) immediately, then stop recording (stop action) after 10 seconds. Even if an event-based rule is activated by an event on one device, you can specify that actions should take place on one or more other devices.
Rule Involving Several Devices	When motion is detected (event condition) on Camera 1, Camera 2 should start recording (action) immediately, and the siren connected to Output 3 should sound (action) immediately. Then, after 60 seconds, Camera 2 should stop recording (stop action), and the siren connected to Output 3 should stop sounding (stop action).
Rule Combining Time, Events, and Devices	When motion is detected (event condition) on Camera 1, and the day of the week is Saturday or Sunday (time condition), Camera 1 and Camera 2 should start recording (action) immediately, and a notification should be sent to the security manager (action). Then, 5 seconds after motion is no longer detected on Camera 1 or Camera 2, the 2 cameras should stop recording (stop action).

Depending on your organization's needs, it is often a good idea to create many simple rules rather than a few complex rules. Even if it means you have more rules in your system, it provides an easy way to maintain an overview of what your rules do. Keeping your rules simple also means that you have much more flexibility when it comes to deactivating/activating individual rule elements. With simple rules, you can deactivate/activate entire rules when required.
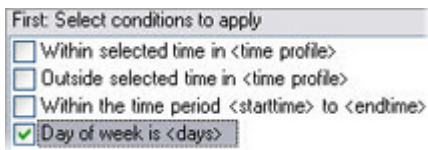
Add a rule

When you create rules, you are guided by the wizard **Manage Rule** which only lists relevant options.

It ensures that a rule does not contain missing elements. Based on your rule's content, it automatically suggests suitable stop actions, that is what should take place when the rule no longer applies, ensuring that you do not unintentionally create a never-ending rule.

1. Right-click the **Rules** item > **Add Rule**. This opens the **Manage Rule** wizard. The wizard guides you through specifying the content of your rule.

2. Specifying a name and a description of the new rule in the **Name** and **Description** fields respectively.

3. Select the relevant type of condition for the rule: either a rule which performs one or more actions when a particular event occurs, or a rule which performs one or more actions when you enter a specific period of time.

4. Click **Next** to go to the wizard's second step. On the wizard's second step, define further conditions for the rule.

5. Select one or more conditions, for example **Day of week is <day>**:

Example only. Your selections may be different

Depending on your selections, edit the rule description in the lower part of the wizard window:

Example only. Your selections may be different

Click the underlined items in **bold italics** to specify their exact content. For example, clicking the **days** link in our example lets you select one or more days of the week on which the rule should apply.

6. Having specified your exact conditions, click **Next** to move to the next step of the wizard and select which actions the rule should cover. Depending on the content and complexity of your rule, you may need to define more steps, such as stop events and stop actions. For example, if a rule specifies that a device should perform a particular action during a time interval (for example, Thursday between 08.00 and 10.30), the wizard may ask you to specify what should happen when that time interval ends.

7. Your rule is by default active once you have created it if the rule's conditions are met. If you do not want the rule to be active straight away, clear the **Active** check box.

8. Click **Finish**.

Edit, copy and rename a rule

1. In the **Overview** pane, right-click the relevant rule.

2. Select either:

   Edit Rule or **Copy Rule** or **Rename Rule**. The wizard **Manage Rule** opens.

3. In the wizard, rename and/or change the rule. If you selected **Copy Rule**, the wizard opens, displaying a copy of the selected rule.

4. Click **Finish**.

Deactivate and activate a rule

Your system applies a rule as soon as the rule's conditions apply which means it is active. If you do not want a rule to be active, you can deactivate the rule. When you deactivate the rule, the system does not apply the rule even if the rule's conditions apply. You can easily activate a deactivated rule later.

Deactivating a rule

1. In the **Overview** pane, select the rule.

2. Clear the **Active** check box in the **Properties** pane.

3. Click **Save** in the toolbar.

4. An icon with a red x indicates that the rule is deactivated in the **Rules** list:

Example: The added x on the icon indicates that the third rule is deactivated

Activating a rule

When you want to activate the rule again, select the rule, select the **Activate** check box, and save the setting.
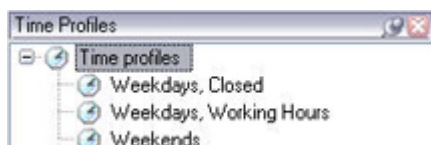
Time profiles

About time profiles

Time profiles are periods of time defined by the administrator. You can use time profiles when creating rules, for example, a rule specifying that a certain action should take place within a certain time period.

Time profiles are also assigned to roles, along with Smart Client profiles. By default, all roles are assigned the default time profile **Always**. This means that members of roles with this default time profile attached has no time-based limits to their user rights in the system. You can also assign an alternative time profile to a role.

Time profiles are highly flexible: you can base them on one or more single periods of time, on one or more recurring periods of time, or a combination of single and recurring times. Many users may be familiar with the concepts of single and recurring time periods from calendar applications, such as the one in Microsoft® Outlook.

Time profiles always apply in local time. This means that if your system has recording servers placed in different time zones, any actions, for example recording on cameras, associated with time profiles are carried out in each recording server's local time. Example: If you have a time profile covering the period from 08.30 to 09.30, any associated actions on a recording server placed in New York is carried out when the local time is 08.30 to 09.30 in New York, while the same actions on a recording server placed in Los Angeles is carried out some hours later, when the local time is 08.30 to 09.30 in Los Angeles.

You create and manage time profiles by expanding **Rules and Events** > **Time Profiles**. A **Time Profiles** list opens:

Example only

For an alternative to time profiles, see Day length time profiles (see "About day length time profiles" on page 151).

Specify a time profile

1. In the **Time Profiles** list, right-click **Time Profiles** > **Add Time Profile**. This opens the **Time Profile** window.

2. In the **Time Profile** window, type a name for the new time profile in the **Name** field. Optionally, type a description of the new time profile in the **Description** field.

3. In the **Time Profile** window's calendar, select either **Day View**, **Week View** or **Month View**, then right-click inside the calendar and select either **Add Single Time** or **Add Recurrence Time**.

4. When you have specified the time periods for your time profile, click **OK** in the **Time Profile** window. Your system adds your new time profile to the **Time Profiles** list. If at a later stage you wish to edit or delete the time profile, you do that from the **Time Profiles** list as well.

Add a single time

When you select **Add Single Time**, the **Select Time** window appears:

Time and date format may be different on your system

1. In the **Select Time** window, specify **Start time** and **End time**. If the time is to cover whole days, select the **All day event** box.

2. Click **OK**.

Specify a recurring time

When you select **Add Recurring Time**, the **Select Recurring Time** window appears:
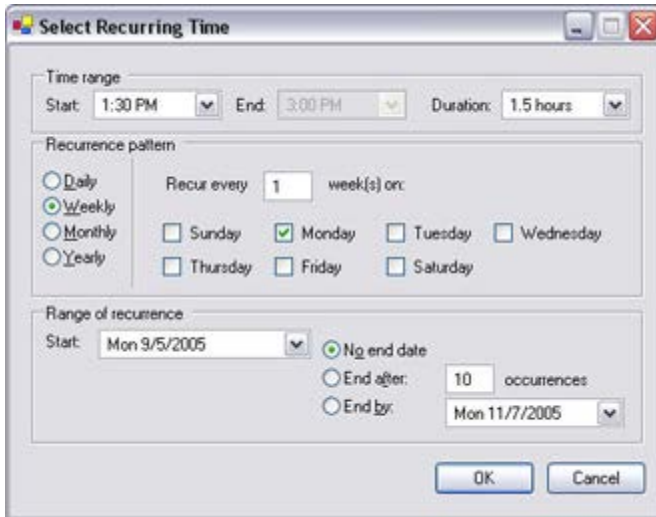
Time and date format may be different on your system

1. In the **Select Time** window, specify time range, recurrence pattern and range of recurrence.

2. Click **OK**.

A time profile can contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.

Edit a time profile

1. In the **Overview** pane's **Time Profiles** list, right-click the relevant time profile, and select **Edit Time Profile**. This opens the **Time Profile** window.

2. Edit the time profile as needed. If you have made changes to the time profile, click **OK** in the **Time Profile** window. You return to the **Time Profiles** list.

You browse months by clicking the small back/forward buttons.

Note: In the **Time Profile Information** window, you can edit the time profile as needed. Remember that a time profile may contain more than one time period, and that time periods may be recurring. The small month overview in the top right corner can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold.

In this example, the bold dates indicate that you have specified time periods on several days, and that you have specified a recurring time on Mondays.

About day length time profiles

When you place cameras outside, you must often lower the camera resolution, enable black/white or change other settings when it gets dark or when it gets light. The further north or south from the equator the cameras are placed, the more the sunrise and sunset time varies during the year. This makes it impossible to use normal fixed time profiles to adjusts camera settings according to light conditions.

In such situations, you can create day length time profiles instead to define the sunrise and sunset in a specified geographical area. Via GPS coordinates, the system calculates the sunrise and sunset time, even incorporating daylight saving time on a daily basis. As a result, the time profile automatically follows the yearly changes in sunrise/sunset in the selected area, ensuring the profile to be active only when needed. All times and dates are based on the management servers time and date settings. You can also set a positive or negative offset (in minutes) for the start (sunrise) and end time (sunset). The offset for the start and the end time can be identical or different.

You can use day length profiles both when you create rules and roles.

Create a day length time profile

1. Expand the **Rules and Events** folder > **Time Profiles**.

2. In the **Time Profiles** list, right-click **Time Profiles**, and select **Add Day Length Time Profile**.

3. In the **Day Length Time Profile** window, fill in the needed information. To deal with transition periods between lightness and darkness, you can offset activation and deactivation of the profile. The time and the name of months are shown in the language used your computer's language/regional settings.

4. To see the location of the entered GPS coordinates in a map, click **Show Position in Browser**. This opens a browser where you can see the location.

5. Click **OK**.

Day length time profile properties

Set the following properties for day length time profile:

Name	Description
Name	The name of the profile.
Description	A description of the profile (optional).
GPS coordinates	GPS coordinates indicating the physical location of the camera(s) assigned to the profile.
Sunrise offset	Number of minutes (+/-) by which activation of the profile is offset by sunrise.
Sunset offset	Number of minutes (+/-) by which deactivation of the profile is offset by sunset.
Time zone	Time zone indicating the physical location of the camera(s).

Notification profiles

About notification profiles

Notification profiles allow you to set up ready-made email notifications, which can automatically be triggered by a rule, for example when a particular event occurs. You can include still images and AVI video clips in the email notifications.

The system does not support TLS (Transport Layer Security) and its predecessor SSL (Secure Socket Layer). If the sender belongs on a server that requires TLS or SSL, email notifications do not work properly. Also, you may need to disable any email scanners that could prevent the application from sending the email notifications.

Prerequisites

Before you can create notification profiles, you must specify settings for the outgoing SMTP mail server for the email notifications.

If you want the email notifications to be able to include AVI movie clips, you must also specify the compression settings to use. To do so, go to **Tools** > **Options**. This opens the **Options** window. Specify the **Outgoing SMTP Mail Server** on the **Mail Server** tab and the compression settings on the **AVI Generation** tab.

Add notification profiles

1. Expand **Rules and Events**, right-click **Notification Profiles** > **Add Notification Profile**. This opens the **Add Notification Profile** wizard.

2. Specify name and description. Click **Next**.

3. Specify recipient, subject, message text and time between emails:

4. To send a test email notification to the specified recipients, click **Test E-mail**.

5. To include pre-alarm still images, select **Include images**, and specify number of images, time between images and whether to embed images in emails or not.

6. To include AVI video clips, select **Include AVI**, and specify the time before and after event and frame rate.

7. Click **Finish**.

Use rules to trigger email notifications

You use the **Manage Rule** for creating rules. The wizard takes you through all relevant steps. You specify the use of a notification profile during the step on which you specify the rule's actions.

When you select the action **Send notification to <profile>**, you can select the relevant notification profile and which cameras any recordings to include in the notification profile's email notifications should come from:

Send notification to '*profile*'
     images from *recording device*

Example only. In **Manage Rule**, you click the links to make your selections

Remember that you cannot include recordings in the notification profile's email notifications unless something is actually being recorded. If you want still images or AVI video clips in the email notifications, verify that the rule specifies that recording should take place. The following example is from a rule which includes both a **Start recording** action and a **Send notification to** action:

Next: Edit the rule description (click an underlined item)

Perform an action on Input Activated
     from Red Sector Door Sensor
start recording 5 seconds before on Red Sector Entrance Cam
     and Send notification to 'Security: Red Sector Entrance'
     images from Red Sector Entrance Cam

Perform action 10 seconds after
stop recording immediately

Notification profile (properties)

Specify the following properties for notification profiles:

Component	Requirement
Name	Type a descriptive name for the notification profile. The name appears later whenever you select the notification profile during the process of creating a rule.
Description (optional)	Type a description of the notification profile. The description appears when you pause your mouse pointer over the notification profile in the Overview pane's **Notification Profiles** list.
Recipients	Type the e-mail addresses to which the notification profile's e-mail notifications should be sent. To type more than one e-mail address, separate addresses with a semicolon. Example: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc

Component	Requirement
Subject	Type the text you want to appear as the subject of the e-mail notification. You can insert system variables, such as **Device name**, in the subject and message text field. To insert variables, click the required variable links in the box below the field.
Message text	Type the text you want to appear in the body of the e-mail notifications. In addition to the message text, the body of each e-mail notification automatically contains this information: • What triggered the e-mail notification. • The source of any attached still images or AVI video clips
Time between e-mails	Specify required minimum time (in seconds) to pass between the sending of each e-mail notification. Examples: • If specifying a value of **120**, a minimum of 2 minutes pass between the sending of each e-mail notification, even if the notification profile is triggered again by a rule before the 2 minutes have passed. • If specifying a value of **0**, e-mail notifications is sent each time the notification profile is triggered by a rule. This can potentially result in a very large number of e-mail notifications being sent. If using the value **0**, you should therefore carefully consider whether you want to use the notification profile in rules which are likely to be triggered frequently.
Number of images	Specify the maximum number of still images you want to include in each of the notification profile's e-mail notifications. Default is five images.
Time between images (ms)	Specify the number of milliseconds you want between the recordings presented on the included images. Example: With the default value of 500 milliseconds, the included images show recordings with half a second between them.
Time before event (sec.)	This setting is used to specify the start of the AVI file. By default, the AVI file contains recordings from 2 seconds before the notification profile is triggered. You can change this to the number of seconds you require.
Time after event (sec.)	This setting is used to specify the end of the AVI file. By default, the AVI file ends 4 seconds after the notification profile is triggered. You can change this to the number of seconds you require.
Frame rate	Specify the number of frames per second you want the AVI file to contain. Default is five frames per second. The higher the frame rate, the higher the image quality and AVI file size.
Embed images in e-mail	If selected (default), images are inserted in the body of e-mail notifications. If not, images are included in e-mail notifications as attached files.

User-defined events

About user-defined events

If the event you require is not on the **Events Overview** list, you can create your own user-defined events. Use such user-defined events to integrate other systems with your surveillance system.

With user-defined events, you can use data received from a third-party access control system as events in the system. The events can later trigger actions. This way, you can, for example, begin recording video from relevant cameras when somebody enters a building.

You can also use user-defined events for manually triggering events while viewing live video in Network Video Management System Smart Client or automatically if you use them in rules. For example, when user-defined event 37 occurs, PTZ camera 224 should stop patrolling and go to preset position 18.

Through roles, you define which of your users are able to trigger the user-defined events. You can use user-defined events in two ways and at the same time if required:

Events	Description
For providing the ability to manually trigger events in Network Video Management System Smart Client	In this case, user-defined events make it possible for end users to manually trigger events while viewing live video in Network Video Management System Smart Client. When a user-defined event occurs because a user of Network Video Management System Smart Client triggers it manually, a rule can trigger that one or more actions should take place on the system.
For providing the ability to trigger events through API	In this case, you can trigger user-defined events outside the surveillance system. Using user-defined events this way requires that a separate API (Application Program Interface. A set of building blocks for creating or customizing software applications) is used when triggering the user-defined event. Authentication through Active Directory is required for using user-defined events this way. This ensures that even if the user-defined events can be triggered from outside the surveillance system, only authorized users are to do it.

Also, user-defined events can via API be associated with meta-data, defining certain devices or device groups. This is highly usable when using user-defined events to trigger rules: you avoid having a rule for each device, basically doing the same thing. Example: A company uses access control, having 35 entrances, each with an access control device. When an access control device is activated, a user-defined event is triggered in the system. This user-defined event is used in a rule to start recording on a camera associated with the activated access control device. It is defined in the meta-data which camera is associated with what rule. This way the company does not need to have 35 user-defined events and 35 rules triggered by the user-defined events. A single user-defined event and a single rule are enough.

When you use user-defined events this way, you may not always want them to be available for manual triggering in Network Video Management System Smart Client. You can use roles to define which user-defined events should be visible in Network Video Management System Smart Client. |

No matter how you want to use user-defined events, you must add each user-defined event through the Management Client.

If you rename a user-defined event, already connected Network Video Management System Smart Client users must log out and log in again before the name change is visible.

Also note that if you delete a user-defined event, this affects any rules in which the user-defined event is in use. Also, a deleted user-defined event only disappears from Network Video Management System Smart Client when the Network Video Management System Smart Client users log out.

Add a user-defined event

1. Expand **Rules and Events** > **User-defined Events**.

2. In the **Overview** pane, right-click **Events** > **Add User-defined Event**.

3. Type a name for the new user-defined event, and click **OK**. The newly added user-defined event now appears in the list in the **Overview** pane.

4. The user can now trigger the user-defined event manually in Network Video Management System Smart Client if the user has rights to do so.

Rename a user-defined event

1. Expand **Rules and Events** > **User-defined Events**.

2. In the **Overview** pane, select the user-defined event.

3. In the **Properties** pane, overwrite the existing name.

4. In the toolbar, click **Save**.

Analytics events

About analytics events

Analytics events are typically data received from an external third-party video content analysis (VCA) providers.

Using analytics events as basis for alarms is basically a three step process:

-   Part one, enabling the analytics events feature and setting up its security. Use a list of allowed addresses to control who can send event data to the system and which port the server listens on.

-   Part two, creating the analytics event, possibly with a description of the event, and testing it.

-   Part three, using the analytics event as the source of an alarm definition.

You set up analytics events on the **Rules and Events** list in the **Site Navigation** pane.

To use VCA-based events, a third-party VCA tool is required for supplying data to the system. Which VCA tool to use is entirely up to you, as long as the data supplied by the tool adheres to the format.   Contact your system provider for more details. Third-party VCA tools are developed by

independent partners delivering solutions based on a Sony open platform. These solutions can impact performance on the system.

Add and edit an analytics event

Add an analytics event

1. Expand **Rules and Events**, right-click **Analytics Events** and select **Add New**.

2. In the **Properties** window, type a name for the event in the **Name** field.

3. Type a description text in the **Description** field if needed.

4. In the toolbar, click **Save**. You can test the validity of the event by clicking **Test Event**. You can continually correct errors indicated in the test and run the test as many times as you want and from anywhere in the process.

Edit an analytics event

1. Click an existing analytics event to view the **Properties** window, where you can edit relevant fields.

2. You can test the validity of the event by clicking **Test Event**. You can continually correct errors indicated in the test and run the test as many times as you want and from anywhere in the process.

Test an analytics event

After you create an analytics event, you can test the requirements (see "Test Analytics Event (properties)" on page 157), for example that the analytics events feature has been enabled in Management Client.

1. Select an existing analytics event.

2. In the properties, click the **Test Event** button. A window appears that shows all the possible sources of events.
Select the source of your test event, for example a camera. The window is closed and a new window appears that goes through four conditions that must be fulfilled for the analytics event to work.

As an additional test, in Network Video Management System Smart Client you can verify that the analytics event was sent to the event server. To do this, open Network Video Management System Smart Client and view the event in the **Alarm Manager** tab.

See also

About analytics events (on page 156)

Test Analytics Event (properties)

When you test the requirements of an analytics event, a window appears that checks four conditions and provides possible error descriptions and solutions.

Condition	Description	Error messages and solutions
Changes saved	If the event is new, is it saved? Or if there are changes to the event name, are these changes saved?	**Save changes before testing analytics event.** Solution/Explanation: Save changes.
Analytics Events enabled	Is the Analytics Event feature enabled?	**Analytics events have not been enabled.** Solution/Explanation: Enable the Analytics Events feature. To do this, click **Tools** > **Options** > **Analytics Events** and select the **Enabled** check box.
Address allowed	Is the IP address/host name of the machine sending the event(s) allowed (listed on the analytics events address list)?	**The local host name must be added as allowed address for the Analytics Event service.** Solution/Explanation: Add your machine to the analytics events address list of allowed IP addresses or host names. **Error resolving the local host name.** Solution/Explanation: The IP address or host name of the machine cannot be found or is invalid.
Send analytics event	Did sending a test event to the Event Server succeed?	See table below.

Each step is marked by either failed: ✗ or successful: ✓.

Error messages and solutions for the condition **Send analytics event**:

Event server not found	Unable to find the event server on the list of registered services.
Error connecting to event server	Unable to connect to the event server on the stated port. The error occurs most likely because of network problems, or the event server service has stopped.
Error sending analytics event	The connection to the event server is established, but the event cannot be sent. The error most likely occurs because of network problems, for example a time out.
Error receiving response from event server	The event has been sent to the event server, but no reply received. The error most likely occurs because of network problems or a port that is busy. See the event server log, typically located at *ProgramData\Sony\-Network VMS Event Server\logs*.
Analytics event unknown by event server	The event server service does not know the event. The error most likely occurs because the event or changes to the event have not been saved.
Invalid analytics event received by event server	The event format is incorrect.
Sender unauthorized by event server	Most likely your machine is not on the list of allowed IP addresses or hostnames.

Internal error in event server.	Event server error. See the event server log, typically located at *ProgramData\Sony\- Network VMS Event Server\logs\.*
Invalid response received from Event server	The response is invalid. Possibly the port is busy or there are network problems. See the event server log, typically located at *ProgramData\Sony\- Network VMS Event Server\logs\.*
Unknown response from event server	The response is valid, but not understood. The error occurs possibly because of network problems, or the port is busy. See the event server log, typically located at *ProgramData\Sony\- Network VMS Event Server\logs\.*
Unexpected error	Please contact Sony support for help.

Edit analytics events settings

In the toolbar, go to the **Tools** > **Options** > **Analytics Events** tab to edit relevant settings.

Generic events

About generic events

Important: This feature does not work if you do not have the Network Video Management System event server installed.

Generic events allow you to trigger actions in the Network Video Management System event server by sending simple strings via the IP network to your system.

You can use any hard- or software, which can send strings via TCP or UDP, to trigger generic events. Your system can analyze received TCP or UDP data packages, and automatically trigger generic events when specific criteria are met. This way, you may integrate your system with external sources, for example access control systems and alarm systems. The aim is to allow as many external sources as possible to interact with the system.

With the concept of data sources, you avoid having to adapt third-party tools to meet the standards of your system. With data sources, you can communicate with a particular piece of hard- or software on a specific IP port and fine-tune how bytes arriving on that port are interpreted. Each generic event type pairs up with a data source and makes up a language used for communication with a specific piece of hard- or software.

Working with data sources requires general knowledge of IP networking and specific knowledge of the individual hard- or software you want to interface from. There are many parameters you can use and no ready-made solution on how to do this. Basically, your system provides the tools, but not the solution. Unlike user-defined events, generic events have no authentication. This makes them easier to trigger but, to avoid jeopardizing security, only events from local host are accepted. You can allow other client IP addresses from the **Generic Events** tab of the **Options** menu.

Add a generic event

You can define generic events to help the video management software recognize specific strings in TCP or UDP packets from an external system. Based on a generic event, you can configure Management Client to trigger actions, for example to start recording, or alarms.

Prerequisites: You have enabled generic events and specified the source destinations allowed. For more information, see Generic Events tab (see "Generic Events tab (options)" on page 203).

1. Expand **Rules and Events**.

2. Right-click **Generic Events** and select **Add New**.

3. Fill in the needed information and properties. For more information, see Generic event properties (see "Generic event (properties)" on page 160).

4. (optional) To validate that the search expression is valid, enter a search string in the **Check if expression matches event string** field that corresponds to the expected packages:

   - **Match** - the string can be validated against the search expression.

   - **No match** - the search expression is invalid. Change it and try again.

In Network Video Management System Smart Client, you can verify whether your generic events have been received by the event server. You do this in the **Alarm List** on the **Alarm Manager** tab by selecting **Events**.

Generic event (properties)

Component	Requirement
Name	Unique name for the generic event. Name must be unique among all types of events, such as user defined events, analytics events, and so on.
Enabled	Generic events are by default enabled. Clear the check box to disable the event.

Expression	Expression that the system should look out for when analyzing data packages. You can use the following operators: • **( ):** Used to ensure that related terms are processed together as a logical unit. They can be used to force a certain processing order in the analysis. **Example:** The search criteria "(**User001** OR **Door053**) AND **Sunday**" first processes the two terms inside the parenthesis, then combines the result with the last part of the string. So, the system first looks for any packages containing either of the terms **User001** or **Door053**, then takes the results and run through them in order to see which packages also contain the term **Sunday**. • **AND:** With an AND operator, you specify that the terms on both sides of the AND operator must be present. **Example:** The search criteria "**User001** AND **Door053** AND **Sunday**" returns a result only if the terms **User001**, **Door053** and **Sunday** are all included in your expression. It is not enough for only one or two of the terms to be present. The more terms you combine with AND, the fewer results you retrieve. • **OR:** With an OR operator, you specify that either one or another term must be present. **Example:** The search criteria "**User001** OR **Door053** OR **Sunday**" returns any results containing either **User001**, **Door053** or **Sunday**. The more terms you combine with OR, the more results you retrieve.
Expression type	Indicates how particular the system should be when analyzing received data packages. The options are the following: • **Search:** In order for the event to occur, the received data package must contain the text specified in the **Expression:** field, but may also have more content. **Example:** If you have specified that the received package should contain the terms **User001** and **Door053**, the event is triggered if the received package contains the terms **User001** and **Door053** and **Sunday** since your two required terms are contained in the received package. • **Match:** In order for the event to occur, the received data package must contain exactly the text specified in the **Expression:** field, and nothing else. • **Regular expression:** In order for the event to occur, the text specified in the **Expression**: field must identify specific patterns in the received data packages. If you switch from **Search** or **Match** to **Regular expression**, the text in the **Expression** field is automatically translated to a regular expression.

Priority	The priority must be specified as a number between 0 (lowest priority) and 999999 (highest priority).
	The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events.
	When the system receives a TCP and/or UDP package, analysis of the packet starts with analysis for the event with the highest priority. This way, when a package matches the criteria for several events, only the event with the highest priority is triggered. If a package matches the criteria for several events with an identical priority, for example two events with a priority of 999, all events with this priority is triggered.
Check if expression matches event string	An event string to be tested against the expression entered in the **Expression:** field.

Generic event data source (properties)

Component	Requirement
Data source	You can choose between two default data sources and define a custom data source. What to choose depends on your third party program and/or the hard- or software you want to interface from:
	Compatible: Factory default settings are enabled, echoes all bytes, TCP and UDP, Ipv4 only, port 1234, no separator, local host only, current code page encoding (ANSI).
	International: Factory default settings are enabled, echoes statistics only, TCP only, Ipv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10).
	[Data source A]
	[Data source B]
	and so on.
New	Click to create a new data source.
Name	Name of the data source.
Enabled	Data sources are by default enabled. Clear the check box to disable the data source.
Reset	Click to reset all settings for the selected data source. The entered name in the **Name** field remains.
Port	The port number of the data source.

Component	Requirement
Protocol type selector	Protocols which the system should listen for, and analyze, in order to detect generic events: **Any:** TCP as well as UDP. **TCP:** TCP only. **UDP:** UDP only. TCP and UDP packages used for generic events may contain special characters, such as @, #, +, ~, and more.
IP type selector	Selectable IP address types: IPv4, IPv6 or both.
Separator bytes	Select the separator bytes used to separate individual generic event records. Default for data source type **International** (see **Data sources** earlier) is **13,10**. (13,10 = <CR><IF>).

Echo type selector	Available echo return formats:
	
	• **Echo statistics:** Echoes the following format:
	
	    [X],[Y],[Z],[Name of generic event]
	
	    [X] = request number.
	
	    [Y] = number of characters.
	
	    [Z] = number of matches with a generic event.
	
	    [Name of generic event] = name entered in the **Name:** field.
	
	• **Echo all bytes:** Echoes all bytes.
	
	• **No echo:** Suppresses all echoing.

Encoding type selector	By default, the list only shows the most relevant options. Select the **Show all** check box to display all available encodings.
Show all	See previous bullet.
Allowed external IPv4 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.
Allowed external IPv6 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.

Tip: Ranges can be specified in each of the four positions, like **100,105,110-120**. As an example, all addresses on the 10.10 network can be allowed by **10.10.[0-254].[0-254]** or by **10.10.255.255**.

Security

Roles

About roles

Roles determine which devices users can access. Roles also determine rights and handle security within the video management system. First, you add roles, then you add users and groups and finally a Smart Client profile as well as other default profiles that belong to each role. Roles you can create in the system have their own view groups in Network Video Management System Smart Client in which their views are created and stored.

The system comes with one predefined role which you cannot delete: the **Administrators** role. Users and groups with the **Administrators** role have complete and unrestricted access to the entire system. For this reason, you cannot specify role settings for the **Administrators** role. The **Administrators** role has the default Smart Client profile and does not have a time profile.

Users with local machine administrator rights on the computer running the management server automatically have administrator rights on the management server. Only users whom you trust as administrators of your system should have local machine administrator rights on the computer running the management server. You cannot turn this off. You add users and groups to the **Administrators** role just as with any other role. See Assign and remove users and groups to/from roles (see "Assign/remove users and groups to/from roles" on page 167).

In addition to the **Administrators** role, you can add as many roles as required to suit your needs. You may, for example, have different roles for users of Network Video Management System Smart Client depending on which cameras you want them to access or similar restrictions. To set up roles in your system, expand the **Security** > **Roles**.

About rights of a role

When you create a role in your system, you can give the role a number of rights to the system components or features that the relevant role can access and use. You may, for example, want to create roles that only have rights to functionality in Network Video Management System Smart Client or other Sony viewing clients, with the rights to view only certain cameras. If you create such roles, these roles should not have rights to access and use the Management Client, but only have access to some or all functionality found in Network Video Management System Smart Client or other clients. To address this, you may want to set up a role that has some or most typical administrator rights, for example, the rights to add and remove cameras, servers and similar functionality.

You can create roles that have some or most rights of a system administrator. This may, for example, be relevant if your organization wants to separate between between people who can administrate a subset of the system and people who can administrate the entire system. The feature allows you to provide differentiated administrator permissions to access, edit or change a large variety of system functions, for example, the right to edit the settings for servers or cameras in your system. You specify these permissions on the Overall Security tab (see "Overall Security tab (roles)" on page 169). As a minimum, to enable that the differentiated system administrator can launch the Management Client, you must grant read permissions on the management server for the role.

To give a role such differentiated administrator rights, the person with the default full administrator role must set up the role under **Security** > **Roles > Info tab > Add new**. When you set up the new role, you can then associate the role with your own profiles must similarly to when you set up any other role in the system or use the system's default profiles. For more information, see Add and manage a role (on page 166).

Once you have specified what profiles you want to associate the role with, go to the **Overall Security** tab to specify the rights of the role.

About users

The term **users** primarily refers to users who connect to the surveillance system through the clients. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.

- As **Windows users**, authenticated based on their Windows login.

Windows Users

You add Windows Users through the use of Active Directory. Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. It identifies resources on a network in order for users or applications to access them. Active Directory uses the concepts of users and groups.

Users are Active Directory objects representing individuals with a user account. Example:

Groups are Active Directory objects with several users. In this example, the Management Group has three users:

Groups can contain any number of users. By adding a group to the system, you add all of its members in one go. Once you have added the group to the system, any changes made to the group in Active Directory, such as new members you add or old members you remove at a later stage, are immediately reflected in the system. Note that a user can be a member of more than one group at a time.

You can use Active Directory to add existing user and group information to the system with some benefits:

- Users and groups are specified centrally in Active Directory so you do not have to create user accounts from scratch.

- You do not have to configure any authentication of users on the system as Active Directory handles authentication.

Before you can add users and groups through the Active Directory service, you must have a server with Active Directory installed on your network.

Basic users

If your system does not have access to Active Directory, create a basic user (see "About basic users" on page 180). For information about how to set up basic users, see Create basic user (see "Create basic users" on page 181).

Add and manage a role

1. Expand **Security** and right-click **Roles**.

2. Select **Add Role**. This opens the **Add Role** dialog box.

3. Type a name and description of the new role and click **OK**.

4. The new role is added to the **Roles** list. By default, a new role does not have any users/groups associated with it, but it does have a number of default profiles associated.

5. To choose different Smart Client profiles or time profiles, click the drop-down lists.

6. You can now assign users/groups to the role, and specify which of the system's features they can access.

See also Assign/remove users and groups to/from roles (on page 167) and Role settings (see "Roles settings" on page 168).

Copy, rename or delete a role

Copy a role

If you have a role with complicated settings and/or rights and need a similar or almost similar role, it might be easier to copy the already existing role and make minor adjustments to the copy than to creating a new role from scratch.

1. Expand **Security**, click **Roles**, right-click the relevant role and select **Copy Role**.

2. In the dialog box that opens, give the copied role a new unique name and description.

3. Click **OK**.

Rename a role

If you rename a role, this does not change the name of the view group based upon the role.

1. Expand **Security**, and right-click **Roles**.

2. Right-click required role and select **Rename Role**.

3. In the dialog box that opens, change the name of the role.

4. Click **OK**.

Delete a role

1. Expand **Security**, and click **Roles**.

2. Right-click the unwanted role and select **Delete Role**.

3. Click **Yes**.

Important: If you delete a role, this does not delete the view group based upon the role.

Assign/remove users and groups to/from roles

To assign or remove Windows users or groups or basic users to/from a role:

1. Expand **Security** and select **Roles**. Then select the required role in the **Overview** pane:

2. In the **Properties** pane, select the **Users and Groups** tab at the bottom.

3. Click **Add**, select between **Windows user** or **Basic user**.

Assign Windows users and groups to a role

1. Select **Windows user**. This opens the **Select Users**, **Computers and Groups** dialog box:

2. Verify that the required object type is specified. If, for example, you need to add a computer, click **Object Types** and mark **Computer**. Also verify that the required domain is specified in the **From this location** field. If not, click **Locations** to browse for the required domain.

3. In the **Enter the object names to select** box, type the relevant user names, initials, or other types of identifier which Active Directory can recognize. Use the **Check Names** feature to verify that Active Directory recognizes the names or initials you have typed. Alternatively, use the **"Advanced..."** function to search for users or groups.

4. Click **OK**. The selected users/groups are now added to the **Users and Groups** tab's list of users who you have assigned the selected role. You can add more users and groups by entering multiple names separated by a semicolon (;).

Assign basic users to a role

1. Select **Basic User**. This opens the **Select Basic Users to add to Role** dialog box:

2. Select the basic user(s) that you want to assign to this role.

3. Optional: Click **New** to create a new basic user.

4. Click **OK**. The selected basic user(s) are now added to the **Users and Groups** tab's list of basic users who you have assigned the selected role.

Remove users and groups from a role

1. On the **Users and Groups** tab, select the user or group you want to remove and click **Remove** in the lower part of the tab. You can select more than one user or group, or a combination of groups and individual users, if you need to.

2. Confirm that you want to remove the selected user(s) or and group(s). Click **Yes**.

A user may also have roles through group memberships. When that is the case, you cannot remove the individual user from the role. Group members may also hold roles as individuals. To find out which roles users, groups, or individual group members have, use the **View Effective Roles** function.

View effective roles

With the Effective Roles feature, you can view all roles of a selected user or group. This is practical if you are using groups and it is the only way of viewing which roles a specific user is a member of.

1. Open the **Effective Roles** window by expanding **Security**, then right-clicking **Roles** and select **Effective Roles**.

2. If you want information about a basic user, type the name in the **User name** field. Click **Refresh** to display the roles of the user.

3. If you use Windows users or groups in Active Directory, click the **"…"** browse button. Select object type, enter the name, and click **OK**. The user's roles appear automatically.

Roles settings

Info tab (roles)

On the **Info** tab of a role, you can set the following:

Name	Description
Name	Type a name for the role.
Description	Type a description for the role.
Smart Client profile	Select a Smart Client profile to associate with the role. Requires permissions to manage security on the management server.
Default time profile	Select a default time profile to associate with the role. You cannot apply this to the default **Administrators** role.
Login authorization required	Select the check box to associate login authorization with the role. It means that Network Video Management System Smart Client or the Management Client asks for a second authorization, typically by a superuser or manager, when the user logs in. To enable administrators to authorize users, configure the management server's **Authorize Users** right on the **Overall Security** tab. You cannot apply this to the default **Administrators** role.

User and Groups tab (roles)

On the **User and Groups** tab, you assign users and groups to roles (see "Assign/remove users and groups to/from roles" on page 167). You can assign Windows users and groups or basic users (see "About users" on page 165).

Name	Description
Name	Displays the name of the user or group assigned to this role.
Description	Displays the description that you entered when the basic user was created.

Overall Security tab (roles)

On the **Overall Security** tab, you set up overall rights for roles. For every component available in your system, decide whether to **Allow** or **Deny** users with the role the rights to access and use different areas on the relevant component.

The overall security settings only apply to the current site.

You can associate a user with more than one role. If you select **Deny** on a security setting for one role and **Allow** for another, the **Deny** right permission overrules the **Allow** right permission.

In the following, the descriptions show what happens on each individual right for the different system components if you select **Allow** for the relevant role.

For every system component or functionality, the full system administrator can use the **Allow** or **Deny** check boxes to set up security permissions for the role. Any security permissions you set up here is set up for the whole system component or functionality. So if, for example, you select the **Deny** check box on **Cameras,** all cameras added to the system are unavailable for the role. In contrast, if you select the **Allow** check box instead, the role can see all added cameras to the system. The result of selecting **Allow** or **Deny** on your cameras is that the camera settings on the **Device** tab then inherit your selections on the **Overall Security** tab so that either all cameras are available or unavailable to the particular role. If you want to set individual security permissions for individual cameras or similar device channels, you can then only set these individual permissions on the tab of the relevant system component or functionality if you have turned off any overall settings for the system component or functionality on the **Overall Security** tab.

The descriptions below also apply to the rights that you can configure through the MIP SDKs.

Management Server

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
System Monitor	Enables the right to view the data of the System Monitor.
Status API	Enables the right to perform queries on the Status API located on the recording server. This means that the role with this right enabled, has access to read the status of the items located on the recording server.
Authorize users	Enables the right to authorize users when they are asked for a second login in Network Video Management System Smart Client or Management Client. You define if a role requires login authorization on the **Info** tab.

Cameras

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view camera devices in the clients.
View Live	Enables the right to view live video from cameras in the clients.

Security right	Description
layback	Enables the right to play back recorded video from cameras in the clients.
Retrieve remote recordings	Enables the right to retrieve edge recordings from cameras or recordings from cameras on remote sites.
Read sequences	Enables the right to read the sequence information related to, for example, the Sequence explorer in the clients.
Smart search	Enables the right to use the Smart search function in the clients.
Export	Enables the right to export recordings from the clients.
Start manual recording	Enables the right to start manual recording of video in the clients.
Stop manual recording	Enables the right to stop manual recording of video in the clients.
AUX commands	Enables the right to use auxillary (AUX) commands on the camera from the clients. **AUX commands** offer users the control of for example, wipers on a camera connected via a video server. Camera-associated devices connected via auxiliary connections are controlled from the client.
Manual PTZ	Enables the right to use PTZ functions on PTZ cameras.
Activate PTZ presets or patrolling profile	Enables the right to move PTZ cameras to preset positions, start and stop patrolling profiles, and pause a patrolling. To allow this role to use other PTZ functions on the camera, enable the **Manual PTZ** right.
Manage PTZ presets or patrolling profiles	Enables the right to add, edit and delete PTZ presets and patrolling profiles on PTZ cameras in the Management Client. To allow this role to use other PTZ functions on the camera, enable the **Manual PTZ** right.

Microphones

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view microphone devices in the clients.
Listen	Enables the right to listen to live audio from microphones in the clients.

Security right	Description
Playback	Enables the right to play back recorded audio from microphones in the clients.
Retrieve remote recordings	Enables the right to retrieve edge recordings from microphones or recordings from microphones on remote sites.
Read sequences	Enables the right to read the sequence information related to, for example, the Sequence explorer in the clients.
Export	Enables the right to export recordings from the clients.
Start manual recording	Enables the right to start manual recording of audio in the clients.
Stop manual recording	Enables the right to stop manual recording of audio in the clients.

Speakers

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view speaker devices in the clients.
Listen	Enables the right to listen to live audio from speakers in the clients.
Speak	Enables the right to speak through the speakers in the clients.
Playback	Enables the right to play back recorded audio from speakers in the clients.
Retrieve remote recordings	Enables the right to retrieve edge recordings from speakers or recordings from speakers on remote sites.
Read sequences	Enables the right to use the Sequences feature while browsing recorded audio from speakers in the clients.
Export	Enables the right to export recorded audio from speakers in the clients.
Start manual recording	Enables the right to start manual recording of audio in the clients.
Stop manual recording	Enables the right to stop manual recording of audio in the clients.

Metadata

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to receive metadata in the clients.
Live	Enables the right to receive live metadata from cameras in the clients.
Playback	Enables the right to play back recorded data from metadata devices in the clients.
Retrieve remote recordings	Enables the right to retrieve edge recordings from metadata devices or recordings from metadata devices on remote sites.
Read sequences	Enables the right to read the sequence information related to, for example, the Sequence explorer in the clients.
Export	Enables the right to export recordings in the clients.
Start manual recording	Enables the right to start manual recording of metadata in the clients.
Stop manual recording	Enables the right to stop manual recording of metadata in the clients.

Input

Security right	Description
Read	Enables the right to view input devices in the clients.

Output

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view output devices in the clients.
Activate	Enables the right to activate outputs in the clients.

Smart Wall

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.

Security right	Description
Read	Enables the right to view Smart Walls in the clients.
Operate	Enables the right to operate Smart Walls, for example to change presets or apply cameras on views in the clients.
Playback	Enables the right to play back recorded data from within Smart Walls in the clients.

View Groups

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view the View Groups created in the Management Client in the clients.
Delete	Enables the right to delete View Groups in the Management Client.
Operate	Enables the right to use View Groups created in the Management Client within the clients, that is to create subgroups and views.

User-defined Events

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view user-defined events in the Management Client and the clients.
Trigger	Enables the right to trigger user-defined events in the clients.

Matrix

Security right	Description
Read	Enables the right to select and send video to the Matrix recipient from the clients.

System Monitors

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.

Security right	Description
Read	Enables the right to edit properties for System Monitors.
Edit	Enables the right to edit properties for System Monitors.

Device tab (roles)

The **Device** tab lets you specify which features users/groups with the selected role can use for each device (for example, a camera) or device group in Network Video Management System Smart Client.

Remember to repeat for each device. You can also select a device group, and specify role rights for all the devices in the group in one go.

You can still select or clear such square-filled check boxes, but note that your choice in that case applies for **all** devices within the device group. Alternatively, select the individual devices in the device group to verify exactly which devices the relevant right applies for.

Camera-related rights

Specify the following rights for camera devices:

Name	Description
Read	The selected camera(s) will be visible in the clients.
View live	Allows live viewing of video from the selected camera(s) in the clients. For Network Video Management System Smart Client, it requires that the role has been granted the right to view the clients' **Live** tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded video from the selected camera(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Smart search	Allows the user to use the Smart search function in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of video from the selected camera(s) in the clients.
Stop manual recording	Allows stopping manual recording of video from the selected camera(s) in the clients.
AUX commands	Allows the use of auxiliary commands from the clients.

Microphone-related rights

Specify the following rights for microphone devices:

Name	Description
Read	The selected microphone(s) will be visible in the clients.
Live > Listen	Allows listening to live audio from the selected microphones(s) in the clients. For Network Video Management System Smart Client, it requires that the role has been granted the right to view the clients' **Live** tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded audio from the selected microphone(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of audio from the selected microphone(s) in the clients.
Stop manual recording	Allows stopping manual recording of audio from the selected microphone(s) in the clients.

Speaker-related rights

Specify the following rights for speaker devices:

Name	Description
Read	The selected speaker(s) is visible in the clients.
Live > Listen	Allows listening to live audio from the selected speaker(s) in the clients. For Network Video Management System Smart Client, it requires that the role has been granted the right to view the clients' **Live** tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded audio from the selected speaker(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of audio from the selected speaker(s) in the clients.
Stop manual recording	Allows stopping manual recording of audio from the selected speaker(s) in the clients.

Metadata-related rights

Specify the following rights for metadata devices:

Name	Description
Read	Enables the right to see metadata devices and retrieve data from them in the clients.
Edit	Enables the right to edit metadate properties. It also allows users to enable or disable metadata devices in the Management Client and via the MIP SDK.
View Live	Enables the right to view metadata from cameras in the clients. For Network Video Management System Smart Client, it requires that the role has been granted the right to view the clients' **Live** tab. This right is granted as part of the application rights.
Playback	Enables the right to play back recorded data from metadata devices in the clients.
Read sequences	Enables the right to use the Sequences feature while browsing recorded data from metadata devices in the clients.
Export	Enables the right to export recorded audio from metadata devices in the clients.
Start manual recording	Enables the right to start manual recording of metadata in the clients.
Stop manual recording	Enables the right to stop manual recording of metadata in the clients.

Input-related rights

Specify the following rights for input devices:

Name	Description
Read	The selected input(s) will be visible in the clients as well as in Network Video Management System Central, an add-on product for providing complete overview of surveillance system status and alarms.

Output-related rights

Specify the following rights for output devices:

Name	Description
Read	The selected output(s) will be visible in the clients. If visible, the output will be selectable on a list in the clients.
Activate	The selected output(s) can be activated from the Management Client and the clients. Specify the time profile or leave the default value.

PTZ tab (roles)

You set up rights for pan-tilt-zoom (PTZ) cameras on the **PTZ** tab. You can specify the features users/groups can use in the clients. You can select individual PTZ cameras or device groups containing PTZ cameras.

Specify the following rights for PTZ:

Name	Description
Manual PTZ	Determines if the selected role can use PTZ functions and pause a patrolling on the selected camera.
	Specify a time profile, select **Always**, or leave the default value that follows the default time profile defined on the **Info** tab for that role.
Activate PTZ presets or patrolling profiles	Determines if the selected role can move the selected camera to preset positions, start and stop patrolling profiles, and pause a patrolling.
	Specify a time profile, select **Always**, or leave the default value that follows the default time profile defined on the **Info** tab for that role.
	To allow this role to use other PTZ functions on the camera, enable the **Manual PTZ** right.
PTZ Priority	Determines the priority of PTZ cameras. When several users on a surveillance system want to control the same PTZ camera at the same time, conflicts may occur.
	You can avoid such a situation by specifying a priority for use of the selected PTZ camera(s) by users/groups with the selected role. Specify a priority from 1 to 3, where 1 is the lowest priority. The role with the highest priority number is the one who can control the PTZ camera(s).
Manage PTZ presets or patrolling profiles	Determines the right to add, edit and delete PTZ presets and patrolling profiles on the selected camera in both the Management Client.
	To allow this role to use other PTZ functions on the camera, enable the **Manual PTZ** right.
Lock/unlock PTZ presets	Determines if the role can lock and unlock preset positions for the selected camera.

Speech tab (roles)

Relevant only if you use speakers on your system. Specify the following rights for speakers:

Name	Description
Speak	Determine if users should be allowed to talk through the selected speaker(s). Specify the time profile or leave the default value.

Name	Description
Speak priority	When several client users want to talk through the same speaker at the same time, conflicts may occur. Solve the problem by specifying a priority for use of the selected speaker(s) by users/groups with the selected role. Specify a priority from **Very low** to **Very high**. The role with the highest priority is allowed use the speaker before other roles. Should two users with the same role want to speak at the same time, the first come, first served-principle applies.

Remote Recordings tab (roles)

Specify the following rights for remote recordings:

Name	Description
Retrieve remote recordings	Enables the right to retrieve recordings in the clients from cameras, microphones, speakers, and metadata devices on remotes sites or from edge storages on cameras.

Smart Wall tab (roles)

Through roles, you can grant your client users Smart Wall-related user rights for the Smart Wall feature:

Name	Description
Read	Allows users to view the selected Smart Wall in the clients.
Edit	Allows users to edit the selected Smart Wall in the Management Client.
Delete	Allows users to delete the selected Smart Wall in the Management Client.
Operate	Allows users to apply layouts on the selected Smart Wall in the client and to activate the selected preset.
Playback	Allows users to play back recorded data from the selected Smart Wall in the clients.

External Event tab (roles)

Specify the following external event rights:

Name	Description
Read	Allows users to search for and view the selected external system event in the clients and the Management Client.

Name	Description
Edit	Allows users to edit the selected external system event in the Management Client.
Delete	Allows users to delete the selected external system event in the Management Client.
Trigger	Allows users to trigger the selected external system event in the clients.

View Group tab (roles)

On the **View Group** tab, you specify which view groups the users and user groups with the selected role can use in the clients.

Specify the following rights for view groups:

Name	Description
Read	Enables the right to view the View Groups in the clients and in the Management Client. View groups are created in the Management Client.
Edit	Enables the right to edit properties on View Groups in the Management Client.
Delete	Enables the right to delete View Groups in the Management Client.
Operate	Enables the right to use View Groups in Network Video Management System Smart Client that is to create and delete subgroups and views.

Matrix tab (roles)

If you have configured Matrix recipients on your system, you may configure Matrix role rights. From a client, you can send video to selected Matrix recipients. Select the users who can receive this on the Matrix tab.

The following rights are available:

Name	Description
Read	Determine if users and groups with the selected role can select and send video to the Matrix recipient from the clients.

Alarms tab (roles)

If you use alarms in your system setup to provide central overview and control of your installation (including any other Network Video Management System servers), you can use the **Alarms** tab to specify the alarm rights users/groups with the selected role should have, for example, how to handle alarms in the clients.

Specify the following rights for alarms:

Name	Description
Manage	Enables the right to manage alarms, for example changing priorities of alarms and re-delegate alarms to other users, acknowledge alarms and change the state, for example from **New** to **Assigned**, of several alarms at the same time.
View	Enables the right to view alarms and print alarm reports.
Disable alarms	Enables the right to disable alarms.
Receive notifications	Enables the right to receive notifications about alarms in the clients.

Access Control tab (roles)

When you add or edit basic users, Windows users or groups, specify access control settings:

Name	Description
Use Access Control	Allows the user to use any access control-related features in the clients.

MIP tab (roles)

Through the MIP Software Development Kit (SDK), a third-party vendor can develop custom plug-ins for your system, for example, integration to external access control systems or similar functionality.

Which settings you change for your plug-in depend on the relevant plug-in. Find the custom settings for the plug-ins on the **MIP** tab.

Basic users

About basic users

When you add a basic user to your system, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. This is in contrast to the Windows user, added through Active Directory.

When working with basic users, it is important to understand the difference between basic user and Windows user.

- Basic users are authenticated by a user name/password combination and are specific to a system.

- Windows users are authenticated based on their Windows login and are specific to a machine.

Create basic users

To create a basic user on your system:

1. Expand **Security** > **Basic Users**.

2. In the **Basic Users** pane, right-click and select **Create Basic User**.

3. Specify a user name and a password, and repeat it to be sure you have specified it correctly.

4. Click **OK** to create the basic user.

System dashboard

About system dashboard

System dashboard provides you with the functionality to monitor your system and its components.

Access the following functionality:

Name	Description
System Monitor	Monitor the status of your servers and cameras by parameters you define.
System Monitor Thresholds	Set threshold values for monitored parameters on server and monitor tiles used in System Monitor.
Current Task	Get an overview of ongoing tasks on a selected recording server.
Configuration Reports	Decide what to include in your system configuration reports before printing.

About system monitor

System monitor provides you with a quick, visual overview of the current state of your system's servers and cameras through colored tiles that represent the system hardware. By default, the system displays tiles that represent all **Recording servers**, **All servers** and **All cameras**.

The color of the tiles:

Tile color	Description
Green	**Normal** state. Everything is running normally.
Yellow	**Warning** state. One or more monitoring parameters is above the threshold value (see "About system monitor thresholds" on page *184*) for the **Normal** state.
Red	**Critical** state. One or more monitoring parameters is above the threshold value for the **Normal** and **Warning** state.

You can customize the server and camera tiles if you want to display more or less tiles on the dashboard. For example, you can set up tiles to represent a single server, a single camera, a group of cameras, or a server group. You can also delete a tile if you do not want to use it or edit its monitoring parameters. Monitoring parameters are, for example, CPU usage or memory available for a server. If you remove these parameters from the server tile, the tile does not monitor these parameters on the relevant tile. Click **Customize** in the upper right corner of the tab to open the Customize dashboard window. See Customize dashboard (on page 182) for more information.

Tiles change their state and thereby color based on threshold values set in System monitor thresholds. While the system does set some default threshold values for you, you can decide for yourself what the threshold value should be for each of the three states. To set up or change threshold values, you can use **System monitor thresholds**. See About system monitor thresholds (on page 184).

If a tile changes color and you want to know which server/parameter that makes the tile change color, click the tile. This opens an overview in the bottom of the screen which shows the colors red, yellow or green for each monitoring parameter you have enabled for your tile. Click the **Details** button to get more detailed information about why the state has changed.

If you see a warning sign on a tile, a data collector for one of your monitored servers or cameras may not be running. If you place your mouse above the tile, the system shows you when it last collected data for the relevant tile.

Customize dashboard

Add a new camera or server tile

1. In the System monitor window, click **Customize**.

2. In the **Customize dashboard** window that opens, click **New** under **Server tiles** or **Camera tiles**.

3. In the **New server tile/New camera tile** window, select the cameras or servers to monitor.

4. Under **Monitoring parameters,** select or clear check boxes for any parameters to add or remove from the relevant tile.

5. Click **OK.** The new server or camera tile is now added to the tiles displayed on your dashboard.

Edit monitoring parameters

1. In the System monitor dashboard window, click **Customize**.

2. In the **Customize dashboard** window that opens, click **Edit** under **Server tiles** or **Camera tiles**.

3. In the **Edit server tile** or **Edit camera tile** window, select the server component or cameras you want to edit.

4. In the **Monitoring parameters** box, select or clear the check boxes for the monitoring parameters you want to add or remove from the relevant tile.

5. Click **OK**. The changed monitoring parameters are now a part of or removed from the relevant tile.

You can enable and disable historical data on the system if you want to. If you disable this data, you cannot see graphs of previous system behavior. If you want to reduce the load on the SQL server database or on your bandwidth, you can reduce the sampling interval of historical data. If you reduce the sampling interval of historical data, less details are available in graphs.

About system monitor details

If you click a server or camera tile, you can see the status of each selected monitoring parameter below the dashboard.

State	Name	Live FPS	Recording FPS	Used space	
	Panasonic SPxxx/SFxxx/SWxxx no I/O Camera Series				Details
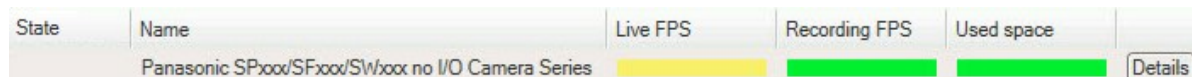
Example: A camera's LIVE FPS monitoring parameters has reached the Warning state.

The **State** field shows the camera's state. For example, a red warning is shown if the connection to the device is broken. The icon includes a tool tip with a short description of the issue that is causing the warning.

The **Used space** field shows data from other recording servers where this device has recordings if, for example, the device has been located on other recording servers previously.

If you click the **Details** button for the relevant camera/server, you can view system information and create reports regarding:

Component	Description
Management server	Shows data from the selected management server
Recording server(s)	Shows data from the selected recording server. You can view these per: • Disk • Storage • Network • Camera
Additional servers	Shows data on log server, event servers and more.
Cameras	Shows data from any camera in any camera group in your setup.

Each of these elements is an area you can click and expand. When you click this area, it provides relevant dynamic data on this server or camera.

The **Cameras** bar contains a list of camera groups to select from. Once you select a group, select a specific camera and see dynamic data for it. All servers display CPU usage and available memory information. Recording servers also display connection status information. Within each view, find a **History** link. Click it to view historic data and reports (to view reports on a camera, click the name of the camera). For each historic report, you can view data for the last 24 hours, 7 days or 30 days. To save and/or print reports, click the **Send to PDF** icon. Use the < and home icons to navigate System Monitor.

You can only create historical reports with data from the recording server where the device is currently located.

Important: If you access the system monitor's details from a server operating system, you may experience a message regarding **Internet Explorer Enhanced Security Configuration**. Follow the instructions in the message to add the **System Monitor** page to the **Trusted sites zone** before proceeding.

About system monitor thresholds

System monitor thresholds allow you to set up and adjust the global thresholds for when tiles on System monitor should visually indicate that your system hardware changes state, for example when the CPU usage of a server changes from a normal state (green) state to a warning state (yellow).

The system is set up with default threshold values so that you can start monitoring your system hardware from the moment your system is set up. You can change these values if you want to (see "Set system monitor thresholds" on page 185).

As a default, the system is set up to show threshold values for all units of a particular hardware, for example all cameras or servers. You can also set up threshold values for individual servers or cameras or a subset of these. Setting threshold values for individual servers or cameras may be a good idea if, for example, some cameras should be allowed to use a higher **Live FPS** or **Recording FPS** that other cameras.

You can set the threshold values for servers, cameras, disks and storage. If you want to change threshold values, you can use the threshold control slider. The threshold control slider allows you to increase or decrease threshold values by dragging the handles separating states either up or down. The threshold control slider is divided into colors similar to those shown in your server or camera tiles present in System monitor (see "About system monitor" on page 181).

To ensure that you do not see a **Critical** or **Warning** state in cases where the usage of or the load on your system hardware reaches a high threshold value only for a second or similar, use the **Calculation interval**. The **Calculation interval** averages out the effect of brief or frequent changes to a system hardware state. In practice, this means that the **Calculation interval** evens out the effect of hardware changes over time so that you do not get alerts every time a threshold is exceeded.

For example, you can set the **Calculation interval** to one (1) minute which ensures that you only get alerts if the average value for the whole minute exceeds the threshold. The benefit of this is that you avoid alerts about frequent and maybe possibly irrelevant changes in hardware states and only receive alerts that reflect sustained issues with, for example, CPU usage or memory consumption.

Server thresholds

Threshold	Description	Unit
Memory	Thresholds for RAM memory in use on the servers you monitor.	MB
CPU Usage	Thresholds for the CPU usage on the servers you monitor.	%

Camera thresholds

Threshold	Description	Unit
Used space	Thresholds for the space used by cameras you monitor.	GB
Recording FPS	Thresholds for cameras' FPS in use when the system is recording video on cameras you monitor.	%
Live FPS	Thresholds for cameras' FPS in use when live video is shown on cameras you monitor.	%

Disk thresholds

Threshold	Description	Unit
Free space	Thresholds for available space on disks you monitor.	GB

Storage thresholds

Threshold	Description	Unit
Retention time	Threshold showing a prediction for when you run out of space on your storage. The state shown is based on your system setup and is updated twice a day.	Days

You can also set up rules (see "About rules" on page 142) to perform specific actions or activate alarms (see "About alarms" on page 191) when a threshold changes from one state to another.

Set system monitor thresholds

1. Select the **Enable** check box for the relevant system hardware if you have not already enabled it.

2. Drag the threshold control slider up or down to increase or decrease the threshold value. There are two sliders available for each piece of system hardware shown in the threshold control, separating the **Normal**, **Warning** and **Critical** levels.

3. Once you have set the relevant thresholds levels, select **File** > **Save** from the menu.

An example of how a threshold control slider could be set. Drag the sliders up and down to increase or decrease any of the three threshold levels. Red indicates you have reached a Critical

state, Yellow is a Warning state indicating that you are close to reaching the Critical state and Green indicates that things are at a normal state and within your selected threshold values.

About current tasks

The **Current Tasks** node shows an overview of tasks under a selected recording server, their begin time, estimated end time and progress. All information shown in **Current Tasks** are snapshots. You can refresh these by clicking on the **Refresh** button in the lower right corner of the **Properties** pane.

About configuration reports

When you create PDF configuration reports, you can include any possible elements of your system in the report. You can, for example, include licenses, device configuration, alarm configuration, and much more. You can also customize your font and page setup and include a customized front page.

Add a configuration report

1. Expand **System Dashboard** and click **Configuration Reports**. This brings up the report configuration page.

2. Select the elements that you want to include in your report.

3. **Optional**: Click **Front Page** to customize your front page. In the window that appears, fill in the needed info. Select **Front page** as an element to include in you report, otherwise the front page you customize is not included in your report.

4. Click **Formatting** to customize your font, page size and margins. In the window that appears, select the wanted settings.

5. When you are ready to export, click **Export** and select a name and save location for you report.

Configure report details

The following is available when setting up reports:

Name	Description
Select All	Selects all elements in the list.
Clear All	Clears all elements in the list.
Front Page	Customize the front page of the report.
Formatting	Format the report.
Export	Select a save location for the report and create a PDF.

Server logs

About logs

You can view and export contents from different logs related to the system. The purpose of the logs is to document activity, events, actions and errors in the system, for later analysis or documentation.

The logs have different purposes:

Name	Description
System log	Logs system-related information.
Audit log	Logs user activity.
Rule log	Logs rules in which users have specified the Make new log entry action.

Your system has a number of default settings related to the different logs. To change the settings, see Server Logs tab (see "Server Logs tab (options)" on page 199) under Options.

You can view logs in a number of different languages and export logs as tab delimited text (.txt) files.

If a log contains more than one page of information, you can navigate between the log pages by clicking the buttons in the bottom right corner of the log pane:
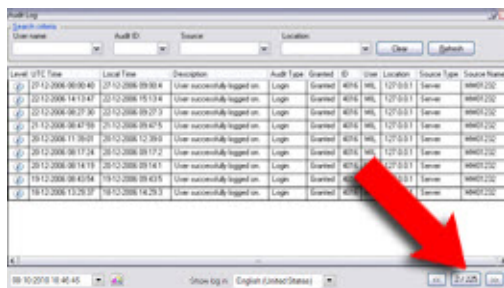
In the lower left corner, jump to a specific date and time in the log:

Search logs

To search a log, use **Search criteria** in the top part of the log pane:

1. Specify your search criteria from the lists.

2. Click **Refresh** to make the log page reflect your search criteria. To clear your search criteria, and return to viewing all of the log's content, click **Clear**.

You can double-click any row to have all details presented in a **Log Details** window. In this way you can also read the log entries that contain more text than can be displayed in a single line.

Export logs

You can export logs as tab delimited text (.txt) files. You can customize the log content by specifying which log, log elements, and time range to include in the export. For example, you can specify to include only the System Log error-related log entries from between January 2nd 2016 08:00:00 and January 6th 2014 07:59:59 in your export.

To export a log:

1. In the **Export Log** window's **File name** field, specify a name for the exported log file.

    By default, exported log files are saved in your **My Documents** folder. However, you can specify a different location by clicking the browse button 🔲 next to the field.

2. Any criteria you have selected to target the content of the exported log is listed in the **Filters** field. You cannot edit this field. If you need to change your criteria, close the window, and repeat steps 1-2.

3. Specify the time period you want the export to cover. Specify the **Start date and time** and **End date and time** fields respectively. You can select the date by clicking the arrow:

    To specify an exact time, overwrite the required time elements (hours:minutes:seconds) with the needed values. In this example, the hours element is being overwritten:

    Start date and time:
    02-01-2011 10:00.00 ▼
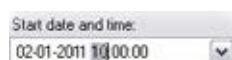
4. Click **Export** to export the log content.

Change log language

1. At the bottom part of the log pane, in the **Show log in** list, select the wanted language.

    Show log in: English (United States) ▼

2. The log is displayed in the selected language. Next time your open the log, it is reset to the default language.

System log (properties)

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Level	Displays an icon that indicates the level of the log entry: ⓘ - indicates info ⚠ - indicates warning ❌ - indicates error 'blank' - indicates an undefined entry.
UTC Time	Timestamped in coordinated universal time (UTC).
Local Time	Timestamped in the local time of your system's server.
ID	The identification number for the logged incident.

Name	Description
Source Type	The type of equipment on which the logged incident occurred, for example, server or device.
Source Name	Management server, the name of the recording server or device on which the logged incident occurred.
Event Type	The type of event represented by the logged incident.
Description	Shows a description of the logged incident.

Audit log (properties)

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Level	Displays an icon that indicates the level of the log entry: 🛈 - indicates info ⚠ - indicates warning ❌ - indicates error 'blank' - indicates an undefined entry.
UTC Time	Timestamped in coordinated universal time (UTC).
Local Time	Timestamped in the local time of your system's server.
ID	The identification number for the logged incident.
User	The user name of the remote user causing the logged incident.
User Location	The IP address or host name of the computer from which the remote user caused the logged incident.
Permission	The information about whether the remote user action was allowed (granted) or not.
Category	The type of logged incident.
Resource Type	The type of equipment on which the logged incident occurred, for example, server or device.
Resource Name	Management server, or the name of the recording server or device on which the logged incident occurred.
Resource Host	The name of the recording server that hosts a device or a storage on which the logged incident occurred. The name of the management server that hosts the recording server or the management server on which the logged incident occurred.
Description	Shows a description of the logged incident.

Rule log (properties)

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Level	Displays an icon that indicates the level of the log entry: ⓘ - indicates info ⚠ - indicates warning ❌ - indicates error 'blank' - indicates an undefined entry.
UTC Time	Timestamped in coordinated universal time (UTC).
Local Time	Timestamped in the local time of your system's server.
ID	The identification number for the logged incident.
Service Name	The name of the service on which the logged incident occurred.
Rule Name	The name of the rule triggering the log entry.
Source Type	The type of equipment on which the logged incident occurred, for example, server or device.
Source Name	Management server, the name of the recording server or device on which the logged incident occurred.
Event Type	The type of event represented by the logged incident.
Generator Type	The type pf equipment on which the logged incident was triggered. Log entries are administrator-defined and relate to incidents in your system.
Generator Name	The name of the equipment on which the logged incident was generated.
Description	Shows a description of the logged incident.

Alarms

About alarm configuration

Alarm configuration includes:

- Dynamic role-based setup of alarm handling

- Central technical overview of all components: servers, cameras, and external units

- Setup of central logging of all incoming alarms and system information

- Handling of plug-ins, allowing customized integration of other systems, for example external access control or VCA-based systems.

In general, alarms are controlled by the visibility of the object causing the alarm. This means that four possible aspects can play a role with regards to alarms and who can control/manage them and to what degree:

Name	Description
Source/device visibility	If the device causing the alarm is not set to be visible to the user's role, the user cannot see the alarm in the alarm list in Network Video Management System Smart Client.
The right to trigger user-defined events	This right determines if the user's role can trigger selected user-defined events in Network Video Management System Smart Client.
External plug-ins	If any external plug-ins are set up in your system, these might control users' rights to handle alarms.
General role rights	Determine whether the user is allowed to only view or also to manage alarms. What a user of **Alarms** can do with alarms depends on the user's role and on settings configured for that particular role.

On the **Event Server** tab in **Options**, you can specify settings for alarms, events and logs.

About alarms

Important: This feature does not work if you do not have the Network Video Management System Event Server installed.

Based on functionality handled in the event server, the alarms feature provides central overview, control and scalability of alarms in any number of installations (including any other Network Video Management Systems) throughout your organization. You can configure it to generate alarms based on either:

- **Internal system related events**

  For example, motion, server responding/not responding, archiving problems, lack of disk space and more.

- **External integrated events**

  This group can consist of several types of external events:

  - **Analytics events**

  Typically data received from an external third-party video content analysis (VCA) providers.

  - **MIP plug-in events**

Through the MIP Software Development Kit (SDK) a third party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) to your system.
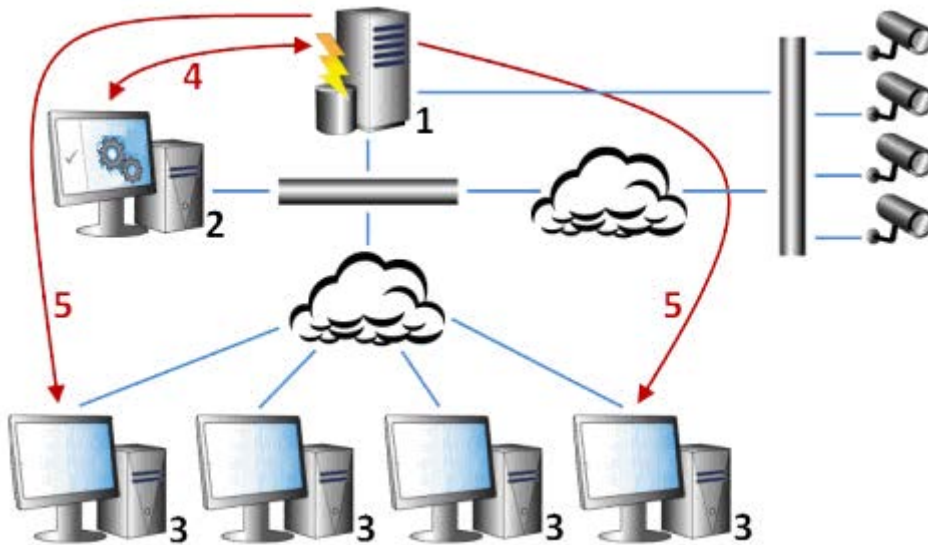
Legend:

1. Surveillance system

2. Management Client

3. Network Video Management System Smart Client

4. Alarm configuration

5. Alarm data flow

You handle and delegate alarms in the alarm list in Network Video Management System Smart Client. You can also integrate alarms with the Network Video Management System Smart Client's map functionality.

Alarm Definitions

When your system registers an event on your system, you can configure the system to generate an alarm in Network Video Management System Smart Client. You must define alarms before you can use them, and alarms are defined based on events registered in your system servers. You can also use user-defined events for triggering alarms and use the same event to trigger several different alarms.

Add an alarm

To define an alarm, you need to create an alarm definition, where you specify, for example, what triggers the alarm, instructions on what the operator needs to do, and what or when the alarm stops. For detailed information about the settings, see Alarm Definitions (properties) (on page 193).

1. In the **Site Navigation** pane, expand **Alarms**, and right-click **Alarm Definitions**.

2. Select **Add New**.

3. Fill in these properties:

- **Name**: Type a name for the alarm definition. The name of the alarm definition appears whenever the alarm definition is listed.

- **Instructions**: You can write instructions for the operator who receives the alarm.

- **Triggering event**: Use the drop-down menus to select an event type and an event message to be used when the alarm is triggered.

```
Motion detected~SW storage area    ▼
Archive Failure (Enterprise)
Archive Move Failure (Enterprise)
Camera Not Responding
Camera Responding
Disabled
Enabled
External Event
Motion Detected
Motion detected~SW storage area
Running Out of Disk Space
Server Not Responding
Server Responding
```
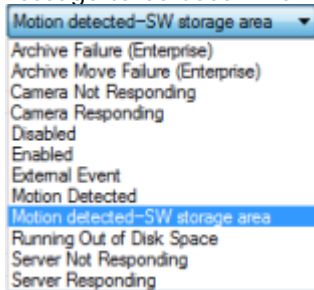
A list of selectable triggering events. The one highlighted is created and customized using analytics events.

- **Sources**: Select the cameras or other devices that the event should originate from to trigger the alarm. Your options depend on the type of event you have selected.

- **Time profile**: If you want the alarm to be activated during a specific time interval, select the radio button and then a time profile in the drop-down menu.

- **Event based:** If you want the alarm to be activated by an event, select the radio button and specify which event will start the alarm. You also need to specify the event that will stop the alarm.

4. In the **Time limit** drop-down menu, specify a time limit for when action is required by the operator.

5. In the **Events triggered** drop-down menu, specify which event to trigger when the time limit has passed.

6. Specify additional settings, for example related cameras and initial alarm owner.

Alarm Definitions (properties)

The table describes the settings you can make when you create an alarm definition.

Alarm definition settings:

Name	Description
Enable	By default, the alarm definition is enabled. To disable it, clear the check box.
Name	Alarm names do not have to be unique, but using unique and descriptive alarm names are advantageous in many situations.
Instructions	Type a descriptive text about the alarm and how to resolve the issue that caused the alarm. The text appears in Network Video Management System Smart Client when the user handles the alarm.

Name	Description
Triggering event	Select the event message to use when the alarm is triggered. Choose from two drop-downs: • The first drop-down: Select the type of event, for example analytics event and system events. • The second drop-down: Select the specific event message to use. The messages available are determined by the event type you selected in the first drop-down menu.
Sources	Specify the sources that the events originate from. Aside from cameras or other devices, sources may also be plug-in defined sources, for example VCA and MIP. The options depend on the type of event you have selected.

Alarm trigger:

Name	Description
Time profile	Select the **Time profile** radio button to specify the time interval during which the alarm definition is active. Only the time profile you have defined under the **Rules and Events** node are displayed in the list. If none are defined, only the **Always** option is available.
Event based	If you want the alarm to be based on an event, select this radio button. Once selected, specify the start and stop event. You can select hardware events defined on cameras, video servers and input (see "Events overview" on page *137*). Also global/manual event definitions can be used (see "About user-defined events" on page *155*).

Operator action required:

Name	Description
Time limit	Select a time limit for when operator action is required. The default value is 1 minute. The time limit is not active before you have attached an event in the **Events triggered** drop-down menu.
Events triggered	Select which event to trigger when the time limit has passed.

Additional settings:

Name	Description
Related cameras	Select up to 15 cameras to include in the alarm definition, even if these cameras themselves do not trigger the alarm. This can be relevant, for example, if you have selected an external event message (such as a door being opened) as the source of your alarm. By defining one or more cameras near the door, you can attach the cameras' recordings of the incident to the alarm.

Name	Description
Related map	Assign a map to the alarm when it is listed in the Network Video Management System Smart Client's **Alarm Manager**.
Initial alarm owner	Select a default user responsible for the alarm.
Initial alarm priority	Select a priority (**High**, **Medium**, **Low** or none) for the alarm. Use these priorities in Network Video Management System Smart Client to determine the importance of an alarm.
Initial alarm category	Select an alarm category for the alarm, for example **False alarm** or **Need investigation**.
Events triggered by alarm	Define an event that the alarm can trigger in Network Video Management System Smart Client.
Auto-close alarm	If you want a particular event to automatically stop the alarm, select this check box. Not all events can trigger alarms. Clear the check box to disable the new alarm from the beginning.

See also

Add an alarm (on page 192)

Alarm Data Settings

When you configure alarm data settings, specify the following:

Alarm Data Levels tab

Priorities

Name	Description
Level	Add new priorities with level numbers of your choosing or use/edit the default priority levels (numbers 1, 2 or 3). These priority levels are used to configure the **Initial alarm priority** setting.
Name	Type a name for the entity. You can create as many as you like.
Sound	Select the sound to be associated with the alarm. Use one if the default sounds or add more in **Sound Settings**.

States

Name	Description
Level	In addition to the default state levels (numbers **1**, **4**, **9** and **11**, which cannot be edited or reused), add new states with level numbers of your choosing. These state levels are only visible in the Network Video Management System Smart Client's *Alarm List*.

Categories

Name	Description
Level	Add new categories with level numbers of your choosing. These category levels are used to configure the **Initial alarm category** setting.
Name	Type a name for the entity. You can create as many as you like.

Alarm List Configuration tab

Name	Description
Available columns	Use > to select which columns should be available in the Network Video Management System Smart Client's *Alarm List*. Use < to clear selection. When done, **Selected columns** should contain the items to be included.

Reasons for Closing tab

Name	Description
Enable	Select to enable that all alarms must be assigned a reason for closing before they can be closed.
Reason	Add reasons for closing that the user can choose between when closing alarms. Examples could be *Solved-Trespasser* or *False Alarm*. You can create as many as you like.

Sound Settings

When you configure sound settings, specify the following:

Name	Description
Sounds	Select the sound to associate with the alarm. The list of sounds contain a number of default Windows sounds. You cannot edit these. However, you can add new sounds of the file type .wav, but only if these are encoded in Pulse Code Modulation (PCM). Even if the default sounds are standard Windows sound-files, local Windows settings might cause these to sound different on different machines. Some users might also have deleted one or more of these sound-files and can therefore not play them. To ensure an identical sound all over, you should import and use your own .wav files encoded in PCM.
Add	Add sounds. Browse to the sound to upload one or several .wav files.
Remove	Remove a selected sound from the list of manually added sounds. Default sounds cannot be removed.
Test	Test the sound. In the list, select the sound. The sound plays once.

Options dialog box

In the **Options** dialog box, you can specify a number of settings related to the general appearance and functionality of the system.

To access the dialog box, select **Tools** > **Options**.
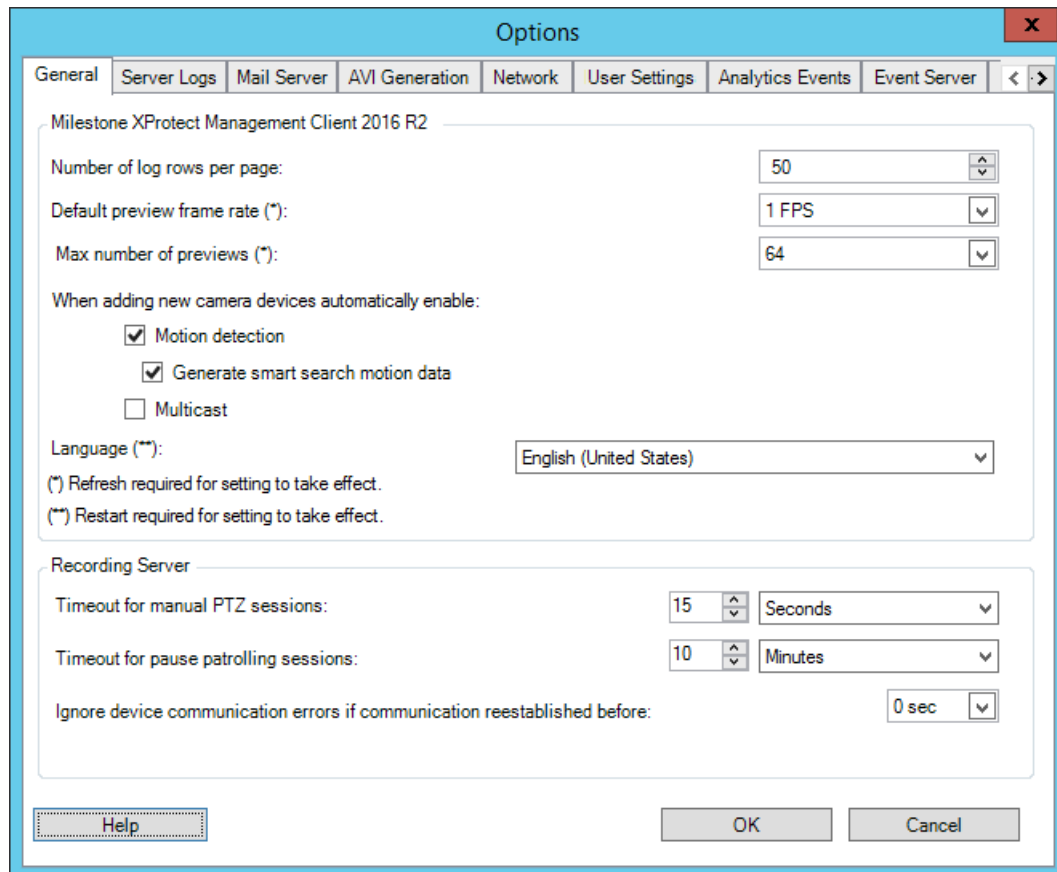
The **Options** dialog box features the following tabs:

- General tab (see "General tab (options)" on page 198)

- Server Logs tab (see "Server Logs tab (options)" on page 199)

- Mail Server tab (see "Mail Server tab (options)" on page 200)

- AVI Generation tab (see "AVI Generation tab (options)" on page 200)

- Network tab (see "Network tab (options)" on page 201)

- User Settings tab (see "User Settings tab (options)" on page 201)

- Analytics Events tab (see "Analytics Events tab (options)" on page 201)

- Event Server tab (see "Event Server tab (options)" on page 202)

- Generic Events tab (see "Generic Events tab (options)" on page 203)

General tab (options)

On the General tab, you can specify general settings for the Management Client and the recording server.

Management Client

Name	Description
Number of log rows per page	Select how many rows a single log page can contain. The default value is 50 rows. If a log contains more rows, it displays the next rows on the following pages.
Default preview frame rate	Select frame rate for the thumbnail camera images displayed in the **Preview** pane. Default is 1 frame per second.
	Select **Action** > **Refresh** from the menu for the change to take effect.
	Note that a high frame rate in combination with a large number of thumbnail images in the **Preview** pane slows down the computer that runs the Management Client. You can limit the number of thumbnail images with the **Max number of previews** setting.
Max number of previews	Select the maximum number of thumbnail images displayed in the **Preview** pane. Default is 64 thumbnail images.
	Select **Action** > **Refresh** from the menu for the change to take effect.
	Note that a large number of thumbnail images in combination with a high frame rate may slow the system down. You can limit the frame rate used for the thumbnail images with the **Default preview frame rate** setting.
When adding new camera devices automatically enable: **Motion detection**	Select the check box to enable motion detection on new cameras, when you add them to the system with the **Add Hardware** wizard.
	This setting does not affect motion detection settings on existing cameras.
	You enable and disable motion detection for a camera on the **Motion** tab for the camera device.
When adding new camera devices automatically enable: **Generate motion data for smart search**	Generation of motion data for smart search requires that motion detection is enabled for the camera.
	Select the check box to enable generation of smart search motion data on new cameras, when you add them to the system with the **Add Hardware** wizard.
	This setting does not affect motion detection settings on existing cameras.
	You enable and disable the generation of smart search motion data for a camera on the **Motion** tab for the camera device.

Name	Description
When adding new camera devices automatically enable: **Multicast**	Select the check box to enable multicast on new cameras when you add them with the **Add Hardware** wizard. This setting does not affect multicast settings on existing cameras. You enable and disable live multicasting for a camera on the **Client** tab for the camera device.
Language	Select the language of the Management Client. Restart the Management Client to use the new language.

Recording server

Name	Description
Timeout for PTZ sessions	Client users with the necessary user rights can manually interrupt the patrolling of PTZ cameras. Select how much time should pass before regular patrolling is resumed after a manual interruption. The setting applies for all PTZ cameras on your system.
Timeout for pause patrolling sessions	Client users with a sufficient PTZ priority can pause patrolling on PTZ cameras. Select how much time should pass before regular patrolling is resumed after a pause. The setting applies for all PTZ cameras on your system. Default setting is 10 minutes. If you want individual timeouts on the cameras, you specify this on the **Presets** tab for the camera.
Ignore device communication errors if communication reestablished before	Select for how long a communication error may exist before the system logs it as an error and triggers the **Communication Error** event.

Server Logs tab (options)

On the **Server Logs** tab, you can specify settings for the system's management server logs.

See also About logs (on page 187) for more information.

Name	Description
Logs	Select the log that you want to configure: • System Log • Audit Log • Rule Log

Name	Description
Settings	Disable/enable the logs and specify the retention period and the maximum number of rows for each log. For **System** logs, specify the level of messages you want to log: • All - includes undefined messages • Information, warnings and errors • Warnings and errors • Errors (default setting) For **Audit** logs, enable user access logging if you want the system to log all user actions in Network Video Management System Smart Client. These are, for example, exports, activating outputs, viewing cameras live or in playback. Specify: • the length of a playback sequence. This means that as long as the user plays back within this period, the system only generates one log entry. When playing back outside the period, the system creates a new log entry. • the number of records (frames) a user has seen before the system creates a log entry.

Mail Server tab (options)

On the **Mail Server** tab, you can specify the settings for your system's outgoing SMTP mail server. See also About notification profiles (on page 152).

Name	Description
Sender e-mail address	Type the e-mail address you want to appear as the sender of e-mail notifications for all notification profiles. Example: sender@organization.org.
Outgoing mail (SMTP) server name	Type the name of the SMTP mail server that sends e-mail notifications. Example: mailserver.organization.org.
Server requires login	Specify a user name and password for the users to log into the mail server.

AVI Generation tab (options)

On the **AVI Generation** tab, you can specify compression settings for the generation of AVI video clip files. The settings are required if you want to include AVI files in e-mail notifications sent by rule-triggered notification profiles.

See also Use rules to trigger email notifications (on page 153).

Name	Description
Compressor	Select the codec (compression/decompression technology) that you want to apply. To have more codecs available in the list, install them on the management server. Not all cameras support all codecs.
Compression quality	(Not available for all codecs). Use the slider to select the degree of compression (**0-100**) to be performed by the codec. **0** means no compression, generally resulting in high image quality and large file size. **100** means maximum compression, generally resulting in low image quality and small file size. If the slider is not available, the compression quality is determined entirely by the selected codec.
Keyframe every	(Not available for all codecs). If you want to use keyframes, select the check box and specify the required number of frames between keyframes. A keyframe is a single frame stored at specified intervals. The keyframe contains the entire view of the camera, whereas the following frames contain only the pixels that change. This helps greatly reduce the size of files. If the check box is not available, or not selected, every frame contains the entire view of the camera.
Data rate	(Not available for all codecs). If you want to use a particular data rate, select the check box and specify the number of kilobytes per second. The data rate specifies the size of the attached AVI file. If the check box is not available, or not selected, the data rate is determined by the selected codec.

Network tab (options)

On the **Network** tab, you can specify the IP addresses of the local clients, if the clients are to connect to the recording server via the Internet. The surveillance system then recognizes them as coming from the local network.

You can also specify the IP version of the system: IPv4 or IPv6. Default value is IPv4.

User Settings tab (options)

On the **User Settings** tab, you can specify user preference settings, for example, if a message should be shown when remote recording is enabled.

Analytics Events tab (options)

On the **Analytics Events** tab, you can enable and specify the analytics events feature.

Name	Description
Enable	Specify if you want to use analytics events. As default, the feature is disabled.
Port	Specify the port used by this feature. The default port is 9090. Make sure that relevant VCA tool providers also use this port number. If you change the port number, remember to change the port number of the providers.
All network addresses or Specified network addresses	Specify if events from all IP addresses/hostnames are allowed, or only events from IP addresses/hostnames that are specified in the **Address list** (see below).
Address list	Specify a list of trusted IP addresses/hostnames. The list filters incoming data so that only events from certain IP addresses/hostnames are allowed. You can use both Domain Name System (DNS), IPv4 and IPv6 address formats. You can add addresses to your list by manually entering each IP address or hostname, or by importing an external list of addresses. • **Manual entering:** Type the IP address/hostname in the address list. Repeat for each required address. • **Import:** Click **Import** to browse for the external list of addresses. The external list must be a .txt file and each IP address or hostname must be on a separate line.

Event Server tab (options)

On the **Event Server** tab, you can specify settings for alarms, events and logs.

Name	Description
Keep closed alarms for	Select the number of days to keep closed alarms. Closed alarms are in the states **Closed**, **Ignore**, and **Reject**.
Keep all other alarms for	Select the number of days to keep all other alarms than alarms in the states **Closed**, **Ignore**, and **Reject**. **Important:** Alarms always have timestamps. If the alarm is triggered by a camera, the timestamp has an image from the time of the alarm. The alarm information itself is stored on the event server, while the video recordings corresponding to the attached image are stored on the relevant surveillance system server. To be able to see the images of your alarms, keep video recordings for at least as long as you intend to keep alarms on the event server.
Keep events for	Specify the number of days for which to keep events.

Name	Description
Keep logs for	Specify the number of days for which to keep the Alarms log. You can define any number up to 99.999 days, server space permitting. You can use the value 0 to keep closed alarms indefinitely, server space permitting.
Log server communication	Select the check box if you want to save a separate log of server communication in addition to the regular log, for the number of days specified.

Generic Events tab (options)

On the **Generic Events** tab, you can specify generic events and data source related settings.

For more information about how to configure actual generic events, see About generic events (on page 159).

Name	Description
Data source	You can choose between two default data sources and define a custom data source. What to choose depends on your third party program and/or the hard- or software you want to interface from: **Compatible:** Factory default settings are enabled, echoes all bytes, TCP and UDP, Ipv4 only, port 1234, no separator, local host only, current code page encoding (ANSI). **International:** Factory default settings are enabled, echoes statistics only, TCP only, Ipv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10). [Data source A] [Data source B] and so on.
New	Click to define a new data source.
Name	Name of the data source.
Enabled	Data sources are by default enabled. Clear the check box to disable the data source.
Reset	Click to reset all settings for the selected data source. The entered name in the **Name** field remains.
Port	The port number of the data source.

Name	Description
Protocol type selector	Protocols which the system should listen for, and analyze, in order to detect generic events: **Any:** TCP as well as UDP. **TCP:** TCP only. **UDP:** UDP only. TCP and UDP packages used for generic events may contain special characters, such as @, #, +, ~, and more.
IP type selector	Selectable IP address types: IPv4, IPv6 or both.
Separator bytes	Select the separator bytes used to separate individual generic event records. Default for data source type **International** (see **Data sources** earlier) is **13,10**. (13,10 = <CR><IF>).

Echo type selector	Available echo return formats:
	
	 • **Echo statistics:** Echoes the following format:
	
	     [X],[Y],[Z],[Name of generic event]
	
	     [X] = request number.
	
	     [Y] = number of characters.
	
	     [Z] = number of matches with a generic event.
	
	     [Name of generic event] = name entered in the **Name:** field.
	
	 • **Echo all bytes:** Echoes all bytes.
	
	 • **No echo:** Suppresses all echoing.

Encoding type selector	By default, the list only shows the most relevant options. Select the **Show all** check box to display all available encodings.
Allowed external IPv4 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.
Allowed external IPv6 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.

Feature configuration

Failover management servers

About multiple management servers (clustering)

The management server can be installed on multiple servers within a cluster of servers. This ensures that the system has very little down-time. If a server in the cluster fails, another server in the cluster automatically takes over the failed server's job running the management server. The automatic process of switching over the server service to run on another server in the cluster only takes a very short time (up to 30 seconds).

It is only possible to have one active management server per surveillance setup, but other management servers may be set up to take over in case of failure.

The allowed number of failovers is limited to two within a six hour period. If exceeded, Management Server services are not automatically started by the clustering service. The number of allowed failovers can be changed to better fit your needs. See Microsoft®'s homepage http://technet.microsoft.com/en-us/library/cc787861%28WS.10%29.aspx for more information.

Prerequisites for clustering

- Two or more servers installed in a cluster:

  - Regarding clusters in Microsoft Windows 2008®, see Failover clusters http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx.

- **Either** an external SQL database installed **outside** the server cluster **or** an **internal** SQL (clustered) service within the server cluster (creating an internal SQL service requires the use of SQL Server Standard or a greater version which is capable of working as a clustered SQL Server).

- A Microsoft® Windows® Server (Enterprise or Data Center edition).

Install in a cluster

Descriptions and illustrations might differ from what your see on your screen.

Installation and change of URL address:

1. Install the management server and all its subcomponents on the first server in the cluster.

   The management server must be installed with a specific user and not as a **network service.** This requires that you use the **Custom** install option. Also, the specific user must have access to the shared network drive and preferably a non-expiry password.

2. After you have installed the management server and the Management Client on the first server in the cluster, open the Management Client, and from the **Tools** menu, select **Registered Services**.

a) In the **Add/Remove Registered Services** window, select **Log Service** in the list, click **Edit**.

b) In the **Edit Registered Service** window, change the URL address of the log service to the URL address of the cluster.
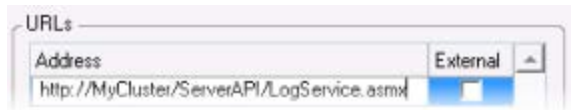
c) Repeat steps a and b for all services listed in the **Add/Remove Registered Services** window. Click **Network**.

d) In the **Network Configuration** window, change the URL address of the server to the URL address of the cluster. (This step only applies to the first server in the cluster.) Click **OK**.
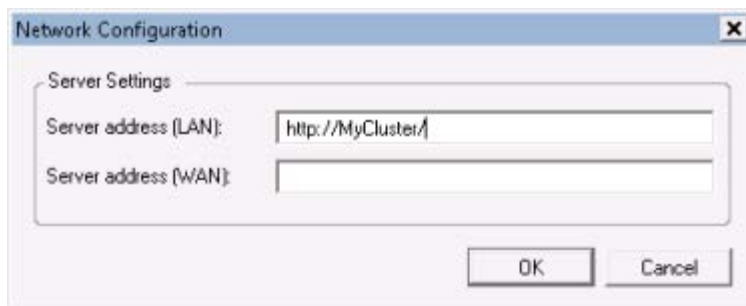
3. In the **Add/Remove Registered Services** window, click **Close**. Exit the Management Client.

4. Stop the management server service and the IIS. Read about how to stop the IIS at Microsoft's® homepage http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx.

5. Repeat steps 1-4 for all subsequent servers in the cluster, this time pointing to the existing SQL database. However, for the **last** server in the cluster on which you install the management server, do not stop the Management Server service.

Next, in order to take effect, the Management Server service must be configured as a generic service in the failover cluster:

1. On the last server on which you have installed the management server, go to **Start** > **Administrative Tools**, open Windows' **Failover Cluster Management**. In the **Failover Cluster Management** window, expand your cluster, right-click **Services and Applications**, and select **Configure a Service or Application**.

2. In the **High Availability** dialog box click **Next**, select **Generic Service** and click **Next**. Do not specify anything on the third page of the dialog box, click **Next**.

3. Select the **Sony Network Video Management System Management Server** service, click **Next**. Specify the name (host name of the cluster) that clients use when accessing the service, click **Next.**

4. No storage is required for the service, click **Next**. No registry settings should be replicated, click **Next.** Verify that the cluster service is configured according to your needs, click **Next**. The management server is now configured as a generic service in the failover cluster. Click **Finish**.

5. In the cluster setup, the event server and the Data Collector should be set as a dependent service of the management server, so the event server stops when the management server is stopped.

6. To add the **Sony Network Video Management System Event Server** service as a resource to the **Sony Network Video Management System Management Server Cluster** service, right-click the cluster service and click **Add a resource** > **4 - Generic Service** and select **Sony Network Video Management System Event Server**.

Upgrade in a cluster

Make sure to have a backup of the database before updating the cluster.

1. Stop the Management Server services on all management servers in the cluster.

2. Uninstall the management server on all servers in the cluster.

3. Use the procedure for installing multiple management servers in a cluster as described for install in a cluster, see Install in a cluster (on page 205).

    Important: When installing, make sure to reuse the existing SQL configuration database (which is automatically upgraded from the old existing database version to the new one).

Network Video Management System Smart Wall

About Network Video Management System Smart Wall

Network Video Management System Smart Wall is an advanced video wall product that provides supreme situation awareness in larger surveillance centers and helps the surveillance operators to focus on what is important ensuring higher efficiency and shorter response times.

Network Video Management System Smart Wall enables swift change of live video displayed on the video wall to meet specific security scenarios and needs. One way to change what is displayed on the video wall is with Smart Wall presets. The surveillance administrator defines the Smart Wall presets in the Management Client for optimizing the surveillance coverage for different recurring surveillance scenarios. Smart Wall presets work for the entire video wall or parts of the video wall and determine which cameras are displayed and the layout of the content on the monitors in the video wall.

With Smart Wall presets, the display changes can be triggered automatically by rules. The display changes can also be triggered manually by the surveillance operators using Network Video Management System Smart Client by dragging and dropping views and cameras onto the logical representation of the video wall in Network Video Management System Smart Client or by selecting the different Smart Wall presets defined by the surveillance administrator.

See the Network Video Management System Smart Client documentation for more information about how to use the Network Video Management System Smart Wall features in Network Video Management System Smart Client.

Network Video Management System Smart Wall requires the following video wall-related licenses:

- A **base license** for Network Video Management System Smart Wall that covers an unlimited number of monitors displaying video on a video wall.

You can purchase a base license for Network Video Management System Smart Wall separately.

Configure Smart Walls

A Smart Wall configuration consists of defining the Smart Wall, adding monitors and defining the monitor layout, and optionally specifying Smart Wall presets and the layout and content of the different monitors.

You need not define Smart Wall presets, if you only want to display cameras and Network Video Management System Smart Client views that your Network Video Management System Smart Client users manually can push onto the video wall.

If you want to use rules to change automatically what is displayed on the video wall and/or if you have typically surveillance scenarios where you want to display the same content on the video wall each time the scenario happens, you should define Smart Wall presets.

The configuration of the Smart Wall is very flexible. You can include all monitors on the video wall in one Smart Wall or group the monitors and configure a Smart Wall for each group. Smart Wall presets can change the layout and content of all monitors in a Smart Wall or only some of the monitors. Monitors can be part of several Smart Walls and Smart Wall presets. Create as many Smart Walls and Smart Wall presets you need to optimize the coverage of your typical surveillance scenarios.

a. Define the Smart Wall

1. Expand **Client**, and select **Smart Wall**.

2. In the **Overview** pane, right-click **Smart Walls** and select **Add Smart Wall**.

3. Specify the settings for the Smart Wall.

4. In the **General View Item Properties** settings, define if you want system status information and title bars to appear above the cameras' layout items.

5. Click **OK**.

b. Add monitors and define the monitor layout

1. Right-click the Smart Wall and select **Add Monitor**.

2. Configure the dimensions of the monitor so it resembles one of the physical monitors on the video wall.

3. Use the preset behavior settings **Empty preset** and **Empty preset item** to define what is displayed on a monitor with an empty preset layout or in a preset's empty preset items when a new Smart Wall preset is automatically triggered or manually selected in Network Video Management System Smart Client. You can use empty presets and empty preset items for content not controlled by the Smart Wall preset.

4. Use the preset behavior setting **Element insertion** to define what should happen when a user of Network Video Management System Smart Client drags a camera onto a layout item in the Smart Wall preset. Select **Independent** to replace the camera already in the preset item with the new camera or **Linked** to push the content of the layout items from left to right from where you inserted the new camera.

5. Add as many monitors as you have on the physical video wall.

6. Select the Smart Wall and on the **Layout** tab, click **Edit** to position the different monitors so their positions resemble the mounting of the physical monitors on the video wall.

7. Click **OK**. The same layout is used in Network Video Management System Smart Client.

c. Add Smart Wall presets (optionally)

1. Select the Smart Wall and from the **Presets** tab, click **Add New**.

2. Enter a name and a description and click **OK**.

3. Click **Activate** to display the Smart Wall preset on the video wall.

4. Create as many Smart Wall presets as you need.

d. Add layout and cameras to the monitors (requires a Smart Wall preset)

1. Select one of the monitors you created and from the **Presets** tab, select a preset from the list to configure what you want the selected monitor to show when used with the selected Smart Wall preset.

2. Click **Edit**.

3. Click the layout button to select which layout to use with your monitor, and click **OK**.

4. Drag cameras from the **Device Groups** or **Recording Servers** tab onto the different layout items. You can leave layout items blank, so they are available for other content not controlled by the Smart Wall preset.

5. If the monitor already has a layout for the selected preset, you can click **Clear** to define a new layout or to exclude the monitor from the Smart Wall preset, so the monitor is available for other content not controlled by the Smart Wall preset.

6. Click **OK**.

7. Repeat the steps, until you have added a layout and cameras on the monitors you want to include in the Smart Wall preset.

Set up user rights for Network Video Management System Smart Wall

You can control the tasks that Network Video Management System Smart Client users can perform in Network Video Management System Smart Wall by specifying user rights for roles. The user rights apply to all users who are assigned to the role. For more information, see Roles with Smart Wall rights properties (see "Smart Wall tab (roles)" on page 178).

Selections for the **Read**, **Edit**, and **Delete** user rights are always applied. For the **Operate** and **Playback** user rights, you can also grant the user rights for a specific period of time by selecting a time profile. For example, this is useful if you want to allow a user to change the content that is displayed on a Smart Wall, but only during their normal working hours.

To specify user rights for a role, follow these steps:

1. In the Site Navigation pane, expand **Security**, and select **Roles**.

2. In the **Roles** pane, select the role, or create a new role by right-clicking in the pane and selecting **Add Role**.

3. In the upper part of the **Role settings** pane, select the Smart Wall.

4. In the lower part of the Role Settings pane, click the **Smart Wall** tab, and then select the user rights to assign.

   - **Read** - View Smart Walls in client applications

   - **Edit** - Modify Smart Walls in client applications

   - **Delete** - Delete Smart Walls in client applications

   - **Operate** - Apply layouts on the selected monitor in client applications, and activate presets

- **Playback** - Review and manage live and recorded video

> **Note:** If you do not select the **Playback** permission, users can view but not change the content that is displayed on the video wall. If a user makes a change, the system automatically disconnects from the shared state and the content on the video wall is not affected. To return to the shared view, click **Reconnect Smart Wall monitor**.

5. Optional: To grant the **Operate** or **Playback** user rights for a specific period of time, select the check box, and then select the time profile.

About using rules with Smart Wall presets

By combining rules and Smart Wall presets, you can control what is displayed on your video wall in similar way as the system uses rules to control the behavior of cameras and more. For example, a rule can trigger your video wall to display a certain Smart Wall preset during a certain day. You can even use rules to control what individual monitors in a video wall display. See Add a rule (on page 146) for information about how to create rules.

Example of a rule triggering a Smart Wall preset.

Smart Wall properties

Info tab (Smart Wall properties)

On the **Info** tab for a Smart Wall, you can add and edit Smart Walls.

Name	Description
Name	The name of the Smart Wall. Displayed in the Network Video Management System Smart Client as the Smart Wall view group name.
Description	A description of the Smart Wall. The description is only used internally in the Management Client.
Status text	If selected, camera and system status information is displayed across cameras' layout items on the video wall.
No title bar	If selected, all Smart Wall layout items have no title bars on the video wall.
Title bar	If selected, all Smart Wall layout items have title bars on the video wall.
Title bar with live indicator	When selected, all Smart Wall layout items' title bars display live and motion indicators on the video wall.

Presets tab (Smart Wall properties)

On the **Presets** tab for a Smart Wall, you can add and edit Smart Wall presets.

Name	Description
Add New	Click to add a preset to your Network Video Management System Smart Wall installation. Define a name and description for the new Smart Wall preset.
Edit	Edit the name and/or description of a Smart Wall preset.
Delete	Delete a Smart Wall preset.
Activate	Click to display the Smart Wall preset on the video wall. You must create rules with the Smart Wall preset before the system can automatically trigger the display of the Smart Wall preset. See also About using rules with Smart Wall presets (on page *211*).

Layout tab (Smart Wall properties)

On the **Layout** tab for a Smart Wall, you position the monitors in your Smart Wall so their positions resemble the mounting of the physical monitors on the video wall. The layout is also used in the Network Video Management System Smart Client.

Name	Description
Edit	Click to adjust the positioning of the monitors.
Movement	To move a monitor to a new position, select the relevant monitor and drag it to the desired position, or click one of the arrow buttons to move the monitor in the selected direction.
Zoom buttons	Click buttons to zoom in/out of the Smart Wall layout preview to ensure you position the monitors correctly.
Name	The name of the monitor. The name is displayed in the Network Video Management System Smart Client.
Size	The size of the physical monitor on the video wall.
Aspect ratio	The height/width relationship of the physical monitor on the video wall.

Monitor properties

Info tab (monitor properties)

On the **Info** tab for a monitor in a Smart Wall preset, you can add monitors and edit the monitors' settings.

Name	Description
Name	The name of the monitor. The name is displayed in the Network Video Management System Smart Client.
Description	A description of the monitor. The description is only used internally in the Management Client.
Size	The size of the physical monitor on the video wall.
Aspect ratio	The height/width relationship of the physical monitor on the video wall.
Empty preset	Defines what should be displayed on a monitor with an empty preset layout when a new Smart Wall preset is triggered or selected in Network Video Management System Smart Client. Select **Preserve** to keep the current content on the monitor. Select **Clear** to clear all content so nothing is displayed on the monitor.
Empty preset item	Defines what should be displayed in an empty preset layout item when a new Smart Wall preset is triggered or selected in Network Video Management System Smart Client. Select **Preserve** to keep the current content in the layout item. Select **Clear** to clear the content so nothing is displayed in the layout item.
Element insertion	Defines how cameras are inserted in the monitor's layout when viewed in the Network Video Management System Smart Client. When selecting **Independent**, only the content of the affected layout item changes, the rest of the content in the layout remain the same. When selecting **Linked**, the contents of the layout items are pushed from left to right. If, for instance, a camera is inserted in position 1, the previous camera of position 1 is pushed to position 2, the previous camera of position 2 is pushed to position 3, and so on as illustrated in this example. Before a new camera is inserted and after.

Presets tab (monitor properties)

On the **Presets** tab for a monitor in a Smart Wall preset, you can edit the layout and content of the monitor in the selected Smart Wall preset.

Name	Description
Preset	A list of Smart Wall presets for the select Smart Wall.
Edit	Click **Edit** to edit the layout and the content of the selected monitor.
	Double-click a camera to remove a single camera.
	Click **Clear** to define a new layout or to exclude the monitor in the Smart Wall preset so the monitor is available for other content not controlled by the Smart Wall preset.
	Click ⬚ to select the layout you want to use with your monitor in the selected preset, and click **OK**.
	Drag cameras from the **Device Groups** or **Recording Servers** tab onto the different layout items. You can leave layout items empty, so they are available for other content not controlled by the Smart Wall preset.

NVMS Mobile

NVMS Mobile introduction

About NVMS Mobile

NVMS Mobile consists of three components:

- **NVMS Mobile client**

- **NVMS Mobile server**

- **NVMS Mobile plug-in**

The NVMS Mobile client is a mobile surveillance app that you can install and use on your Android device or Apple device. You can use as many installations of NVMS Mobile client as you need.

For more information, download the NVMS Mobile client User Guide from the Sony Corporation website http://www.sony.net/CameraSystem/NVMS/Manuals.

The NVMS Mobile server and NVMS Mobile plug-in are covered in this manual.

Prerequisites for using NVMS Mobile

Before you can start using NVMS Mobile, you must make sure that you have the following:

- A running VMS installed and configured with at least one user.

- Cameras and views set up in Network Video Management System Smart Client.

- A mobile device running Android or iOS with access to Google Play or App Store[SM] from which you can download the NVMS Mobile client application.

NVMS Mobile configuration

About NVMS Mobile server

NVMS Mobile server handles log-ins to the system from NVMS Mobile client from a mobile device or Network Video Management System Web Client.

A NVMS Mobile server distributes video streams from recording servers to NVMS Mobile clients. This offers a secure setup where recording servers are never connected to the Internet. When a NVMS Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

You must install NVMS Mobile server on any computer from which you want to access recording servers. When you install NVMS Mobile server, make sure you log in using an account that has administrator rights. Otherwise, installation will not complete successfully.

Add or edit a Mobile server

1. Go to **Servers** > **Mobile Servers**. From the menu that appears, select **Create New**. Enter or edit the settings.

Important: If you edit settings for **Login method**, **All cameras view**, and **Outputs and events** while you or others are connected to the NVMS Mobile client, you must restart the NVMS Mobile client for the new settings to take effect.

Set up investigations

Set up investigations so that people can use Web Client and NVMS Mobile to access recorded video and investigate incidents, and prepare and download video evidence.

To set up investigations, follow these steps:

1. In Management Client, click the mobile server, and then click the **Investigations** tab.

2. Select the **Enabled** check box. By default, the check box is selected.

3. In the **Investigations folder** field, specify where to store video for investigations.

4. In the **Limit size of investigations to** field, enter the maximum number of megabytes that the investigation folder can contain.

5. Optional: To allow users to access investigations that other users create, select the **View investigations made by others** check box. If you do not select this check box, users can see only their own investigations.

6. Optional: To include the date and time that a video was downloaded, select the **Include timestamps for AVI exports** check box.

7. In the **Used codec for AVI exports** field, select the compression format to use when preparing AVI packages for download.

   Note: The codecs in the list can differ, depending on your operating system. If you do not see the codec you want to use, you can install it on the computer where Management Client is running and it will display in this list.

> Additionally, codecs can use different compression rates, which can affect video quality. Higher compression rates reduce storage requirements but can also reduce quality. Lower compression rates require more storage and network capacity, but can increase quality. It's a good idea to research the codecs before you select one.

8. In the **Failed export data (for MKV and AVI export)** field, specify whether to keep the data that was successfully downloaded, although it can be incomplete, or delete it.

9. To enable users to save investigations, you must grant the following permissions to the security role assigned to the users:

   - In Network Video Management System Enterprise Edition products, grant the **Export** permission.

   - In Network Video Management System Standard Edition products, grant the **Database** permission.

Clean up investigations

If you have investigations or video exports that you no longer need to keep, you can delete them. For example, this can be useful if you want to make more disk space available on the server.

- To delete an investigation, and all of the video exports that were created for it, select the investigation in the list, and then click **Delete**.

- To delete individual video files that were exported for an investigation, but keeping the investigation, select the investigation in the list. In the **Investigation details** group, click the **Delete** icon to the right of the **Database**, **AVI**, or **MKV** fields for exports.

About using Video Push to stream video

You can set up Video Push so that users can keep others informed about a situation, or record video to investigate it later, by streaming video from their mobile device's camera to your Network Video Management System surveillance system.

Set up Video Push to stream video

To let users stream video from their mobile devices to an Network Video Management System surveillance system, set up Video Push on a NVMS Mobile server.

In Management Client, perform these steps in the following order:

1. Set up a channel that the mobile device can use to stream video to the recording server.

2. Add the Video Push Driver as a hardware device on the recording server. The driver simulates a camera device so that you can stream video to the recording server.

3. Assign the Video Push Driver device to the channel.

This topic describes each of these steps.

Set up a channel for streaming video

Note: Each channel requires a hardware device license.

To add a channel, follow these steps:

1. In the navigation pane, select **Mobile Server**, and select the mobile server.

2. On the **Video Push** tab, select the **Video Push** check box.

3. In the bottom right corner, click **Add** to add a video push channel under **Channels mapping**.

4. Enter the user name of the user account that will use the channel. This user account must be allowed to access the NVMS Mobile server and recording server.

   Note: To use Video Push, users must log in to NVMS Mobile on their mobile device using the user name and password for this account.

5. Make a note of the port number. You will need it when you add the Video Push driver as a hardware device on the recording server.

6. Click **OK** to close the Video Push Channel dialog box and the save the channel.

Add the Video Push Driver as a hardware device on the recording server

1. In the navigation pane, click **Recording Servers**.

2. Right-click the server that you want to stream video to, and click **Add Hardware** to open the **Add Hardware** wizard.

3. Select **Manual** as the hardware detection method, and click **Next**.

4. Enter credentials for the camera, as follows:

   - To use the factory default credentials from the camera factory, click **Next**. Typically, factory settings are used.

   - If you have changed the credentials on the device, enter that information, and then click **Next**.

   Note: These are the credentials for the hardware, not for the user. They are not related to the user name for the channel.

5. In the list of drivers, expand **Other**, select the **Video Push Driver** check box, and then click **Next**.

   Note: The system generates a MAC address for the Video Push Driver device. We recommend that you use this address. Change it only if you experience problems with the Video Push Driver device. For example, if you need to add a new address and port number.

6. In the **Address** field, enter the IP address of the computer where NVMS Mobile server is installed.

7. In the **Port** field, enter the port number for the channel you created for streaming video. The port number was assigned when you created the channel.

8. In the **Hardware model** column, select **Video Push Driver**, and then click **Next**.

9. When the system detects the new hardware, click **Next**.

10. In the **Hardware name template** field, specify whether to display either the model of the hardware and the IP address, or the model only.

11. Specify whether to enable related devices by selecting the **Enabled** check box. You can add related devices to the list for **Video Push Driver**, even though they are not enabled. You can enable them later.

> **Note:** If you want to use location information when you stream video, you must enable the **Metadata** port.

12. Select the default groups for the related devices on the left, or select a specific group in the **Add to Group** field. Adding devices to a group can make it easier to apply settings to all devices at the same time or replace devices.

Add the Video Push Driver device to the channel for video push

1. In the **Site navigation** pane, click **Mobile Servers**, and then click the **Video Push** tab.

2. Click **Find Cameras**. If successful, the name of the Video Push Driver camera displays in the Camera Name field.

3. Save your configuration.

Remove a channel that you don't need

You can remove channels that you no longer use.

- Select the channel to remove, and then click **Remove** in the lower right corner.

About actions

You can manage the availability of the **Actions** tab in the NVMS Mobile client by enabling or disabling this on the Mobile server tab. **Actions** are by default enabled, and all available actions for the connected devices are shown here.

About naming an output for use in NVMS Mobile

In order to get actions shown correctly together with current camera, it is important that the output uses the exact same name as the camera.

Example:

If you have a camera named "AXIS P3301,P3304 - 10.100.50.110 - Camera 1", you must also name the action "AXIS P3301,P3304 - 10.100.50.110 - Camera 1".

You can add a further description to the title afterwards, for example "AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch".

Important: If you do not follow these naming conventions, actions are not available in the action list for the associated camera's view. Instead, actions appear in the list of other actions on the **Actions** tab.

Add an automatic export rule

1. In the Management Client, click the relevant Mobile server **> Export** Tab.

2. Under **Automatic Exports**, click **Add** to open the **Auto Export Rule** window**.**

3. Set the relevant Auto Export Rule window settings.

4. When finished, click **OK**.

Mobile server settings

General

The following table describes the settings on this tab.

Name	Description
Server name	Enter a name of the NVMS Mobile server.
Description	Enter an optional description of the NVMS Mobile server.
Mobile server	Choose between all NVMS Mobile servers currently installed to the specific system. Only NVMS Mobile servers that are running are shown in the list.
Login method	Select the authentication method to use when users log in to the server. You can choose between the following options: **Automatic**, **Windows authentication,** or **Basic authentication**.
Enable Network Video Management System Web Client	Enable access to Network Video Management System Web Client.
Enable all cameras view	Include the **All Cameras** view. This view displays all of the cameras that a user is allowed to view on a recording server.
Enable actions (outputs and events)	Enable access to actions in NVMS Mobile clients.
Enable keyframes	Stream only keyframes when streaming video. This uses less bandwidth.
Enable full-size images	Enable the NVMS Mobile server to send full-size images to the NVMS Mobile client or Network Video Management System Web Client. Note that enabling full-size images uses more bandwidth. Additionally, enabling this option disables all rules set up in the **Performance** settings.
Enable direct streaming	Choose how to handle direct streaming in Network Video Management System Web Client. Choose between enforcing the use of direct streaming, enforcing it when possible, or never enforcing it.
Enabled	Enable/disable logging of NVMS Mobile client's actions in a separate log file.
Log file location	Path to where log files are saved.
Keep logs for	Number of days to keep logs for (default three days).
Configuration backup	Import or export your NVMS Mobile server configuration. Your system stores the configuration in an XML file.

Connectivity

In the **General** section, specify the following settings.

Name	Description
Connection type	Choose how clients should connect to the NVMS Mobile server. You can choose between the following options: **HTTP only**, **HTTP and HTTPS** or **HTTPS Only**.
	Note: If you select **HTTPS Only**, devices running iOS 9.0 or later, can connect only if you have a certificate from a certificate authority (CA) installed on your NVMS Mobile server. CAs issue digital certificates that verify the identities of users and websites that exchange data on the Internet. Examples of CAs are companies like Comodo, Symantec, and GoDaddy. Before you turn on secure connections, make sure that you are familiar with digital certificates. To learn how to add a certificate in NVMS Mobile server, see Edit certificate (on page *227*).
Client timeout (HTTP)	Set a time frame for how often the NVMS Mobile client must indicate to the Mobile server that it is up and running. The default value is 30 seconds.
	Sony recommends that you do **not** increase the time frame.

Settings in the **Internet Access** section are used in the following tasks:

- Configure connection settings.

- Send an email message to help users connect their mobile device to NVMS Mobile servers.

- Enable connections to NVMS Mobile servers on a complex network.

Server Status

See the status details for your Mobile server. The details are read-only:

Name	Description
Server active since	Shows how long the Mobile server has been running since it was last stopped.
CPU usage	Shows current CPU usage on the Mobile server.
Internal bandwidth	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
External bandwidth	Shows the current bandwidth in use between the mobile device and Mobile server.
User Name column	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
State column	Shows the current relation between the Mobile server and the NVMS Mobile client user in question. Is the user connected (a state preliminary to servers exchanging keys and encrypting credentials) or is he/she actually logged in? Possible states are: **Connected** and **Logged In** Network Video Management System.

Name	Description
Bandwidth Usage column	Shows the level of bandwidth used by the Mobile server client user in question.
Live Streams column	Shows the number of live video streams currently open for the NVMS Mobile client user in question.
Playback Streams column	Shows the number of playback video streams currently open for the relevant mobile client user.
Video Push streams	Shows the number of Video Push stream currently open for the relevant mobile client user.
Direct Streams	Shows the number of live video streams using Direct Streaming that are currently open for the relevant mobile user.

Video Push

You can specify the following settings if you enable Video push:

Name	Description
Video push	Enable Video push on the Mobile server.
Number of channels	Specify the number of enabled Video push channels in your Network Video Management System.
Channel column	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video push channel.
MAC	MAC address for the relevant Video push channel.
User Name	Enter the user name associated with the relevant video push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see "Set up Video Push to stream video" on page 217), click **Find Cameras** to search for the relevant camera.

Investigations

You can enable investigations so that people can use Network Video Management System Web Client and NVMS Mobile to access recorded video and investigate incidents, and prepare and download video evidence.

The following table describes the settings for investigations.

Name	Description
Investigations folder	Specify where to store video for investigations.
Limit size of investigations to	Enter the maximum number of megabytes that the investigations folder can contain.

Name	Description
View investigations made by others	Select this check box to allow users to access investigations that they did not create.
Include timestamps for AVI exports	Select this check box to include the date and time that the AVI file was downloaded.
Used codec for AVI exports	Select the compression format to use when preparing AVI packages for download. The codecs you can choose from can differ, depending on your operating system. If you do not see the codec you want, you can add it to the list by installing it on the computer where the NVMS Mobile server is running.
Failed export data (for MKV and AVI export)	Select whether to keep the data that was not successfully prepared for download in an investigation, or delete it.

Performance

On the **Performance** tab, you can set the following limitations on the NVMS Mobile server's performance:

Level 1

Level 1 is the default limitation placed on the NVMS Mobile server. Any limitations you set here are always applied to the NVMS Mobile's video stream.

Name	Description
Level 1	Select the check box to enable the first level of limitations to NVMS Mobile server performance.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the NVMS Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the NVMS Mobile server to clients.

Level 2

If you would rather like to enforce a different level of limitations that the default one in **Level 1**, you can select the **Level 2** check box instead. You cannot set any settings higher than what you have set them to in the first level. If you, for example, set the Max FPS to 45 on **Level 1**, you can set the Max FPS on **Level 2** only to 44 or below.

Name	Description
Level 2	Select the check box to enable the second level of limitations to NVMS Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the NVMS Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the NVMS Mobile server before the system enforces video stream limitations.

Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the NVMS Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the NVMS Mobile server to clients.

Level 3

You can also select a **Level 3** check box to create a third level for limitations. You cannot set any settings higher than what you have set them to in **Level 1** and **Level 2**. If you, for example, set the **Max FPS** to 45 on **Level 1** and to level 32 on **Level 2**, you can set the **Max FPS** on **Level 3** only to 31 or below.

Name	Description
Level 3	Select the check box to enable the second level of limitations to NVMS Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the NVMS Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the NVMS Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the frames per second (FPS) to send from the NVMS Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the NVMS Mobile server to clients.

The system does not instantly switch from one level to another level. If your CPU or bandwidth threshold goes less than five percent above or below the indicated levels, the current level stays in use.

Note that if you enable **Enable full-size images** on the **General** tab, none of the **Performance** levels are applied.

Log Settings

Fill in and specify the following log settings:

Name	Description
Enabled	Enable/disable logging of NVMS Mobile client's actions in a separate log file.
Log file location	Path to where log files are saved.
Keep logs for	Number of days to keep logs for (default three days).
CPU usage	Default level of CPU usage which will trigger a warning in the log.
Internal bandwidth	Default internal bandwidth usage which will trigger a warning in the log.

External bandwidth	Default external bandwidth usage which will trigger a warning in the log.
Check every	Default time frame (30 sec.) for checking warning levels.

Mobile Server Manager

About Mobile Server Manager

The Mobile Server Manager is a tray-controlled feature connected to the Mobile server. Right-clicking the Mobile Server Manager icon in the system tray opens a menu from which you can easily access Mobile server functionality.

You can:

- Open Network Video Management System Web Client (see "Access Network Video Management System Web Client" on page 226)

- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 229)

- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 228)

- Show/edit port numbers (on page 229)

- Edit certificate (on page 227)

- Open today's log file (see "About accessing logs and exports" on page 227)

- Open log folder (see "About accessing logs and exports" on page 227)

- Open export folder (see "About accessing logs and exports" on page 227)

- Show Mobile server status (see "About show status" on page 227)

Access Network Video Management System Web Client

If you have a NVMS Mobile server installed on your computer, you can use the Network Video Management System Web Client to access your cameras and views. Because you do not need to install Network Video Management System Web Client, you can access it from the computer where you installed the NVMS Mobile server, or any other computer you want to use for this purpose.

1. Set up the NVMS Mobile server in the Management Client.

2. If you are using the computer where NVMS Mobile server is installed, you can right-click the NVMS Mobile Server icon in the system tray, and select **Open Network Video Management System Web Client**.

3. If you are not using the computer where NVMS Mobile server is installed, you can access it from a browser. Continue with step 4 in this process.

4. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome or Safari).

5. Type the external IP address, that is, the external address and port of the server on which the NVMS Mobile server is running.

   Example: The NVMS Mobile server is installed on a server with the IP address 127.2.3.4 and is configured to accept HTTP connections on port 8081 and HTTPS connections on port 8082 (default settings of the installer).

In the address bar of your browser, type: http://1.2.3.4:8081 or https://1.2.3.4:8082, depending on whether you want to use a standard HTTP connection or a secure HTTPS connection. You can now begin using Network Video Management System Web Client.

6. Add the address as a bookmark in your browser for easy future access to Network Video Management System Web Client. If you use Network Video Management System Web Client on the local computer on which you installed the NVMS Mobile server, you can also use the desktop shortcut which the installer creates. Click the shortcut to launch your default browser and open Network Video Management System Web Client.

You must clear the cache of Internet browsers running the Network Video Management System Web Client before you can use a new version of the Network Video Management System Web Client. System administrators must ask their Network Video Management System Web Client users to clear their browser cache after upgrading, or force this action remotely (you can do this action only in Internet Explorer in a domain).

About show status

Right-click the Mobile Server Manager icon and select **Show Status** or double-click the Mobile Server Manager icon to open a window that shows the status of the Mobile server. You can see the following information:

Name	Description
Server running since	Time and date of the time when the Mobile server was last started.
Connected users	Number of users currently connected to the Mobile server.
Hardware decoding	Indicates if hardware accelerated decoding is in action on the Mobile server.
CPU usage	How many % of the CPU is currently being used by the Mobile server.
CPU usage history	A graph detailing the history of CPU usage by the Mobile server.

About accessing logs and exports

The Mobile Server Manager lets you quickly access the log file of the day, open the folder to which logs files are saved, and open the folder to which exports are saved.

To open any one of these, right-click the Mobile Server Manager and select **Open Today's Log File**, **Open Log Folder** or **Open Export Folder** respectively**.**

Important: If you uninstall NVMS Mobile from your system, its log files are not deleted. Administrators with proper rights can access these log files at a later timer, or decide to delete them if they are not needed any longer. The default location of the log files is in the ProgramData folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Edit certificate

If you want to use a secure HTTPS protocol to establish connection between a NVMS Mobile server and your mobile device or the Network Video Management System Web Client, you must have a valid certificate for the device or web browser to accept the connection. The certificate confirms that the certificate holder is authorized to establish the connection.

When you install NVMS Mobile server, you generate a self-signed certificate if you run a **Typical** installation. If you run a **Custom** installation, you can choose between generating a self-signed certificate or loading a file that contains a certificate issued by another trusted site.

Note: If you want to use secure connections (HTTPS), devices running iOS 9.0 or later, can connect only if you have a certificate from a certificate authority (CA) installed on your NVMS Mobile server. CAs issue digital certificates that verify the identities of users and websites that exchange data on the Internet. Examples of CAs are companies like Comodo, Symantec, and GoDaddy. Before you turn on secure connections, make sure that you are familiar with digital certificates.

If you want use a different certificate, you can do the following.

1. On a computer where Management Client are installed, right-click the **NVMS Mobile Server** icon and select **Edit Certificate...**

2. Choose one of the following:

   - Generate a self-signed certificate

   - Load a certificate file

Generate a self-signed certificate

1. Choose the **Generate a self-signed certificate** option and click **OK**.

2. Wait for a few seconds while the system installs the certificate.

3. When finished, a window opens and informs you that the certificate was installed successfully. The Mobile service restarts to apply the change.

Locate a certificate file

1. Choose the **Load a certificate file** option.

2. Fill in the path for the certificate file or click the ... box to open a window where you can browse for the file.

3. Fill in the password connected to the certificate file.

4. When finished, click **OK**.

Fill in/edit surveillance server credentials

1. Right-click the Mobile Server Manager and select **Surveillance Server Credentials**.

2. Fill in the **Server URL**.

3. Select what user you want to log in as:

   - Local system administrator (no credentials needed) or

   - A specified user account (credentials needed).

4. If you have chosen a specified user account, fill in **User Name** and **Password**.

5. When finished, click **OK**.

Show/edit port numbers

1. Right-click the **Mobile Server Manager** and select **Show/Edit Port Numbers**.

2. To edit the port numbers, type the relevant port number. You can indicate a standard port number (for HTTP connections) and/or a secured port number (for HTTPS connections).

3. When you are done, click **OK**.

Start, stop and restart Mobile service

If needed, you can start, stop and restart the Mobile service from the Mobile Server Manager.

- To perform any of these tasks, right-click the **Mobile Server Manager** and select **Start Mobile service**, **Stop Mobile service** or **Restart Mobile service** respectively**.**

Frequently asked questions (FAQs)

1. **Why can't I connect from my NVMS Mobile client to my recordings/NVMS Mobile server?**

   In order to connect to your recordings, the NVMS Mobile server must be installed on the server that runs your Network Video Management System or alternatively on a dedicated server. The relevant NVMS Mobile settings are also needed in your Network Video Management System video management setup. These are installed as either plug-ins or as part of a product installation or upgrade. For details on how to get the NVMS Mobile server and how to integrate the NVMS Mobile client-related settings in your Network Video Management System, see the configuration section (see "NVMS Mobile configuration" on page 216).

2. **I installed the NVMS Mobile server to Network Video Management System Enterprise Edition, but I can't connect to the server from my device. What is the problem?**

   After you have installed the NVMS Mobile server to your Network Video Management System Enterprise Edition (4.0+), you must install the NVMS Mobile plug-in to see the NVMS Mobile server in your Network Video Management System Enterprise Edition setup (see "Install NVMS Mobile server" on page 40). When you have installed the NVMS Mobile plug-in, locate the plug-in under **Servers** > **Mobile Servers** and right-click to add a new mobile server. Here, you add the details about your NVMS Mobile server (Server name, Description (optional), Server Address, Port and more). Once you finish, restart the NVMS Mobile Service (from Windows Services) and try to reconnect with your device.

3. **How do I add a NVMS Mobile server/location/site to my NVMS Mobile client?**

   You do this from the NVMS Mobile client. When you open it for the first time, you must add one or more mobile servers in order to retrieve video from your cameras. Your added NVMS Mobile servers will be listed alphabetically. You can add as many NVMS Mobile servers as needed, as long as you have the needed log-in credentials.

4. **Why is the image quality sometimes poor when I view video in the NVMS Mobile client?**

   The NVMS Mobile server automatically adjusts image quality according to the available bandwidth between the server and client. If you experience lower image quality than in the Network Video Management System Smart Client, you might have too little bandwidth to get full resolution images through the NVMS Mobile client. The reason for this can either be

too little upstream bandwidth from the server or too little downstream bandwidth on the client. See the **Network Video Management System Smart Client User Manual** which you can download from our website http://www.sony.net/CameraSystem/NVMS/Manuals.

If you are in an area with mixed wireless bandwidth, you may notice that the image quality improves when you enter an area with better bandwidth.

5. **How do I create views?**

You cannot create or configure views in the NVMS Mobile client. It uses views and related names already created in the Network Video Management System Smart Client. If you do not have any views set up, you can use the **All cameras** view to see all the cameras in your system. You can always add more views to the Network Video Management System Smart Client at a later time.

6. **How do I add a new NVMS Mobile user?**

A NVMS Mobile user is just like any other Network Video Management System user. You add a new NVMS Mobile user the same way you normally add a new user in your Management Client: right-click on **Users** in the Navigation Pane and select **Add new basic user** or **Add new Windows user**. If you select new basic user, you must change the server login method to **Automatic** or **Basic Only** depending on your system. You change your server login method from the **Login method** drop-down menu on the **General** tab of the Mobile Server entry under **Servers** > **Mobile Servers** in the Management Client.

7. **Can I control my pant-tilt-zoom (PTZ) cameras and use presets from NVMS Mobile client?**

Yes, in the NVMS Mobile client, you can control your connected PTZ cameras and use presets in live mode.

8. **How can I navigate my recordings?**

Android: You can navigate through your recordings in playback mode. Select the camera you wish to view in playback mode and choose **Menu** > **Playback**. Once you are in playback mode you can search through your recordings using the control buttons. You also have the option to go to a specific time by choosing **Menu** > **Go to time**. Once you have chosen **Go To time**, select the date and time you want to view.

iOS: You can navigate through your recordings in playback mode. Select the camera you wish to view in playback mode and tap Playback. Once you are in playback mode, you can search through your recordings using the control buttons. You also have the option to go to a specific time by choosing **Menu** > **Go to time**. Once you have chosen **Go to time**, select the date and time you want to view and click **Confirm**.

9. **Can I view live and recorded video at the same time?**

Yes, in playback mode, you get a small picture-in-picture (PiP) view live from the same camera.

10. **Can I use the NVMS Mobile client without a 3G data plan?**

Yes, you can use NVMS Mobile through Wi-Fi. Either locally on the same network as your Network Video Management System or at a different location, such as a public network in a café or a home network. Note that bandwidth on public networks vary and may affect the image quality of the video streams.

11. **Can I use the NVMS Mobile client with a 4G/LTE data plan?**

Yes, you can use any data connection on your mobile device that allows you to access the internet to connect to your Network Video Management System video management system.

12. **Can I add multiple servers to the NVMS Mobile client?**

   When you open the NVMS Mobile client for the first time, you must add one or more mobile servers in order to retrieve video from your cameras. These mobile servers are listed alphabetically. If you want to retrieve video from additional servers, repeat this process. You can add as many mobile servers as needed, as long as you have the relevant log-in credentials.

13. **Why is the image quality poor when I connect to my Network Video Management System video management system at home through Wi-Fi at my office?**

   Check your home internet bandwidth. Many private internet connections have different download and upload bandwidths often described as, for example, 20 Mbit/2 Mbit. This is because home users rarely need to upload large amounts of data to the internet, but consume a lot of data instead. The Network Video Management System video management system needs to send video to the NVMS Mobile client and is limited by your connection's upload speed. If low image quality is consistent on multiple locations where the download speed of the NVMS Mobile client's network is good, the problem might be solved by upgrading the upload speed of your home internet connection.

14. **Where are my screenshots saved?**

   Android: Snapshots are saved to your device's SD card at: **/mnt/sdcard/Network Video Management System**.

   iOS: Snapshots are saved to your device and can be accessed from **Photos** on your device.

   You cannot change the default settings on neither Android nor iOS.

15. **How do I avoid the security warning when I run Network Video Management System Web Client through an HTTPS connection?**

   The warning appears because the server address information in the certificate is incorrect. The connection will still be encrypted.
   The self-signed certificate in the NVMS Mobile server needs to be replaced with your own certificate matching the server address used to connect to the NVMS Mobile server. These certificates are obtained through official certificate signing authorities such as Verisign. Consult the chosen signing authority for more details.
   NVMS Mobile server does not use Microsoft IIS. This means that instructions provided for generating certificate signing request (CSR) files by the signing authority using the IIS is not applicable for the NVMS Mobile server. You must manually create CSR-file using command line certificate tools or other similar third-party application. Note that this process should be performed by system administrators and advanced users only.

16. **Does my processor support hardware-accelerated decoding?**

   Only newer processors from Intel support hardware accelerated decoding. Check Intel website
   http://ark.intel.com/search/advanced?s=t&MarketSegment=DT&QuickSyncVideo=true if your processor is supported.

   In the menu, make sure **Technologies** > **Intel Quick Sync Video** is set to **Yes**.

   If your processor is supported, hardware-accelerated decoding is enabled by default. You can see the current status in **Show status** in the Mobile Server Manager (see "About show status" on page 227).

17. **Does my operating system support hardware-accelerated decoding?**

   Only Windows 8 and Windows Server 2012 or newer are supported.

Make sure you install the newest graphic drivers from the Intel website on your system. These drivers are not available from Windows Update.

Hardware-accelerated decoding is not supported, if the mobile server is installed in a virtual environment.

18. **How do I disable hardware-accelerated decoding on the mobile server? (Advanced)**

If the processor on the mobile server supports hardware accelerated decoding, it is by default enabled. To turn hardware-accelerated decoding off, do the following:

1. Locate the file VideoOS.MobileServer.Service.exe.config. The path is typically: C:\Program Files\Sony\NVMS Mobile Server\VideoOS.MobileServer.Service.exe.config.

2. Open the file in Notepad or a similar text editor. If necessary, associate the file type .config with Notepad.

3. Locate the field <add key="HardwareDecodingMode" value="Auto" />.

4. Replace the value "Auto" with "Off".

5. Save and close the file.

19. **I just turned on my firewall, and now I can't connect a mobile device to my server. Why not?**

If your firewall was turned off while you installed NVMS Mobile server, you must manually enable TCP and UDP communications.

Multi-domain with one-way trust

Setup with one-way trust

If you run your system in a multi-domain environment, you can configure this setup with one-way trust. The system is installed on the **trusting** domain and users log in from **trusting** and **trusted** domains.

1. Create a service account in the **trusted** domain. You can name it whatever you want, for example, **svcSony**.

2. Add the new service account to the following local Windows user groups on the server running the system, in the **trusting** domain:

   - Administrators

   - IIS_IUSRS (Windows Server 2008, necessary for Internet Information Services (IIS) Application Pools)

   - IIS_WPG (Windows Server 2003, necessary for IIS Application Pools).

3. Make sure that the service account has system administrator rights on your SQL Database or SQL Server Express, either directly or through the **BUILTIN\Administrators** group.

4. Set the identity of the **ManagementServerAppPool** Application Pool in the IIS to the service account.

5. Reboot the server to make sure that all group membership and permission changes take effect.

Important: To add **trusted** domain users to new or existing Network Video Management System roles, log in to Windows as a **trusted** domain user. Next, launch the Management Client and log in as user of either the **trusting** domain or the **trusted** domain. If you log in to Windows as a **trusting** domain user, you are asked for credentials for the **trusted** domain in order to browse for users.
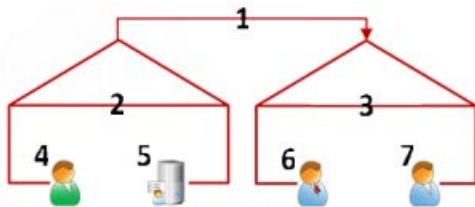
Example illustration of multi-domain environments with one-way trust.

Legend:

1. One-way outgoing domain trust
2. MyDomain.local
3. OtherDomain.edu
4. Trusting domain user
5. Management server
6. Sony service account
7. Trusted domain user

SNMP

About SNMP support

Your system supports Simple Network Management Protocol (SNMP), a standard protocol for monitoring and controlling network devices, for managing their configuration, collecting statistics and more.

The system acts as an SNMP agent, which can generate an SNMP trap as a result of a triggered rule. A third-party SNMP management console can then receive information about the rule-triggering event, and operators of the SNMP management console can configure their system for further action as required.

The implementation uses Microsoft® Windows® SNMP Service for triggering SNMP traps. This means that you must install the SNMP Service on recording servers. When you have configured the SNMP Service through its own user interface, this enables recording servers to send .mib (Management Information Base) files to the SNMP management console.

Install SNMP service

1. On the relevant recording servers, open Windows' **Programs and Features** functionality.

2. In the left side of the **Programs and Features** dialog box, click **Turn Windows functionality on or off**. This opens the **Windows feature** window.

3. In the dialog box, select the check box next to **Simple Network Management Protocol (SNMP)** and click **OK**.

Configure SNMP service

1. On the required recording servers, select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

2. Double-click the SNMP Service.

3. Select the **Traps** tab.

4. Specify a community name, and click **Add to list**.

5. Select the **Destinations** tab.

6. Click **Add**, and specify the IP address or host name of the server running your third-party SNMP management station software.

7. Click **OK**.

System maintenance

Ports used by the system

If nothing else is mentioned, the ports are both inbound and outbound. The port numbers are the default numbers. You can change the port numbers if needed. Contact Sony Support, if you need to change ports that are not configurable through the Management Client.

Port number	Protocol	Used by	Purpose
25	SMTP	Recording servers	Listening for messages from devices to activate events and for receiving images pre and post recording. The port is disabled per default.
80	HTTP	The IIS on the management server	Running the Management Server service.
443	HTTPS	Management server and service channel	Authentication of basic users.
554	RTSP	Recording servers	Traffic that controls streaming from cameras.
1024 and higher (except the ports mentioned below)	HTTP	Recording servers	Outbound only. Traffic between cameras and servers.
1234	TCP/UDP	Event Server	Listening for generic events from external systems or devices.
1235	TCP	Event Server	Listening for generic events from external systems or devices.
1433	TCP	All processes in the system (among others management server, log server and event server)	Communication with the SQL Server.
5432	TCP	Recording servers	Listening for event messages from devices.

Port number	Protocol	Used by	Purpose
7474	TCP	Recording servers	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP.
7475	TCP	Management server	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP.
7563	TCP	Recording servers and Network Video Management System Smart Client	Communication with the ImageServer interface. Also handling of PTZ camera control commands and for retrieving image streams from clients etc.
7609	HTTP	Report server and Data Collector Server service	Communication between the two. The port must always be kept open on the server running the Data Collector Server service.
8080	UDP	Management server	Communication between internal processes on the server.
9090	TCP	Event Server	Listening for analytics events from external systems or devices.
9993	TCP	Recording servers and management server	Communication between the two.
12345	TCP	Management server and Network Video Management System Smart Client	Communication between the system and Matrix recipients. You can change the port number in the Management Client.
22331	TCP	Event server, Network Video Management System Smart Client and Management Client	Inbound must be enabled to make Network Video Management System add-on products, Network Video Management System Smart Client maps, Network Video Management System Smart Client alarm lists, and MIP plug-ins work.
52111	TCP	Network Video Management System Screen Recorder and recording servers	Communication between the two. You can change the port number in the Management Client.
65101	UDP	Recording servers	Listening for event notifications from the drivers.

Backing up and restoring system configuration

About backing up and restoring your system configuration

Sony recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

The system offers a built-in feature that backs up all the system configuration you can define in the Management Client. Note that the log server database and the log files, including audit log files, are not included in this backup.

If your system is large, Sony recommends that you define scheduled backups. This is done with the third-party tool: Microsoft® SQL Server Management Studio. This backup includes the same data as a manual backup.

During a backup, your system stays online. Depending on your system configuration, your hardware, and on whether you have installed the SQL server, Event Server service and Management Client on a single server or several servers (a distributed setup), backing up the system configuration can take some time.

Each time you make a backup both manual and scheduled, the SQL Server's transaction log file is flushed. For additional information about how to flush this log file, go to the Microsoft website and search for "SQL Server transaction log".

Back up log server database

Handle the **SurveillanceLogServer** database by using the method that you use when handling system configuration as described earlier. The **SurveillanceLogServer** database (the name may be different if you renamed the system configuration database) contains all your system logs, including errors reported by recording servers and cameras.

The database is located where the Log Server's SQL server is installed, typically the same place as your management server's SQL server. Backing up this database is not vital since it does not contain any system configuration, but you may later appreciate having access to system logs from before the management server backup/restore.

Manual backup and restore of system configuration

About manually backing up your system configuration

When you want to perform a manual backup of your system configuration, make sure that your system stays online. Here are a few things to consider before you start the backup:

- You cannot use a backup to copy configurations to other systems.

- It can take some time to back up your configuration. It depends on your system configuration, your hardware, and on whether your SQL server, management server and Management Client are installed on the same computer.

- Logs, including audit logs, are **not** part of the configuration backup.

About backing up and restoring the event server configuration

The content of your event server configuration is included when you back up and restore system configuration.

The first time you run the event server, all its configuration files are automatically moved to the SQL server. You can apply the restored configuration to the event server without needing to restart the event server, and the event server can start and stop all external communication while the restoration of the configuration is being loaded.

About back up/restore fail and problem scenarios

If, after your last system configuration backup, you have moved the event server or other registered services such as the log server, you must select which registered service configuration you want for the new system. You can decide to keep the new configuration after the system is restored to the old version. You decide by looking at the host names of the services.

If your restore of the system configuration fails because the event server is not located at the specified destination (for example, if you have chosen the old registered service setup), do another restore.

Back up system configuration manually

1. From the menu bar, select **File** > **Backup Configuration**.

2. Read the note in the dialog box and click **Backup**.

3. Enter a file name for the .cnf file.

4. Enter a folder destination and click **Save**.

5. Wait until the backup is finished and click **Close**.

Note: All relevant system configuration files are combined into one single .cnf file that is saved at a specified location. During the backup, all backup files are first exported to a temporary system backup folder on the management server. You can select another temporary folder by right-clicking the notification area's management server service icon and by selecting Select shared backup folder.

Restore system configuration from a manual backup

Important information:

- Both the user who installs and the user who restores must be local administrator of the database on the management server **and** on the SQL server.

- Except for your recording servers, your system is completely shut down for the duration of the restore, which can take some time.

- A backup can only be restored on the system installation where it was created. Make sure that the setup is as similar as possible to when the backup was made. Otherwise, the restore might fail.

- If you do a backup of the database and restore it on a clean SQL server, then the raise errors from the database will not work and you will only receive one generic error message

from the SQL server. To avoid that, first reinstall your Network Video Management System using the clean SQL server and then restore the backup on top of that.

- If restoring fails during the validation phase, you can start the old configuration again because you have made no changes.
  If restoring fails elsewhere in the process, you cannot roll back to the old configuration.
  As long as the backup file is not corrupted, you can do another restore.

- Restoring replaces the current configuration. This means that any changes to the configuration since last backup are lost.

- No logs, including audit logs, are restored.

- Once restoring has started, you cannot cancel it.

Restoring:

1. Right-click the notification area's Management Server service icon and select **Restore Configuration**.

2. Read the important note and click **Restore**.

3. In the file open dialog box, browse to the location of the configuration backup file, select it, and click **Open**.

   The backup file is located on the Management Client computer. If the Management Client is installed on a different server, copy the backup file to this server before you select the destination.

4. The **Restore Configuration** window opens. Wait for the restore to finish and click **Close**.

Select shared backup folder

Before backing up and restoring any system configuration, you must set a backup folder for this purpose.

1. Right-click the notification area's management server service icon and select **Select shared backup folder**.

2. In the window that appears, browse to the wanted file location.

3. Click **OK** twice.

4. If asked if you want to delete files in the current backup folder, click **Yes** or **No** depending on your needs

Scheduled backup and restore

About scheduled backup and restore of system configuration

Sony recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration. Regular backups also have the added benefit that they flush your Microsoft® SQL Server's transaction log.

If you have a smaller setup and do not need scheduled backups, you can back up your system configuration manually. For instructions, see Manual backup and restore of system configuration (on page 237).

The management server stores your system's configuration in a database. When you back up/restore management server(s), make sure that this database is included in the backup/restore.

Prerequisites for using scheduled backup and restore

Microsoft® SQL Server Management Studio, a tool download-able for free from their website http://www.microsoft.com/downloads.

Apart from managing SQL Server databases, the tool includes some easy-to-use backup and restoration features. Download and install the tool on your management server.

About the SQL server transaction log

Each time a change in the system's data occurs, the SQL Server log this change in its transaction log, regardless whether it is a SQL Server on your network or a SQL Server Express edition.

The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server database. By default, the SQL Server stores its transaction log indefinitely, and over time the transaction log build up more and more entries. The SQL Server's transaction log is by default located on the system drive, and if the transaction log keeps growing, it may in the end prevent Windows from running properly.

To avoid such a scenario, flushing the SQL Serve's transaction log from time to time is a good idea. However, flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. Your system does not, however, automatically flush the SQL Server's transaction log at specific intervals. You can also do several things on the SQL Server itself to keep the size of the transaction log down.

For more information on this topic, go to the Microsoft support page http://support.microsoft.com and search for SQL Server transaction log.

Back up system configuration with scheduled backup

1. From Windows' **Start** menu, launch Microsoft® SQL Server Management Studio..

2. When connecting, specify the name of the required SQL Server. Use the account under which you created the database.

   a) Find the **Surveillance** database that contains your entire system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, and more.

      We assume that the database uses the default name.

   b) Make a backup of the **Surveillance** database and make sure to:

      - Verify that the selected database is **Surveillance**.

      - Verify that the backup type is **full**.

      - Set the schedule for the recurrent backup. You can read more about scheduled and automated backups on the Microsoft website https://support.microsoft.com/en-us/kb/2019698.

      - Verify that the suggested path is satisfactory or select alternative path.

      - Select to **verify backup when finished** and to **perform checksum before writing to media**.

3. Follow the instructions in the tool to the end.

Also consider backing up the **SurveillanceLog** database by using the same method.

Backup and restore event server configuration

The content of your event server configuration is included when you backup and restore system configuration. The first time you run the event server, all its configuration files are automatically moved to the SQL server. You can apply the restored configuration to the event server without needing to restart the event server, and the event server is capable of starting and stopping all external communication while the restoration of the configuration is being loaded.

Restore system configuration from a scheduled backup

Prerequisite: To prevent configuration changes being made while you restore the system configuration database, stop the:

- Management Server service (see "Managing server services" on page 249)

- Event Server Service (can be done from Windows **Services** (search for **services.msc** on your machine. Within **Services**, locate **Sony Network Video Management System Event Server**))

- World Wide Web Publishing Service, also known as the Internet Information Service (IIS). Learn how to stop the IIS http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx.

Open Microsoft® SQL Server Management Studio from Windows' **Start** menu.

In the tool do the following:

1. When connecting, specify the name of the required SQL Server. Use the account under which the database was created.

2. Find the **Surveillance** database that contains your entire system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.

3. Make a restore of the **Surveillance** database and make sure to:

   - Select to back up **from** device

   - Select backup media type **file**

   - Find and select your backup file **Surveillance.bak**

   - Select to **overwrite the existing database**.

4. Follow the instructions in the tool to the end.

If you also backed up the **SurveillanceLog** database from the old log server, restore it on the new log server by using the same method.

Note that the system does not work while the Management Server service is stopped. It is important to remember to start the services again once you have finished restoring the database.

Moving the management server

About moving the management server

You may sometimes need to move the management server installation from one physical server to another. The management server stores your system configuration in a database. If you are moving the management server from one physical server to another, it is vital that you make sure that your new management server also gets access to this database. The system configuration database can be stored in two different ways:

- **Network SQL Server:** If you are storing your system configuration in a database on an existing SQL Server on your network, you can point to the database's location on that SQL Server when installing the management server software on your new management server. In that case, only the following paragraph about management server hostname and IP address applies and you should ignore the rest of this topic:

  Management server hostname and IP address: When you move the management server from one physical server to another physical server, it is by far the easiest to give the new server the same hostname and IP address as the old one. This is due to the fact that the recording server connects to the hostname and IP address of the old management server. If you have given the new management server a new hostname and/or IP address, the recording server cannot find the management server. Manually stop each recording server in your system, change their management server URL, and when done, restart them.

- **Local SQL Server:** If you are storing your system configuration in a local SQL Server database on the management server itself, it is important that you back up the existing management server's system configuration database before the move. By backing up the database, and subsequently restoring it on the new server, you avoid having to reconfigure your cameras, rules, time profiles, etc. after the move.

Prerequisites

- **Your software installation file for installation on the new management server**.

- **Your software license file (.lic)**, that you received when you purchased your system and initially installed it. You should not use the activated software license file which you have received after a manual offline license activation. An activated software license file contains information about the specific server on which the system is installed. Therefore, an activated software license file cannot be reused when moving to a new server.

Note that if you are also upgrading your system software in connection with the move, you have received a new software license file. Simply use this.

- **Local SQL Server users only: Microsoft® SQL Server Management Studio**.

- What happens while the management server is unavailable? (see "About unavailable management servers" on page 242)

- Copy log server database (see "Back up log server database" on page 237)

About unavailable management servers

- **Recording servers can still record:** Any currently working recording servers received a copy of their configuration from the management server, so they can work and store recordings on their own while the management server is down. Scheduled and

motion-triggered recording therefore works, and event-triggered recording works unless based on events related to the management server or any other recording server because these go through the management server.

- **Recording servers temporarily store log data locally:** They automatically send log data to the management server when it becomes available again.

  - **Clients cannot log in:** Client access is authorized through the management server. Without the management server, clients cannot log in.

  - **Clients that are already logged in can remain logged in for up to one hour:** When clients log in, they are authorized by the management server and can communicate with recording servers for up to one hour. If you can get the new management server up and running within an hour, many of your users are not affected.

  - **No ability to configure the system:** Without the management server, you cannot change the system configuration.

Sony recommends that you inform your users about the risk of losing contact with the surveillance system while the management server is down.

Move the system configuration

Moving your system configuration is a three step process:

1. Make a backup of your system configuration. This is identical to making a scheduled backup (see "Back up system configuration with scheduled backup" on page 240).

2. Install the new management server on the new server. See scheduled backup, step 2.

3. Restore your system configuration to the new system. See Restore system configuration from scheduled backup (see "Restore system configuration from a scheduled backup" on page 241).

Managing the SQL server

About updating the SQL server address

When you install a system as a trial, or if you restructure a large installation, you may need to use a different SQL database. You can do this with the **Update SQL Server Address** tool.

With the tool, you can change the addresses of the SQL servers used by the management server, the event server and the log server. The only limitation is that you cannot change the management server and event server SQL address at the same time as the log server's SQL address. You can do it one after another.

You must do SQL updates locally on the computer where you have installed the management server/event server **or** log server. You cannot do it from the Management Client. If your management server and event server are not located on the same computer, you can still use the tool, but you must run it on both the computer on which the management server is installed and on the computer on which the event server is installed.

You must copy the SQL databases before you proceed.

Update the log server's SQL address

Management server and log server located on the same computer

1. Go to the computer where your management server is installed.

2. Go to the notification area of the taskbar. Right-click the **Management Server** icon, select **Update SQL address**. The **Update SQL Server Address** dialog box appears.

3. Select **Log Server** and click **Next**.

4. Enter or select the new SQL server and click **Next**.

5. Select the new SQL database and click **Select**.

6. Wait while the address change takes place. Click **OK** to confirm.

Management server and log server located on different computers

1. Go to the computer where your management server is installed and copy the directory *%ProgramFiles%\Sony\- Network VMS Management Server\Tools\ChangeSqlAddress* (with content) to a temporary directory on the event server.

2. Paste the directory that you copied to a temporary place on the computer where the log server is installed and run the included file: *VideoOS.Server.ChangeSqlAddress.exe*. The **Update SQL Server Address** dialog box appears.

3. Select **Log Server** and click **Next**.

4. Enter or select the new SQL server and click **Next**.

5. Select the new SQL database and click **Select**.

6. Wait while the address change takes place. Click **OK** to confirm.

Update the management server or event server SQL server address

1. If your management server and event server are located:

   a) together on the same computer and you wish to update both SQL addresses, go to the computer where your management server is installed.

   b) on different computers and you wish to update the management server SQL address (and later the event server SQL address), go to the computer where your management server is installed.

   c) on different computers and you wish to update the event server SQL address only (or you have already updated it on the management server), go to the computer where your management server is installed and copy the directory *%ProgramFiles%\Sony\-Network VMS Management Server\Tools\ChangeSqlAddress* (with content) to temporary directory on the event server.

2. If:

    - **a** and **b**, go to the notification area of the taskbar. Right-click the **Management Server** icon, select **Update SQL address**.

    - **c,** paste the directory you copied to a temporary place on the computer where the event server is installed and run the included file: *VideoOS.Server.ChangeSqlAddress.exe.*

3. The **Update SQL Server Address** dialog box appears. Select **Management Server and Event Server** and click **Next**.

4. Enter or select the new SQL server and click **Next**.

5. Select the new SQL database and click **Select**.

6. Wait while the address change takes place. When a confirmation message is presented, click **OK**.

If you acted according to step **2 b**, you have by now only updated the **management server** SQL address. You must repeat the process to update the **event server** SQL address. When doing so, make sure to select the scenario in step **2 c.**

Replace hardware

When you replace a hardware device on your network with another hardware device, you must know the IP address, port, user name and password of the new hardware device.

You must manually activate your licenses **after** replacing hardware devices. If the new number of hardware devices exceeds your total number of hardware device licenses, you have to purchase new hardware device licenses.

1. Expand the required recording server, right-click the hardware you want to replace.

2. Select **Replace Hardware**.

3. The **Replace Hardware** wizard appears. Click **Next**.

4. In the wizard, in the **Address** field (marked by red arrow in the image), enter the IP address of the new hardware. If known, select the relevant driver from the **Hardware Driver** drop-down list. Otherwise select **Auto Detect**. If port, user name or password data is different for the new hardware, correct this **before starting the auto detect process (if needed)**.
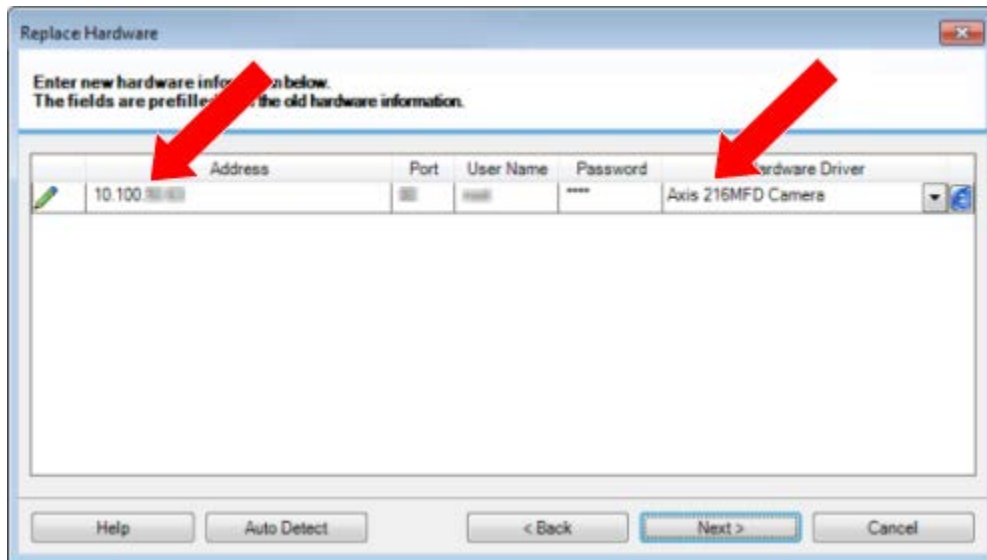
The wizard is prefilled with data from the existing hardware. If you replace it with a similar hardware device, you can reuse some of this data - for example, port and driver information.

5. Do one of the following:

   - If you selected the required hardware device driver directly from the list, click **Next**.

   - If you selected **Auto Detect** in the list, click **Auto Detect**, wait for this process to be successful (marked by a ✔ to the far left), click **Next**.

This step is designed to help you map devices and their databases, depending on the number of individual cameras, microphones, inputs, outputs and so on attached to the old hardware device and the new respectively.

It is important to consider **how** to map databases from the old hardware device to databases of the new hardware device. You do the actual mapping of individual devices by selecting a corresponding camera, microphone, input, output or **None** in the right-side column.

> **Important:** Make sure to map **all** cameras, microphones, inputs, outputs, etc. Contents mapped to **None**, are **lost**.
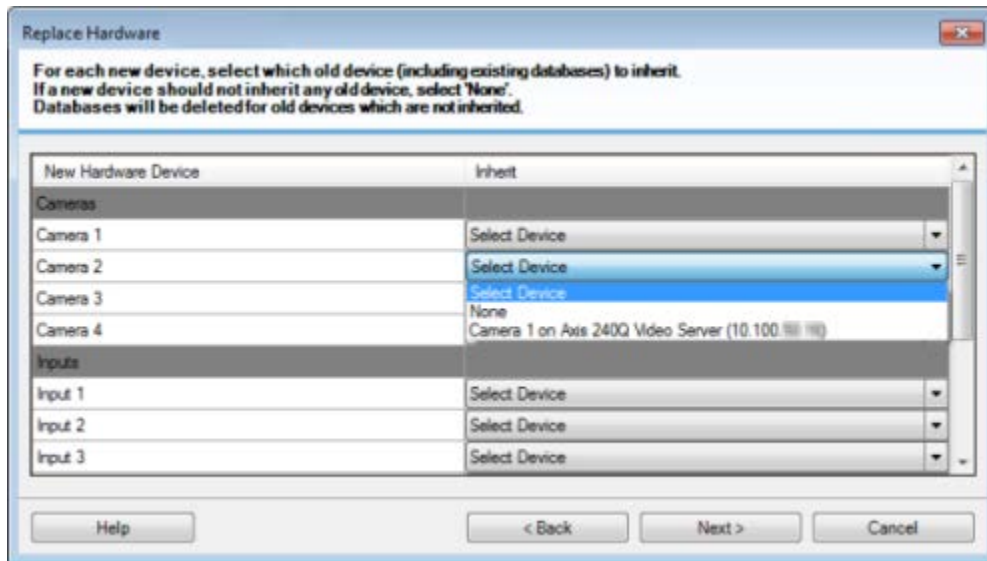
Example of the old hardware device having more individual devices than the new one.

Click **Next**.

6. You are presented with a list of hardware to be added, replaced or removed. Click **Confirm**.

7. Final step is a summary of added, replaced and inherited devices and their settings. Click **Copy to Clipboard** to copy contents to the Windows clipboard or/and **Close** to end the wizard.

Replace a recording server

If a recording server is malfunctioning and you want to replace it with a new server that inherits the settings of the old recording server:

1. Retrieve the recording server ID from the old recording server:

1. Select **Recording Servers**, then in the **Overview** pane select the old recording server.

2. Select the **Storage** tab.

3. Press and hold down the CTRL key on your keyboard while selecting the **Info** tab.

4. Copy the recording server ID-number in the lower part of the **Info** tab. Do not copy the term *ID*, only the number itself.

2. Replace the recording server ID on the new recording server:

   1. Stop the Recording Server service on the old recording server, then in Windows' **Services** set the service's **Startup type** to **Disabled**.

      It is very important that you do not start two recording servers with identical IDs at the same time.

   2. On the new recording server, open an explorer and go to *C:\ProgramData\Sony\-Network VMS Recording Server* or the path where your recording server is located.

3. Open the file *RecorderConfig.xml*.

4. Delete the ID stated in between the tags *<id>* and *</id>*.

5. Paste the copied recording server ID in between the tags *<id>* and *</id>*. Save the *RecorderConfig.xml* file.

6. Go to the registry: *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation*.

7. Open **RecorderIDOnMachine** and change the old recording server ID with the new ID.

8. Restart the Recording Server service. When the new Recording Server service starts up, it has inherited all settings from the old recording server.

Video device drivers

About video device drivers

Your system uses video device drivers to control and communicate with the camera devices connected to a recording server. You must install video device drivers on each recording server on your system.

When you install your system, video device drivers are part of the initial installation process. Sony releases new versions of video device drivers regularly and makes them available on the download page http://www.sony.net/CameraSystem/NVMS/Software on our website. When you update video device drivers, you can install the latest version on top of any version you may have installed. Stop the Recording Server before you install, otherwise you need to restart the computer.

To ensure best performance, always use the latest version of video device drivers.

About removing video device drivers

If you no longer require video device drivers on your computer, you can delete the device packs from your system. To do so, follow the standard Windows procedure for removing programs.

If you remove video device drivers, the recording server and the camera devices cannot communicate any longer. Do not remove device packs when you upgrade because you can install a new version on top of an old one. Only if you uninstall the entire system, you may remove the device pack.

Managing server services

On the computer running the servers, there is a notification area with tray icons. Through the icons, you can get information about the server services and perform certain actions. This includes, for example, checking the state of the services, viewing logs or status messages, and starting and stopping the services.

Start or stop the Management Server service

In the notification area, a tray icon indicates the state of the Management Server service, for example **Running**. Through this icon, you can start or stop the Management Server service. If you stop the Management Server service, you cannot use Management Client.

1. In the notification area, right-click the tray icon for the Management Server. A context-menu appears.

   Start Management Server Service
   Stop Management Server Service

   Show Status Messages...

   Change License...
   Restore Configuration...
   Select shared backup folder...
   Update SQL Address...
   Help...
   About...
   Exit Management Server Manager
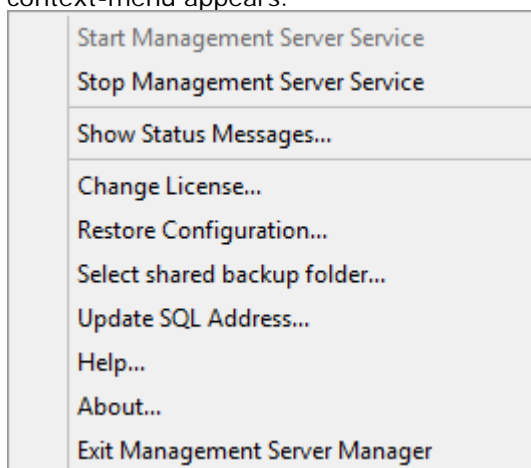
2. If the service has stopped, click **Start Management Server service** to start it. The tray icon changes to reflect the new state.

3. To stop the service, click **Stop Management Server service**.

For more information about the tray icons, see About the tray icons (on page 252).

See also

Start, stop, or restart the Event Server service (on page 251)

Start or stop the Recording Server service (on page 250)

Start or stop the Recording Server service

In the notification area, a tray icon indicates the state of the Recording Server service, for example **Running**. Through this icon, you can start or stop the Recording Server service. If you stop the Recording Server service, your system cannot interact with devices connected to the server. This means you cannot view live video or record video.

1. In the notification area, right-click the tray icon for the Recording Server. A context-menu appears.

   Start Recording Server Service

   Stop Recording Server Service

   Show Status Messages...

   Change Settings...

   About...

   Exit Recording Server Manager
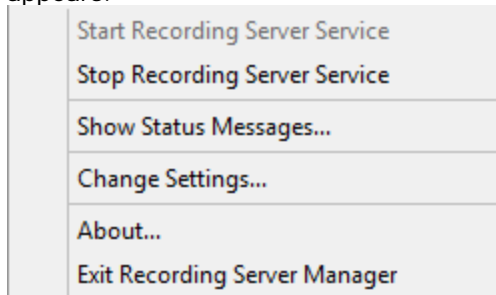
2. If the service has stopped, click **Start Recording Server service** to start it. The tray icon changes to reflect the new state.

3. To stop the service, click **Stop Recording Server service**.

For more information about the tray icons, see About the tray icons (on page 252).

See also

Start, stop, or restart the Event Server service (on page 251)

Start or stop the Management Server service (on page 249)

View status messages for Management Server or Recording Server

In the notification area on the computer running the servers, tray icons indicate the state of the Management Server and Recording Server. Through these icons, you can view status messages, for example "Service started".

1. In the notification area, right-click the relevant tray icon. A context-menu appears.

2. Select **Show Status Messages**. Depending on the server type, either the **Management Server Status Messages** or **Recording Server Status Messages** window appears, listing time-stamped status messages:

Start, stop, or restart the Event Server service

In the notification area, a tray icon indicates the state of the Event Server service, for example **Running**. Through this icon, you can start, stop, or restart the Event Server service. If you stop the service, parts of the system will not work, including events and alarms. However, you can still view and record video. For more information, see Stopping the Event Server service.

1. In the notification area, right-click the tray icon for the Event Server. A context-menu appears.
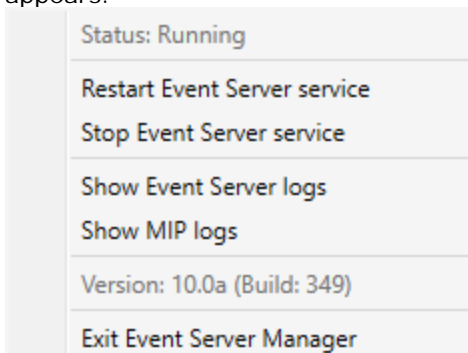
2. If the service has stopped, click **Start Event Server service** to start it. The tray icon changes to reflect the new state.

3. To restart or stop the service, click **Restart Event Server service** or **Stop Event Server service**.

For more information about the tray icons, see About the tray icons (on page 252).

See also

Start or stop the Recording Server service (on page 250)

Stopping the Event Server service

When installing MIP plug-ins in the Event Server, first you must stop the Event Server service and then, afterward, restart it. However, while the service is stopped, many areas of the VMS system will not function:

- No events or alarms are stored in the Event Server. However, system and device events still trigger actions, for example start recording.

- Analytic events do not work.

- Generic events do not work in Network Video Management System Enterprise Edition.

- No alarms are triggered.

- In Network Video Management System Smart Client, map view items, alarm list view items, and the Alarm Manager workspace do not work.

- MIP plug-ins in the Event Server cannot run.

- MIP plug-ins in Management Client and Network Video Management System Smart Client do not work correctly.

About the tray icons

The tray icons in the table represent the possible states of the services running on Management Server, Recording Server, and Event Server. They are all visible on the computers where the servers are installed, in the notification area:

Manage-ment Server service icon	Recording Server service icon	Event Server service icon	Description
			Running Appears when a server service is enabled and started.
			Stopped Appears when a server service has stopped.
			Starting Appears when a server service is in the process of starting. Under normal circumstances, the tray icon changes after a short while to **Running**.
			Stopping Appears when a server service is in the process of stopping. Under normal circumstances, the tray icon changes after a short while to **Stopped**.

Manage-ment Server service icon	Recording Server service icon	Event Server service icon	Description
			In indeterminate state Appears when the server service is initially loaded and until the first information is received, upon which the tray icon, under normal circumstances, changes to **Starting** and afterwards to **Running**.
			Running offline Typically appears when the Recording Server service is running but the Management Server service is not.
			Must be authorized by administrator Appears when the Recording Server service is loaded for the first time. Administrators authorize the recording server through the Management Client: Expand the **Servers** list, select the **Recording Server** node and in the **Overview** pane, right-click the relevant recording server and select **Authorize Recording Server**.

Change settings for the Recording Server service

You can change the basic settings for the Recording Server service, such as which port numbers to use.

Prerequisites: To change the settings, first you must stop the Recording Server service. While the Recording Server service is stopped, the system cannot interact with devices connected to the recording server. This means you cannot view live video or record video.

1. In the notification area, right-click the Recording Server tray icon. A context-menu appears.

    Start Recording Server Service
    Stop Recording Server Service

    Show Status Messages...

    Change Settings...

    About...
    Exit Recording Server Manager
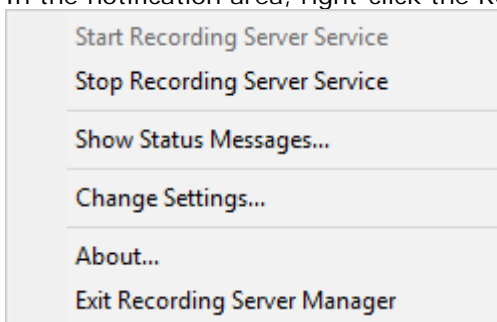
2. Select **Stop Recording Server service**.

3. Right-click tray icon again.

4. Select **Change Settings**. The **Recording Server Settings** window appears. Change the appropriate settings.

See also

Recording Server Settings

When you configure Recording Server settings, specify the following:

Name	Description
Address	IP address (example: 123.123.123.123) or host name (example: ourserver) of the management server to which the recording server should be connected. This information is necessary so that the recording server can communicate with the management server.
Port	Port number to be used when communicating with the management server. Default is port 9993. You can change this if you need to.
Web server port	Port number to be used for handling web server requests, for example for handling PTZ camera control commands and for browse and live requests from Network Video Management System Smart Client. Default is port 7563. You can this if you need to.
Alert server port	Port number to be used when the recording server listens for TCP information (some devices use TCP for sending event messages). Default is port 5432. You can change this if you need to.
SMTP server port	Port number to be used when the recording server listens for Simple Mail Transfer Protocol (SMTP) information. SMTP is a standard for sending e-mail messages between servers. Some devices use SMTP for sending event messages or images to the surveillance system server via e-mail. Default is port 25, which you can enable and disable. You can change the port number if you need to.

Restart Data Collector Server service

Your system automatically installs the Data Collector Server service on the same computers as the Management Server, Recording Server, Log Server, Event Server, and NVMS Mobile Server.

Normally, the Data Collector Server service requires no maintenance, but if the service **does** stop, no live feed is sent to the System Monitor. This is indicated in the System Monitor with error messages.

1. On the computer where the Data Collector Server service is installed:

2. In Windows' **Start** menu, select **Control Panel**, and then:

    • If using **Category** view, find the **System and Security** category and click **Administrative Tools**.

- If using **Small icons** or **Large icons**, click **Administrative Tools**.

3. Double-click **Services**.

4. Locate the **Sony Network Video Management System Data Collector Server**. Right-click it and select **Start** to restart the service.

Registered services

Occasionally, you have servers and/or services which should be able to communicate with the system even if they are not directly part of the system. Some services, but not all, can register themselves automatically in the system. Services that can automatically be registered are:

- Event Server service

- Log Server service

- Service Channel service

Automatically registered services are displayed in the list of registered services.

You can manually specify servers/services as registered services in the Management Client.

About the service channel

The service channel enables automatic and transparent configuration communication between servers and clients in your system. For example, it is the service channel that makes sure that when a shared view is changed on one client, the change is immediately reflected on other clients using the relevant shared view. The service channel also facilitates configuration-related communication between servers and clients in cases where you use various plug-ins or add-on products with your system.

The service channel is typically installed as part of the management server installation and resides on the management server computer, but if needed, you may just as well install it on another server in your surveillance system.

Once installed, the service channel can register itself automatically with your system (meaning that it automatically becomes listed by the registered services feature in the Management Client). Its location is known by the system, and clients logging into the system can automatically benefit from it.

If you later change the IP address or hostname of the server running the service channel service, you must manually edit the information under **Tool** > **Registered Services** in the Management Client. Also, if you later need to change the user under which the service channel service was installed, you must remove the Service Channel service and afterwards install it again under the new user.

It is important that any instance of Network Video Management System Smart Client is time-synchronized with the computer running the Service Channel service. If the Network Video Management System Smart Client is not time-synchronized with the management server and the computer running the Service Channel service, the Network Video Management System Smart Client is not updated with information about configuration changes made by other users in Network Video Management System Smart Client. This means that users risk overwriting each other's configuration changes. If your Network Video Management System Smart Clients are not time-synchronized with the computer running the Service Channel service, you see an error informing you of this.

Add and edit registered services

1. In the **Add/Remove Registered Services** window, click **Add** or **Edit**, depending on your needs.

2. In the **Add Registered Service** or **Edit Registered Service** window (depending on your earlier selection), specify or edit settings.

3. Click **OK**.

Manage network configuration

With the network configuration settings, you can specify the management server's server LAN and WAN addresses so the management server and the trusted servers can communicate.

1. In the **Add/Remove Registered Services** window, click **Network**.

2. Specify the LAN and/or WAN IP address of the management server.

   If all involved servers (both the management server and the trusted servers) are on your local network, you can simply specify the LAN address. If one or more involved servers access the system through an internet connection, you must also specify the WAN address.
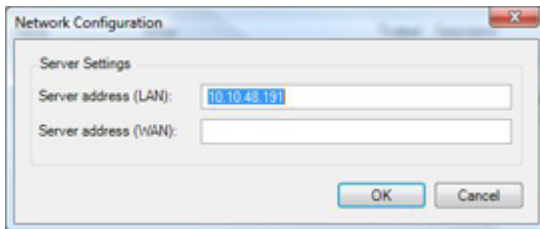
3. Click **OK**.

Registered services properties

In the **Add Registered Service** or **Edit Registered Service** window, specify the following:

Component	Requirement
Type	Prefilled field.
Name	Name of the registered service. The name is only used for display purposes in the Management Client.
URLs	Click **Add** to add the IP address or hostname of the registered service. If specifying a hostname as part of a URL, the host must exist and be available on the network. URLs must begin with *http://* or *https://* and must not contain any of the following characters: *< > & ' " * ?	[ ] "*.
	Example of a typical URL format: http://ipaddress:port/directory (where port and directory are optional). Note that you can add more than one URL if required.

Component	Requirement
Trusted	Select if the registered service should be trusted immediately (this is often the case, but the option gives you the flexibility to add the registered service and then mark it as trusted by editing the registered service later). Note that changing the trusted state also changes the state of other registered services sharing one or more of the URLs defined for the relevant registered service.
Description	Description of the registered service. The description is only used for display purposes in the Management Client.
Advanced	When a service is advanced, it has specific URI schemes (for example, http, https, tcp or udp) that need to be set up for each host address you define. A host address therefore has multiple endpoints, each with its own scheme, host address and IP port for that scheme.

Index