

Milestone Systems

XProtect® Advanced VMS 2014

Administrator's Manual



The Open Platform Company



Contents

COPYRIGHT, TRADEMARKS AND DISCLAIMER	11
BEFORE YOU START	12
INTRODUCTION TO THE HELP	12
NAVIGATE THE BUILT-IN HELP SYSTEM.....	12
SYSTEM OVERVIEW	14
PRODUCT OVERVIEW.....	14
A DISTRIBUTED SYSTEM SETUP	15
SYSTEM COMPONENTS	15
Management server.....	15
Failover management server	16
Recording server.....	16
Failover recording server	16
Event server	17
Log server	17
SQL server	17
Active Directory.....	18
Virtual servers	18
Clients	18
ABOUT LICENSES.....	21
PRODUCT COMPARISON CHART.....	22
ABOUT LOCAL IP ADDRESS RANGES	23
ABOUT IPV6 AND IPV4.....	23
About using the system with IPv6.....	23
About writing IPv6 addresses	24



SYSTEM REQUIREMENTS.....	25
INSTALLATION.....	26
INSTALLATION PRECONDITIONS	26
Determine installation method.....	26
Determine SQL server type	26
Select service account	27
Active Directory.....	27
Customize IIS.....	28
About virus scanning.....	28
Register Software License Code	29
Prerequisites for offline installation	30
INSTALL THE SYSTEM	30
Install your system - Single Server option	30
Install your system - Distributed option	31
Install your system - Custom option	32
Install the recording server	33
Installation for workgroups.....	34
Installation troubleshooting	34
CONFIGURE THE SYSTEM IN MANAGEMENT CLIENT.....	37
Change Software License Code	39
INSTALL CLIENTS	39
Install XProtect Smart Client silently	39
Install Milestone Mobile server	40
DOWNLOAD MANAGER/DOWNLOAD WEB PAGE.....	40
Download Manager's default configuration	42
Download Manager's standard installers (user)	43
Add/publish Download Manager installer components	43
Hide/remove Download Manager installer components	44
Device pack installer - must be downloaded	45



UPGRADE.....	45
About upgrade.....	45
Upgrade prerequisites	46
Alternative upgrade for workgroup	46
FIRST TIME USE.....	48
BEST PRACTICES	48
Protect recording databases from corruption	48
About daylight saving time	49
About time servers.....	49
MANAGEMENT CLIENT OVERVIEW	50
About login authorization.....	50
Management Client window overview.....	50
Panels overview	52
Menu overview.....	53
MANAGEMENT CLIENT ELEMENTS.....	56
BASICS	56
License information	56
Site information	60
SERVERS AND HARDWARE.....	61
Recording servers.....	61
Hardware and remote servers.....	78
Remove a recording server	86
Delete all hardware on a recording server	87
DEVICES	87
Working with device groups	87
Working with devices.....	90
CLIENT	133
About clients.....	133



View groups	133
Smart Client profiles	134
Management Client profiles	138
Matrix	141
RULES AND EVENTS	143
About rules and events	143
About actions and stop actions	144
Events overview	152
Rules	159
Time profiles	167
Notification profiles	171
User-defined events	175
Analytics events	177
Generic events	180
SECURITY	187
Roles	187
Basic users	220
SYSTEM DASHBOARD	221
About system dashboard	221
About system monitor	221
About evidence lock	223
About current tasks	223
About configuration reports	223
SERVER LOGS	224
About logs	224
Search logs	225
Export logs	225
Change log language	226
System log (properties)	226
Audit log (properties)	227



Rule log (properties)	228
ALARMS.....	229
About alarm configuration	229
About alarms	230
Alarm Definitions.....	231
Alarm Data Settings	233
Sound Settings	234
About setting up alarms using Enterprise slaves	234
OPTIONS DIALOG BOX	235
General tab (options)	236
Server Logs tab (options).....	238
Mail Server tab (options)	239
AVI Generation tab (options)	240
Network tab (options)	241
Bookmark tab (options).....	241
Evidence Lock tab (options)	242
User Settings tab (options)	242
Access Control Settings tab (options).....	242
Analytics Events tab (options).....	243
Event Server tab (options)	244
Generic Events tab (options)	244
FEATURE CONFIGURATION	247
FAILOVER RECORDING SERVERS (REGULAR AND HOT STANDBY).....	247
About failover recording servers.....	247
About failover steps.....	248
About failover recording server functionality	249
Install a failover recording server.....	250
Set up and enable failover recording servers	251
Assign failover recording servers	251
Group failover recording servers	252



Read failover recording server status icons	252
Failover recording server properties	253
Failover group properties	253
About failover recording server services	254
View status messages	254
Change the management server address	254
View version information	254
FAILOVER MANAGEMENT SERVERS	255
About multiple management servers (clustering)	255
Prerequisites for clustering	255
Install in a cluster	255
Upgrade in a cluster	257
REMOTE CONNECT SERVICES	258
About remote connect services	258
Install STS environment for One-click camera connection	258
Add/edit STSs	259
Register new Axis One-click camera	259
Axis One-Click Camera connection properties	260
MILESTONE FEDERATED ARCHITECTURE	260
About selecting Milestone Interconnect or Milestone Federated Architecture	260
About Milestone Federated Architecture	261
Set up your system to run federated sites	264
Add site to hierarchy	265
Accept inclusion in the hierarchy	266
Refresh site hierarchy	266
Connect to another site in hierarchy	266
Detach a site from the hierarchy	267
Federated site properties	267
MILESTONE INTERCONNECT	269
About selecting Milestone Interconnect or Milestone Federated Architecture	269



About Milestone Interconnect.....	269
About possible Milestone Interconnect setups	271
Milestone Interconnect and licensing	272
Update remote site hardware.....	272
Establish remote desktop connection to remote system	272
Enable playback directly from remote site camera	272
Retrieve remote recordings from remote site camera	273
XPROTECT SMART WALL	273
About XProtect Smart Wall	273
Configure Smart Walls.....	274
Manage roles with Smart Walls	275
About using rules with Smart Wall presets	276
Smart Wall properties	276
Monitor properties.....	277
XPROTECT ACCESS CONTROL MODULE.....	279
About access control integration	279
Configure an integrated access control system	280
Wizard for access control system integration	280
Access control properties.....	282
XPROTECT LPR.....	286
LPR system overview	286
About preparing cameras for LPR.....	289
LPR installation	302
LPR configuration	303
LPR maintenance	322
MULTI-DOMAIN WITH ONE-WAY TRUST	325
Setup with one-way trust.....	325
SNMP	326
About SNMP support	326



Install SNMP service	326
Configure SNMP service	326
XPROTECT ENTERPRISE SERVERS	327
About XProtect Enterprise servers	327
Add XProtect Enterprise servers.....	327
Define roles with access to XProtect Enterprise servers	328
Edit XProtect Enterprise servers.....	328
SYSTEM MAINTENANCE	329
PORTS USED BY THE SYSTEM.....	329
BACKING UP AND RESTORING SYSTEM CONFIGURATION	332
About backing up and restoring your system configuration	332
Back up log server database	332
Manual backup and restore of system configuration.....	332
Scheduled backup and restore	334
MOVING THE MANAGEMENT SERVER	337
About moving the management server.....	337
About unavailable management servers	338
Move the system configuration	338
MANAGING THE SQL SERVER	338
About updating the SQL server address	338
Update the log server's SQL address	339
Update the management server or event server SQL server address	339
REPLACE HARDWARE.....	340
REPLACE A RECORDING SERVER.....	343
VIDEO DEVICE DRIVERS	344
About video device drivers	344
About removing video device drivers	344
SERVICES	344



About the Management Server service and Recording Server service.....	344
View status messages	345
Read server service icons - management, recording and failover	345
Change recording server settings	346
Recording server properties	347
REGISTERED SERVICES	348
About the service channel	348
Add and edit registered services.....	348
Manage network configuration	349
Registered services properties.....	349
INDEX.....	351



Copyright, trademarks and disclaimer

Copyright © 2015 Milestone Systems A/S.

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

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.

Milestone Systems A/S 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 Milestone 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 14)

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 26)

Provides installation preconditions and step by step procedures that help you install and upgrade your system.

First time use (on page 48)

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 56)

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 247)

Provides self-contained, detailed information about the additional features and add-on products that your system supports.

System maintenance (on page 329)

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.
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 XProtect 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 **XProtect Management Clients**
- The **XProtect Download Manager**
- One or more **XProtect® Smart Clients**.
- One or more **XProtect Web Clients** and/or **Milestone 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 XProtect Smart Client installed.

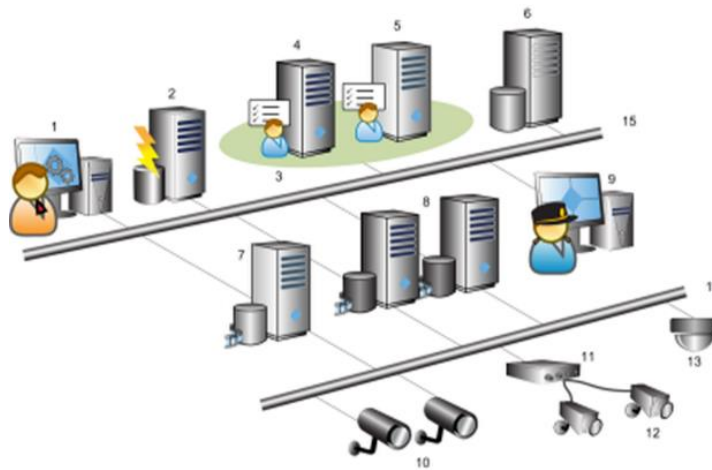
You can install your XProtect system on virtualized servers or on multiple physical servers in a distributed setup.

The system also offers the possibility of including the standalone XProtect® Smart Client – Player when you export video evidence from the XProtect Smart Client. XProtect Smart Client – Player allows recipients of video evidence (such as police officers, internal or external investigators, etc.) 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. Failover recording server
8. Recording server(s)
9. XProtect Smart Client(s)
10. IP video cameras
11. Video server
12. Analog cameras
13. PTZ IP camera
14. Camera network
15. Server network

System components

Management server

The management server 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. To improve system performance,



you can run several management servers as a Milestone Federated Architecture™. 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.

Furthermore, the recording server is responsible for communicating with other Milestone products connected via the Milestone Interconnect technology.

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.
- The media database supports various unique features like; multistage archiving, video grooming, encryption and adding a digital signature to the recordings.

Failover recording server

The failover recording server is responsible for taking over the recording task should a recording server fail.

The failover recording server can operator in two modes:

- Standard failover – for monitoring multiple recording servers
- Hot-standby – for monitoring a single recording server

The difference between the standard and hot-standby failover modes is that in the standard failover mode the failover recording server does not know which server to take over from, so it cannot start until a recording server fails. In the hot-standby mode the failover time is significantly shorter, as the



failover recording server already knows which recording server it should take over from and can preload the configuration and start up completely - except for the last step of connecting to the cameras.

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 XProtect 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 messages.

The system installer includes Microsoft SQL Server 2008 R2 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

You normally add users from Active Directory, but you can also add users without Active Directory. Active Directory is a distributed directory service included with several Windows Server operating systems. It identifies resources on a network in order for users or applications to access them.

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 50).



About XProtect Smart Client

Designed for Milestone XProtect® IP video management software, the XProtect Smart Client is an easy-to-use client application that provides intuitive control over security installations. Manage security installations with XProtect 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, XProtect 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 XProtect Smart Client.

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

To download XProtect 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 XProtect Download Manager to control what clients and language versions should be available to users on the welcome page of the XProtect Download Manager.

About Milestone Mobile client

Milestone® Mobile client is a mobile surveillance solution closely integrated with the rest of your XProtect system. It runs on your Android tablet or smartphone, your Apple® tablet, smartphone or portable music player or your Windows Phone 8 tablet or smartphone and gives you access to cameras, views and other functionality set up in the management clients.



Use the Milestone 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 XProtect system.

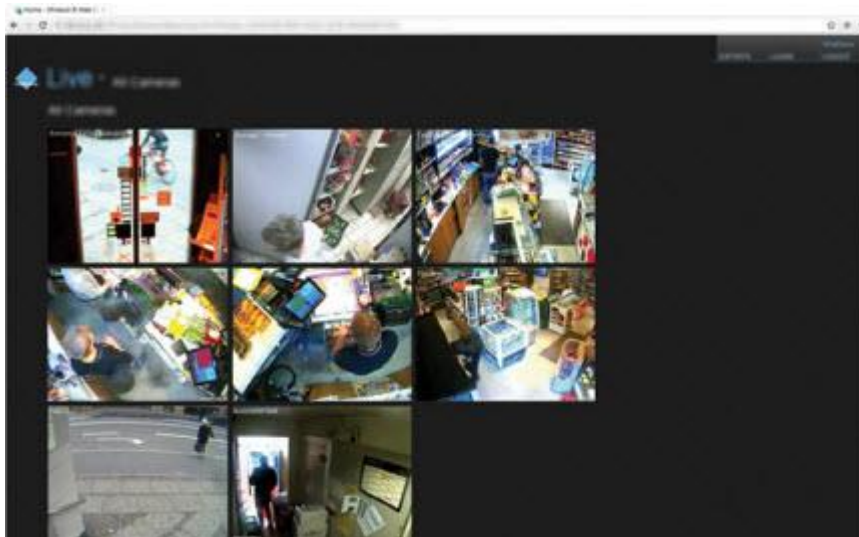


If you want to use Milestone Mobile client with your system, you must add a Mobile server to establish the connection between the Milestone Mobile client and your system. Once the Mobile server is set up, download the Milestone Mobile client for free from Google Play, App Store or Windows Phone Store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



About XProtect Web Client

XProtect 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 XProtect Web Client, you must install a Mobile server to establish the connection between the XProtect Web Client and your system. The XProtect 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 XProtect system anywhere from any computer or tablet with Internet access (provided you know the right external/Internet address, user name and password).

About licenses

When you purchase the system, you also purchase a certain number of licenses for the number of hardware devices, for example video encoders or cameras, that you want to run on the system. One hardware device license enables you to run as many camera, speaker, microphone, input, output and metadata devices that the hardware device consists of. It also enables you to run the hardware device multiple times on one site or multiple times on multiple sites.

You need a camera license for each enabled interconnected camera in a Milestone Interconnect setup.

If you purchase XProtect Access Control Module, you need a license for each door you want to configure for access control.

At first, when you have installed the various system components, configured the system, and added recording servers and cameras through the Management Client, the surveillance system runs on temporary licenses which need to be activated before a certain period ends. This is known as the grace period. You also need to activate licenses if you later add more cameras to the system.

When the new surveillance system is working, Milestone recommends that you activate your licenses before you make the final adjustments. If you do not activate your licenses before the grace period expires, all recording servers and cameras without activated licenses stop sending data to the surveillance system.



Product comparison chart

XProtect Advanced VMS comes in two versions:

- XProtect Expert
- XProtect Corporate

The complete feature list is available on the product overview page on the Milestone website
<http://www.milestonesys.com/Software/XProtect-IP-Video-Surveillance/xprotectproducts/>.

Below is a list of the differences between the two products:

Name	XProtect Expert	XProtect Corporate
Milestone Interconnect	Remote site	Central/remote site
Milestone Federated Architecture	Remote site	Central/remote site
Recording server failover and hot stand-by recording server	-	✓
Remote connect services	-	✓
Multi-stage video storage	XProtect Corporate database Live databases + 1 archive	XProtect Corporate database Live databases + unlimited archives
Reduce frame rate (grooming)	-	✓
Video data encryption (recording server)	-	✓
Database signing (recording server)	-	✓
Time controlled user access rights	-	✓
Bookmark function	Manual only	Manual and rule-based
Overall security	Client user rights	Client user rights/ administrator user rights
XProtect Management Client profiles	-	✓
XProtect Smart Client profiles	3	Unlimited
XProtect Smart Wall	optional	✓
Evidence lock	-	✓



About local IP address ranges

When a client, such as XProtect 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.

About IPv6 and IPv4

Your system supports IPv6 as well as IPv4. So does XProtect 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. IPv6 offers more than ten billion billion billion times as many addresses as IPv4.

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, recording server or failover 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.

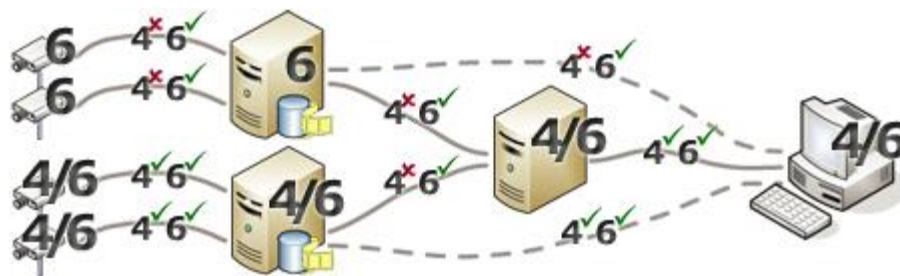
Clients

If your system uses IPv6, users should connect with the XProtect Smart Client. The XProtect Smart Client supports IPv6 as well as IPv4.

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

However, the XProtect 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 XProtect 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: *2001:0B80:0000:0000:0F80:3FA8:18AB*

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, www.iana.org <http://www.iana.org/numbers/>. IANA, the Internet Assigned Numbers Authority, is the organization responsible for the global coordination of IP addressing.

System requirements

Important: Your system no longer supports Microsoft® Windows® 2003 (however, you can still run/access clients from computers with Windows 2003).

Important: Your system no longer supports Microsoft® Windows® 32-bit OS (however, you can still run/access XProtect Web Client and XProtect Smart Client from computers with Windows 32-bit OS).

For information about the **minimum** system requirements to the various components of your system, go to the Milestone website <http://www.milestonesys.com/SystemRequirements>.



Installation

If you upgrade from a previous XProtect version, see About upgrade (on page 45).

Installation preconditions

Read the installation preconditions before you start the actual installation.

Determine installation method

As part of the installation wizard, you must decide which installation method to use. Your selection depends on the organization needs, but has typically been determined when purchasing the system.

The options are:

- **Single Server:** installs all management server components, recording server, and XProtect 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. 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 XProtect Smart Client are not visible in the un-editable component list. You must install the recording server, XProtect Smart Client, and SQL server on other computers.
- **Custom:** allows you to select freely among all management server components, recording server, and XProtect Smart Client to install on the current computer. By default, 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.

For easy user and group management, Milestone recommends that you have Microsoft Active Directory® in place before you install your system. If you add the management server to the Active Directory after installing, you must re-install the management server, and replace users with new users defined in the Active Directory.

Determine SQL server type

Read the following information to determine which SQL server type is right for your organization:

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 sufficient for systems with less than 300 cameras.

If you plan to perform frequent/regular backups of your database, Milestone recommends to use an existing SQL server on the network. You must have administrator rights on the SQL server.

For large installations (300 cameras or more), Milestone recommends using a full-scale existing SQL server on a dedicated computer on the network.



Milestone recommends that you install the database on a dedicated hard disk drive that is not used for anything else but the database. Installing the database on its own drive prevents low disk performance.

If 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 2008 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 upgrading to a newer version of the system, and you want to use your existing database.

Select service account

As part of the installation wizard, you are asked to specify an account to run the services on the servers. The service always runs on that account when the server is running - no matter which account is used to log in:

- **This predefined account**

In a domain environment, you can choose to use a predefined network service account.

- **This account**

In a domain environment, you can select a user account from the domain.

In a workgroup environment, you must first set up an identical user account with access to the network drives on all servers in the system and then select this as your service account. The service only runs when this user is logged in.

Active Directory

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

If you do not install Active Directory, follow Installation for workgroups (on page 34) when you start the installation.



Customize IIS

If you install on Windows Server 2008, Milestone recommends that you customize the standard IIS installation:

1. In Windows **Start** menu, select **Control Panel**, then select **Programs and Features**.
2. In the **Programs and Features** window, click **Turn Windows features on or off**. This opens the **Windows Features** window (window name may be different depending on which operating system you are installing the service channel on).
3. In the **Windows Features** window, expand **Internet Information Services**.
4. Expand and select **Web Management Tools**, then expand and select **IIS 6 Management Compatibility**, then select **IIS Metabase and IIS 6 configuration compatibility**.
5. Expand and select **World Wide Web Services**, then expand and select **Application Development Features**, then select the following:
 - .NET Extensibility
 - ASP
 - ASP.NET
 - ISAPI Extensions
 - ISAPI Filters.
6. Expand and select **Security**, then select **Windows Authentication**.
7. Click **OK**.

About virus scanning

As is the case with any other database software, if an antivirus program is installed on a computer running XProtect® software, it is important that you exclude specific file types and locations, 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 likely results in a disruption in the recording process or even database corruption.

When you need to perform virus scanning, do not scan Recording Server directories containing recording databases (by default c:\mediadatabase\, as well as all folders under that location). Avoid also to perform virus scanning on archive storage directories.

Create the following additional exclusions:

- File types: .blk, .idx, .pic
- C:\Program Files\Milestone or C:\Program Files (x86)\Milestone and all subdirectories.
- Exclude network scanning on the following TCP ports:



Product	TCP ports
XProtect® Advanced VMS system	80, 8080, 7563, 25, 21, 9993
XProtect® Mobile	8081
XProtect® Transact	9001

or

- Exclude network scanning of the following processes:

Product	Processes
XProtect Advanced VMS system	VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe
XProtect Transact	VideoOS.Transact.TransactService.exe

Organizations may have strict guidelines regarding virus scanning, however it is important that the above locations and files are excluded from virus scanning.

Register Software License Code

Before installing, you must have the name and location of the license file that you received from Milestone.

The Software License Code (SLC) is printed on your order confirmation. Milestone recommends that you register your SLC before installation.

1. Go to the Milestone website <http://www.milestonesys.com>.
2. At the bottom of the page, click **Software Registration**. Alternatively select the **SOFTWARE** tab and then **Register your software**.
3. Log into the software registration system with your user name and password.
If you have not used the software registration system before, click the **New to the system?** link for registering yourself as a user and then log in.
4. In the software registration system, click the **Add SLC** link.
5. Type your SLC. When asked whether you want to add the SLC to your account, click **OK**.
6. Once you have added your SLC, log out.



Prerequisites for offline installation

If you install the system on a server that is offline, you need the following:

- The `MilestoneXProtectAdvVMSSystemInstaller.exe` file.
- The Milestone XProtect Advanced VMS license file.
- OS installation media.

Install the system

Select one of the installation options:

- Install your system - Single Server option (on page 30)
- Install your system - Distributed option (on page 31)
- Install your system - Custom option (on page 32)

Install your system - Single Server option

1. If you are installing a version downloaded from the Internet, run the `MilestoneXProtectAdvancedVMSSystemInstaller.exe` file from the location where you saved it.

Alternatively, insert the software DVD. If the dialog box does not open automatically, run the `MilestoneXProtectAdvancedVMSSystemInstaller.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 **Milestone XProtect Advanced VMS** 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 XProtect provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.
 - c) Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box. Optionally, select the **Sign me up for the Customer Experience Improvement Program** check box. Follow the on-screen *Read more* link for further information on this.
4. Select **Single Server**. A list of components to install appears (you cannot edit this list). Click **Continue**.
5. Select **Files location** for the program file. In **Product language**, select the language in which your XProtect 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 Management Client" on page 37).

Install your system - Distributed option

1. If you are installing a version downloaded from the Internet, run the `MilestoneXProtectAdvancedVMSSystemInstaller.exe` file from the location where you saved it.

Alternatively, insert the software DVD. If the dialog box does not open automatically, run the `MilestoneXProtectAdvancedVMSSystemInstaller.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 **Milestone XProtect Advanced VMS** 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 XProtect provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.
 - c) Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box. Optionally, select the **Sign me up for the Customer Experience Improvement Program** check box. Follow the on-screen *Read more* link for further information on this.
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 **Files location** for the program file. In **Product language**, select the language in which your XProtect 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 the recording server on a separate computer, see Install the recording server (on page 33).



Install your system - Custom option

Note that with this option you can select or clear all of the components to install, except the management server. The management server is by default selected in the component list and is always installed. If one is already installed, it is updated.

1. If you are installing a version downloaded from the Internet, run the `MilestoneXProtectAdvancedVMSSystemInstaller.exe` file from the location where you saved it.

Alternatively, insert the software DVD. If the dialog box does not open automatically, run the `MilestoneXProtectAdvancedVMSSystemInstaller.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 **Milestone XProtect Advanced VMS** 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 XProtect provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.
 - c) Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box. Optionally, select the **Sign me up for the Customer Experience Improvement Program** check box. Follow the on-screen *Read more* link for further information on this.
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 **Files location** for the program file. In **Product language**, select the language in which your XProtect 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 > Milestone > 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 33).

Install the recording server

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

See Install a failover recording server (on page 250) if you want to install a failover server.

1. On the management server, go to the Management server's download web page from Windows' **Start** menu.
2. Select **Programs > Milestone > 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 now installs. When done, 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 Management Client" on page 37).

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.
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 **upgrading** 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**.

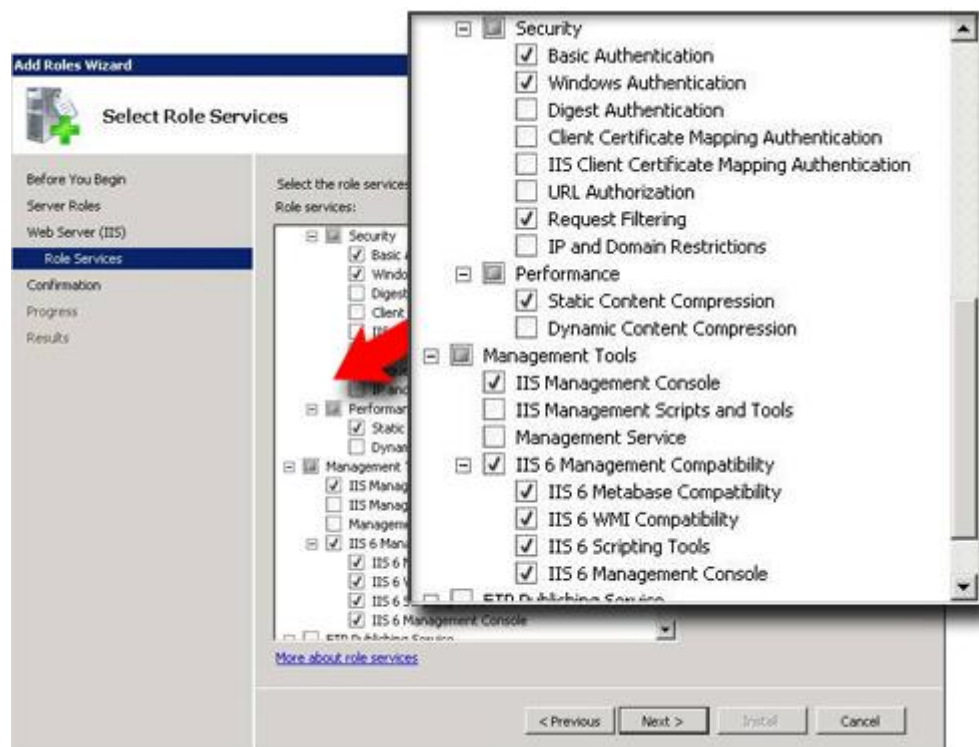


Issue: Automatic installation of IIS failed

The Internet Information Services (IIS) is normally installed automatically. If the automatic installation fails, you must install the IIS manually:

1. If automatic IIS installation fails, you see an error message asking you to install the IIS manually. In the error message box, click **Install IIS Manually**.
2. Select **Server Manager** from Windows' **Start** menu. In the left side of the **Server Manager** window, select **Roles**, then the **Roles Summary**.
3. Now select **Add Roles** to start a wizard.
4. In the wizard, click **Next**, select **Web Server (IIS)**, and follow the wizard's steps.
5. When you reach the wizard's **Select Role Services** step, you see that some role services are selected by default. However you should select some additional role services:
 - Under **Security**, select **Basic Authentication** and **Windows authentication**.
 - Under **Management Tools**, select **IIS Management Console**, expand it, and select **IIS 6 Metabase Compatibility**, **IIS 6 WMI Compatibility**, **IIS 6 Scripting Tools**, and **IIS 6 Management Console**.

When ready, the relevant part of the **Role services** tree should look like this:



6. Complete the wizard by following the remaining steps.



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 Management Client

Here are the tasks typically involved in setting up the system.

Even if information is presented 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, Milestone 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 (day/night, windy calm weather, and so on) once the system is running. The setup of rules, which determines most of the actions performed by the system (including when to record video), is another example of configuration which to a large extent depends on your organization's needs.



<input checked="" type="checkbox"/>	You have finished the initial installation of your system. See Install the system (on page 30).
<input checked="" type="checkbox"/>	Change the trial SLC to a permanent SLC (if required). See Change Software License Code (on page 39).
<input checked="" type="checkbox"/>	Log in to the Management Client.
<input type="checkbox"/>	Authorize use of your system's recording servers. See Authorize a recording server (on page 62).
<input type="checkbox"/>	Verify that each recording server's storage settings meet your needs. See About storage and archiving (on page 65).
<input type="checkbox"/>	Verify that each recording server's archiving settings meets your needs. See Archive settings properties (on page 73).
<input type="checkbox"/>	Detect the hardware (cameras or video encoders) to add to each recording server. See Add hardware (on page 78).
<input type="checkbox"/>	Configure each recording server's individual cameras. See About camera devices (on page 91).
<input type="checkbox"/>	Enable storage and archiving for individual cameras or 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 68).
<input type="checkbox"/>	Enable and configure devices. See Working with devices (on page 90).
<input type="checkbox"/>	The behavior of the system is to a large extent determined by rules, such as when cameras should record, when PTZ (pan-tilt-zoom) cameras should patrol, when notifications should be sent. Create rules. See About rules and events (on page 143).
<input type="checkbox"/>	Add roles to the system. See About roles (on page 187).
<input type="checkbox"/>	Add users and/or groups of users to each of the roles. See Assign/remove users and groups to/from roles (on page 190).
<input type="checkbox"/>	Activate licenses. See Activate licenses (online) (see "Activate licenses online" on page 58) or Activate licenses (offline) (see "Activate licenses offline" on page 59).



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.

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 SLC license file saved for this purpose. When done, the selected 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 29).

Install clients

Install XProtect Smart Client silently

You can deploy XProtect 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 XProtect Smart Client, over local networks.

1. Locate the Smart Client installation program (.exe) file - *MilestoneXProtectSmart Client.exe* or *MilestoneXProtectSmart Client_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 Milestone surveillance software is installed.

The path is typically:

C:\Program Files\Milestone\XProtect Management Server\IIS\httpdocs\XProtect Smart Client Installer\[version number] [bit-version]\All Languages\en-US

For example:

C:\Program Files\Milestone\XProtect Management Server\IIS\httpdocs\XProtect Smart Client Installer\2014 (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 the following command:

>MilestoneXProtectSmart Client.exe --quiet

This performs a quiet installation of the XProtect 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:

>MilestoneXProtectSmart Client.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.

>MilestoneXProtectSmart Client.exe --arguments=args.xml --quiet

Install Milestone Mobile server

All XProtect system components, including the Milestone Mobile server, are available for separate download and installation from the management server's download web page (controlled by XProtect Download Manager):

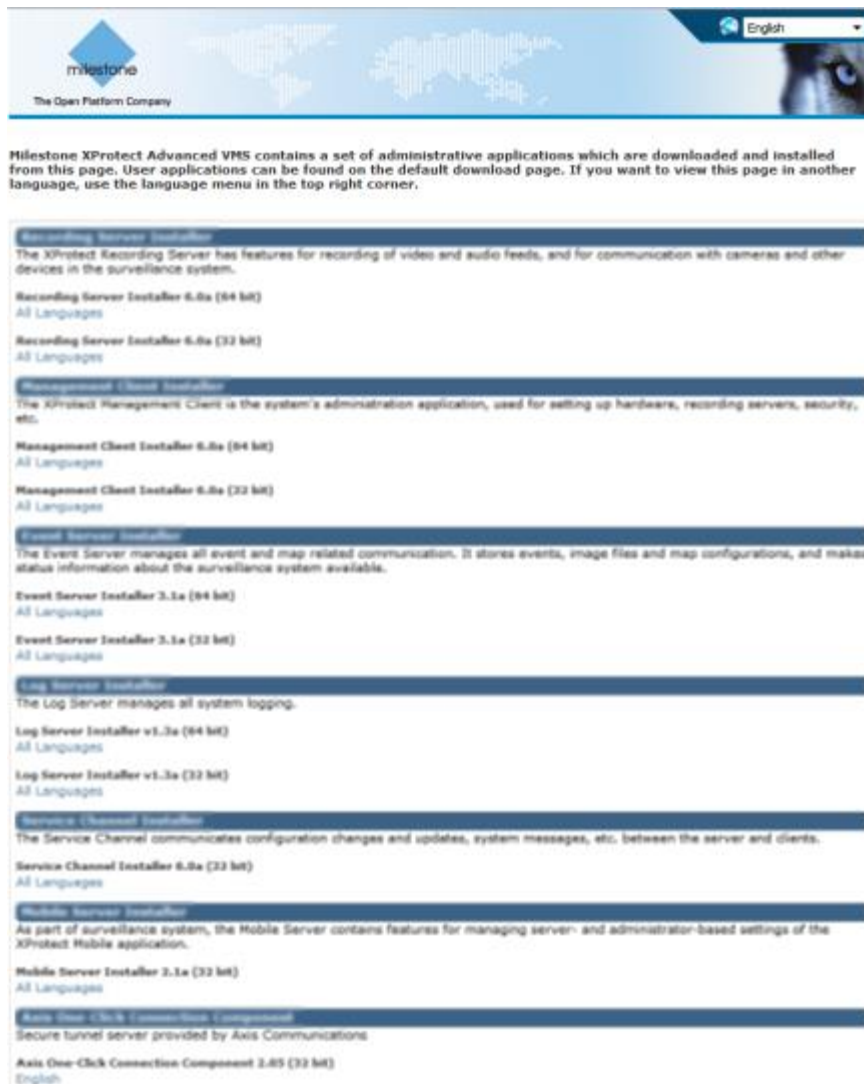
1. On the management server, go to the Management server's download web page from Windows' **Start** menu, select **Programs, Milestone, Administrative Installation Page**.
2. Select the Milestone Mobile server installer. Save the installer somewhere appropriate and run it from here or run it directly from the web page.
3. Follow the instructions on the screen to install.

Once you have installed the Milestone Mobile server, you can use Milestone Mobile client and XProtect Web Client with your system. To reduce the overall use of system resources on the computer running the management server, install the Milestone Mobile server on a separate computer. For more information about how to do this, see the Milestone Mobile server manual, available on the Milestone website.

For more information about XProtect Download Manager, see Download Manager/download web page (on page 40).

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 XProtect 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 > Milestone > Administrative Installation Page**. Otherwise you can enter the URL:

[http://\[management server address\]:\[port\]/installation/admin/](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 > Milestone > Public Installation Page**. Otherwise you can enter the URL:

[http://\[management server address\]:\[port\]/installation/](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.

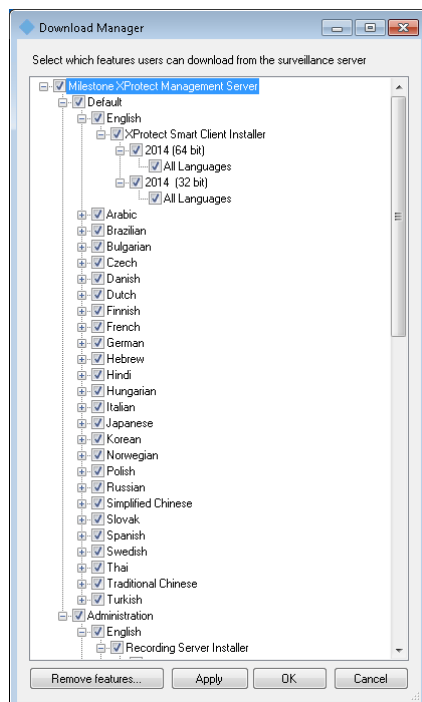
Even though you can control which components users can download and install in Download Manager, you cannot use it as a users' rights management tool. Such rights are determined by roles defined in the Management Client.

On the management server, you can access the XProtect Download Manager from Windows' **Start** menu, select **Programs > Milestone > XProtect 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 XProtect 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, including failover recording servers. Failover recording servers are initially downloaded and installed as recording servers, during the installation process you specify that you want a failover recording server.
- Management Client
- XProtect 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
- Axis One-click Connection Component - **only available here**
- Milestone 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 45).

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.

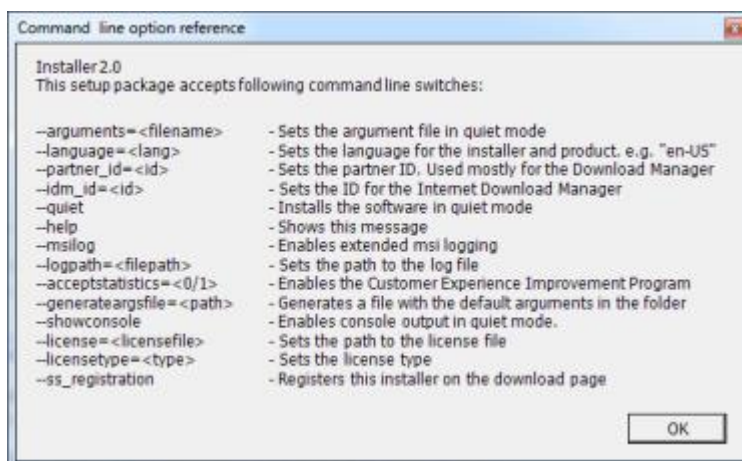
Adding new/non-standard files to the Download Manager:

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.

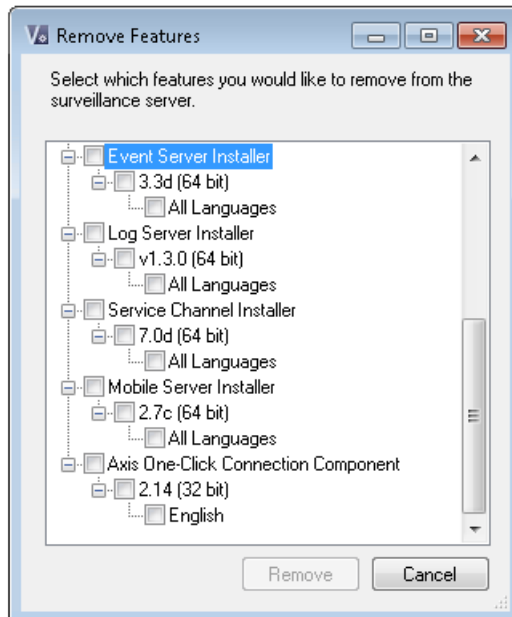
Hide/remove Download Manager installer components

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)\Milestone\XProtect Download Manager*, so you can re-install them later if required.
1. In the Download Manager, click **Remove features**.



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 Milestone website <http://www.milestonesys.com/downloads>.
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 XProtect installation.



Important: Your XProtect 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 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. Therefore, it is highly recommended to 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 **temporary license (.lic) file** ready. The license file changes when your SLC changes, so you may have received a new license file when you purchased the new version. When you install the management server, the wizard asks you to specify the location of your license (.lic) file, which the system verifies before you can continue.

If you do not have your license file, contact your XProtect product vendor.

- Have your **new product version** ready. If you have not purchased the software on a DVD, you can download it from <http://www.milestonesys.com/downloads>.
- 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, being the database owner of the management server's system configuration database on the SQL Server is sufficient.

When you are ready to start the upgrade, follow the procedures in Install the system (on page 30).

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 **Milestone XProtect 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 34).



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, Milestone 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 be 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. Typically, 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. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day has 25 hours. In that case, 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, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, your system forcefully archives the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour is not viewable directly from clients. However, the data is recorded and safe, and it can be browsed using the XProtect 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, Milestone 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 www.microsoft.com for **time server**, **time service**, or similar.



Management Client overview

About login authorization

If you encounter a second dialog during login, you need additional login authorization to get access to the Management Client.

When you log into the Management Client, you may be asked to for additional authorization of your login. You need a person who has the rights to authorize you to enter their credentials in the authorization login window.

If you do not know who can authorize you, ask your system administrator.

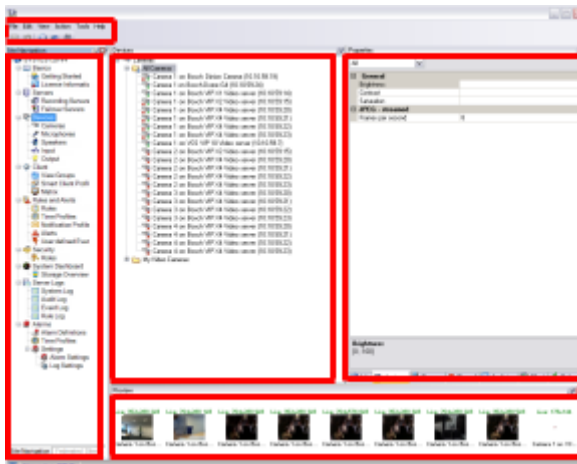
Management Client window overview

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

- system configuration
- task
- available functions.

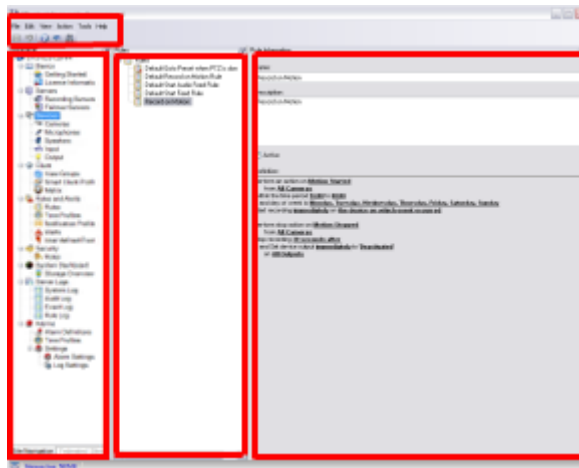
Below are some examples of typical layouts:

- When you work with recording servers and devices:

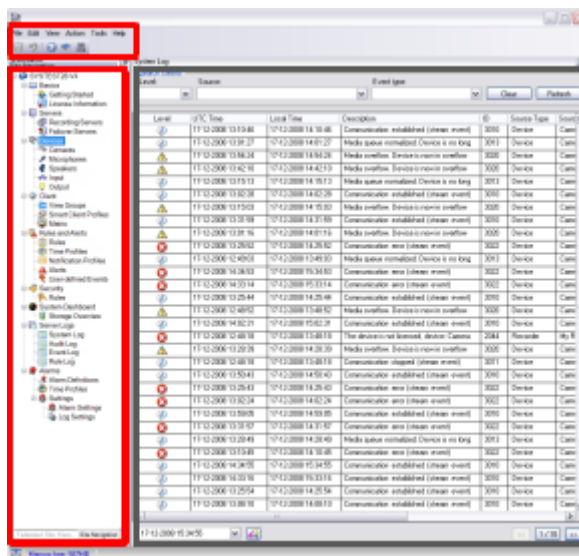




- When you work with rules, time and notification profiles, users, roles:



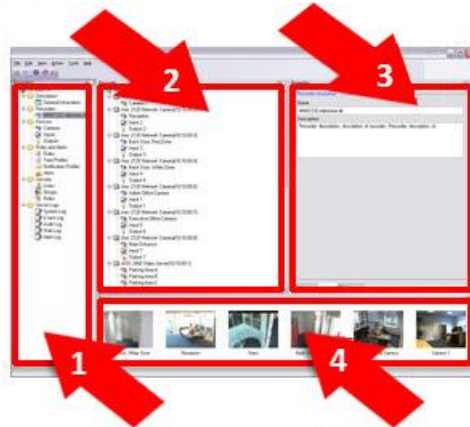
- When you view logs:





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 and Federated Sites Hierarchy 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 in to. The site name is visible at the top of the pane. The features are grouped into categories that reflect the functionality of the software.

Federated Site Hierarchy pane: This is your navigation element that displays Milestone Federated Architecture sites and their parent/child links.

The parent server that you are logged in to, your home site, is always at the top. If you adopt its point of view, you can view all its linked children and downwards in the parent/child hierarchy.

Overview pane: Provides an overview of the element you have selected in the **Site Navigation** pane, for example 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 properties of the element selected in the **Overview** pane. Often, properties are displayed across a number of 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:

Live: 640x480 88kB

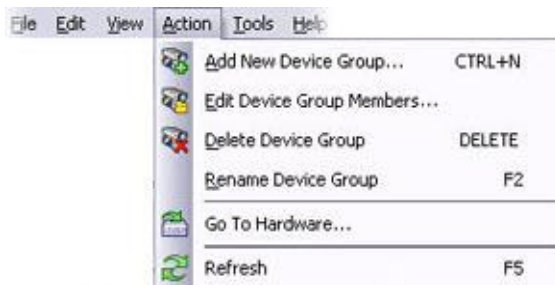


Camera 5

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 332).

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 .
Federated Site Hierarchy	By default, the Federated Site Hierarchy pane is enabled.
Site Navigation	By default, the Site Navigation pane is enabled.

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 56).



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 348).
Enterprise Servers	Add XProtect Enterprise servers to your system and manage the integration of the added servers. See About XProtect Enterprise servers (on page 327). You can also use the feature to migrate from an XProtect Enterprise system to XProtect Corporate. This is described in a separate document. Only supported if your system: <ul style="list-style-type: none"> - runs XProtect Corporate - uses IPv4 - works with XProtect Enterprise servers running XProtect Enterprise version 6.0 and up
Effective Roles	View all roles of a selected user or group. Only relevant if you run XProtect Corporate.
Options	Opens the Options dialog box, which lets you define and edit global system settings. Only relevant if you run XProtect Corporate.

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 the licenses on this site and on all other sites licensed on the same software license code (SLC).

Installed Products

Lists all installed products on this site:

- Product version.
- Software license code (SLC).
- Expiry date of your SLC. Typically unlimited.
- Expiry date of your software upgrade plan (SUP).

 **Installed Products**

Product Version	Software License Code	Expiry Date	Software Upgrade Plan Expiry
XProtect Corporate 2014	C70-A00C-xxxx	Unlimited	1/2/2014
Milestone XProtect Smart Wall	9A0-A09D-xxxx	Unlimited	
Milestone XProtect Access Control Module	C70-A00C-xxxx	N/A	

Licensed to:
Milestone Systems A/S

Contact details:
Banemarksvej 50C
2605 Brøndby
Greater Copenhagen Area Denmark

Log on to edit details [Link](#)

Contact details on the owner of the SLC

- Contact details of the customer (license owner) have been added during software registration. Click [Link](#) to edit the license owner information.



License Information

License Information

Type	Total - All Sites		Current Site			
	Obtained	Activated	Activated	Temporary	Expired	Missing
Hardware Device	100	26	1	0	0	0
Milestone Interconnect Camera	10	3	0	0	0	0
Door	4	0	0	0	0	0

Activate License

All Sites

Information refreshed Thursday, March 27, 2014 10:11:34 AM



Example only. Numbers and dates may be different on your system

- Unlicensed hardware devices do not send data to the surveillance system, so the hardware device's cameras cannot be used for monitoring and recording.
- Hardware devices that you add after all available licenses are used, are listed as missing so they cannot be used for monitoring and recording.
- Devices connected to unlicensed hardware devices are identified by an exclamation mark in the Management Client. Note that the exclamation mark is used for other purposes.

Total - All Sites lists the status of licenses on all sites obtained with this SLC:

- License type - hardware device:
 - The total number of obtained and activated hardware device licenses on all sites using this SLC.
 - If you run Milestone Interconnect, the total number of obtained and activated Milestone Interconnect camera licenses on all sites using this SLC.
- License type - doors:
 - If you run XProtect Access Control Module, the total number of obtained and activated door licenses on all sites using this SLC. Door licenses are only listed if you have purchased XProtect Access Control Module. You can also see license details for each door under the **Access Control** node.

Current Site:

- The number of licenses on the current site:
 - The number of activated licenses and temporary (not activated) licenses.



- If you need additional licenses for new hardware devices, add the number of missing licenses to the number of expired licenses to get the total number of required licenses.
- Expiry date of the next hardware device license appears in red below the table (if applicable). The date is counted from the day you added the hardware device.
- Drop-down list box to activate licenses online or offline.
- Button to access a license overview for all sites licensed via this SLC.

Devices which require a license

You need licenses for the number of hardware devices, for example video encoders or cameras, that you want to run on the system. One hardware device license enables you to run as many camera, speaker, microphone, input, output and metadata devices that the hardware device consists of. It also enables you to run the hardware device multiple times on one site or multiple times on multiple sites.

You need a camera license for each enabled interconnected camera in a Milestone Interconnect setup.

If you purchase XProtect Access Control Module, you need a license for each door you want to configure for access control.

You can always get more licenses as your surveillance system grows, see [Get additional licenses](#) (on page 60).

View license overview

You can access a license overview that lists activated, temporary, expired and missing licenses for all sites licensed via this SLC.

- Click **License Overview**.

If the site is not a federated site or the connection is down, you can only view the number of activated licenses. N/A appears for temporary, expired, and missing licenses.

Activate licenses online

Activate your licenses online if the computer that runs the Management Client has Internet access.

1. On the **License Information** node, select **Activate License** and then **Active License Online**.
2. The **Activate Online** dialog box opens.
 - If you are an existing user, enter your user name and password to log into the software registration system.
 - If you are a new user, click the **Create new user** link to set up a new user account and then follow the registration procedure. If you have not yet registered your Software License Code (SLC), you must do so.
3. If you select **Save password**, the password is saved on the computer.



4. Click **Next** and follow the wizard's remaining steps to activate your licenses. Use the exact same user name under which you registered the SLC.
5. When you have activated your licenses, you see a confirmation.
6. Click **Finish** to end the activation.

If you receive an error message during online activation, follow the instructions on the screen to solve the issue.

If you have followed the instructions and still cannot access online activation, contact Milestone Support, who investigates the issue for you.

Activate licenses offline

If the computer that runs the Management Client does not have Internet access, you can activate licenses offline. First you export the license request and provide it to Milestone, who then activates the licenses. When you receive the activated licenses, you import them into your system:

1. To export a file with your currently added cameras, click **Activate License**, and select **Activate License Offline > Export License For Activation**.
2. Specify a file name and a location for the license request (*.lrq*) file.
3. Open an Internet browser and go to the Milestone website <http://www.milestonesys.com>.
4. Locate the software registration page.
5. If you have used the software registration system before, log in with your username and password. Otherwise, click **New to the System?** to create a new user account and add the SLC to the account.
 - a) Select the SLC under **Active SLCs**.
 - b) In the menu for SLC properties, use the **Upload License Request** function to upload the generated LRQ file.
 - c) An email is sent to you.
6. When you have received the updated license file (*.lic*), save it at a location accessible from the Management Client.
7. In the Management Client, click **License Information**.
8. Click **Activate License Offline > Import Activated License**, and select the *.lic* file to import it.
9. Click **Finish** to end the activation process.

Activate licenses after grace period

If you do not activate an expired license (hardware, Milestone Interconnect system, or door license) within the grace period, the device becomes unavailable and cannot be used in the surveillance system.



- Configuration, added cameras, and other settings are not removed from the Management Client.
- The license is not deleted from the system configuration, so to enable the unavailable devices again, activate the license online or offline as usual.

Get additional licenses

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

1. To get additional licenses for your system, contact your XProtect product reseller.
2. When you have received an updated license file (.lic) with the new licenses, you must activate your licenses.

Licenses and hardware device replacement

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

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

If you, for example, 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, and then activate the license.

If you replace a hardware device with a different model, you must use the **Replace Hardware** wizard (see Replace hardware (on page 340)) to map all relevant databases of cameras, microphones, inputs, outputs, and settings. When done, remember to activate the license.

Over time, there is a limit to the number of hardware devices you can replace depending on the number of hardware devices in your system. You receive a message from the system to contact Support, when you try to active a license online that exceeds the maximum number of allowed replacements.

Site information

You can add additional information to a site for an easier identification of each site, for example, in a large Milestone Federated Architecture 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**.

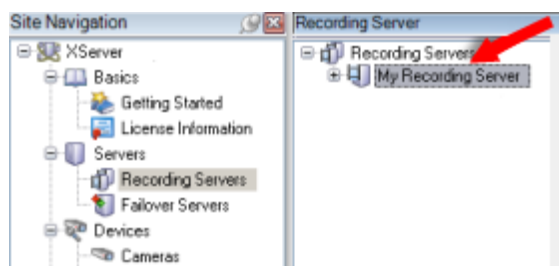
Servers and hardware

Recording servers

About recording servers

You use recording servers for recording video feeds, and for communicating with cameras and other devices. A surveillance system typically contains several recording servers, even though you only need a single recording server for the system to work.

Recording servers on your system, that is computers with the recording server software installed, and configured to communicate with a management server, are listed 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 servers from product versions older than this current version is limited. You can still access recordings on such older recording servers, but if you want to change their configuration, make sure they match the current version. Milestone recommends that you upgrade all recording servers in your system to the same version as your management server.

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, the recording server might not be able to rename or move relevant media files, which might bring the recording server to a halt. If this situation has already occurred, 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.

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
	<p>Recording server requires attention: This icon typically appears because the Recording Server service is stopped.</p> <ol style="list-style-type: none"> 1) Right-click the recording server icon in the notification area. 2) Start/stop the Recording Server service and view recording server status messages.
	<p>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:</p> <ol style="list-style-type: none"> 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.
	<p>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.</p> <p>See Protect recording databases from corruption (on page 48) for information about how to avoid corrupt databases.</p> <p>Important: During a database repair at startup, you cannot record video from cameras connected to the recording server. Only live viewing is available.</p> <p>A database repair at normal operation does not affect any recordings.</p>



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.

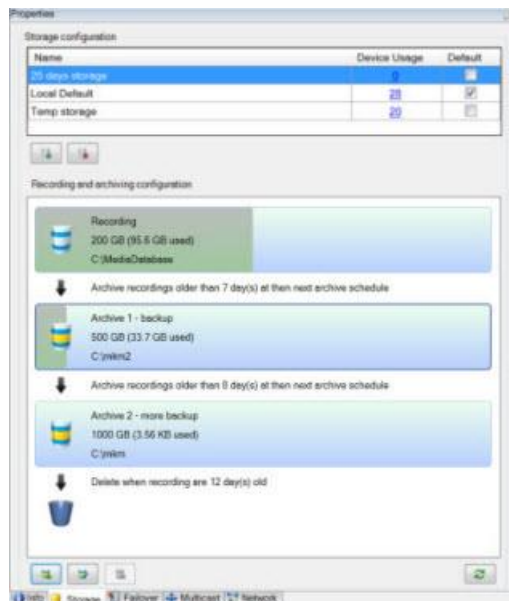
Info tab properties

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 XProtect 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 setup, manage and view storages for selected recording servers.



About storage and archiving

When a camera records video or audio, all specified recordings are per default stored in the storage defined for the device, in the default recording database named **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. You can also create archives within each storage and start an archiving process to store data.

Archiving is the automatic transfer of recordings from, for example, a camera's default 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 XProtect Smart Client to view them with. 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: Milestone 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 at <http://support.microsoft.com/kb/140365/en-us> <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 recording server

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 68).

Effective archiving

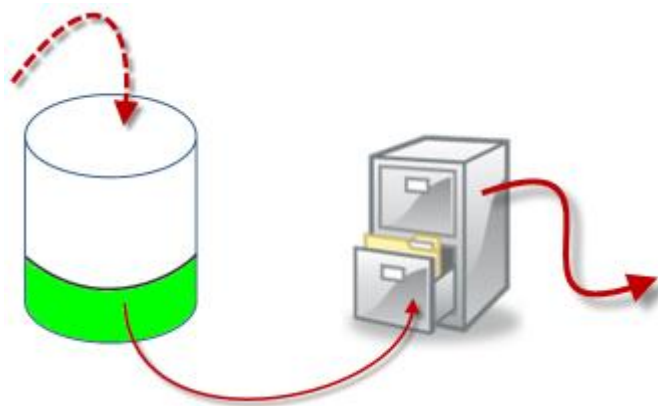
When you enable archiving for a camera or a group of cameras, the content of the camera database is automatically moved to an archive at intervals that you define.

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 and grooming 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
- Encryption
- 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 71).
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 67).

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 73)).
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  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 XProtect 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 69) and Backing up and restoring configuration (see "Backing up and restoring system configuration" on page 332).

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 XProtect 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 XProtect Smart Client to do very fast searches.
- **Signature:** This folder holds the signatures generated for the media data (in the Media folder). With this information you can verify that the media data has not been tampered with since it was recorded.
- **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 XProtect 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 XProtect 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 area

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 an entire storage area


The storage area that you want to delete must **not** be set as default storage area and it must **not** be used by any devices to hold recordings.



This means that you may need to move devices and any not yet archived recordings that they have to another storage area before you delete the storage area.

1. To see the list of devices that use this storage area, click the device usage number.
2. Follow Move non-archived recordings from one storage to another (on page 71).
3. Continue until you have moved all devices.
4. Select the storage area that you want to delete.

Storage configuration		
Name	Device Usage	Default
25 days storage	0	<input type="checkbox"/>
Local Default	28	<input checked="" type="checkbox"/>

5. Click the  button located below the **Storage configuration** list.
6. Click **Yes**.

Move non-archived recordings from one storage to another

You move contents from one 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 whether already existing - but **non-archived** - recordings should be moved along to the new storage or deleted.
6. Click **OK**.

Storage and Recording Settings properties

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

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



Name	Description
Name	Rename the storage if needed. Names must be unique.
Path	<p>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.</p> <p>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\\.</p>
Retention time	<p>Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings).</p> <p>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.</p>
Maximum size	<p>Select the maximum number of gigabytes of recording data to save in the recording database.</p> <p>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.</p> <p>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.</p>
Signing	Enables a digital signature to the recordings. This means, for example, that the system confirms that exported video has not been modified or tampered with when played back.
Encryption	<p>Select the encryption level of the recordings:</p> <ul style="list-style-type: none"> ▶ None ▶ Ligth (Less CPU usage) ▶ Strong (More CPU usage) <p>If you choose to enable encryption, you must also specify a password for the users that are allowed to view encrypted data.</p>
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	<p>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.</p> <p>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\\.</p>
Retention time	<p>Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings).</p> <p>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.</p>
Maximum size	<p>Select the maximum number of gigabytes of recording data to save in the recording database.</p> <p>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.</p> <p>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.</p>
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).
Reduce frame rate	<p>To reduce FPS when archiving, select the Reduce frame rate check box and set a frame per second (FPS).</p> <p>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.</p> <p>MPEG/H.264 reduces automatically to key-frames as a minimum.</p> <p>0.1 = 1 frame per 10 seconds.</p>



Failover tab (recording server)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

If your organization uses failover recording servers, use the **Failover** tab to assign failover servers to recording servers, see Failover tab properties (on page 74).

For details on failover recording servers, installation and settings, failover groups and their settings, see About failover recording servers (regular and hot standby) (see "About failover recording servers" on page 247).

Failover tab properties

Name	Description
None	Select a setup without failover.
Primary failover server group / Secondary failover sever group	Select a regular failover setup with one primary and possibly one secondary failover server group. Also, from the attached dropdown, select a primary failover group and possibly a secondary failover group.
Hot standby server	Select a hot standby setup. Also, from the dropdown, select a hot standby server.
Advanced failover settings	Opens the Advanced Failover Settings window. <ul style="list-style-type: none"> ▶ Full Support: Select to get full failover support for the device. ▶ Live Only: Select to get live failover support for the device. ▶ Disabled: Select to disable failover support for the device.
Failover service communication port (TCP)	By default, the port number is 11000. You use this port for communication between recording servers and failover recording servers. If you change the port, the recording server must be running and must be connected to the management server.

Multicast tab (recording server)

Your system supports multicasting of live streams from recording servers. If multiple XProtect 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.
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.
Source IP address for all multicast streams	<p>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.</p> <p>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.</p> <ul style="list-style-type: none">▶ IPv4: 224.0.0.0 to 239.255.255.255.▶ IPv6, the range is described on 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 XProtect 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 (and failover 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**.



Hardware and remote servers

About hardware

Hardware represents either:

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

See *Add hardware* (on page 78) 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 are 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. The wizard also helps you add remote recording servers for Milestone Interconnect setups. 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)	<p>The system scans automatically for new hardware on the recording server's local network.</p> <p>Select the Show hardware running on other recording servers check box to see if detected hardware is running on other recording servers.</p> <p>You can select this option every time you add new hardware to your network and want to use it in your system.</p> <p>You cannot use this option to add remote systems in Milestone Interconnect setups.</p>
Address range scanning	<p>The system scans your network for relevant hardware and Milestone Interconnect remote systems based on your specifications of:</p> <ul style="list-style-type: none"> ▶ hardware user names and passwords. Not needed if your hardware use the factory default user names and passwords. ▶ drivers ▶ IP ranges (IPv4 only) ▶ port number (default = 80) <p>You can select this option when you only want to scan a part of your network, for example, when you expand your system.</p>
Manual	<p>Specify details about each hardware and Milestone Interconnect remote systems 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.</p>
Remote connect hardware	<p>The system scans for hardware connected via a remotely connected server.</p> <p>You can use this option if you have installed servers for, for example, the Axis One-click Camera Connection.</p> <p>You cannot use this option to add remote systems in Milestone Interconnect setups.</p>

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 basic hardware settings

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

1. Expand 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.




Manage hardware

Info tab (hardware)

For information about the **Info** tab for remote servers, see Info tab (remote server) (on page 85).

Info tab (hardware)

Name	Description
Name	<p>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.</p> <p>When you rename hardware, the name is changed globally in the Management Client.</p>
Description	<p>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:</p>  <p>Example from a camera.</p>
Model	Identifies the hardware model.
Version	Displays the firmware version of the system as specified by the manufacturer.
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 remote system.
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.

For information about the **Settings** tab for remote servers, see Settings tab (remote server) (on page 85).

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:

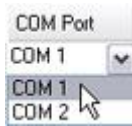
1. In the list of devices connected to the video encoder, select the **Enable PTZ** box for the relevant cameras:



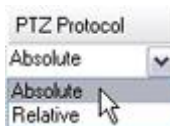
2. In the **PTZ Device ID** column, verify the ID of each camera.



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 112)
- Add a patrolling profile (on page 116)



Manage remote servers

Info tab (remote server)

Name	Description
Name	The system uses the name whenever the remote server is listed in the system and clients. The name does not have to be unique. When you rename a server, the name is changed globally in the Management Client.
Description	Enter a description of the remote server (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.
Model	Displays the XProtect product installed at the remote site.
Version	Displays the version of the remote system.
Software license code	The software license code of the remote system.
Driver	Identifies the driver that handles the connection to the remote server.
Address	The host name or IP address of the remote system.
IE	(Applies only to Arcus-enabled hardware) Opens the default home page of the hardware vendor. You can use this page for administration of the hardware or system.
Remote system ID	The unique system ID of the remote site used by XProtect to, for example, manage licenses.
Windows user name	(Does not apply to Arcus-enabled hardware) Enter the Windows user name for access through the remote desktop.
Windows password	(Does not apply to Arcus-enabled hardware) Enter the Windows password for access through the remote desktop.
Connect	(Does not apply to Arcus-enabled hardware) Opens a remote connection to the remote site (if Windows credentials are approved).

Settings tab (remote server)

On the **Settings** tab, you can view the name of the remote system.

Events tab (remote server)

You can add events from the remote system to your central site in order to create rules and thereby respond immediately to events from the remote system. The number of events depend on the events configured in the remote system. You cannot delete default events.



If the list appears to be incomplete:

1. Right-click the relevant remote server in the **Overview** pane and select **Update Hardware**.
2. The dialog box lists all changes (devices removed, updated and added) in the remote system since you established or last refreshed the Milestone Interconnect setup. Click **Confirm** to update your central site with these changes.

Remote Retrieval tab

On the **Remote Retrieval** tab, you can handle remote recording retrieval settings for the remote site in a Milestone Interconnect setup:

Specify the following properties:

Name	Description
Retrieve recordings at max	Determines the maximum bandwidth in Kbits/s to be used for retrieving recordings from a remote site. Select the check box to enable limiting retrievals.
Retrieve recordings between	<p>Determines that retrieval of recordings from a remote site are limited to a specific time interval.</p> <p>Unfinished jobs at the end time continue until completion, so if the end time is critical, you need to set it earlier to allow for unfinished jobs to complete.</p> <p>If the system receives an automatic retrieval or request for retrieval from the XProtect Smart Client outside the time interval, it is accepted, but not started until the selected time interval is reached.</p> <p>You can view pending remote recording retrieval jobs initiated by the users from System Dashboard -> Current Tasks.</p>
Retrieve on devices in parallel	Determines the maximum number of devices from which recordings are retrieved simultaneously. Change the default value if you need more or less capacity depending on your system's capabilities.

When you change the settings, it may take several minutes until the changes are reflected in the system.

None of the above applies to direct playback of remote recordings.

All cameras set to be played back directly is available for direct playback and use bandwidth as needed.

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.

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 87).

You can also manage the devices individually:

- Cameras
- Microphones
- Speakers
- Metadata
- Inputs
- Outputs

See About devices (on page 90).

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.

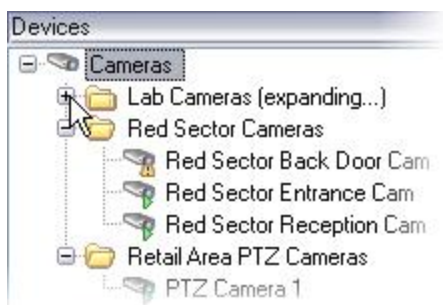
You can benefit from grouping different types of devices (cameras, microphones, speakers, metadata, inputs, and outputs) on your system:

- 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 88)

Specify which devices to include in a device group (on page 89)

Specify common properties for all devices in a device group (on page 90)

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.

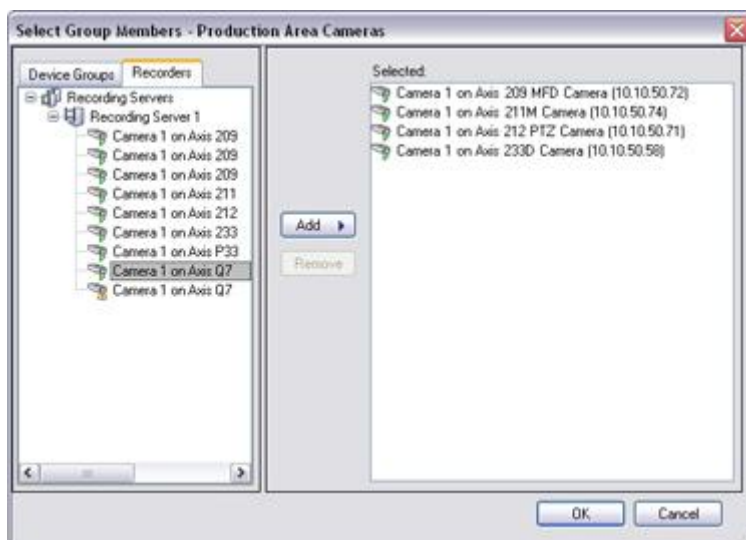
4. Click **OK**. A folder representing the new device group appears in the list.
5. Continue with Specify which devices to include in a device group (on page 89).

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.
- In a Milestone Interconnect setup, the remote system appears as hardware with all devices from the remote system listed in one list.

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

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.



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.

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.

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 96).

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 100)).
2. Configure streams (see Streams tab (see "Streams tab (devices)" on page 102)).
3. Configure motion (see Motion tab (see "Motion tab (devices)" on page 129)).
4. Configure recording (see Record tab (see "Record tab (devices)" on page 104)).
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 per 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.

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.



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 96).

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 98)
- Settings tab (see "Settings tab (devices)" on page 100)
- Record tab (see "Record tab (devices)" on page 104)
- Events tab (see "Events tab (devices)" on page 122)

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 per 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.

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.

The system sends an audio stream to the speakers when a user presses the talk button in XProtect Smart Client. Speaker audio is only recorded when talked to by an 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 96).

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 98)
- Settings tab (see "Settings tab (devices)" on page 100)
- Record tab (see "Record tab (devices)" on page 104)

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 3rd 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.

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.

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 96).

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 98)
- Settings tab (see "Settings tab (devices)" on page 100)
- Record tab (see "Record tab (devices)" on page 104)

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 recognizes 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 per 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.

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See *Enable/disable devices via device groups* (on page 96).

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.

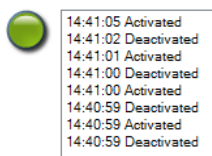
You can configure input devices on these tabs:

- Info tab (see "Info tab (devices)" on page 98)
- Settings tab (see "Settings tab (devices)" on page 100)
- Events tab (see "Events tab (devices)" on page 122)

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 XProtect 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 per 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.

For information about supported hardware, see the supported hardware page on the Milestone website <http://www.milestonesys.com/Support/Technical-Support/supportedhardware/xprotectcorporate/>.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See *Enable/disable devices via device groups* (on page 96).

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 98)
- Settings tab (see "Settings tab (devices)" on page 100)

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** pane, 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 per default enabled and all other devices are per 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.

A screenshot of a software window titled 'Properties'. Inside, there's a section labeled 'Device information'. It contains several input fields: 'Name:' with the text 'Axis 211W Camera (10.100.50.65) - Camera 1'; 'Description:' with an empty text area; 'Hardware name:' with the text 'Axis 211W Camera (10.100.50.65)' and a blue arrow button to its right; and 'Port number:' with the value '1'.

Example of **Info** tab from a camera.

Info tab properties



Name	Description
Name	<p>The name is used whenever the device is listed in the system and clients.</p> <p>When you rename a device, the name is changed globally in the Management Client.</p>
Description	<p>Enter a description of the device (optional).</p> <p>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.</p>
Hardware name	<p>Displays the name of the hardware, with which the device is connected. The field is non-editable from here, but you can be change it by clicking Go To next to it. This takes you to hardware information where you can change the name.</p>
Port number	<p>Displays the port on which the device is attached on the hardware.</p> <p>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.</p>



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:

Properties

Axis 211W Camera

General	
Brightness	50
Include Date	No
Include Time	No
Rotation	0
Saturation	50
Sharpness	0
JPEG - streamed	
Compression	30
Frames per second	8
Resolution	640x480
JPEG 2 - streamed	
Compression	30
Frames per second	8
Resolution	640x480
JPEG 3 - streamed	
Compression	30
Frames per second	8
Resolution	640x480
MPEG-4 - streamed	
Bit rate control priority	Framerate
Frames per second	30
Maximum bit rate	3000
Maximum compression	100
Minimum compression	0
Resolution	640x480
Target bit rate	9900

Saturation
A numeric value between 0 and 100.

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 MPEG4, MJPEG, and H.264, you can use multi-streaming, see About multi-streaming (on page 103).

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 XProtect Smart Client. For example, XProtect Smart Client requires a keyframe to start up showing video, so a longer period between keyframes, prolongs the XProtect 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.

Properties

Stream information

Stream	Name	Live Mode	Default	Record	Remote Record
MPEG-4 - 1 - stream...	MPEG-4 - 1 - streamed	Always	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MPEG-4 - 2 - stream...	MPEG-4 - 2 - streamed	When needed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Delete

Info Settings Streams Record 360° Lens Events Client Privacy Mask Motion



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. The number of available streams in a Milestone Interconnect setup depends on the capabilities of the interconnected system.

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 XProtect Smart Client.
3. In the **Live Mode** column, select when live streaming is needed.
 - **Always**: the stream runs even if no XProtect 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 an XProtect Smart Client user 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**.



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.

Properties

Recording settings

☒ Recording

☒ Record on related devices

☒ Pre-buffer: seconds

☒ Stop manual recording after: minutes

Recording frame rate:

JPEG: FPS

H.264/MPEG4: ☐ Record keyframes only

Storage

Local Default

Select...

Status: Active

Status	Database	Path	Used space
OK	Local Default	C:\MediaDatabase	17.7 MB

Total used space: 17.7 MB

Delete All Recordings

Remote recordings

☐ Automatically retrieve remote recordings when connection is restored

Info

Settings

Streams

Record

360° Lens

Events

Client

Privacy Mask

Motion

Record tab, example from camera



Enable playback directly from remote site camera

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.
3. In the Properties pane, select the **Record** tab, and select the **Play back recordings from remote system** option.
4. In the toolbar, click **Save**.

In a Milestone Interconnect™ setup, the central system disregards privacy masking defined in a remote system.

Enable/disable recording

Recording is by default enabled. To enable/disable recording:

1. Select the device.
2. Select/clear the **Record** tab's **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 the device.

Enable recording on related devices

For camera devices, you can enable recording for related devices 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. Select/clear the **Record on related devices** box.
2. On **Camera > 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 in the media database 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.

Devices that support pre-buffering

Cameras, microphones and speakers support pre-buffering. For speakers, the streams are only sent when an XProtect 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 XProtect 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.

1. To enable/disable pre-buffering, select/clear the **Pre-buffer (in seconds)** check box.
2. When you enable it, specify a pre-buffer size. The number of seconds you specify must be sufficiently large to accommodate your requirements in the various recording rules you define.

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.

Perform an action on **Motion Started**
from **Red Sector Entrance Cam**
start recording **5 seconds before** on **the device on which event occurred**

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 XProtect Smart Client users.

☒ Stop manual recording after: minutes

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.

A screenshot of a user interface element. It shows a label "Recording frame rate:" followed by a text input field containing the number "5". To the right of the input field is a small icon with up and down arrows, and further right is the text "FPS".

Specifying a specific recording frame rate

Enable keyframe recording

You can enable keyframe recording for H.264 and MPEG4 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.

A screenshot of a user interface element. It shows two rows of settings. The first row is "Recording frame rate:" with a text input field containing "5", a small icon with up and down arrows, and the text "FPS". The second row is "H.264/MPEG4:" followed by a checked checkbox and the text "Record keyframes only".

Enabling keyframe recording

2. Set up a rule that activates the function, see About actions and stop actions (on page 144).

About storage



Under **Storage**, you can monitor and edit database settings for the device.

Status	Database	Path	Used space
OK	Local Default	C:\MediaDatabase	5.40 GB

At the top, you can see the selected database and its status. In this example, the selected database is the default **Local Default** and the status is **Active**.

Possible statuses for selected database:

Name	Description
Active	Database is active and running.
Archives also located in old storage	Database is active and running and has archives located in other storage areas as well.
Data for some of the devices chosen is currently moving to another location	Database is active and running and 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	Database is active and running and is moving data for the selected device from one location to another.
Information unavailable in failover mode	Status information about the database cannot be collected when database is in failover mode.

Further down in the window, you can see the individual status of the databases (**OK** or **Old Storage**), location and how much space they each use.

In the **Total used space** field, you can see the total spaced used for the entire storage.

For information about configuration of storage, see About storage and archiving (on page 65).

About remote recording

The remote recording option is only available if the selected camera supports edge storage or is a camera in a Milestone Interconnect setup.

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.



- For a Milestone Interconnect remote system, recordings are retrieved from the remote systems' recording servers.

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:

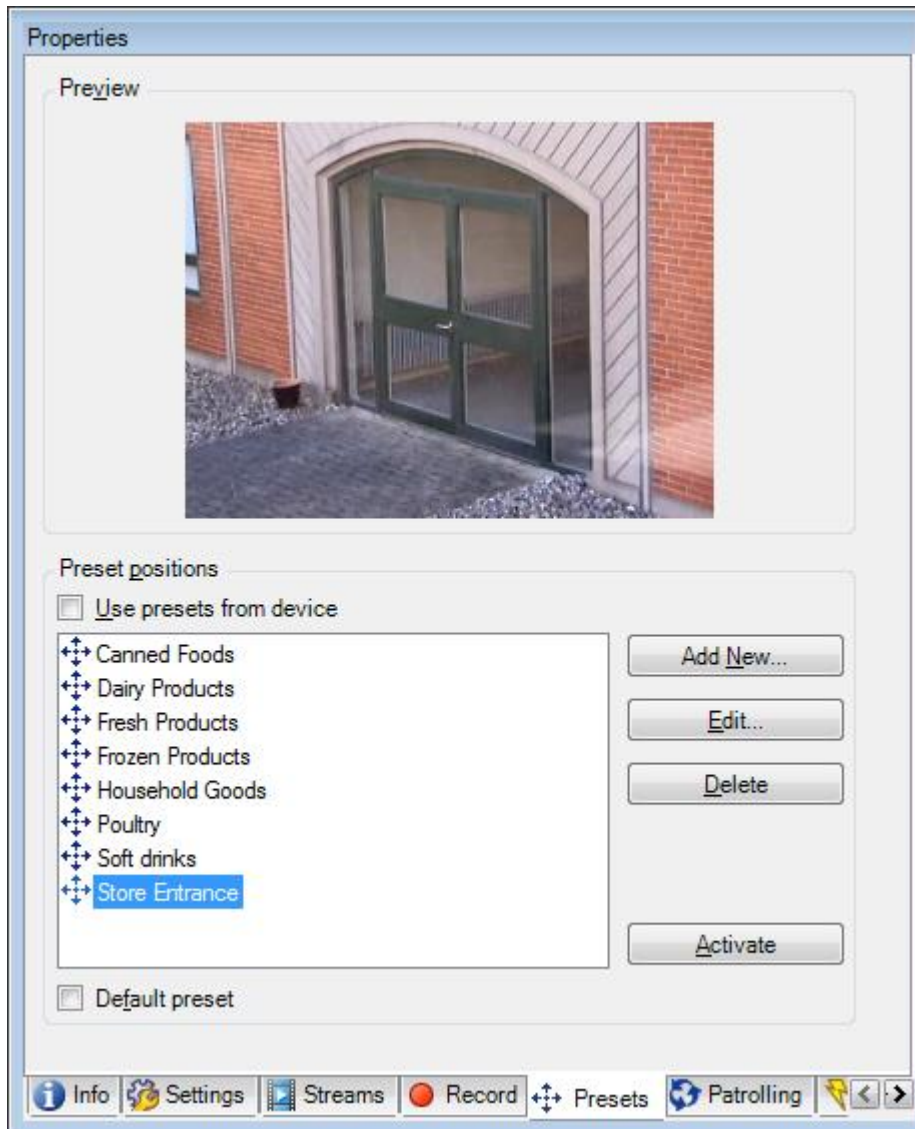
- PTZ cameras that support preset positions

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 XProtect Smart Client users.

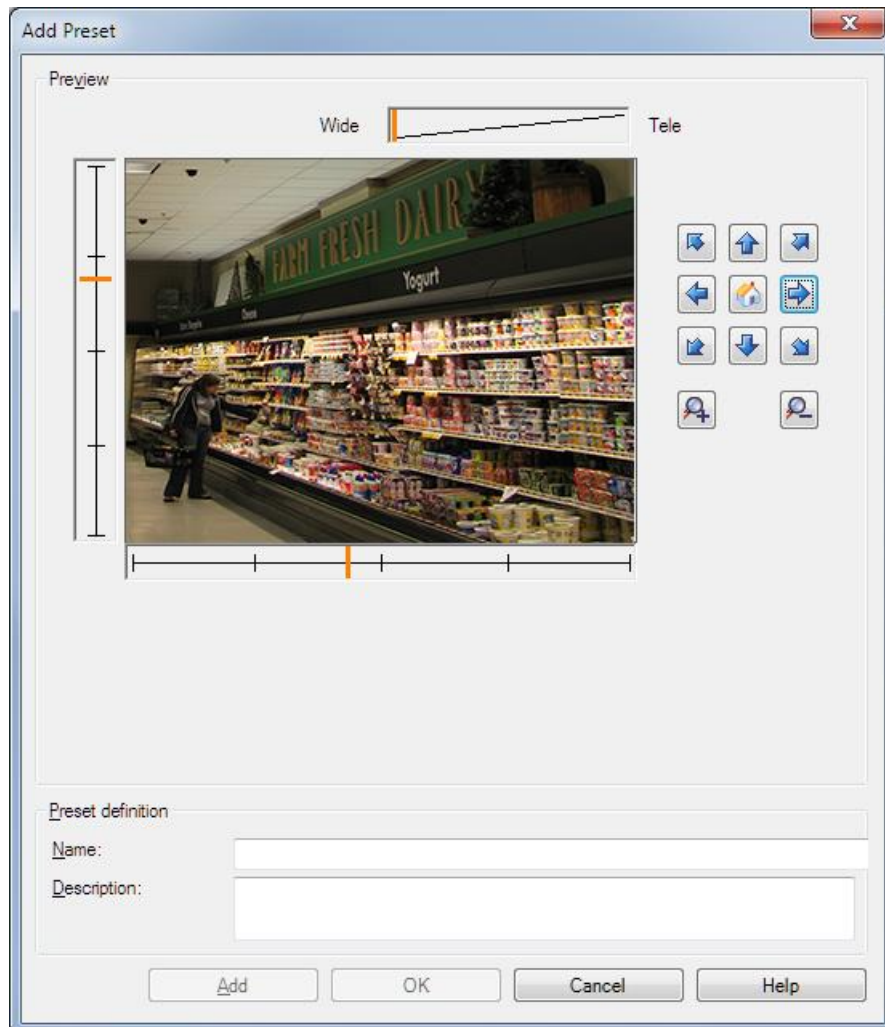


Presets tab, with eight preset positions defined

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. Click **Add** if you want to specify more presets.
6. 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**.
2. 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 XProtect Smart Client users.
3. 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.

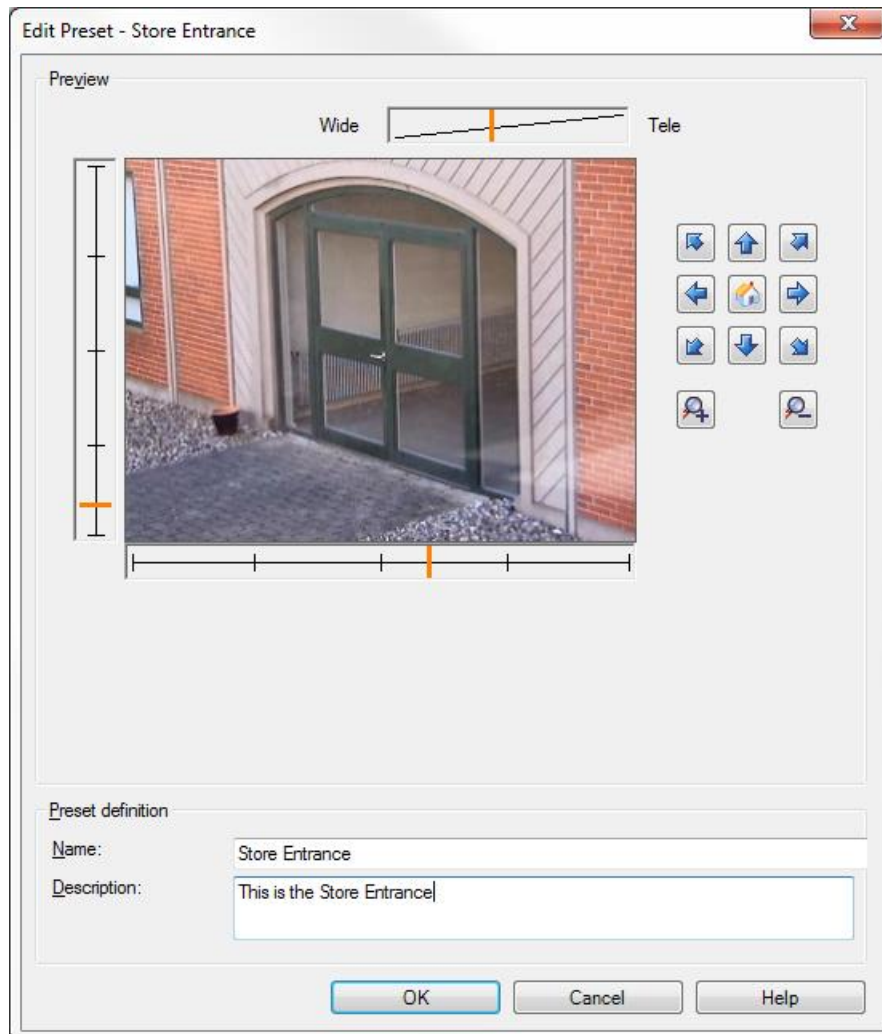
Edit a preset position (type 1 only)

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 a live preview image 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 as required.
5. Click **OK**.

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.



Patrolling tab (devices)

About the Patrolling tab

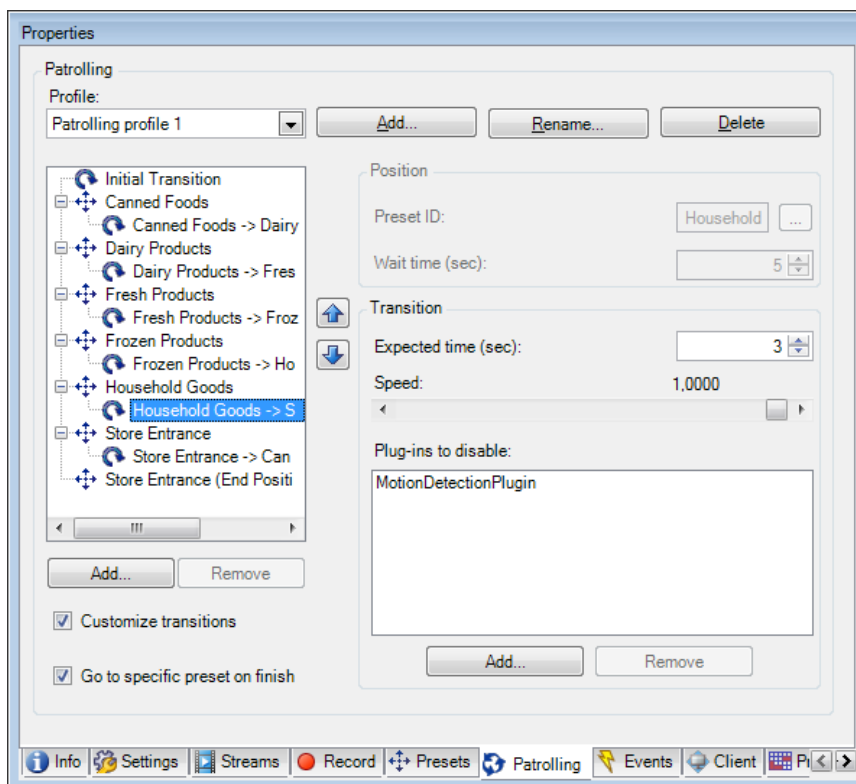
The following devices have a **Patrolling** tab:

- 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 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

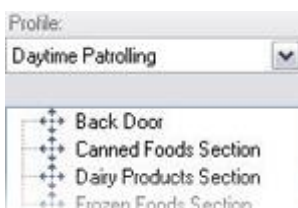
1. Select the patrolling profile in the **Profile** list:



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 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:

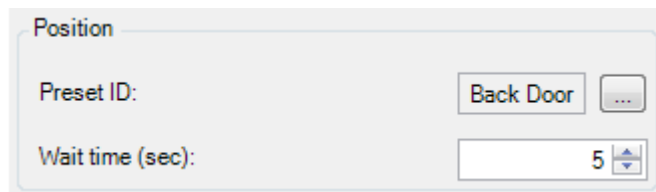
1. Select the patrolling profile in the **Profile** list.



2. Select the preset position for which you want to change the time:



3. Specify the time in the **Wait time (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
- Which plug-ins to disable during 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:

Expected time (secs.)

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. In the **Plug-ins to disable** list, specify any plug-ins you want to disable during the selected transition. By default, the plug-in used for motion detection on the camera (*MotionDetectionPlugin*) is disabled in order to avoid irrelevant motion being detected during transition.
 1. To add a plug-in that you want to disable during the transition, click **Add**, and select the plug-in.
 2. To remove a plug-in from the list, for example if you want motion detection enabled during the transition, select the plug-in and click **Remove**.
7. 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 preset on finish** check box. This opens the **Select Preset** dialog box.
3. In the **Select Preset** dialog box, 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.

Specify manual PTZ session timeout

XProtect Smart Client users can manually interrupt the patrolling of PTZ cameras.



You can specify how much time should pass before regular patrolling is resumed after a manual interruption:

1. Select **Tools > Options**.
2. On the **Options** window's **General** tab, select the amount of time in the **PTZ manual session timeout** list (default is 15 seconds).

The setting applies for all PTZ cameras on your system.



360° Lens tab (devices)

About the 360° Lens tab

The following devices have a **360° Lens** tab:

- Fixed cameras with a dedicated ImmerVision 360° lens

On the **360° Lens** tab, you can enable and configure panomorph support for the selected camera.



Enable and disable panomorph support

The panomorph feature is disabled by default.

To enable or disable it, select or clear the **360° Lens** tab's **Enable panomorph support** check box.

Specify Panomorph settings

When you enable the panomorph support functionality:

1. 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 <http://www.immervision.com/en/home/index.php>
<http://www.immervision.com/en/home/index.php>.

2. Specify the physical position/orientation of the camera from the **Camera position/orientation** list.



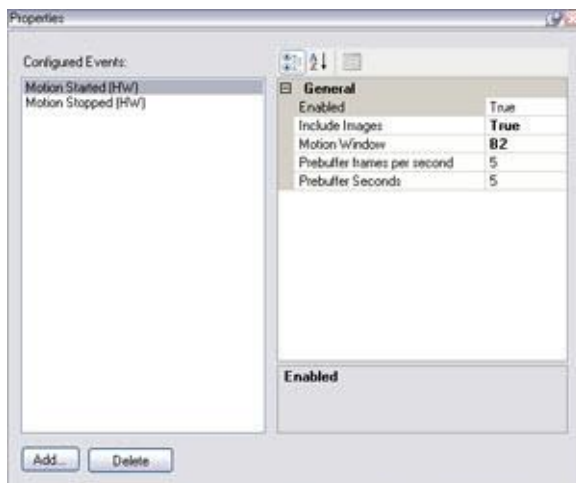
Events tab (devices)

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 122)
- Specify event properties (on page 123)
- Use several instances of an event (on page 123)

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.

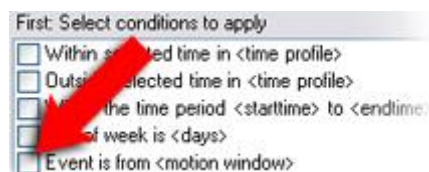
Use several instances of an event

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)

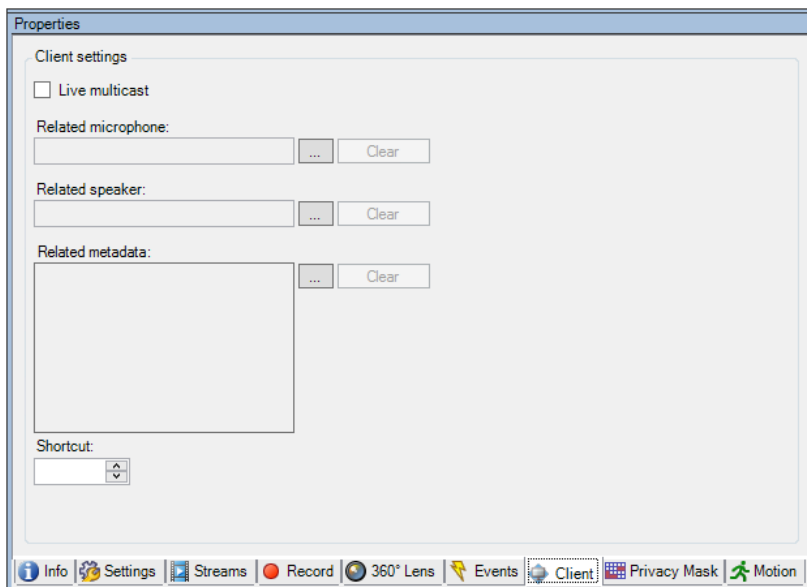
About the Client tab

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 XProtect Smart Client.

The related devices also record when the camera records, see Enable recording on related devices (on page 106).





Client tab properties

Name	Description
Live multicast	<p>The system supports multicast of live streams from the recording server to XProtect Smart Client. To enable multicast of live streams from the selected camera, select the check box.</p> <p>You must also configure multicasting for the recording server. See About multicasting (on page 75).</p> <p>If multicast streams do not work, for example due to restrictions on the network or on individual clients, the system reverts to unicast.</p>
Related microphone	<p>Specify from which microphone on the camera, that XProtect Smart Client users by default receive audio. The XProtect Smart Client user can manually select to listen to another microphone if needed.</p> <p>The related microphones record when the camera records.</p>
Related speaker	<p>Specify through which speakers on the camera, that XProtect Smart Client users speak by default. The XProtect Smart Client user can manually select another speaker if needed.</p> <p>The related speakers record when the camera records.</p>
Related metadata	<p>Specify one or more metadata devices on the camera, that XProtect Smart Client users receive data from.</p> <p>The related metadata devices record when the camera records.</p>
Shortcut	<p>To ease the selection of cameras for the XProtect Smart Client users, define keyboard shortcuts to the cameras.</p> <ul style="list-style-type: none"> ▶ Create each shortcut so it uniquely identifies the cameras. ▶ A camera shortcut number cannot be longer than four digits.



Privacy mask tab (devices)

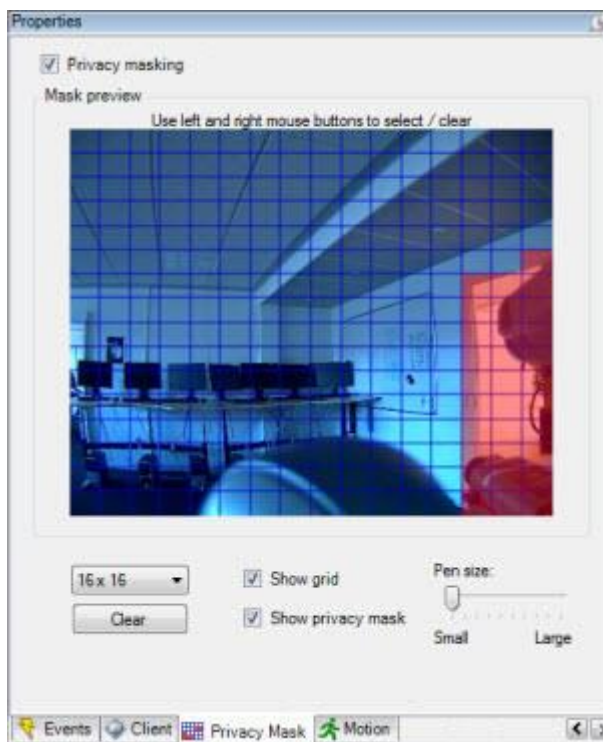
About the Privacy Mask tab

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 XProtect 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 Milestone Interconnect™ setup, the central system disregards privacy masking defined in a remote system.

Enable/disable privacy masking

The privacy masking feature is disabled by default.



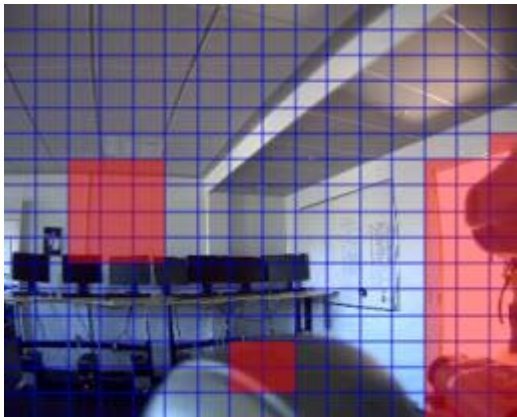
To enable/disable the privacy masking feature for a camera:

- 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 appears in the preview image on the **Motion** tab.



Privacy mask tab (properties)

Name	Description
Grid Size	<p>The value you selected in the Grid size list determines the density of the grid, regardless whether the grid is shown or not.</p> <p>Select between the values 8×8, 16×16, 32×32 or 64×64.</p>
Show Grid	<p>Select the Show grid check box to make the grid visible.</p>
Show Privacy Mask	<p>When you select the Show privacy mask check box (default), selected regions are highlighted in red in the preview image.</p> <p>Hiding regions may provide a less obscured view of the preview image.</p> <p>Milestone recommends that you keep the Show privacy mask box selected to avoid that regions exist without you or your colleagues being aware of it.</p>
Pen size	<p>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.</p>



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, Milestone 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 130)



- Specify motion detection settings (on page 130)

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 per default set up for dynamic sensitivity. To adjust the sensitivity level manually, see Enable manual sensitivity (on page 130).

Milestone 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 MPEG4 and H.264.

Motion detection on keyframes reduces the amount of processing power used to carry out the analysis.

- Select **Keyframes only (MPEG)** 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 is 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** drop down-box, 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.

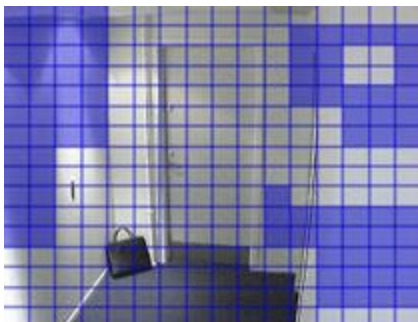
When you use exclude regions with PTZ cameras and you pan-tilt-zoom the camera, the excluded area does **not** move accordingly because the area is locked to the camera image, and not the object.

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

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

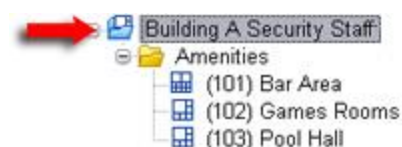
The Client section of the Management Client consists of:

Name	Description
XProtect Smart Wall	XProtect Smart Wall is an add-on that allows you to send view content from XProtect Smart Client to dedicated video wall. For more detailed information about XProtect Smart Wall, see About XProtect Smart Wall (on page 273).
View groups	The way in which video from cameras is presented is called a view. To control who can see what in XProtect 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 XProtect Smart Client users, you can create Smart Client profiles, prioritize these and customize their profiles as needed for the different tasks at hand.
Management Client profiles	To differentiate Management Client administrator users, you can create Management 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 XProtect 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 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 XProtect 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

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

Smart Client profiles allows system administrators to control how XProtect Smart Client should look and behave and what features and panes XProtect 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 135).



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 XProtect 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 XProtect Smart Client user rights.

Example: You need a user in your XProtect 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.

Smart Client profile properties

There are the following tabs with options for Smart Client profiles. You can lock the settings in the Management Client if required:



Name	Description
Info	<p>Name and description, priority of existing profiles and an overview of which roles use the profile.</p> <p>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.</p>
General	<p>Settings such as show/hide and mini- and maximize menu settings, login/-out, startup, timeout, info and messaging options, and Sequence Explorer settings.</p>
Advanced	<p>Advanced settings such as maximum decoding threads, deinterlacing and time zone settings.</p> <p>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, for which the performance improvement potential can be significant, and less relevant if using, for example, JPEG or MPEG-4.</p> <p>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.</p>
Live	<p>Availability of live tabs/panes, camera playback and overlay buttons, bookmarks, bounding boxes, and live-related MIP plug-ins.</p>
Playback	<p>Availability of playback tabs/panes, layout of print reports, independent playback, bookmarks, bounding boxes, and playback-related MIP plug-ins.</p>
Setup	<p>Availability of general setup/panes/buttons, setup-related MIP plug-in and rights to edit a map and to edit live video buffering.</p>
Exports	<p>Paths, privacy masks, video and still image formats and what to include when exporting these, export formats for XProtect Smart Client – Player and much more.</p>
Timeline	<p>Whether to include audio or not, visibility of indication of time and motion, and finally how to handle playback gaps.</p>
Access Control	<p>Select if access request notifications should pop up on the XProtect Smart Client screen when triggered by events.</p>
View Layouts	<p>Which type(s) of views should be available. Expand the Layouts folder and, if relevant, use Select All or Select None as shortcuts when making your selections.</p>



Management Client profiles

About Management Client profiles

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

Management Client profiles allow system administrators to modify the Management Client user interface. Associate Management Client profiles with roles to limit the user interface to represent the functionality available for each administrator role.

To associate a role with a management client profile, see the Role Settings' Info tab (see "Info tab (roles)" on page 191). Note that Management Client profiles only handle the visual representation of system functionality, not the actual access to it.

To limit the overall access to system functionality for a role, see the Role Settings' Overall Security tab (see "Overall Security tab (roles)" on page 193).

You can change settings for the visibility of all Management Client elements. By default, the Management Client profile can see all functionality in the Management Client.

- To limit visibility of functionality, clear the check boxes for the relevant functionality in order to remove the functionality visually from the Management Client for any Management Client user with a role associated with this Management Client profile.

Add and configure a Management Client profile

If you do not want to use the default profile, you can create a Management Client profile before you can configure it.

1. Right-click **Management Client Profiles**.
2. Select **Add Management Client Profile**.
3. In the **Add Management 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. On the **Profile** tab, select or clear functionality from the Management Client profile.

Copy a Management Client profile

If you have a Management Client profile with settings that you would like to reuse, you can copy an already existing profile and make minor adjustments to the copy instead of creating a new profile from scratch.

1. Click **Management Client Profile**, right-click the profile in the **Overview** pane, select **Copy Management 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 and go to the **Info** tab or **Profile** tab to configure the profile.



Management Client profile properties

Info tab (Management Client Profiles)

On the **Info** tab, you can set the following for Management Client profiles:

Component	Requirement
Name	Enter a name for the Management Client profile.
Priority	Use the up and down arrows to set a priority for the Management Client profile.
Description	Enter a description for the profile. This is optional.
Roles using the Management Client profile	This field shows the roles that you have associated with the Management Client profile. You cannot edit this.

Profile tab (Management Client Profiles)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

On the **Profile** tab, you can enable or disable the visibility of the following elements from the Management Client's user interface:

Navigation

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the various features and functionality located in the **Navigation** pane.



Navigation element	Description
Basics	Allows the administrator user associated with the Management Client profile to see License Information and Site Information .
Remote Connect Services	Allows the administrator user associated with the Management Client profile to see Axis One-click Camera Connection .
Servers	Allows the administrator user associated with the Management Client profile to see Recording Servers and Failover Servers .
Devices	Allows the administrator user associated with the Management Client profile to see Cameras, Microphones, Speakers, Metadata, Input and Output .
Client	Allows the administrator user associated with the Management Client profile to see Smart Wall, View Groups, Smart Client Profiles, Management Client Profiles and Matrix .
Rules and Events	Allows the administrator user associated with the Management Client profile to see Rules, Time Profiles, Notification Profiles, User-defined Events, Analytics Events and Generic Events .
Security	Allows the administrator user associated with the Management Client profile to see Roles and Basic Users .
System Dashboard	Allows the administrator user associated with the Management Client profile to see System Monitor, Evidence Lock, Current Tasks and Configuration Reports .
Server Logs	Allows the administrator user associated with the Management Client profile to see System Log, Audit Log and Rule Log .
Access Control	Allows the administrator user associated with the Management Client profile to see Access Control features, if you have added any access control system integrations or plug-ins to your system.

Details

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the various tabs for a specific device channel, for example the **Settings** tab or **Record** tab for cameras.



Device channel	Description
Cameras	Allows the administrator user associated with the Management Client profile to see some or all camera-related settings and tabs.
Microphones	Allows the administrator user associated with the Management Client profile to see some or all microphone-related settings and tabs.
Speakers	Allows the administrator user associated with the Management Client profile to see some or all speaker-related settings and tabs.
Metadata	Allows the administrator user associated with the Management Client profile to see some or all metadata-related settings and tabs.
Input	Allows the administrator user associated with the Management Client profile to see some or all input-related settings and tabs.
Output	Allows the administrator user associated with the Management Client profile to see some or all output-related settings and tabs.

Tools Menu

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the elements that are part of the **Tools** menu.

Tool Menu option	Description
Registered Services	Allows the administrator user associated with the Management Client profile to see Registered Services .
Effective Roles	Allows the administrator user associated with the Management Client profile to see Effective Roles .
Options	Allows the administrator user associated with the Management Client profile to see Options .
Enterprise Servers	Allows the administrator user associated with the Management Client profile to see Enterprise Servers .

Federated Sites

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the Federated Sites Hierarchy pane.

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 XProtect 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 XProtect Smart Client, must be configured to receive Matrix-triggered video. See the Matrix Monitor and XProtect Smart Client documentation for more information.

Add Matrix recipients

To add an existing Matrix recipient, for example an existing Matrix Monitor or XProtect 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 XProtect Smart Client, see the separate Matrix Monitor or XProtect 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 XProtect Smart Client views

If the Matrix-recipient is XProtect Smart Client, you can send the same video to Matrix positions in several of XProtect Smart Client's views, provided the views' Matrix positions share the same port number and password:

1. In XProtect 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 XProtect 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.

Perform an action on [Motion Start](#)
from [Camera 2](#)
start recording [3 seconds before](#) on [the device on which event occurred](#)

Perform stop action on [Motion End](#)
from [Camera 2](#)
stop recording [immediately](#)

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**:

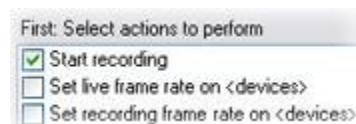


- **Rules:** Rules are a central element in the system. The behavior of your surveillance system is to a very large extent determined by rules. When creating a rule, you can work with all types of events.
- **Time profiles:** Time profiles are periods of time defined in the Management Client. You use 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 XProtect event server by sending simple strings via the IP network to your system.

See Events overview (on page 152) for a list of events.

About actions and stop actions

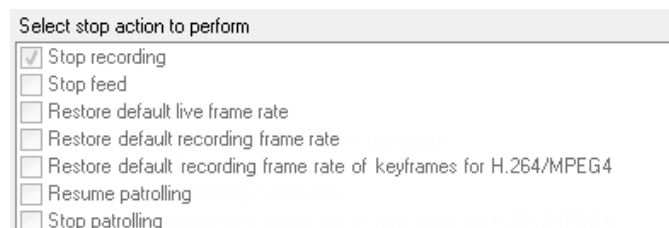
When you add rules in the **Manage Rule** wizard, you can select between different actions:



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 XProtect 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>	<p>Start recording and saving data in the database from the selected devices.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to specify:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Without this stop action, recording would potentially continue indefinitely. You also have the option of specifying further stop actions.</p>
Start feed on <devices>	<p>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.</p> <p>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.</p> <p>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.</p> <p>You can also specify further stop actions.</p> <p>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.</p> <p>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.</p>
Set <Smart Wall> to <preset>	<p>Sets the XProtect Smart Wall to a selected preset. Specify the preset on the Smart Wall Presets tab.</p> <p>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.</p>



Action	Description
Set <Smart Wall> <monitor> to show	<p>Sets a specific XProtect Smart Wall monitor to display live video from the selected cameras on this site or any child site configured in Milestone Federated Architecture.</p> <p>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.</p>
Set live frame rate on <devices>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Without this stop action, the default frame rate would potentially never be restored. You also have the option of specifying further stop actions.</p>
Set recording frame rate on <devices>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Without this stop action, the default recording frame rate would potentially never be restored. You also have the option of specifying further stop actions.</p>
Set recording frame rate to all frames for H.264/MPEG4 on <devices>	<p>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.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to select which devices the action should apply for.</p> <p>You can only enable keyframe recording for H.264 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.</p> <p>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</p>



Action	Description
	<p>the stop action:</p> <p>Restore default recording frame rate of keyframes for H.264/MPEG4</p> <p>Without this stop action, the default setting would potentially never be restored. You also have the option of specifying further stop actions.</p>



Action	Description
Start patrolling on <device> using <profile> with PTZ priority <priority>	<p>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.</p> <p>If you have upgraded your system from an older version of the system, the old values (Very Low, Low, Medium, High and Very High) have been translated as follows:</p> <ul style="list-style-type: none"> ○ Very Low = 1000 ○ Low = 2000 ○ Medium = 3000 ○ High = 4000 ○ Very High = 5000 <p>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.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the Patrolling tab.</p> <p>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:</p> <p>Stop patrolling</p> <p>Without this stop action, patrolling would potentially never stop. You can also specify further stop actions.</p>
Pause patrolling on <devices>	<p>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.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the Patrolling tab.</p> <p>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</p> <p>Without this stop action, patrolling would potentially pause indefinitely. You have also the option of specifying further stop actions.</p>
Move <device> to <preset> position with PTZ priority	<p>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</p>



Action	Description
<priority>	<p>one camera can be selected. It is not possible to select several preset positions.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>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.</p> <p>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.</p>
Move to default preset on <devices> with PTZ priority <priority>	<p>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.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>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.</p> <p>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.</p>
Set device output to <state>	<p>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.</p> <p>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.</p> <p>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.</p>
Create bookmark on <device>	<p>Creates a bookmark on live streaming or recordings from a selected device. A bookmark makes it easy to retrace a certain event or period in time. Bookmark settings are controlled from the Options dialog box. When you select this type of action, the Manage Rule wizard prompts you to specify bookmark details and select devices.</p> <p>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.</p>



Action	Description
Send notification to <profile>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Make new <log entry>	<p>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.</p> <p>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.</p>
Start plug-in on <devices>	<p>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.</p> <p>This type of action requires that you have at least one or more plug-ins installed on your system.</p> <p>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.</p>
Stop plug-in on <devices>	<p>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.</p> <p>This type of action requires that you have at least one or more plug-ins installed on your system.</p> <p>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.</p>



Action	Description
Apply new settings on <devices>	<p>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.</p> <p>If you define settings for more than one device, you can only change settings that are available for all of the specified devices.</p> <p>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.</p> <p>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.</p>
Set Matrix to view <devices>	<p>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 XProtect Smart Client or the Matrix Monitor application.</p> <p>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.</p> <p>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 XProtect 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.</p> <p>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 the management server, or any router or firewall used.</p>
Send SNMP trap	<p>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.</p> <p>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.</p>
Retrieve and store remote recordings from <devices>	<p>Retrieves and stores remote recordings from selected devices (that support edge recording) in a specified period before and after the triggering event.</p> <p>Note that this rule is independent of the Automatically retrieve remote recordings when connection is restored setting.</p> <p>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.</p>



Action	Description
Retrieve and store remote recordings between <start and end time> from <devices>	<p>Retrieves and stores remote recordings in a specified period from selected devices (that support edge recording).</p> <p>Note that this rule is independent of the Automatically retrieve remote recordings when connection is restored setting.</p> <p>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.</p>
Save attached image	<p>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.</p> <p>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.</p>
Activate archiving on <archives>	<p>Starts archiving on one or more archives. When you select this type of action, the Manage Rule wizard prompts you to select relevant archives.</p> <p>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.</p>
On <site> trigger <user-defined event>	<p>Relevant mostly within Milestone Federated Architecture, but you can also use this in a single site setup. Use the rule to trigger a user-defined event on a site, normally a remote site within a federated hierarchy.</p> <p>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.</p>
Show <access request notification>	<p>Lets access request notifications pop up on the XProtect Smart Client screen when the criteria for the triggering events are met. Milestone recommends that you use access control events as triggering events for this action, because access request notifications typically are configured for operating on related access control commands and cameras.</p> <p>This type of action requires that you have at least one access control plug-in installed on your system.</p> <p>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.</p>

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 a 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
Bookmark Reference Requested	Occurs when a bookmark is made in live or playback mode in the clients. Also, a requirement for using the Default record on bookmark rule.
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.
Evidence Lock Changed	Occurs when an evidence lock is changed for devices by a client user or via the MIP SDK.
Evidence Locked	Occurs when an evidence lock is created for devices by a client user or via the MIP SDK.
Evidence Unlocked	Occurs when an evidence lock is removed for devices by a client user or via the MIP SDK.
Feed Overflow Started	<p>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.</p> <p>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.</p> <p>You can use this event to trigger actions that helps you avoid the problem, for example, to lower the recording frame rate.</p>
Feed Overflow Stopped	Occurs when feed overflow (see description of the Feed Overflow Started event) ends.
Live Client Feed Requested	<p>Occurs when client users request a live stream from a device.</p> <p>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.</p>
Live Client Feed Terminated	Occurs when client users no longer request a live stream from a device.
Manual Recording Started	<p>Occurs when a client user starts a recording session for a camera.</p> <p>The event is triggered even if the device already is being recorded via rule actions.</p>



Event	Description
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.
Marked Data Reference Requested	Occurs when an evidence lock is made in playback mode in the clients or via the MIP SDK. An event is created that you can use in your rules.
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.
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.



Event	Description
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 175) 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	<p>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.</p> <p>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.</p>
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.
Database Disk Full	<p>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:</p> <p>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.</p>
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	<p>Occurs when a storage for a recording server becomes available after having been unavailable (see Database Storage Unavailable).</p> <p>You can, for example, use the event to start recording if it has been stopped by a Database Storage Unavailable event.</p>
Database Storage Unavailable	<p>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.</p> <p>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.</p>
Failover Started	Occurs when a failover recording server takes over from a recording server. See About failover recording servers (on page 247).



Event	Description
Failover Stopped	Occurs when a recording server becomes available again, and can take over from a failover recording server.

Events from add-on products and integrations:

Events from add-on products and integrations can be used in the rule system, for example:

- XProtect Access Control Module: Select between individual events or by category. You configure access control events on the Access Control Events tab in the Access Control node. See also Access Control Events (properties) (see "Access Control Events tab (Access Control)" on page 283).
- 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, Milestone 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	<p>Ensures that PTZ cameras go to their respective default preset positions after you have operated them manually. This rule is not enabled by default.</p> <p>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.</p>
Record on Bookmark	<p>Ensures that video is recorded automatically when an operator sets a bookmark in XProtect Smart Client. This is provided you have enabled recording for the relevant cameras. Recording is enabled by default.</p> <p>The default recording time for this rule is three seconds before the bookmark is set and 30 seconds after the bookmark is set. You can edit the default recording times in the rule. Note that the pre-buffer which you set on the Record Tab must match or be longer than the pre-recording time.</p>
Record on Motion	<p>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.</p> <p>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.</p>
Record on Request	<p>Ensures that video is recorded automatically when an external request occurs, provided recording is enabled for the relevant cameras. Recording is enabled by default.</p> <p>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.</p>
Start Audio Feed	<p>Ensures that audio feeds from all connected microphones and speakers are automatically fed to the system.</p> <p>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.</p>
Start Feed	<p>Ensures that video feeds from all connected cameras are automatically fed to the system.</p> <p>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.</p>



Default rule	Description
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.
Show Access Request Notification	Ensures that all access control events categorized as 'Access Request', will cause an access request notification to pop up in XProtect Smart Client, unless the notification function is disabled in the Smart Client profile.

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 Bookmark	Perform an action on Bookmark Reference Requested from All Cameras, All Microphones, All Speakers start recording three seconds before on the device on which event occurred Perform action 30 seconds after stop recording immediately
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
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
Show Access Request Notification	Perform an action on Access request (Access Control Categories) from Systems [+ units] Show built-in access request notification

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 validate more than one rule and one or more rules did not succeed, the dialog box lists the names of the affected rules.



Rule validated.



All rules validated.



Rule did not validate.



Rules that did not validate:
- My first rule

About rule complexity

Your 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>**:

First: Select conditions to apply

- ☐ Within selected time in <time profile>
- ☐ Outside selected time in <time profile>
- ☐ Within the time period <starttime> to <endtime>
- ☒ Day of week is <days>

Example only. Your selections may be different

Depending on your selections, edit the rule description in the lower part of the wizard window:

Next: Edit the rule description (click an underlined item)

Perform an action on Motion Start
from Blue Sector Back Door, Blue Sector Entrance
day of week is days

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.

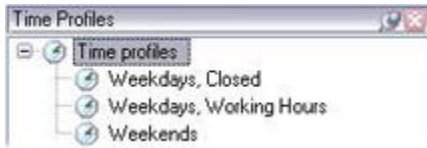
Time profiles are also assigned to roles, along with Smart Client profiles. Per default, all roles are assigned the default time profile **Always**. This means that members of roles with this default time profile attached has no time-based limits to their user rights in the system. You can also assign 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

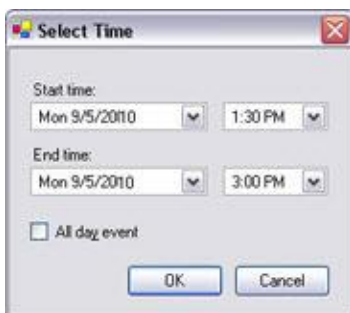
For an alternative to time profiles, see Day length time profiles (see "About day length time profiles" on page 170).

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 adjust 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. Verify that you have selected **Email**, click **Next**.



4. Specify recipient, subject, message text and time between emails:

5. To send a test email notification to the specified recipients, click **Test E-mail**.
6. 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.
7. To include AVI video clips, select **Include AVI**, and specify the time before and after event and frame rate.
8. 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
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: <ul style="list-style-type: none"> ▶ 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: <ul style="list-style-type: none"> ▶ 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.



Component	Requirement
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 XProtect 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 XProtect Smart Client	In this case, user-defined events make it possible for end users to manually trigger events while viewing live video in XProtect Smart Client. When a user-defined event occurs because an XProtect Smart Client user 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	<p>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.</p> <p>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.</p> <p>When you use user-defined events this way, you may not always want them to be available for manual triggering in XProtect Smart Client. You can use roles to define which user-defined events should be visible in XProtect Smart Client.</p>

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 XProtect 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 XProtect Smart Client when the XProtect 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 XProtect 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. This format is set out in the Milestone Analytics Events: Developers Manual. Contact your system provider for more details. Third-party VCA tools are developed by independent partners delivering solutions based on a Milestone 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**. Select **Add New**. The **Analytics Events Information** window appears.
2. 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.

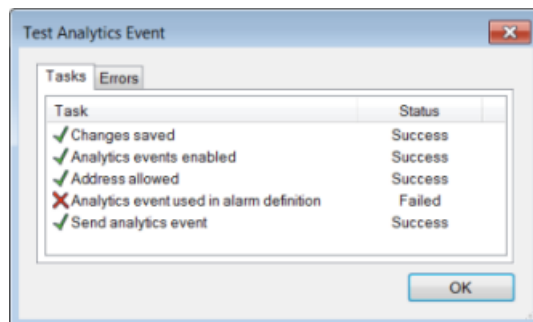
Edit an analytics event

1. Click an existing analytics event to open the **Analytics Event Information** 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 analytics event

To test an analytics event, you must first create one. See Create a new analytics event.

1. Click on an existing analytics event. This opens a new window.
2. In this window, click **Test Event**.
3. This opens the **Test Analytics Event** window which goes through a number of conditions that must be successful for analytics events to work. The window consists of two tabs, **Tasks** and **Errors**. See more information about the information on these tabs below this procedure.



Example of the **Test Analytics Event** window. May look different in different contexts.

4. Remember to save any changes made during the test. In the toolbar, click **Save**.

When you are done, check the presence of your test event in the XProtect Smart Client's Alarm list. Sort by type: **Test Alarm**. See the XProtect Smart Client documentation for more details. You can carry out this test at any step of the analytics event creation/editing process and as many times as you want to.

Information on the Tasks tab

The first tab, the **Task** tab, lists these conditions in the order they are tested:



Changes saved (step 1)	If the event is new, is it saved? Or if there are changes to the event name, are these changes saved?
Analytics Events enabled (step 2)	Is the analytics event feature enabled?
Address allowed (step 3)	Is the IP address/hostname of the computer that sends the event(s) allowed (listed on the address list)?
Analytics event used in alarm definition (step 4)	Is the analytics event used actively in any alarm definitions?
Send analytics event (step 5)	Did sending a test event to the event server succeed?

Each step is marked by either failed:  or successful: .

Information on the Errors tab

The second tab, the **Errors** tab, shows a list of errors corresponding to any possibly failed conditions. Possible errors are:

Step 1:

Error	Solution/explanation
Save changes before testing analytics event	Save changes.

Step 2:

Analytics events have not been enabled	Enable analytics events.
-----------------------------------------------	--------------------------

Step 3:

The local host name must be added as allowed address for the Analytics Event service	Add your computer to the list of allowed IP addresses/hostnames.
Error resolving the local host name	The IP address/hostname of the computer cannot be found or is invalid.

Step 4:

Analytics event is not used in any alarm definition	Use the analytics event in an alarm definition.
------------------------------------------------------------	-------------------------------------------------

Step 5:



Event server not found	Unable to find event server on the list of registered services.
Error connecting to event server	Unable to connect to event server on the stated port, most likely due to network problems, event server being stopped or similar incident.
Error sending analytics event	Connection to event server established but event cannot be sent (most likely due to network problems, for example time out).
Error receiving response from event server.	Event sent to event server but no reply received, most likely due to network problems or the port being busy. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\logs\</i> .
Analytics event unknown by event server	Event server does not know the event (most likely due to the event or changes to the event not having been saved).
Invalid analytics event received by event server.	Event format is somehow incorrect.
Sender unauthorized by event server	Most likely because your computer is not on the list of allowed IP addresses/hostnames.
Internal error in event server.	Event server error. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\logs\</i> .
Invalid response received from Event server	Response is invalid (possibly due to port being busy or network problems. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\logs\</i> .
Unknown response from event server	Response is valid, but not understood (possibly due to port being busy or network problems. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\logs\</i> .
Unexpected error	Not likely to occur, but if the accompanying text in the error does not provide enough information and problem continues, contact Milestone 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 XProtect event server installed.

Generic events allow you to trigger actions in the XProtect 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 has 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

1. Expand **Rules and Events**, right-click Generic Events, and select **Add New**.
2. Fill in the needed information and properties. See Generic event properties (see "Generic event (properties)" on page 183).
3. Optional: In the **Check if expression matches event string:** field, enter the expression you want to validate.
4. Optional: Below the **Check if expression matches event string:** field, you see either **Match** or **No match** as indication of whether your string can be validated against the expression entered in the **Expression:** field or not. If not, change the string and/or relevant settings and try again.
5. Click **Yes**.

Test a generic event

1. Expand **Rules and Events > Generic Events**.
2. Select the top-node **Generic Event**.
3. In the **Properties** pane, fill in the needed information.
4. Click **Send**.
5. Depending on your selected data source, you may get a response (an echo from the event server) in the **Echo from event server and local error message** field. This can be either successful or failed.

See also Generic event test properties (see "Generic event test (properties)" on page 185).



Example: Create and test a basic generic event

To trigger recording on **Camera1**, send the string **RecordCamera1** to a TCP port on the event server and teach the event server to understand what **RecordCamera1** means.

Create the scenario

1. Expand **Rules and Events**, right-click **Generic Events**, and select **Add New**.
 - In the **Name:** field enter, for example, `RecCam1`.
 - In the **Expression:** field enter `RecordCamera1`.
 - In the **Data source:** field select **International**.
2. Save your changes. Add a rule defining that when the generic event **RecCam1** is triggered, recording should start on **Camera1**.

Test scenario

1. Expand **Rules and Events**, select **Generic Events**.
2. In the **Overview** pane, select the top-node Generic Event.
3. In the **Properties** pane:
 - In **String to send as generic event:** enter `Please RecordCamera1 that would be nice`.
 - In **Data source to send event string to:** select **International**.
4. Click **Send**.

If you did not change default echo settings, you should get the following response in **Echo from event server and local error message: 4,39,1,RecCam1**. This means that request number **4** had **39** characters and that there was **1** match with a generic event named **RecCam1**.

To try out the event from a non-XProtect application, start a DOS box, enter `telnet localhost 1235` and press **Enter**. Next, type `RecordCamera1 that would be nice` and press **Enter**. You should get the same response.



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	<p>Expression that the system should look out for when analyzing data packages. You can use the following operators:</p> <ul style="list-style-type: none"> ▶ (): 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. <p>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.</p> <ul style="list-style-type: none"> ▶ AND: With an AND operator, you specify that the terms on both sides of the AND operator must be present. <p>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.</p> <ul style="list-style-type: none"> ▶ OR: With an OR operator, you specify that either one or another term must be present. <p>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.</p>



<p>Expression type</p>	<p>Indicates how particular the system should be when analyzing received data packages. The options are the following:</p> <ul style="list-style-type: none"> ▶ 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. <p>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.</p> <ul style="list-style-type: none"> ▶ 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. <p>If you switch from Search or Match to Regular expression, the text in the Expression field is automatically translated to a regular expression.</p>
<p>Priority</p>	<p>The priority must be specified as a number between 0 (lowest priority) and 999999 (highest priority).</p> <p>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.</p> <p>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.</p>
<p>Check if expression matches event string</p>	<p>An event string to be tested against the expression entered in the Expression: field.</p>



Generic event test (properties)

Component	Requirement
String to send as generic event	An event string to be tested from within the system by the event server as a generic event.
Data source to send event string to	See Generic event data source properties (see "Generic event data source (properties)" on page 186).
Echo from event server and local error message	<p>A window displaying the echo of the string from the event server in the following default format:</p> <p>[X],[Y],[Z],[Name of generic event]</p> <p>[X] = request number.</p> <p>[Y] = number of characters.</p> <p>[Z] = number of matches with a generic event.</p> <p>[Name of generic event] = name entered in the Name: field.</p> <p>If no generic events are defined or if no data sources are enabled, an information message is displayed instead. Other echo formats can be selected (see "Generic Events tab (options)" on page 244).</p>



Generic event data source (properties)

Component	Requirement
Data source	<p>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:</p> <p>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).</p> <p>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).</p> <p>[Data source A]</p> <p>[Data source B]</p> <p>and so on.</p>
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.
Protocol type selector	<p>Protocols which the system should listen for, and analyze, in order to detect generic events:</p> <p>Any: TCP as well as UDP.</p> <p>TCP: TCP only.</p> <p>UDP: UDP only.</p> <p>TCP and UDP packages used for generic events may contain special characters, such as @, #, +, ~, and more.</p>
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><LF>).



Component	Requirement
Echo type selector	<p>Available echo return formats:</p> <ul style="list-style-type: none">▶ 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 and a Management 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 XProtect 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 the default evidence lock profiles 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 190).

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 XProtect 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

Available functionality depends on the system you are using. See *Product comparison chart* (on page 22) for more information.

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 XProtect Smart Client or other Milestone 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 XProtect 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 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 can also reflect the same limitations in the user interface of the Management Client for each role by associating the role with a Management Client profile that has removed the corresponding system functions from the user interface. See *About Management Client profiles* (on page 138) for information.

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 189).

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.

The rights you can set for a role are different between your products. You can only give all available rights to a role in XProtect Corporate.



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 and Management Client profiles, evidence lock profiles or time profiles, click the drop down dialog boxes.
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 190) and Role settings (see "Roles settings" on page 191).

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 > Effective Roles**.
2. In the **Effective Roles** window's **User name** field, type the user name of the relevant user or use the "..." browse button.
3. If you typed the user name directly into the **User name**, click **Refresh** in the lower part of the window to display the roles of the user. If you used Active Directory to browse for the user, the user's roles are displayed automatically.

Roles settings

Info tab (roles)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

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.
Management Client profile	Select a Management Client profile to associate with the role. You cannot apply this to the default Administrators role.
Smart Client profile	Select a Smart Client profile to associate with the role.
Default time profile	Select a default time profile to associate with the role. You cannot apply this to the default Administrators role.
Evidence lock profile	Select an evidence lock profile to associate with the role.
Smart Client login within time profile	Select a time profile for which the XProtect Smart Client user associated with this role is allowed to log in. If the XProtect Smart Client user is logged in when the period expires, he or she is logged off automatically. 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 XProtect 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)

The term **users** primarily refers to users who connect to the surveillance system through the clients. You can configure such users in two ways:

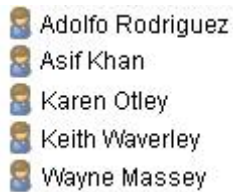
- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

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 instead. For information about how to set up basic users, see Create basic user (see "Create basic users" on page 221).

Overall Security tab (roles)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

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.

The **Overall Security** tab is available in both XProtect Corporate and XProtect Expert, but the tab gives you the possibility to change more functionality in XProtect Corporate than in XProtect Expert. This is because you can set up differentiated administrator rights in XProtect Corporate, while such rights are not available in XProtect Expert. However, you can set overall rights for a role that uses XProtect Smart Client in both XProtect products.

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. If you use XProtect Expert, you can see which settings are not available to you under each system component.

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.

If you switch your license from XProtect Corporate to XProtect Expert, you can only do this if you have not set any security rights for the role for functionality that is not available in XProtect Expert. Therefore, to complete such a switch, make sure that you remove all security rights that are available to XProtect Corporate only.



Management Server

Security right	Description	XProtect Expert
Full control	Enables the right to manage all security entries on this part of the system.	
Read	<p>Enables read access to general data on the Management Server which the individual object security does not handle:</p> <ul style="list-style-type: none"> ‣ Logging in with the Management Client ‣ List of current tasks ‣ Server Logs <p>It also enables access to the following features:</p> <ul style="list-style-type: none"> ‣ Remote Connect Services ‣ Smart Client Profiles ‣ Management Client Profiles ‣ Matrix ‣ Time Profiles ‣ Registered Servers and Service Registration API ‣ Enterprise Servers 	Not available



Security right	Description	XProtect Expert
Edit	<p>Enables write access to general data on the server which the individual object security does not handle:</p> <ul style="list-style-type: none"> ▶ Options ▶ License Management <p>It also enables users to create, delete and edit the following features:</p> <ul style="list-style-type: none"> ▶ Remote Connect Services ▶ Device groups ▶ Smart Client Profiles ▶ Management Client Profiles ▶ Matrix ▶ Time Profiles ▶ Registered Servers ▶ Enterprise Servers <p>Enables the right to configure local IP ranges when configuring the network on the recording server.</p>	Not available
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.	Not available
Manage Federated site hierarchy	<p>Enables the right to add and detach the current site to other sites in a federated site hierarchy.</p> <p>If you set this permission to allowed on the child site only, the user can still detach the site from the parent site.</p>	
Backup Configuration	Enables the right to create backups of the system configuration using the system's backup/restore functionality.	
Manage security	Enables the right to manage permissions for the Management Server. It also enables users to manage roles, to add or remove members of roles and to create and delete basic users.	



Security right	Description	XProtect Expert
Authorize users	Enables the right to authorize users when they are asked for a second login in XProtect Smart Client or Management Client. You define if a role requires login authorization on the Info tab.	Not available

Recording Servers

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Edit	Enables the right to edit properties on the recording servers, except for network configuration settings that require Edit right on the management server.
Delete	<p>Enables the right to delete recording servers. To do this, you must also give the user delete permissions on:</p> <ul style="list-style-type: none">▶ Hardware security group if you have added hardware to the recording server. <p>If any of the devices on the recording server contains evidence locks, you can only delete the recording server if it is offline.</p>
Manage hardware	Enables the right to add hardware on recording servers.
Manage storage	Enables the right to administrate storage containers on recording server, that is to create, delete, move and empty storage containers.
Authorize recording server	Enables the right to authorize new recording servers.
Manage security	Enables the right to manage security permissions for recording servers.

Failover Servers

The following settings are only available in XProtect Corporate.



Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to see and access failover servers in the Management Client.
Edit	Enables the right to edit properties on failover servers in the Management Client.
Manage security	Enables the right to manage security permissions for the failover servers.

Mobile Servers

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to see and access mobile servers in the Management Client.
Edit	Enables the right to edit properties on mobile servers in the Management Client.
Manage security	Enables the right to manage security permissions for the mobile servers.
Create	Enables the right to add mobile servers to the system.

Hardware

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Edit	Enables the right to edit properties on hardware.
Delete	Enables the right to delete hardware. If any of the hardware devices contains evidence locks, you can only delete the hardware if the recording server is offline.
Manage security	Enables the right to manage security permissions for the hardware.



Cameras

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit properties for cameras in the Management Client. It also enables users to enable or disable a camera.	Not available
View Live	Enables the right to view live video from cameras in the clients.	
Playback	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.	
Create bookmarks	Enables the right to create bookmarks in recorded and live video in the clients.	
Read bookmarks	Enables the right to search for and read bookmark details in the clients.	
Edit bookmarks	Enables the right to edit bookmarks in the clients.	
Delete bookmarks	Enables the right to delete bookmarks in the clients.	
Create evidence lock	Enables the right to create and extend evidence locks in the clients.	Not available
Read evidence lock	Enables the right to search and read evidence locks in the clients.	Not available
Delete evidence lock	Enables the right to delete or reduce evidence locks in the clients.	Not available
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.	



Security right	Description	XProtect Expert
AUX commands	Enables the right to use auxiliary (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.	
PTZ control	Enables the right to use the pan, tilt and zoom features of PTZ cameras.	
Activate PTZ preset	Enables the right to move PTZ cameras to preset positions.	
Delete recordings	Enables the right to delete stored video recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for the camera.	Not available



Microphones

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit microphone properties in the Management Client. It also allows users to enable or disable microphones.	Not available
Listen	Enables the right to listen to live audio from microphones in the clients.	
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.	
Create bookmarks	Enables the right to create bookmarks in the clients.	
Read bookmarks	Enables the right to search for and read bookmark details in the clients.	
Edit bookmarks	Enables the right to edit bookmarks in the clients.	
Delete bookmarks	Enables the right to delete bookmarks in the clients.	
Create evidence lock	Enables the right to create or extend evidence locks in the clients.	Not available
Read evidence lock	Enables the right to search and read evidence lock details in the clients.	Not available
Delete evidence lock	Enables the right to delete or reduce evidence locks in the clients.	Not available
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.	
Delete recordings	Enables the right to delete stored recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for microphones.	Not available



Speakers

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit properties for speakers in the Management Client. It also allows users to enable or disable speakers.	Not available
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.	
Create bookmarks	Enables the right to create bookmarks in the clients.	
Read bookmarks	Enables the right to search for and read bookmark details in the clients.	
Edit bookmarks	Enables the right to edit bookmarks in the clients.	
Delete bookmarks	Enables the right to delete bookmarks in the clients.	
Create evidence lock	Enables the right to create or extend evidence locks on recorded audio in the clients.	Not available
Read evidence lock	Enables the right to view evidence locks on recorded audio in the clients.	Not available
Delete evidence lock	Enables the right to delete or reduce evidence locks on recorded audio in the clients.	Not available
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.	
Delete recordings	Enables the right to delete stored recordings from the system.	Not available



Security right	Description	XProtect Expert
Manage security	Enables the right to manage security permissions for speakers.	Not available

Metadata

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit metadata properties in the Management Client. It also allows users to enable or disable metadata devices.	Not available
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.	
Create evidence lock	Enables the right to create evidence locks in the clients.	Not available
Read evidence lock	Enables the right to view evidence locks in the clients.	Not available
Delete evidence lock	Enables the right to delete or reduce evidence locks in the clients.	Not available
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.	
Delete recordings	Enables the right to delete stored recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for metadata.	Not available



Input

Security right	Description	XProtect Expert
Full control	Enables the right to manage all security entries on this part of the system.	Not available
Read	Enables the right to view input devices in the clients.	
Edit	Enables the right to edit properties for input devices in the Management Client. It also enables users to enable or disable an input device.	Not available
Manage security	Enables the right to manage security permissions for input devices.	Not available

Output

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit properties for output devices in the Management Client. It also enables users to enable or disable an output device.	Not available
Activate	Enables the right to activate outputs in the clients.	
Manage security	Enables the right to manage security permissions for output devices.	Not available



Smart Wall

Security right	Description	XProtect Expert
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view Smart Walls in the clients.	
Edit	Enables the right to edit properties for the Smart Wall in the Management Client.	Not available
Delete	Enables the right to delete existing Smart Walls in the Management Client.	Not available
Operate	Enables the right to operate Smart Walls, for example to change presets or apply cameras on views in the clients.	
Manage security	Enables the right to manage security permissions for the Smart Wall.	Not available
Create Smart Wall	Enables the right to create new Smart Walls in the Management Client.	Not available

View Groups

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit properties on the View groups in the Management Client.	Not available
Delete	Enables the right to delete View Groups in the Management Client.	Not available
Operate	Enables the right to use View Groups created in the Management Client within the clients, that is to create subgroups and views.	
Manage security	Enables the right to manage security permissions for View Groups.	Not available
Create view group	Enables the right to create new View Groups in the Management Client.	Not available



User-defined Events

Security right	Description	XProtect Expert
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.	
Edit	Enables the right to edit properties on user-defined events in the Management Client.	Not available
Delete	Enables the right to delete user-defined events in the Management Client.	Not available
Trigger	Enables the right to trigger user-defined events in the clients.	
Manage security	Enables the right to manage security permissions for user-defined events.	Not available
Create user-defined event	Enables the right to create new user-defined events in the Management Client.	Not available

Analytics Events

The following settings are only available in XProtect Corporate.

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 analytics events in the Management Client. Only when you set this to allowed, the Analytics Events tab in the Options dialog appears.
Edit	Enables the right to edit properties on analytics events in the Management Client.
Delete	Enables the right to delete analytics events in the Management Client.
Manage security	Enables the right to manage security permissions for analytics events.
Create	Enables the right to create new analytics events in the Management Client.

Generic Events

The following settings are only available in XProtect Corporate.



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 generic events in the Management Client. Only when you set this to allowed, the Generic Events tab in the Options dialog appears.
Edit	Enables the right to edit properties on generic events in the Management Client.
Delete	Enables the right to delete generic events in the Management Client.
Manage security	Enables the right to manage security permissions for generic events.
Create	Enables the right to create new generic events in the Management Client.

Matrix

Security right	Description	XProtect Expert
Full control	Enables the right to manage all security entries on this part of the system.	Not available
Read	Enables the right to select and send video to the Matrix recipient from the clients.	
Edit	Enables the right to edit properties for the Matrix's.	Not available
Delete	Enables the right to delete Matrix's.	Not available
Manage security	Enables the right to manage security permissions for all Matrix's.	Not available
Create Matrix	Enables the right to create new Matrix's.	Not available

Rules

The following settings are only available in XProtect Corporate.



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 existing rules in the Management Client.
Edit	Enables the right to edit properties for rules and to define rule behavior in the Management Client. It also requires that the user has read permissions on all devices that are impacted by the rule.
Delete	Enables the right to delete rules from the Management Client. It also requires that the user has read permissions on all devices that are impacted by the rule.
Manage security	Enables the right to manage security permissions for all rules.
Create rule	Enables the right to create new rules. It also requires that the user has read permissions on all devices that are impacted by the rule.

Sites

The following settings are only available in XProtect Corporate.

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 other sites in the Management Client. Connected sites are connected via Milestone Federated Architecture.
Edit	Enables the right to edit properties on other sites in the Management Client. Connected sites are connected via Milestone Federated Architecture.
Manage security	Enables the right to manage security permissions all sites.

Access Control

The following settings are only available in XProtect Corporate.



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 properties for the Access Control systems in the Management Client. Only when you set this to allowed, the Access Control Settings tab in the Options dialog appears.
Edit	Enables the right to edit properties for the Access Control systems in the Management Client.
Delete	Enables the right to delete Access Control systems in the Management Client.
Manage security	Enables the right to manage security permissions for all Access Control systems.
Create	Enables the right to create new Access Control systems in the Management Client.

Alarms

The following settings are only available in XProtect Corporate.

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 alarm definitions, alarm sounds, and alarm data settings in the Management Client. Only when you set this to allowed, the Event Server tab in the Options dialog appears.
Edit	Enables the right to edit properties for alarm definitions, alarm sounds, and alarm data settings in the Management Client.
Delete	Enables the right to delete alarm definitions in the Management Client.
Manage security	Enables the right to manage security permissions for alarms.
Create	Enables the right to create new alarm definitions in the Management Client.

MIP Plug-ins

The following settings are only available in XProtect Corporate.

The list of MIP plug-ins depends on the actual plug-ins integrated in your system.



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 MIP plug-ins in the Management Client.
Edit	Enables the right to edit properties on MIP plug-ins in the Management Client.
Delete	Enables the right to delete MIP plug-ins in the Management Client.
Manage security	Enables the right to manage security permissions for MIP plug-ins.
Create	Enables the right to create new MIP plug-ins in the Management Client.

Device tab (roles)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

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 XProtect 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 XProtect 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 > Within time profile	Allows playback of recorded video from the selected camera(s) in the clients. 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.
Read bookmarks	Allows search for and read bookmark details in the clients.
Edit bookmarks	Allows editing bookmarks in the clients.
Create bookmarks	Allows adding bookmarks in the clients.
Delete bookmarks	Allows deleting bookmarks in the clients.
AUX commands	Allows the use of auxiliary commands from the clients.
Create evidence lock	<p>Allows the client user to:</p> <ul style="list-style-type: none"> ▶ Add the camera to new or existing evidence locks. ▶ Extend the expiry time for existing evidence locks. ▶ Extend the protected interval for existing evidence locks. <p>Requires user rights to all devices included in the evidence lock.</p>



Name	Description
Delete evidence lock	<p>Allows the client user to:</p> <ul style="list-style-type: none">▶ Remove the camera from existing evidence locks.▶ Delete existing evidence locks.▶ Shorten the expiry time for existing evidence locks.▶ Shorten the protected interval for existing evidence locks. <p>Requires user rights to all devices included in the evidence lock.</p>
Read evidence locks	<p>Allows the client user to search for and read evidence lock details.</p>

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 XProtect 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 > Within time profile	Allows playback of recorded audio from the selected microphone(s) in the clients. 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.
Read bookmarks	Allows search for and read bookmark details in the clients.
Edit bookmarks	Allows editing bookmarks in the clients.
Create bookmarks	Allows adding bookmarks in the clients.
Delete bookmarks	Allows deleting bookmarks in the clients.
Create evidence lock	Allows the client user to: <ul style="list-style-type: none"> ▶ Add the microphone to new or existing evidence locks. ▶ Extend the expiry time for existing evidence locks. ▶ Extend the protected interval for existing evidence locks. Requires user rights to all devices included in the evidence lock.
Delete evidence lock	Allows the client user to: <ul style="list-style-type: none"> ▶ Remove the microphone from existing evidence locks. ▶ Delete existing evidence locks. ▶ Shorten the expiry time for existing evidence locks. ▶ Shorten the protected interval for existing evidence locks. Requires user rights to all devices included in the evidence lock.
Read evidence lock	Allows the client user to search for and read evidence lock details.



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 XProtect 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 > Within time profile	Allows playback of recorded audio from the selected speaker(s) in the clients. 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.
Read bookmarks	Allows search for and read bookmark details in the clients.
Edit bookmarks	Allows editing bookmarks in the clients.
Create bookmarks	Allows adding bookmarks in the clients.
Delete bookmarks	Allows deleting bookmarks in the clients.
Create evidence locks	Allows the client user to: <ul style="list-style-type: none"> ▶ Add the speaker to new or existing evidence locks. ▶ Extend the expiry time for existing evidence locks. ▶ Extend the protected interval for existing evidence locks. Requires user rights to all devices included in the evidence lock.
Delete evidence locks	Allows the client user to: <ul style="list-style-type: none"> ▶ Remove the speaker from existing evidence locks. ▶ Delete existing evidence locks. ▶ Shorten the expiry time for existing evidence locks. ▶ Shorten the protected interval for existing evidence locks. Requires user rights to all devices included in the evidence lock.
Read evidence locks	Allows the client user to search for and read evidence lock details.



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 metadata 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 XProtect 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.
Create evidence lock	Enables the right to create and extend the evidence locks on metadata in the clients.
Read evidence lock	Enables the right to view evidence locks on metadata in the clients.
Delete evidence lock	Enables the right to delete or reduce evidence locks on metadata 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 XProtect 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
PTZ Control	Determines if the selected role can use PTZ features on the selected camera. Specify the time profile or leave the default value.
Activate PTZ preset	Determines if the selected role can move the selected PTZ cameras to preset positions. Specify the time profile or leave the default value.
PTZ Priority	<p>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.</p> <p>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 32,000, where 1 is the lowest priority. The default priority is 3,000. The role with the highest priority number is the one who can control the PTZ camera(s).</p>

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.
Speak priority	<p>When several client users want to talk through the same speaker at the same time, conflicts may occur.</p> <p>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.</p> <p>Should two users with the same role want to speak at the same time, the first come, first served-principle applies.</p>

Remote Recordings tab (roles)

Specify the following rights for remote recordings:

Name	Description
Retrieve remote recordings	Determines if users/groups with the selected role can retrieve remote recordings.

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 see Smart Walls in the clients.
Edit	Allows users to edit Smart Walls in the clients.
Delete	Allows users to delete Smart Walls in the clients.
Operate	Allows users to apply layouts on the selected monitor in the client and to activate the selected preset.

External Event tab (roles)

Specify the following external event rights:



Name	Description
Read	Allows users to search for and view external system events in the clients.
Edit	Allows users to edit external system events in the clients.
Delete	Allows users to delete external system events in the clients.
Trigger	Allows users to trigger external system events 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	Determine if the selected role can see the selected view group (and any views contained in the view group) in the clients.
Edit	Determine if the selected role can make changes to the selected view group (and any views contained in the view group) in the clients.
Delete	Determine if the selected role can delete the selected view group (and any views contained in the view group) in the clients.
Operate	Determine if the selected role can create subgroups and views in the clients.

Servers tab (roles)

Specifying role rights on the **Servers** tab is only relevant if you have integrated XProtect Enterprise servers into your system or your system works in a Milestone Federated Architecture setup.

See About XProtect Enterprise servers (on page 327) or About Milestone Federated Architecture (on page 261) for more information.

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 federated installation (including any other XProtect 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	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	View alarms and print alarm reports.
Disable alarms	Disable alarms.

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. See the User and Groups tab (see "User and Groups tab (roles)" on page 192) under **Roles** for more information.

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

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

On System Dashboard, find the following functionality:

Name	Description
System Monitor	View and print detailed system reports on servers, devices and cameras.
Evidence Lock	Get an overview of all protected data in the system.
Current Task	Get an overview of tasks under a selected recording server.
Configuration Report	Decide what to include in your system configuration reports before printing.

About system monitor

System Monitor allows you to view system information and create reports regarding:



Component	Description
Management server	Shows data on your management server
Recording server(s)	Shows data on any number of recording servers in your setup. You can view these per: <ul style="list-style-type: none">▶ Disk▶ Storage▶ Network▶ Camera
Failover recording servers	Shows data on any number of failover recording servers in your setup.
Additional servers	Shows data on log server, event servers and more.
Cameras	Shows data on any camera in any camera group in your setup.

Each of these elements are a clickable, expandable area and most of these include sub-areas. Each sub-area represents a server. When clicked, they provide relevant dynamic data on this server.

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.

Important: If you access system monitor from a server operating system, you may experience a message regarding **Internet Explorer Enhanced Security Configuration**. Follow instructions in the message to add the **System Monitor** page to the **Trusted sites zone** before proceeding.

Restart Data Collector Server service

Your system automatically installs the Data Collector Server service on the same computers as the management, recording, log, event and XProtect Mobile server(s).

Normally, the Data Collector Server service requires no maintenance, but if the service **does** stop, no live feed is sent to the System Monitor (clearly indicated in System Monitor by error texts). On the computer on which you have installed the Data Collector Server service, do the following:

1. 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**.
2. Double-click **Services**.



3. Locate the **Milestone XProtect Data Collector Server**. Right-click it and select **Start** to restart the service.

About evidence lock

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

With the evidence lock functionality, client users can protect video sequences, including audio and other data, from deletion if required, for example, while an investigation or trial is ongoing. For information about how client users can lock evidence, see the XProtect Smart Client documentation.

When protected, the data cannot be deleted, neither automatically by the system after the system's default retention time or in other situations nor manually by the client users. The system or a user cannot delete the data until a user with sufficient user rights unlocks the evidence.

By default, all client users have the default evidence lock profile assigned to them but no user access rights to the feature. To specify the evidence lock access rights of a role, see the Device tab (see "Device tab (roles)" on page 210) for role settings. To specify the evidence lock profile of a role, see the Info tab (see "Info tab (roles)" on page 191) for role settings.

In the Management Client, you can edit the properties of the default evidence lock profile and create additional evidence lock profiles and assign these to the roles instead.

Evidence Lock under **System Dashboard** shows an overview of all protected data on the current surveillance system:

- start and end date for the protected data
- the user who locked the evidence
- when the evidence is no longer locked
- where the data is stored
- the size of each evidence lock

All information shown in **Evidence Lock** are snapshots. Press F5 to refresh.

About current tasks

Current Tasks show 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 238) 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 2014 08:00:00 and January 4th 2014 07:59:59 in your export.

To export a log:

1. In the **Export Log** window's **Filename** 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.

- 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.
- 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:

A screenshot of a software interface showing a date and time selection field. The text 'Start date and time:' is above the field. The field itself contains '02-01-2011 10:00:00' and has a small downward arrow on the right side, indicating it is a dropdown menu.

- Click **Export** to export the log content.

Change log language

- At the bottom part of the log pane, in the **Show log in** drop down-box, select the wanted language.

A screenshot of a software interface showing a dropdown menu. The text 'Show log in:' is to the left of the dropdown. The dropdown menu is open, showing 'English (United States)' as the selected option.

- The log is displayed in the selected language. Next time you 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.
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: i - indicates info ! - indicates warning x - 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 of 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 XProtect Smart Client.
The right to trigger user-defined events	This right determines if the user's role can trigger selected user-defined events in XProtect 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 XProtect 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 federated installations (including any other XProtect 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:

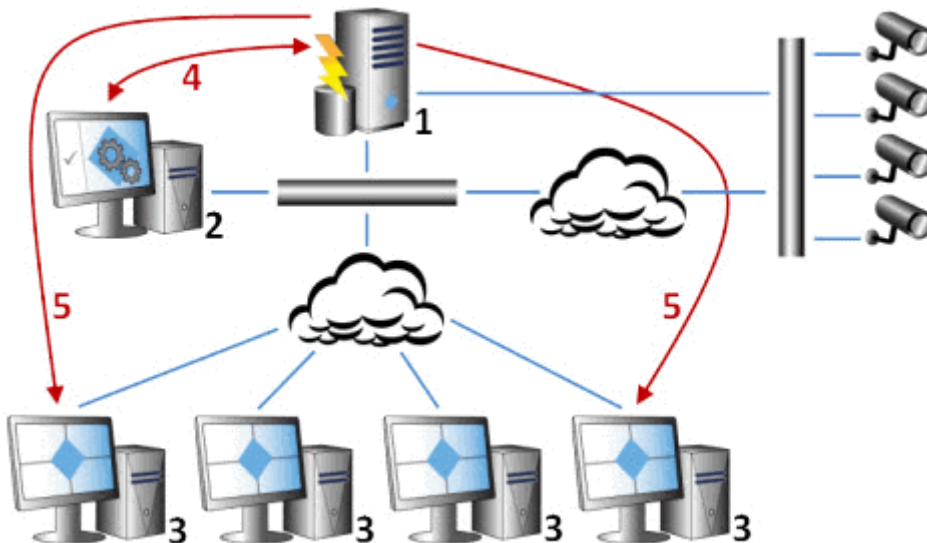
- **Analytics events**

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. XProtect Smart Client
4. Alarm configuration
5. Alarm data flow

You handle and delegate alarms in the alarm list in XProtect Smart Client. You can also integrate alarms with the XProtect 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 XProtect 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.

Alarms can also register and handle events from federated sites in a Milestone Federated Architecture.

Alarm Definitions (properties)

You can set a number of alarm-related settings when you select **Alarms**, right-click **Alarm Definitions** > **Add New**:



Alarm definition settings:

Enable	Enable the Alarms feature.
Name	Type a name for the alarm. The name of the alarm appears whenever the alarm is listed.
Instructions	Type a descriptive text about the alarm and how to resolve the issue that caused the alarm. The text appears in XProtect Smart Client when the user handles the alarm.
Triggering event	Select the event message to use when the alarm is triggered. Choose from two drop-downs: <ul style="list-style-type: none"> ▶ The first drop-down: Select the type of event to use. Choose, for example, between analytics events, system events and relevant plug-in related events. ▶ The second drop-down: Select the specific event message to use. What messages you can select are based on what type of event you have chosen.
Sources	Select which cameras and/or other devices, including plug-in defined sources (VCA, MIP, and more), the event should come from in order to trigger the alarm. Your options depend on the type of event you have selected.

Alarm trigger:

Time profile	If you select Time profile , you must select when the alarm should be enabled for triggering. If you have defined one or more time profiles, select them from this list. If you have not defined time profiles, you can only select Always .
Event based	If you select Event based , you must select which events should start and stop the alarm. You can select hardware events defined on cameras, video servers and input. You can also use global/manual event definitions. If you use Event based alarm activation, you cannot define alarms based on outputs, only on inputs.

Operator action required:

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 an event is attached.
Events triggered	Select which event to trigger when the time limit has been reached.

Additional settings:



Related cameras	Select up to 15 cameras to include in the alarm definition even if they are not themselves triggering 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.
Related map	Assign a map to the alarm when it is listed in the XProtect 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 XProtect Smart Client to determine the importance of an alarm.
Initial alarm category	Select an alarm category for the alarm, for example <i>False alarm</i> or <i>Need investigation</i> .
Events triggered by alarm	Define an event that the alarm can trigger in XProtect Smart Client.
Auto-close alarm	Select the check box if a particular event should close the alarm automatically. Note that not all events can trigger alarms. Clear the checkbox to disable the new alarm from the beginning.

Alarm Data Settings

When you configure alarm data settings, specify the following:

Alarm Data Levels tab

Priorities

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

Level	In addition to the default state levels (numbers 1 , 4 , 9 and 11 , which can not be edited or reused), add new states with level numbers of your choosing. These state levels are only visible in the XProtect Smart Client's <i>Alarm List</i> .
--------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Categories



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

Available columns	Use > to select which columns should be available in the XProtect Smart Client's <i>Alarm List</i> . Use < to clear selection. When done, Selected columns should contain the items to be included.
--------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Reasons for Closing tab

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 <i>Solved-Trespasser</i> or <i>False Alarm</i> . You can create as many as you like.

Sound Settings

When you configure sound settings, specify the following:

Sounds	<p>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).</p> <p>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.</p>
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.

About setting up alarms using Enterprise slaves

Only relevant if you run XProtect Corporate.



User name and password

If your surveillance setup includes one or more XProtect Enterprise slaves and you want to include one or more of these in your alarms, setup, you must specify the same login name and password when adding the slave as the one you use in the XProtect Central add-on in the XProtect Enterprise server. If you do not, the server cannot log in to the XProtect Central add-on in XProtect Enterprise and collect status information.

Update port number information

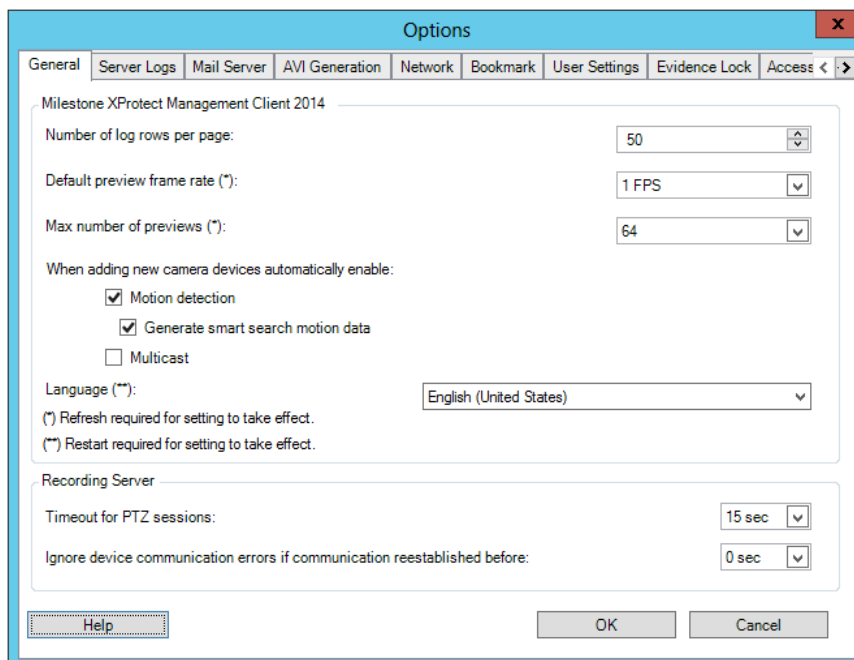
If you have changed port number settings in the XProtect Central add-on in the XProtect Enterprise server, you must update port number information in the XML file containing configurations for the event server. You do this directly in the affected configuration file.

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.

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

To access the dialog box, select **Tools > Options**.



The **Options** dialog box features the following tabs:

- General tab (see "General tab (options)" on page 236)
- Server Logs tab (see "Server Logs tab (options)" on page 238)
- Mail Server tab (see "Mail Server tab (options)" on page 239)



- AVI Generation tab (see "AVI Generation tab (options)" on page 240)
- Network tab (see "Network tab (options)" on page 241)
- Evidence Lock tab (see "Evidence Lock tab (options)" on page 242)
- Bookmark tab (see "Bookmark tab (options)" on page 241)
- User Settings tab (see "User Settings tab (options)" on page 242)
- Access Control Settings tab (see "Access Control Settings tab (options)" on page 242)
- Analytics Events tab (see "Analytics Events tab (options)" on page 243)
- Event Server tab (see "Event Server tab (options)" on page 244)
- Generic Events tab (see "Generic Events tab (options)" on page 244)

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	<p>Select frame rate for the thumbnail camera images displayed in the Preview pane. Default is 1 frame per second.</p> <p>Select Action > Refresh from the menu for the change to take effect.</p> <p>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.</p>
Max number of previews	<p>Select the maximum number of thumbnail images displayed in the Preview pane. Default is 64 thumbnail images.</p> <p>Select Action > Refresh from the menu for the change to take effect.</p> <p>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.</p>
When adding new camera devices automatically enable: Motion detection	<p>Select the check box to enable motion detection on new cameras, when you add them to the system with the Add Hardware wizard.</p> <p>This setting does not affect motion detection settings on existing cameras.</p> <p>You enable and disable motion detection for a camera on the Motion tab for the camera device.</p>
When adding new camera devices automatically enable: Generate motion data for smart search	<p>Generation of motion data for smart search requires that motion detection is enabled for the camera.</p> <p>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.</p> <p>This setting does not affect motion detection settings on existing cameras.</p> <p>You enable and disable the generation of smart search motion data for a camera on the Motion tab for the camera device.</p>
When adding new camera devices automatically enable: Multicast	<p>Select the check box to enable multicast on new cameras when you add them with the Add Hardware wizard.</p> <p>This setting does not affect multicast settings on existing cameras.</p> <p>You enable and disable live multicasting for a camera on the Client tab for the camera device.</p>



Name	Description
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.
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 224) for more information.



Name	Description
Logs	<p>Select the log that you want to configure:</p> <ul style="list-style-type: none"> ▶ System Log ▶ Audit Log ▶ Rule Log
Settings	<p>Disable/enable the logs and specify the retention period and the maximum number of rows for each log.</p> <p>For System logs, specify the level of messages you want to log:</p> <ul style="list-style-type: none"> ▶ All - includes undefined messages ▶ Information, warnings and errors ▶ Warnings and errors ▶ Errors (default setting) <p>For Audit logs, enable user access logging if you want the system to log all user actions in XProtect Smart Client. These are, for example, exports, activating outputs, viewing cameras live or in playback.</p> <p>Specify:</p> <ul style="list-style-type: none"> ▶ 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 171).



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 172).



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.

Bookmark tab (options)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

On the **Bookmarks** tab, you can specify settings for bookmarks, their IDs and function in XProtect Smart Client.



Name	Description
Bookmark ID prefix	Specify a prefix for all the bookmarks that is made by the users of XProtect Smart Client.
Default bookmark time	<p>Specify the default start and end time of a bookmark is set in XProtect Smart Client.</p> <p>This setting needs to be aligned with:</p> <ul style="list-style-type: none"> ▶ The default bookmark rule, see Default record on bookmark rule. ▶ The pre-buffer period for each camera, see Manage pre-buffering (on page 107).

To specify the bookmark rights of a role, see Device rights (see "Device tab (roles)" on page 210).

Evidence Lock tab (options)

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

On the **Evidence Lock** tab, you define and edit evidence lock profiles and the duration your client users can select to keep the data protected.

Name	Description
Evidence lock profiles	<p>A list with defined evidence lock profiles.</p> <p>You can add and remove existing evidence lock profiles. You cannot remove the default evidence lock profile but you can change its time options and its name.</p>
Time options	<p>The duration the client users can select to lock evidence.</p> <p>Available time options are hour(s), day(s), week(s), month(s), year(s), indefinite or user-defined.</p>

To specify the evidence lock access rights of a role, see the Device tab (see "Device tab (roles)" on page 210) for role settings.

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.

Access Control Settings tab (options)

The use of XProtect Access Control Module requires that you have purchased a license that allows you to access this feature.

Specify the following Access Control Settings:



Name	Description
Show development property panel	<p>If selected, additional developer information appears for Access Control > General Settings.</p> <p>This setting is only meant to be used by developers of access control system integrations.</p>
Keep access control events for	<p>Specify the number of days that you want the system to keep access control events visible in XProtect Smart Client. The default period is 30 days.</p> <p>The setting applies to future events only. It has no effect on the events already stored in the database.</p> <p>The value of 0 indicates that the system does not store any events.</p>

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	<p>Specify the port used by this feature. The default port is 9090.</p> <p>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.</p>
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	<p>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.</p> <p>You can add addresses to your list by manually entering each IP address or hostname, or by importing an external list of addresses.</p> <ul style="list-style-type: none">▶ 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	<p>Select the number of days to keep all other alarms than alarms in the states Closed, Ignore, and Reject.</p> <p>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.</p> <p>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.</p>
Keep events for	Specify the number of days for which to keep events.
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 180).



Name	Description
Data source	<p>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:</p> <p>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).</p> <p>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).</p> <p>[Data source A]</p> <p>[Data source B]</p> <p>and so on.</p>
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.
Protocol type selector	<p>Protocols which the system should listen for, and analyze, in order to detect generic events:</p> <p>Any: TCP as well as UDP.</p> <p>TCP: TCP only.</p> <p>UDP: UDP only.</p> <p>TCP and UDP packages used for generic events may contain special characters, such as @, #, +, ~, and more.</p>
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><LF>).



Name	Description
Echo type selector	<p>Available echo return formats:</p> <ul style="list-style-type: none"> ▶ 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	<p>By default, the list only shows the most relevant options. Select the Show all check box to display all available encodings.</p>
Allowed external IPv4 addresses	<p>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.</p>
Allowed external IPv6 addresses	<p>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.</p>



Feature configuration

Failover recording servers (regular and hot standby)

About failover recording servers

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

A failover recording server is an extra recording server which takes over from a normal recording server if this becomes unavailable. You can configure a failover recording server in two ways, as a **regular failover recording server** or as a **hot standby server**.

You install failover recording servers like regular recording servers. Once you have installed failover recording servers, they are visible in the Management Client. You should install all failover recording servers on separate computers. Make sure that you configure failover recording servers with the correct IP address/hostname of the management server and that you verify that the user account under which the Failover Server service runs has access to your system with administrator rights.

You can specify what type of failover support you want on device-level. For each device on a recording server, select full, live only or no failover support. This helps you prioritize your failover resources and, for example, only set up failover for video and not for audio, or only have failover on essential cameras, not on less important ones.

Regular failover servers

In a regular failover recording server setup, you can group a failover recording server with other failover recording servers in a failover group. The entire failover group is dedicated to taking over from any of several preselected recording servers, should one of these become unavailable.

A failover group can contain one or more regular failover recording servers. Grouping has a clear benefit: when you later specify which failover recording servers should take over from a recording server, you select a group of failover recording servers. If the selected group contains more than one failover recording server, this offers you the security of having more than one failover recording server ready to take over if a recording server becomes unavailable. You can create as many failover groups as needed group them as needed. A failover recording server can only be a member of one group at a time.

Failover recording servers in a failover group are ordered in sequence. This sequence determines in which order the failover recording servers should take over from a recording server. By default, this sequence reflects the order in which you have incorporated the failover recording servers have in the failover group: first in is first in sequence. You can change this if you need to.

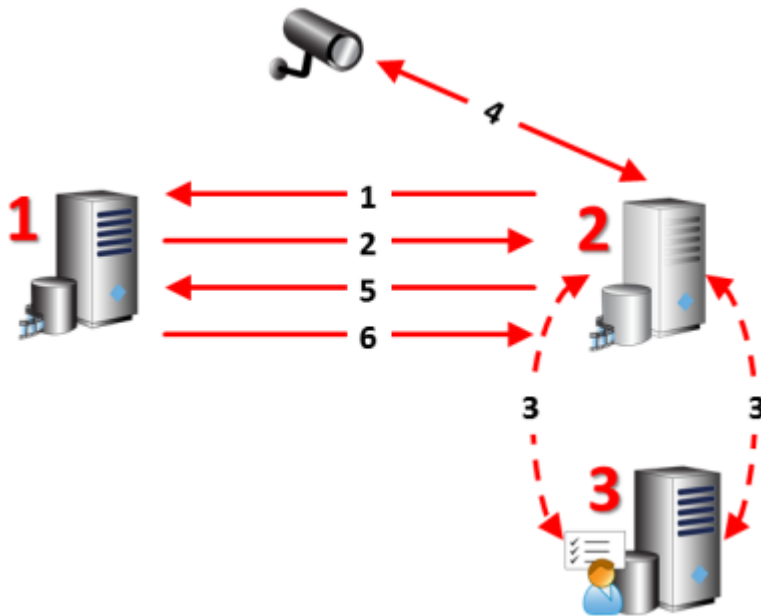
Hot standby failover recording servers

In a hot standby recording server setup, you can dedicate a failover recording server to take over from **one** recording server only. Because of this, the system can keep this failover recording server in a "standby" mode which means that it already starts with the correct/current configuration of the recording server it is dedicated to and can take over faster than a regular failover recording server. As



mentioned, you assign hot standby servers to one recording server only and cannot group it. You cannot select to use failover servers that are already part of a failover group as hot standby recording servers.

About failover steps





Involved **servers** (numbers in red):

1. Recording server
2. Failover recording server
3. Management server.

Failover steps for **Regular failover** setups:

1. To check whether it is running or not, a failover recording server has a non-stop TCP connection to a recording server.
2. This connection is interrupted.
3. The failover recording server requests the current configuration of the recording server from the management server. The management server sends the requested configuration, the failover recording server receives the configuration, starts up, and starts recording on behalf of the recording server.
4. The failover recording server and the relevant camera(s) exchange video data.
5. The failover recording server continually tries to re-establish connection to the recording server.
6. When the connection to the recording server is re-established, the failover recording server shuts down and the recording server fetches video data (if any) recorded during its down-time and the video data is merged back in to the recording server database.

Failover steps for **Hot standby** setups:

1. To check whether it is running or not, a hot standby server has a non-stop TCP connection to its assigned recording server.
2. This connection is interrupted.
3. From the management server, the hot standby server already knows the current configuration of its assigned recording server and starts recording on its behalf.
4. The hot standby server and the relevant camera(s) exchange video data.
5. The hot standby server continually tries to re-establish connection to the recording server.
6. When the connection to the recording server is re-established and the hot standby server goes back to hot standby mode, the recording server fetches video data (if any) recorded during its down-time and the video data is merged back in to the recording server database.

About failover recording server functionality

- A failover recording server checks the state of relevant recording servers every single 0.5 seconds. If a recording server does not reply within 2 seconds, the recording server is considered unavailable and the failover recording server takes over.
- A regular failover recording server takes over for the recording server that has become unavailable after five seconds plus the time it takes for the failover recording server's Recording Server service to start and the time it takes to connect to the cameras. In contrast, a hot standby recording server takes over faster because the Recording Server service is already running with the correct configuration and only has to start its cameras to deliver feeds. During the start up period, you can neither store recordings nor view live video from affected cameras.
- When a recording server becomes available again, it automatically takes over from the failover or hot standby recording server. Recordings stored by the failover or hot standby recording server are automatically merged into the standard recording server's databases. How long the merging process takes depends on the amount of recordings, on network capacity and more. During the merging process, you cannot browse recordings from the period during which the failover or hot standby recording server took over.



- If a failover recording server must take over from another recording server during the merging process in a regular failover recording server setup, it postpones the merging process with recording server A, and takes over from recording server B. When recording server B becomes available again, the regular failover recording server takes up the merging process with recording server A, after which it begins merging with recording server B.
In a hot standby setup, a hot standby server cannot take over for another recording server because it can only be hot standby for a single recording server. But if that recording server fails again, the hot standby takes over again and keeps the recordings from the previous period. The recording server keeps recordings until they are merged back to the primary recorder or until the failover recording server runs out of disk space.
- A failover solution does not provide complete redundancy. It can only serve as a reliable way of minimizing the downtime. If a recording server becomes available again, the Failover Server service makes sure that the recording server is ready to store recordings again. Only then is the responsibility for storing recordings handed back to the standard recording server. So, a loss of recordings at this stage of the process is very unlikely.
- Client users hardly notice that a failover recording server is taking over. A short break occurs, usually only for a few seconds, when the failover recording server takes over. During this break, users cannot access video from the affected recording server. Client users can resume viewing live video as soon as the failover recording server has taken over. Because recent recordings are stored on the failover recording server, they can play back recordings from after the failover recording server took over. Clients cannot play back older recordings stored only on the affected recording server until that recording server is functioning again and has taken over from the failover recording server. You cannot access archived recordings. When the recording server is functioning again, a merging process takes place during which failover recordings are merged back into the recording server's database. During this process, you cannot play back recordings from the period during which the failover recording server took over.
- In a regular failover setup, setting up one failover recording server as backup for another failover recording server is not necessary. This is because you do not allocate particular failover recording servers to take over from a standard recording server. Instead, you allocate failover groups. A failover group must contain at least one failover recording server, but you can add as many failover recording servers as needed. Provided a failover group contains more than one failover recording server, more than one failover recording server can take over. In a hot standby setup, you cannot set up a failover recording servers or hot standby servers for a hot standby server.

Install a failover recording server

Important: During the installation process, you are asked to specify a user account under which the **Failover Server service** should run. This user account must have administrator rights in the system. Note also that if you run workgroups, you should ignore the normal installation guidelines for installing recording servers and use the alternative installation method for workgroups.

Once you have installed the management server using the common installer, download the separate recording server installer from the management server's web page. As part of this installer, specify if you want to install a standard recording server or a failover recording server.

1. Go to the Management server's download web page and select the Recording Server installer. Save the installer somewhere appropriate and run it from here or run it directly from the web page.



2. Select the **Language** you want to use during the installation. Click **Continue**.
3. From the selection list, select **Failover** to install a recording server as a failover recording server.
4. Specify failover recording server properties. Click **Continue**.
5. When installing a failover recording server you must use the particular user account labeled **This account**. If needed, enter a password and confirm this. Click **Continue**.
6. Select **Files location** for the program file. In **Product language**, select the language in which to install your system. Click **Install**.
7. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

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

Set up and enable failover recording servers

Important: If you have disabled the failover recording server, you must enable it before it can take over from the standard recording servers.

Do the following to enable a failover recording server and edit its basic properties:

1. In the **Site Navigation** pane, select **Servers > Failover Servers**. This opens a list of installed failover recording servers and failover groups.
2. In the **Overview** pane, select the required failover recording server.
3. Right-click and select **Enabled**. The failover recording server is now enabled.
4. To edit failover recording server properties, go to the **Info** tab.
5. When done, go to the **Network** tab. Here you can define the failover recording server's public IP address and more. This is relevant if you use NAT (Network Address Translation) and port forwarding. See the standard recording server's **Network** tab for more information.

To see the status of a failover recording server, hold your mouse over the icon in the system tray. A tooltip appears containing the text entered in the Description field of the failover recording server. This may help you determine which recording server the failover recording server is configured to take over from.

Important: The failover recording server pings the management server on a regular basis to verify that it is online and able to request and receive the configuration of the standard recording servers when needed. If you block the pinging, the failover recording server is not able to take over from the standard recording servers.

Assign failover recording servers

On the **Failover** tab of a recording server, you can choose between 3 different types of failover setups:

- a No failover setup



- b** A primary/secondary failover setup
- c** A hot standby setup.

If you select **b** and **c**, you must select the specific server/groups. With **b**, you can also select a secondary failover group. If the recording server becomes unavailable, a failover recording server from the primary failover group takes over. If you have also selected a secondary failover group, a failover recording server from the secondary group takes over in case all failover recording servers in the primary failover group are busy. This way you only risk not having a failover solution in the rare case when all failover recording servers in the primary, as well as in the secondary, failover group are busy.

1. In the **Site Navigation** pane, select **Servers > Recording Servers**. This opens a list of recording servers.
2. In the **Overview** pane, select the wanted recording server, go to the **Failover** tab.
3. To choose failover setup type, select either **None**, **Primary failover server group/Secondary failover sever group** or **Hot standby server**. You cannot select the same failover group as both primary and secondary failover group nor select regular failover servers already part of a failover group as hot standby servers.
4. Next, click **Advanced failover settings**. This opens the **Advanced Failover Settings** window, listing all devices attached to the selected recording server. If you selected **None**, Advanced failover settings are available. Any selections are kept for later failover setups.
5. To specify the level of failover support, select **Full Support**, **Live Only** or **Disabled** for each device in the list. Click **OK**.
6. In the **Failover service communication port (TCP)** field, edit the port number if needed.

Group failover recording servers

1. Select **Servers > Failover Servers**. This opens a list of installed failover recording servers and failover groups.
2. In the **Overview** pane, right-click the top-node **Failover Groups** and select **Add Group**.
3. Specify a name (in this example *Failover Group 1*) for and a description (optional) of your new group. Click **OK**.
4. Right-click the group (*Failover Group 1*) you just created. Select **Edit Group Members**. This opens the **Select Group Members** window.
5. Drag and drop or use the buttons to move the selected failover recording server(s) from the left side to the right side. Click **OK**. The selected failover recording server(s) now belongs to the group (*Failover Group 1*) you just created.
6. Go to the **Sequence** tab. Click **Up** and **Down** to set the internal sequence of the regular failover recordings servers in the group.

Read failover recording server status icons

The following icons represent the status of failover recording servers (icons are visible in the **Overview** pane):



Icon	Description
	The failover recording server is either waiting or "watching". When waiting, the failover recording server is not configured to take over from any recording server yet. When "watching", the failover recording server is configured to watch one or more recording servers.
	The failover recording server has taken over from the designated recording server. If you place your cursor over the server icon, you see a tooltip. Use the tooltip to see which recording server the failover recording server has taken over from.
	Connection to the failover recording server is broken.

Failover recording server properties

Specify the following failover recording server properties:

Name	Description
Name	The name of the failover recording server as it appears in the Management Client, logs and more.
Description	An optional field that you can use to describe the failover recording server, for example which recording server it takes over from.
Host name	Displays the network address of the failover recording server. You cannot change this.
UDP port	The port number used for communication between failover recording servers. By default, the system uses port 8844.
Database location	Specify the path to the database used by the failover recording server for storing recordings. You cannot change the database path while the failover recording server is taking over from a recording server. The system applies the changes when the failover recording server is no longer taking over from a recording server.
Enable this failover server	Clear to disable the failover recording server (selected by default). Note that you must disable failover recording servers before they can take over from recording servers.

Failover group properties

The **Info** tab:

Name	The name of the failover group is it appears in the Management Client, logs and more.
Description	An optional description, for example the server's physical location.



The **Sequence** tab:

Specify the failover sequence

Use **Up** and **Down** to set the wanted sequence of regular failover recording servers within the group.

About failover recording server services

A failover recording server has two services installed:

- A Failover Server service, which handles the processes of taking over from the recording server. This service is always running, and constantly checks the state of relevant recording servers.
- A Failover Recording Server service, which enables the failover recording server to act as a recording server.

In a failover group setup, this service is only started when required, that is when the regular failover recording server should take over from the recording server. Starting this service typically takes a couple of seconds, but may take longer depending on local security settings and more.

In a hot standby setup, this service is always running, allowing the hot standby server to take over faster than the regular failover recording server.

View status messages

1. On the failover recording server, right-click the **Milestone Failover Server service** icon.
2. Select **Show Status Messages**. The **Failover Server Status Messages** window appears, listing time-stamped status messages.

Change the management server address

The failover recording server must be able to communicate with your system's management server. You specify the IP address/hostname of the management server during the installation of the failover recording server. If you want to change the address of the management server, do as follows:

1. On the failover recording server, stop the Failover Recording Server service.
2. Right-click the notification area's Failover Recording Server service icon again.
3. Select **Change Settings**. The **Failover Recording Server Settings** window appears, so you can specify the IP address or host name of the management server with which the failover recording server should communicate.

View version information

Knowing the exact version of your **Failover Recording Server service** is an advantage if you need to contact product support.



1. On the failover recording server, right-click the **Milestone Failover Recording Server service** icon.
2. Select **About**.
3. A small dialog box opens that shows the exact version of your **Failover Recording Server service**.

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](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 you see on your screen.

Installation and change of URL address:

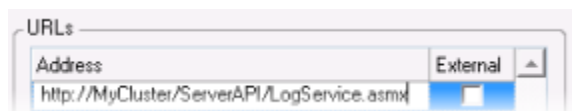
1. Install the management server and all its subcomponents on the first server in the cluster.



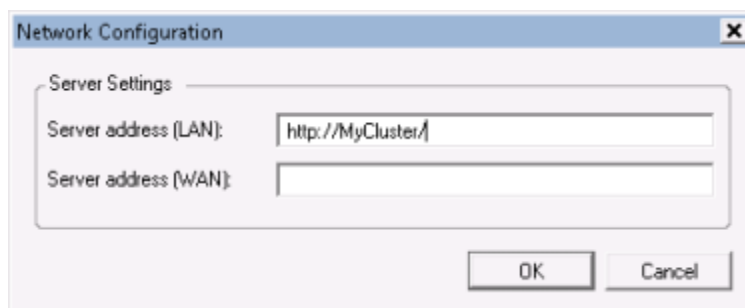
The management server must be installed with a specific user and not as a **network service**. This requires that you use the **Custom** install option. Also, the specific user must have access to the shared network drive and preferably a non-expiry password.

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](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 **Milestone XProtect 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 **Milestone XProtect Event Server** service as a resource to the **Milestone XProtect Management Server Cluster** service, right-click the cluster service and click **Add a resource > 4 - Generic Service** and select **Milestone XProtect Event Server**.
7. Repeat step 6, but instead of the event server, select to add **Milestone XProtect Data Collector Server**.

The service channel and the IIS should both be installed normally with the exact same user, and **not** as cluster services.

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 255).

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).



Remote connect services

About remote connect services

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

The remote connect services feature contains the Axis One-click Camera Connection technology developed by Axis Communications. It enables the system to retrieve video (and audio) from external cameras where firewalls and/or router network configuration normally prevents initiating connections to such cameras. The actual communication takes place via secure tunnel servers (ST servers). ST servers use VPN. Only devices that hold a valid key work within a VPN. This offers a secure tunnel where public networks can exchange data in a safe way.

Remote connect services allows you to:

- Edit credentials within the Axis Dispatch Service
- Add, edit, and remove ST servers
- Register/unregister and edit Axis One-click cameras
- Go to the hardware related to the Axis One-Click camera.

Before you can use Axis One-click Camera Connection, you must first install a suitable ST server environment. To work with secure tunnel server (ST server) environments and Axis One-click cameras, you must first contact your system provider to obtain the needed user name and password for Axis Dispatch Services.

Install STS environment for One-click camera connection

Prerequisites:

- Contact your system provider to obtain the needed user name and password for Axis Dispatch Services
 - Make sure your camera(s) support Axis Video Hosting System. Go to <http://www.axis.com/products/avhs/> <http://www.axis.com/products/avhs/>.
 - If needed, update your Axis cameras with the newest firmware. Go to <http://www.axis.com/techsup/firmware.php> <http://www.axis.com/techsup/firmware.php>
1. On each camera's homepage, go to **Basic Setup, TCP/IP**, and select **Enable AVHS** and **Always**.
 2. From your management server's download web page (controlled by the Download Manager), install the **Axis One-Click Connection Component** to setup a suitable Axis secure tunnel framework.



Add/edit STSs

1. Do one of the following:
 - a) To add an ST servers, right-click the **Axis Secure Tunnel Servers** top node, select **Add Axis Secure Tunnel Server**.
 - b) To edit an ST server, right-click it, select **Edit Axis Secure Tunnel Server**.
2. In the window that opens, fill in the relevant information.
3. If you chose to use credentials when you installed the **Axis One-Click Connection Component**, select the **Use credentials** check box and fill in the same user name and password as used for the **Axis One-Click Connection Component**.
4. Click **OK**.

Register new Axis One-click camera

1. To register a camera under an ST server, right-click it and select **Register Axis One-click Camera**.
2. In the window that opens, fill in the relevant information.
3. Click **OK**.
4. The camera now appears under the relevant ST server.

The camera can have the following color codings:

Color	Description
Red	Initial state. Registered, but not connected to the ST server.
Yellow	Registered. Connected to the ST server, but not added as hardware.
Green	Added as hardware. May or may not be connected to the ST server.

When you add a new camera, its status is always green. The connection status is reflected by **Devices on Recording Servers** in the **Overview** pane. In the **Overview** pane, you may group your cameras for an easier overview. If you choose **not** to register your camera at the Axis dispatch service at this point, you can do so later from the right-click menu (select **Edit Axis One-click Camera**).



Axis One-Click Camera connection properties

Name	Description
Camera password	Enter/edit. Provided with your camera at purchase. For further details, see your camera's manual or www.axis.com http://www.axis.com .
Camera user	See details for Camera password .
Description	Enter/edit a description for the camera.
External address	Enter/edit the http address of the ST server to which the camera(s) connect.
Internal address	Enter/edit the http address of the ST server to which the recording server connects.
Name	If needed, edit the name of the item.
Owner authentication key	See Camera password .
Passwords (for Dispatch Server)	Enter password. Must be identical to the one received from your system provider.
Passwords (for ST server)	Enter password. Must be identical to the one entered when the Axis One-Click Connection Component was installed.
Register/Unregister at the Axis Dispatch Service	Indicate whether you wish to register your Axis camera with the Axis dispatch service. Can be done at time of setup or later.
Serial number	Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
Use credentials	Select the check box if you decided to use credentials during the installation of the ST server.
User name (for Dispatch Server)	Enter a user name. The user name must be identical to the one received from your system provider.
User name (for ST server)	Enter user name. Must be identical to the one entered when the Axis One-Click Connection Component was installed.

Milestone Federated Architecture

About selecting Milestone Interconnect or Milestone Federated Architecture

In a physically distributed system where users on the central site need to access the video on the remote site, you can choose between Milestone Interconnect™ or Milestone Federated Architecture™.

Milestone recommends Milestone Federated Architecture when:



- The network connection between the central and federated sites is stable.
- The network uses the same domain.
- There are fewer larger sites.
- The bandwidth is sufficient for the required use.

Milestone recommends Milestone Interconnect when:

- The network connection between the central and remote sites is unstable.
- You or your organization want to use another XProtect product on the remote sites.
- The network uses different domains or workgroups.
- There are many smaller sites.

About Milestone Federated Architecture

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

Milestone Federated Architecture™ links multiple individual standard systems into a parent/child hierarchy of sites. With Milestone Federated Architecture, client users with sufficient rights have seamless access to video, audio and other resources across individual sites. Through a single login, administrators can centrally manage all sites within the federated hierarchy, based on administrator rights for the individual sites.

Milestone Federated Architecture does not require additional licenses.

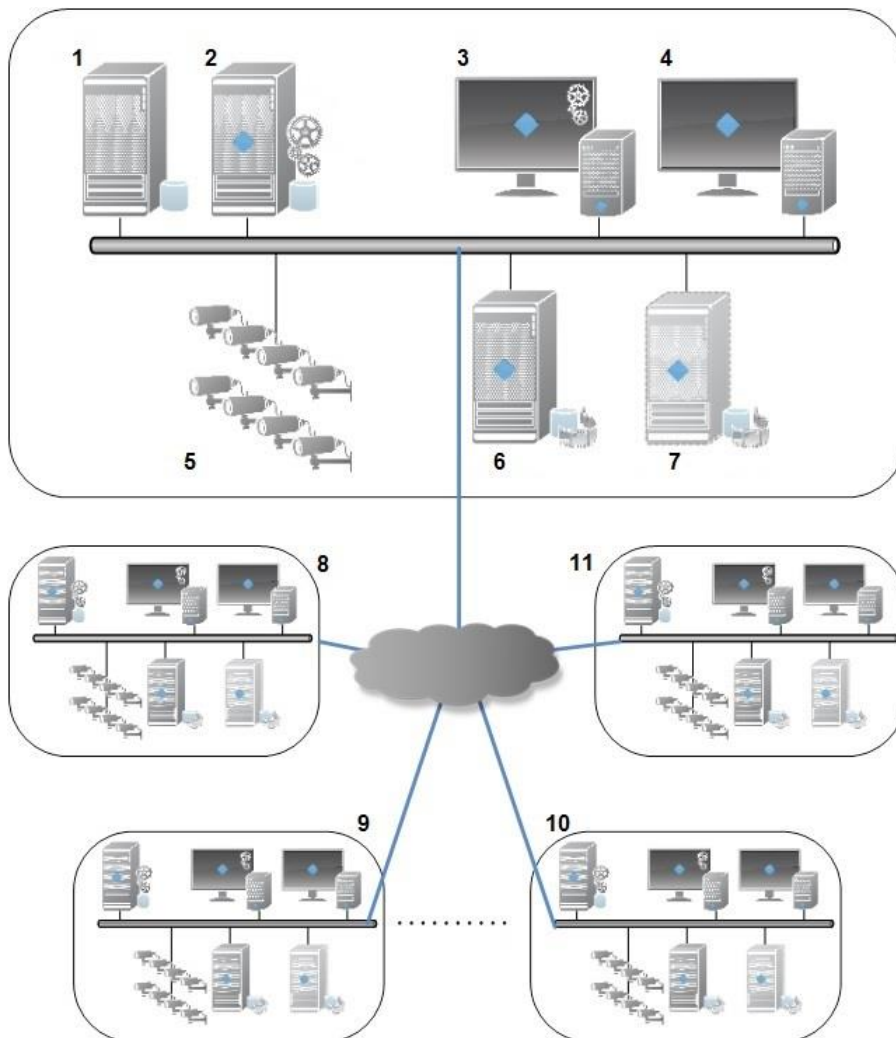
Important: You can only centrally manage a Milestone Federated Architecture hierarchy if all sites use the same version of your XProtect product.

You install and configure each site in a federated hierarchy as a normal standalone system with standard system components, settings, rules, schedules, administrators, users, and user rights. Once you have installed each site, you connect these by requesting a link from one site (the parent site) to another (the child site). When the link is established, the two sites automatically create a federated hierarchy to which you can add more sites. Once you have created the hierarchy, it allows users and administrators logged into a site to access that site and any child or sub-child sites it may have. Access to child sites depend on the user rights.

Important: You can only add sites that use the same version of your XProtect product as the site you are adding to.



You can only have one central site, but the central site can have an unlimited number of child sites. The link between a parent site and a child site is established, when you request the link from the parent site. If you are not the administrator of the child site, the request must be accepted by the child site administrator. A parent site includes information about all of its child sites and the child sites' child sites, but only controls them one level down. Similarly, a child site only knows about and answers to its parent site one level up. Your home site is the parent site you are logged in to.



The contents of a Milestone Federated Architecture setup:

1. SQL server
2. Management server
3. Management Client
4. Smart Client
5. Cameras
6. Recording server
7. Failover recording server
8. to 11. Federated sites



Hierarchy synchronization

A parent site contains an updated list of all its currently attached child sites, child sites' child sites and so on. The federated hierarchy has a regularly scheduled synchronization between sites, as well as management-triggered synchronization every time a site is added or removed. When the system synchronizes the hierarchy, it takes place level by level, each level forwarding and returning communication, until it reaches the server that requests the information. The system sends less than 1MB each time. Depending on the number of levels, changes to a hierarchy can take some time to become visible in the Management Client. You cannot schedule your own synchronizations.

Data traffic

The system sends video or configuration data when a user or administrator views live or recorded video or configures a site. The amount of data depends on what and how much is being viewed.

Milestone Federated Architecture with other products






With XProtect Smart Wall installed on a parent site in a federated architecture, you can use the XProtect Smart Wall features. See *Configure XProtect Smart Walls* (see "Configure Smart Walls" on page 274) on how set up an XProtect Smart Wall.

With XProtect Access Control Module installed and if an XProtect Smart Client logs into a parent site in a federated hierarchy, access request notifications from the child sites also appear in XProtect Smart Client.

For more information about use cases and benefits, see the white paper about Milestone Federated Architecture technology on the Milestone website <http://www.milestonesys.com>.

Status icons in Milestone Federated Architecture

The following icons represent the different states in which a site can be:

Description	Icon
The top site in the entire hierarchy is operational.	
The top site in the entire hierarchy is still operational, but one or more issues need attention. Shown on top of the top site icon.	
The site is operational.	
The site is awaiting to be accepted in the hierarchy.	
The site is attaching, but is not yet operational.	



Set up your system to run federated sites

To prepare your system for Milestone Federated Architecture, you must make certain choices when you install the product on the management server. Depending on how your system is set up, choose between three different alternatives.

Alternative 1: Connect sites from the same domain (with a common domain user) and customize the installation of the management server to Milestone Federated Architecture

Before you install the management server, you must create a common domain user and use this as the administrator on all computers involved in the hierarchy.

Custom installation

1. Start the installation of XProtect Advanced VMS on the management server and select **Custom**.
2. Select to install the Management Server service using a user account. The selected user account must be the administrator on all management servers and you must also use this when you install XProtect Advanced VMS on the other management servers in the hierarchy.
3. Finish the installation. Repeat steps 1-3 to install any other systems you want to connect in the hierarchy.

Single Server or Distributed Installation - set up network service on all servers

1. Start the installation of XProtect Advanced VMS on the management server and select **Single Server** or **Distributed**. This installs the product as a **network service**. Repeat this step for all the sites in your hierarchy.
2. Log into the management server that you want as your parent site in the hierarchy.
3. Expand **Security > Roles > Administrators**.
4. On the **Users and Groups** tab, click **Add** and select **Windows User**.
5. In the dialog box, select **Computers** as object type, type the name of the child site computer and click **OK** to add the computer to the parent server's **Administrator** role. Repeat this step until you have added all child site computers and exit the application.
6. Log into the management server for each child site, and add the parent site computer plus the child site computers that are connected directly to the parent site, to the **Administrator** role, in the same way as above.

Alternative 2: Connecting sites from different domains

To connect to sites across domains, make sure that these domains are trusted by each other. Setting up domains to trust each other has nothing to do with Milestone Federated Architecture, but has to do with Microsoft Windows Domain configuration. When you have established trust between the domains on which the sites you want to connect to each other in a hierarchy, follow the same description as seen in Alternative 1. For more information about how to set up trusted domains, see the Microsoft website <http://technet.microsoft.com/en-us/library/cc961481.aspx>.

Milestone recommends Milestone Interconnect for creating multi-site systems when your system works with multiple domains.



Alternative 3: Connect sites in workgroup(s)

When you connect sites inside workgroups, Milestone Federated Architecture must have the same administrator account present on all computers you want connected in the hierarchy to work properly. You must have this in place before installing the system.

1. Log in to **Windows** using a common administrator account.
2. Start the management server installation and click **Custom**.
3. Select to install the Management Server service using a common administrator account.
4. Finish the installation. Repeat steps 1-4 to install any other systems you want to connect. You must all of these systems using a common administrator account.

Milestone recommends Milestone Interconnect for creating multi-site systems when the sites are not part of a domain.


You cannot mix domain(s) and workgroup(s). This means that you cannot connect sites from a domain to sites from a workgroup and vice versa.

Add site to hierarchy

As you expand your system, you can add sites to your top site and to its child sites as long as the system is set up correctly.


1. Select the **Federated Site Hierarchy** pane.
2. Select the site to which you want to add a child site, right-click, and click **Add Site to Hierarchy**.
3. Enter the URL of the requested site in the **Add Site to Hierarchy** window and click **OK**.
4. The parent site sends a link request to the child site and after a while, a link between the two sites is added to the **Federated Site Hierarchy** pane.
5. If you can establish the link to the child site without requesting acceptance from the child site administrator, go to step 7.

If **not**, the child site has the awaiting acceptance  icon until the administrator of the child site has authorize the request.

6. Make sure that the administrator of the child site authorizes the link request from the parent site (see "Accept inclusion in the hierarchy" on page 266).
7. The new parent/child link is established and the **Federated Site Hierarchy** pane is updated with the  icon for the new child site.




Accept inclusion in the hierarchy

When a child site has received a link request from a potential parent site where the administrator did not have administrator rights to the child site, it has the awaiting acceptance  icon.

To accept a link request:

1. Log into the site.
2. In the **Federated Site Hierarchy** pane, right-click the site and click **Accept Inclusion in Hierarchy**.

If the site runs an XProtect Expert version, you right-click the site in the **Site Navigation** pane.

3. Click **Yes**.
4. The new parent/child link is established and the **Federated Site Hierarchy** pane is updated with the normal site  icon for the selected site.

Changes that you make to child sites located far from the parent site can take some time to be reflected in the **Federated Site Hierarchy** pane.

Refresh site hierarchy

Regularly the system automatically synchronizes the hierarchy through all levels of your parent/child setup. You can refresh it manually, if you want to see changes reflected instantly in the hierarchy, and do not want to wait for the next automatic synchronization.

You need to be logged into a site to perform a manual refresh. Only changes saved by this site since the last synchronization are reflected by a refresh. This means that changes made further down in the hierarchy might not be reflected by the manual update, if the changes have not reached the site yet.

1. Log into the relevant site.
2. Right-click the top site in the **Federated Site Hierarchy** pane and click **Refresh Site Hierarchy**.

This will take a few seconds.

Connect to another site in hierarchy

If you have administrator rights, you can connect to other sites and administrate these.

1. Click the relevant site in the **Federated Site Hierarchy** pane.

A brief dialog box informs you that you are being connected to the selected site.

2. When connection is complete, your view in the Federated Sites Hierarchy pane changes to reflect that you are connected to a different site.



In this example, the user logged into the home site **Rome Server** and connected to the child **Paris Server**:



Detach a site from the hierarchy

When you detach a site, the link between the sites are broken.



The process of detaching a site from its hierarchy depends on the site you want to detach.

Detach a child site from the hierarchy

You can only detach child sites that are directly connected to the site you are logged in to.

1. In the **Federated Site Hierarchy** pane, right-click the site you want to detach and select **Detach Site from Hierarchy**.
2. Click **Yes** to remove the detached site and update the **Federated Site Hierarchy** pane.

Detach a home site from the hierarchy

1. In the **Federated Site Hierarchy** pane, right-click the home site, and click **Detach Site from Hierarchy**.
2. Click **Yes** to update the **Federated Site Hierarchy** pane. If the detached site has child sites, it becomes the new top site for this branch of the hierarchy, and the normal site icon  changes to a top site  icon.
3. Click **OK**.

Changes to the hierarchy are reflected after a manual refresh or an automatic synchronization.

Federated site properties

General tab

You can change some of the information related to the site that you are currently logged in to.



Name	Description
Name	Enter the name of the site.
Description	Enter a site description.
URLs	Use the list to add and remove URL(s) for this site and indicate if they are external and not. External addresses can be reached from outside the local network.
Version	The version number of the site's management server.
Service account	The service account under which the management server is running.
Time for last synchronization	Time and date of the last synchronization of the hierarchy.
Status for last synchronization	The status of the last synchronization of the hierarchy. It can be either Successful or Failed .

Parent Site tab

This tab shows information about the parent site of the site that you are currently logged in to. The tab is not visible if your site has no parent site.

Name	Description
Name	Shows the name of the parent site.
Description	Shows a description of the parent site (optional).
URLs	Lists URL(s) for the parent site and indicates if they are external or not. External addresses can be reached from outside the local network.
Version	The version number of the site's management server.
Service account	The service account under which the management server is running.
Time for last synchronization	Time and date of the last synchronization of the hierarchy.
Status for last synchronization	The status of the last synchronization of the hierarchy. It can be either Successful or Failed .



Milestone Interconnect

About selecting Milestone Interconnect or Milestone Federated Architecture

In a physically distributed system where users on the central site need to access the video on the remote site, you can choose between Milestone Interconnect™ or Milestone Federated Architecture™.

Milestone recommends Milestone Federated Architecture when:

- The network connection between the central and federated sites is stable.
- The network uses the same domain.
- There are fewer larger sites.
- The bandwidth is sufficient for the required use.

Milestone recommends Milestone Interconnect when:

- The network connection between the central and remote sites is unstable.
- You or your organization want to use another XProtect product on the remote sites.
- The network uses different domains or workgroups.
- There are many smaller sites.

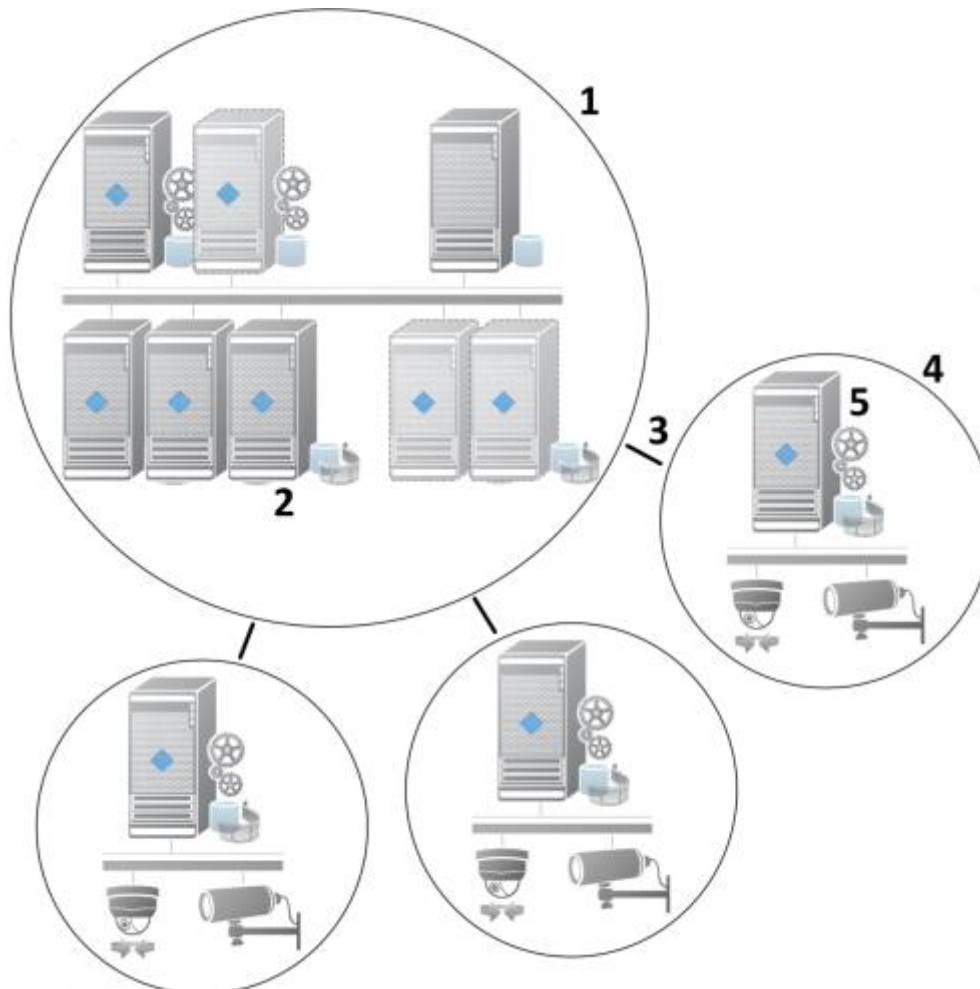
About Milestone Interconnect

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

Milestone Interconnect™ allows you to integrate a number of smaller, physically fragmented, and remote XProtect installations with an XProtect Corporate central site. You can install these smaller sites, called remote sites, on mobile units, for example, boats, busses or trains. This means that such sites do not need to be permanently connected to a network.



The following illustration shows how you could set up Milestone Interconnect on your system:



1. Milestone Interconnect™ central XProtect Corporate site
2. Milestone Interconnect drivers (handles the connection between the central sites' recording servers and the remote site, must be selected in the list of drivers when adding remote systems via the **Add Hardware** wizard)
3. Milestone Interconnect connection
4. Milestone Interconnect remote site (the complete remote site with system installation, users, cameras and so on)
5. Milestone Interconnect remote system (the actual technical installation at the remote site)

Each remote site runs independently and can perform any normal surveillance tasks. Depending on the network connections and appropriate user rights, Milestone Interconnect offers you direct live viewing of remote site cameras and play back of remote site recordings from the central site. It also offers you the possibility to transfer remote site recordings to the central site based on either events, rules/schedules, or manual requests by XProtect Smart Client users. It also allows central site users to employ events originally triggered on remote sites on the central site.

Which XProtect product can act as central site and which can act as remote sites depends on the specific setup. It differs from setup to setup which versions, how many cameras, and how devices and events originating from the remote site are handled - if at all - by the central site. For further details on how specific XProtect products interact in a Milestone Interconnect setup, go to the Milestone Interconnect website <http://www.milestonesys.com/our-products/milestone-interconnect/>.



You add remote sites to the central site by using the **Address range scanning** or **Manual** options in the **Add Hardware** (on page 78) wizard. When you add the remote site, you must specify an account on the remote site. This account can be either a basic user, local Windows user, or domain user. You can reuse an existing user or create a new one to use with Milestone Interconnect. You must create a new user on the remote system before creating the Milestone Interconnect setup. Depending on the user rights for the selected user on the remote site, the central site gets access to all cameras and functions or a sub-set of them.

About possible Milestone Interconnect setups

There are multiple ways to run Milestone Interconnect™.

In the following, the three most likely scenarios are described. How to run your setup depends on your network connection, whether you request playback, and whether you retrieve remote recordings and to what degree.

Direct playback from remote sites on request (good network connections)

The most straight forward setup. The central site is continuously online with its remote sites which send remote recordings on request. Central site users play back remote recordings directly from the remote sites. This requires use of the **Play back recordings from remote system** option.

Rule- or XProtect Smart Client-based retrieval of selected remote recording sequences from remote sites (periodically limited network connections)

Used when selected recording sequences (originating from remote sites) should be stored centrally to ensure independence from remote sites. Independence is crucial in case of network failure or network restrictions. Configuring retrieval of remote recordings when the network connection is optimal, that is not used for other priority data, can be done from the **Remote Recordings** tab.

Alternatively, remote recordings retrieval can be started from the XProtect Smart Client when needed or a rule can be set up. In some scenarios, remote sites are on-line and in others, offline most of the time. This is often industry specific. For some industries it is common for the central site to be permanently on-line with its remote sites (for example a retail HQ (central site) and a number of shops (remote sites)). For other industries, like transportation, the remote sites are mobile (for example, busses, trains, ships, and so on) and can only establish network connection randomly. Should the network connection fail during a commenced remote recording retrieval, the job continues at next given opportunity.

If the system receives an automatic retrieval, or request for retrieval from the XProtect Smart Client, outside the time interval that you specified on the **Remote Retrieval** tab, it is accepted, but not started until the selected time interval is reached. New remote recording retrieval jobs will queue and start when the allowed time interval is reached. You can view pending remote recording retrieval jobs from System Dashboard -> Current Tasks.

After connection failure, missing remote recordings are per default retrieved from remote sites

Uses remote sites like a recording server uses the edge storage on a camera. Typically, remote sites are on-line with their central site, feeding it a live stream that the central site records. Should the network fail for some reason, the central site miss out on recording sequences. However, once the network is re-established, the central site automatically retrieves remote recordings covering the



down-period. This requires use of the **Automatically retrieve remote recordings when connection is restored** option.

You can mix any of the above solutions to fit your organizations special needs.

Milestone Interconnect and licensing

Cameras under remote sites in a Milestone Interconnect™ setup are listed on the **License Information** page of the central site. They are listed according to the same rules as other cameras, but with Milestone Interconnect in front:

- **Milestone Interconnect Camera**

Update remote site hardware

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Right-click it.
3. Select **Update Hardware**. This opens the **Update hardware** dialog box.
4. The dialog box lists all changes (devices removed, updated and added) in the remote system since your Milestone Interconnect setup was established or refreshed last. Click **Confirm** to update your central site with these changes.

Establish remote desktop connection to remote system

Preconditions: The remote desktop connections to the computer you want to remote to must be up and running and its management application must be open.

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system.
3. In the Properties pane, select the **Info** tab.
4. In the **Remote administration** area, type the appropriate Windows user name and password.
5. Once user name and password are saved, click **Connect** to establish remote desktop connection.
6. In the toolbar, click **Save**.

Enable playback directly from remote site camera

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.



3. In the Properties pane, select the **Record** tab, and select the **Play back recordings from remote system** option.
4. In the toolbar, click **Save**.

In a Milestone Interconnect™ setup, the central system disregards privacy masking defined in a remote system.

Retrieve remote recordings from remote site camera

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.
3. In the Properties pane, select the **Record** tab, and select the **Automatically retrieve remote recordings when connection is restored** option.
4. In the toolbar, click **Save**.

As an alternative, you can use rules or start remote recording retrievals from XProtect Smart Client when needed.

In a Milestone Interconnect™ setup, the central system disregards privacy masking defined in a remote system.

XProtect Smart Wall

About XProtect Smart Wall

Available functionality depends on the system you are using. See Product comparison chart (on page 22) for more information.

XProtect 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.



XProtect 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 XProtect Smart Client by dragging and dropping views and cameras onto the logical representation of the video wall in XProtect Smart Client or by selecting the different Smart Wall presets defined by the surveillance administrator.

See the XProtect Smart Client documentation for more information about how to use the XProtect Smart Wall features in XProtect Smart Client.

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 XProtect Smart Client views that your XProtect 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 XProtect 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 an XProtect Smart Client user 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 XProtect 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**, **Recording Servers** or **Federated Site Hierarchy** tab onto the different layout items. The cameras on the **Federated Site Hierarchy** tab are accessible in a Milestone Federated Architecture setup. 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.

Manage roles with Smart Walls

You can grant your XProtect Smart Client users different Smart Wall-related user rights to control what is displayed on the video wall.

1. Expand **Security**, and right-click **Roles**.



2. Select the role you want to assign user rights.
3. Specify relevant user rights on the **Smart Wall** tab. The properties differ depending on the selected user right. See Roles with Smart Wall rights properties (see "Smart Wall tab (roles)" on page 218).

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 165) for information about how to create rules.

```
Perform an action in a time interval  
day of week is Thursday  
Set smart wall London to preset Factory  
and Set smart wall London monitor UK Monitor 9 using current layout  
to show Camera 1 starting in position 6
```

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 XProtect 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 XProtect 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 276).

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 XProtect Smart Client.

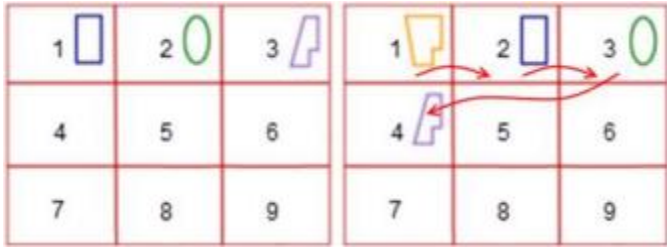
Name	Description
Edit	Click to adjust the positioning of the monitors.
Movement	To move a monitor to a new position, select the relevant monitor and drag it to the desired position, or click one of the arrow buttons to move the monitor in the selected direction.
Zoom buttons	Click buttons to zoom in/out 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 XProtect 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 XProtect 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	<p>Defines what should be displayed on a monitor with an empty preset layout when a new Smart Wall preset is triggered or selected in XProtect Smart Client.</p> <p>Select Preserve to keep the current content on the monitor.</p> <p>Select Clear to clear all content so nothing is displayed on the monitor.</p>
Empty preset item	<p>Defines what should be displayed in an empty preset layout item when a new Smart Wall preset is triggered or selected in XProtect Smart Client.</p> <p>Select Preserve to keep the current content in the layout item.</p> <p>Select Clear to clear the content so nothing is displayed in the layout item.</p>
Element insertion	<p>Defines how cameras are inserted in the monitor's layout when viewed in the XProtect 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.</p>  <p>Before a new camera is inserted and after.</p>

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	<p>Click Edit to edit the layout and the content of the selected monitor.</p> <p>Double-click a camera to remove a single camera.</p> <p>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.</p> <p>Click  to select the layout you want to use with your monitor in the selected preset, and click OK.</p> <p>Drag cameras from the Device Groups, Recording Servers or Federated Sites 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.</p>

XProtect Access Control Module

About access control integration

The use of XProtect Access Control Module requires that you have purchased a license that allows you to access this feature.

You can use XProtect Access Control Module with access control systems from vendors that have a vendor-specific plug-in for XProtect Access Control Module.

The access control integration feature introduces new functionality that makes it simple to integrate customers' access control systems with XProtect. You get:

- A common operator user interface for multiple access control systems in the XProtect Smart Client
- Faster and more powerful integration of access control systems
- More functionality (see below)

In the XProtect Smart Client, the operator gets:

- Live monitoring of access control events
- Operator aided passage for access requests
- Map integration
- Alarm definitions for access control events



- Investigation of access control events
- Centralized door state overview and control
- Cardholder information

Apart from a license, you need a vendor-specific integration plug-in installed on the event server before you can start an integration.

Configure an integrated access control system

The steps for a successful creation and configuration of an integrated access control system:

1. Add the integrated access control system to your XProtect system. See Wizard for access control system integration (on page 280). The wizard takes you through the most basic steps.
2. Specify additional properties for the access control system integration, especially the access control events may require that you map events from the access control system with event categories that XProtect recognizes. See Access control properties (on page 282).
3. You need to create a role with permission to use access control features in XProtect Smart Client. See Access Control tab (see "Access Control tab (roles)" on page 220).
4. You also need to associate this role with a Smart Client profile. See Smart Client profile properties (on page 136).
5. The system provides a default rule that lets access request notifications appear on the XProtect Smart Client screen in case of access denied. You can add and modify access request notifications, see Access Request Notification (properties) (see "Access Request Notification tab (Access Control)" on page 285).
6. You can create additional rules based on actions and events from the access control system. See About actions and stop actions (on page 144) and Events overview (on page 152).
7. If required, change the overall access control settings in **Options > Access Control Settings**. See Access Control Settings tab (see "Access Control Settings tab (options)" on page 242).

Wizard for access control system integration

The **Access control system integration** wizard is for step-by-step configuration of the initial integration with an access control system. Use the wizard to get through the most basic configuration tasks. You can do more detailed configuration afterwards.

Before you start the access control integration wizard make sure you have the integration plug-in installed on the event server.

Some of the fields to fill out and their default values are inherited from the integration plug-in. Therefore the appearance of the wizard may differ depending on the access control system you integrate with.

To start the wizard, select **Access Control** in the node tree, right-click, and click **Create new**.



Steps in this wizard:

Create access control system integration	281
Connecting to the access control system	281
Associated cameras	281
Final summary	281

Create access control system integration

Enter the name and specify the connection details for the access control system you want to add. The parameters that you must specify depend on the type of system, but are typically the network address of the access control system server and an access control administrator user name and password.

The video management system uses the specified user name and password to log into the access control system for retrieving the full configuration.

The integration plug-in may also define secondary parameters which are not listed in the wizard, but you can change these in **General Settings** after setting up the integration. The default values for the parameters are supplied by the plug-in or the XProtect system.

Connecting to the access control system

When the plug-in has been successfully integrated, a summary of the retrieved access control system configuration appears. Review the list to ensure that all items have been integrated before you continue to the next step of the wizard.

Associated cameras

Map access points in the access control system with the cameras in the XProtect system, to show related video for events from the doors.

You can map several cameras to one access point. The XProtect Smart Client user is then able to view video from all the cameras when investigating events, for example.

The XProtect Smart Client user is also able to add one of the cameras when configuring **Access Monitor** view items.

Licensed doors are by default enabled. Clear the check box to disable a door and thereby free a license.

Final summary

Your access control system integration has been successfully created in XProtect with default settings inherited from the integration plug-in. Client users must log into XProtect Smart Client to see and use the new access control system.



You can refine the configuration in the Management Client.

Access control properties

General Settings tab (Access Control)

Name	Description
Enable	<p>Systems are by default enabled, meaning that they are visible in XProtect Smart Client for users with sufficient rights and that the XProtect system receives access control events.</p> <p>You can disable a system, for example during maintenance, to avoid creating unnecessary alarms.</p>
Name	The name of the access control integration as it appears in the management application and in the clients. You can overwrite the existing name with a new one.
Description	Provide a description of the access control integration. This is optional.
Integration plug-in	Shows the type of access control system selected during the initial integration.
Last configuration refresh	Shows the date and time of the last time the configuration was imported from the access control system.
Refresh configuration	<p>Click the button when you need to reflect configuration changes made in the access control system in XProtect, for example you have added or deleted a door.</p> <p>A summary of the configuration changes from the access control system appears. Review the list to ensure that your access control system is reflected correctly before you apply the new configuration.</p>
Operator login required	<p>Enable an additional login for the client users, if the access control system supports differentiated user rights.</p> <p>This option is only visible if the integration plug-in supports differentiated user rights.</p>

The naming and content of the following fields are imported from the integration plug-in. Below are examples of some typical fields:



Name	Description
Address	Type the address of the server that hosts the integrated access control system.
Port	Specify the port number on the server to which the access control system is connected.
User name	Type the name of the user, as defined in the access control system, who should be administrator of the integrated system in XProtect.
Password	Specify the password for the user.

Associated Cameras tab (Access Control)

Provides mappings between door access points and cameras, microphones or speakers. You associate cameras as part of the integration wizard, but you can change the setup at any time. Mappings to microphones and speakers are implicit through the related microphone or speaker on the camera.

Name	Description
Doors	<p>Lists the available door access points defined in the access control system, grouped by door.</p> <p>Enabled: Licensed doors are by default enabled. You can disable a door to free a license.</p> <p>License: Shows if a door is licensed or if the license has expired. The field is blank when the door is disabled.</p> <p>Remove: Click Remove to remove a camera from an access point. If you remove all cameras, the check box for associated cameras is automatically cleared.</p>
Cameras	<p>Lists the cameras configured in the XProtect system.</p> <p>Select a camera from the list, and drag and drop it at the relevant access point to associate the access point with the camera.</p>

Access Control Events tab (Access Control)

Event categories allow you to group events. The configuration of event categories affects the behavior of access control in the XProtect system and allows you to, for example, define an alarm to trigger a single alarm on multiple event types.



Name	Description
Access Control Event	<p>Lists the access control events imported from the access control system. The integration plug-in controls default enabling and disabling of events. You can disable or enable events any time after the integration.</p> <p>When an event is enabled, it is stored in the XProtect event database and is, for example, available for filtering in the XProtect Smart Client.</p>
Source Type	Shows the access control unit that can trigger the access control event.
Event Category	<p>Assign none, one or more event categories to the access control events. The system automatically maps relevant event categories to the events during integration. This enables a default setup in the XProtect system. You can change the mapping at any time.</p> <p>Built-in event categories are:</p> <ul style="list-style-type: none"> ▶ Access denied ▶ Access granted ▶ Access request ▶ Alarm ▶ Error ▶ Warning <p>Events and event categories defined by the integration plug-in also appear, but you can also define your own event categories, see User-defined Categories.</p> <p>Important: If you change the event categories in a Corporate system, ensure that the existing access control rules still work.</p>
User-defined Categories	<p>Allows you to create, modify or delete user-defined event categories.</p> <p>You can create event categories when the built-in categories do not meet your requirements, for example, in connection with defining triggering events for access control actions.</p> <p>The categories are global for all integration systems added to the XProtect system. They allow setting up cross-system handling, for example on alarm definitions.</p> <p>If you delete a user-defined event category, you receive a warning if it is used by any integration. If you delete it anyway, all configurations made with this category, for example access control actions, do not work anymore.</p>



Access Request Notification tab (Access Control)

You can specify access request notifications that appear on the XProtect Smart Client screen when a given event occurs.

Name	Description
Name	Enter a name for the access request notification.
Add Access Request Notification	<p>Click to add and define access request notifications.</p> <p>To delete a notification, click X on the right side.</p> <p>If an XProtect Smart Client logs into a parent site in a Milestone Federated Architecture hierarchy, access request notifications from the child sites also appear in XProtect Smart Client.</p>
Access request notification details	<p>Specify which cameras, microphones or speakers that appear in the access request notifications when a given event occurs. Also specify the sound to alert the user when the notification pops up.</p>
Add command	<p>Select which commands that should be available as buttons in the access request notification dialogs in the XProtect Smart Client.</p> <p>Related access request commands:</p> <ul style="list-style-type: none">▶ Enables all commands related to access request operations available on the source unit. For example Open door. <p>All related commands:</p> <ul style="list-style-type: none">▶ Enables all commands on the source unit. <p>Access control command:</p> <ul style="list-style-type: none">▶ Enables a selected access control command. <p>System command:</p> <ul style="list-style-type: none">▶ Enables a command predefined in the XProtect system. <p>To delete a command, click X on the right side.</p>

Cardholders tab (Access Control)

Use the **Cardholders** tab to review information about cardholders in the access control system.



Name	Description
Search cardholder	Type the characters of a cardholder name and it appears in the list, if it exists.
Name	Lists the names of the cardholders retrieved from the access control system.
Type	Lists the type of cardholder, for example: <ul style="list-style-type: none">▶ Employee▶ Guard▶ Guest

If your access control system supports adding/deleting pictures in the XProtect system, you can add pictures to the cardholders. This is useful if your access control system does not include pictures of the cardholders.

Name	Description
Select picture	<p>Specify the path to a file with a picture of the cardholder. This button is not visible if the access control system manages the pictures.</p> <p>Allowed file-formats are .bmp, .png, and .jpg.</p> <p>Pictures are resized to maximize the view.</p> <p>Milestone recommends that you use a quadratic picture.</p>
Delete picture	Click to delete the picture. If the access control system had a picture, then this picture is shown after deletion.

XProtect LPR

LPR system overview

About XProtect LPR

XProtect LPR offers video-based content analysis (VCA) and recognition of vehicle license plates that interacts with your surveillance system and your XProtect Smart Client.

To read the characters on a plate, XProtect LPR uses optical character recognition on images aided by specialized camera settings.

You can combine LPR (license plate recognition) with other surveillance features such as recording and event-based activation of outputs.

Examples of events in XProtect LPR:

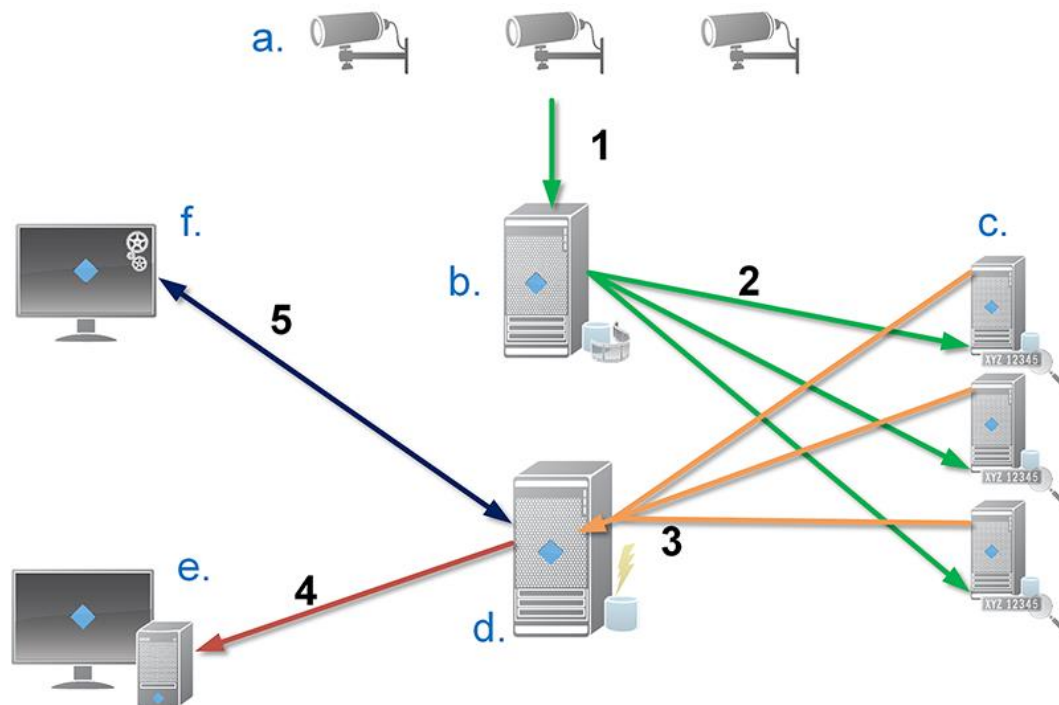


- Trigger surveillance system recordings in a particular quality.
- Activate alarms.
- Match against positive/negative license plate match lists.
- Open gates.
- Switch on lights.
- Push video of incidents to computer screens of particular security staff members.
- Send mobile phone text messages.

With an event, you can activate alarms in XProtect Smart Client.

LPR system architecture

Basic data flow:



1. LPR cameras (a) send video to the recording server (b).
2. The recording server sends video to the LPR servers (c) to recognize license plates by comparing them with the license plate characteristics in the installed country modules.
3. LPR servers send recognitions to the event server (d) to match with the license plate match lists.
4. The event server sends events and alarms to XProtect Smart Client (e) when there is a match.
5. The system administrator manages the entire LPR configuration, for example, setting up events, alarms, and lists from the Management Client (f).

LPR server: The LPR server handles LPR video recorded by your surveillance system. It analyzes the video and sends information to the event server that uses it for triggering the defined events and



alarms. Milestone recommends that you install the LPR server on a computer especially allocated for this purpose.

LPR camera: The LPR camera captures video as any other camera, but some cameras are dedicated for LPR use. The better suited camera you use, the more successful recognitions you will get.

Country module: A country module is a set of rules that defines license plates of a certain type and form as belonging to a certain country or region. It dictates plate and character specifics such as color, height, spacing, and similar, which is used during the recognition process.

License plate match list: A license plate match list is a user-defined list that you create. License plate match lists are collections of license plates that you want your system to treat in a special way. Once you have specified a list, you can set up events to recognize license plates on these lists and in this way trigger events and alarms.

Compatibility

XProtect LPR 2015 is compatible with the version 2014 SP3 or newer of:

- XProtect Corporate
- XProtect Expert
- XProtect Enterprise
- XProtect Professional
- XProtect Express
- Milestone HUSKY M30
- Milestone HUSKY M50.

Minimum system requirements

For information about the minimum system requirements for the various components of your system, go to the Milestone website <http://www.milestonesys.com/SystemRequirements>.

Milestone recommends that you install the LPR server on a computer especially allocated for this purpose.

LPR licenses

XProtect LPR requires the following LPR-related licenses:

- An **XProtect LPR Base License** that covers an unlimited number of LPR servers.
- An **XProtect LPR Device License** per LPR camera.
- An **XProtect LPR Country Module License** for each country, state or region you need in your LPR solution. **One** Country Module license is included with the XProtect LPR Base



License. All country modules are automatically installed when you install your XProtect LPR product. However, the installed modules are by default disabled and you must enable the modules (see "Country modules tab" on page 313) that you want to use. You can only enable as many country modules as you have country module licenses for.

Example: You have an XProtect LPR Country Module license that includes five country modules. You have installed 10 country modules. Once you have selected five country modules, you cannot select any more. You must clear some of your selections before you can select other modules.

To find information about the current status of your licenses, see View LPR server information (on page 303).

To buy additional LPR licenses or country modules, contact your vendor, or go to the Milestone website <http://www.milestonesys.com/SystemRequirements>.

About preparing cameras for LPR

LPR differs from other kinds of video surveillance. Normally, you choose cameras based on their ability to provide the best possible images for viewing by the human eye. When you choose cameras for LPR, only the area where you expect to detect license plates is important. The more clear and consistent you capture an image in that small area, the higher recognition rate you will get.

This section helps you to prepare cameras for license plate recognition, but it also introduces you to important theories about cameras and lenses that are crucial to understand in order to get optimal images.

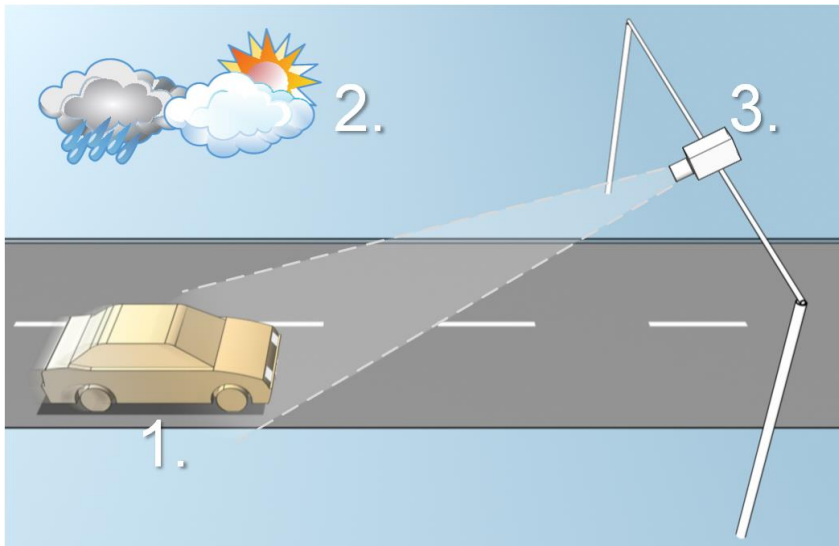


Illustration of an LPR solution

Factors that influence your configuration of LPR:



- | 1. Vehicle | 2. Physical surroundings | 3. Camera |
|---------------------------|--------------------------|-----------------|
| ▶ Speed | ▶ Lightning conditions | ▶ Exposure |
| ▶ Plate size and position | ▶ Weather | ▶ Field of view |
| | | ▶ Shutter speed |
| | | ▶ Resolution |
| | | ▶ Positioning |

It is important to take these factors into consideration as they have a critical influence on successful license plate recognition. You must mount cameras and configure XProtect LPR in a way that matches each specific environment. You cannot expect the product to run successfully without configuration. A camera used for LPR has a CPU consumption that is about five times higher than a normal camera. If a camera has not been set up correctly, it will highly affect the level of successful recognitions and the CPU performance.

Read the following sections to learn about the factors that influence your LPR solution:

Positioning the camera (on page 290)

Camera angles (on page 291)

Plate width recommendations (on page 293)

Image resolution (on page 294)

Understanding camera exposure (on page 296)

Physical surroundings (on page 298)

Lens and shutter speed (on page 299)

Contrast (on page 301)

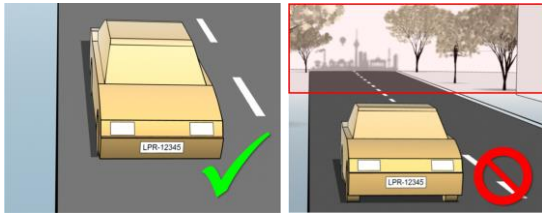
Unwanted camera features (on page 301)

Positioning the camera

When you mount cameras for LPR use, it is important to get a good, clear view of the area of interest so the plate can be detected consistently. This ensures the best possible performance and low risk of false detection:

- The area should cover **only** the part of the image where the license plate is visible as the vehicle moves in and out of the image.
- Avoid to have objects that block the view path of the camera, such as pillars, barriers, fences, gates.
- Avoid irrelevant moving objects such as people, trees, or traffic in

If too many irrelevant items are included, they will interfere with the detection, and the LPR server will use CPU resources on analyzing irrelevant items instead of license plates.

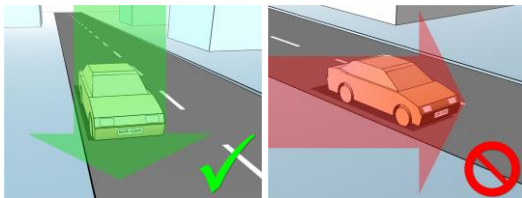


Left image shows a correct mounting without interference in the field of view. Right image shows an incorrect mounting. The camera is mounted too low and with too much background 'noise' in the view.

To help you obtain a clear and undisturbed view, you can:

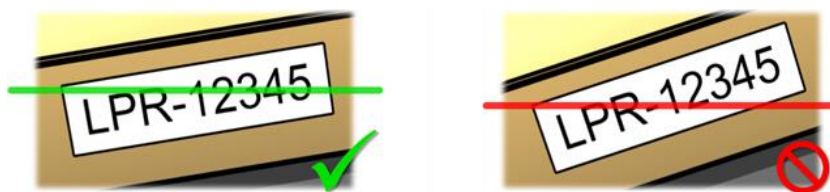
- Mount the camera as close as possible to the area of interest.
- Angle your camera.
- Zoom. If you zoom, always use the camera's optical zoom.

Mount the camera so the license plate appears from the top of the image (or bottom if traffic is driving away from the camera) instead of from the right or left side. In this way you make sure that the recognition process of a license plate only starts when the whole plate is in the view:



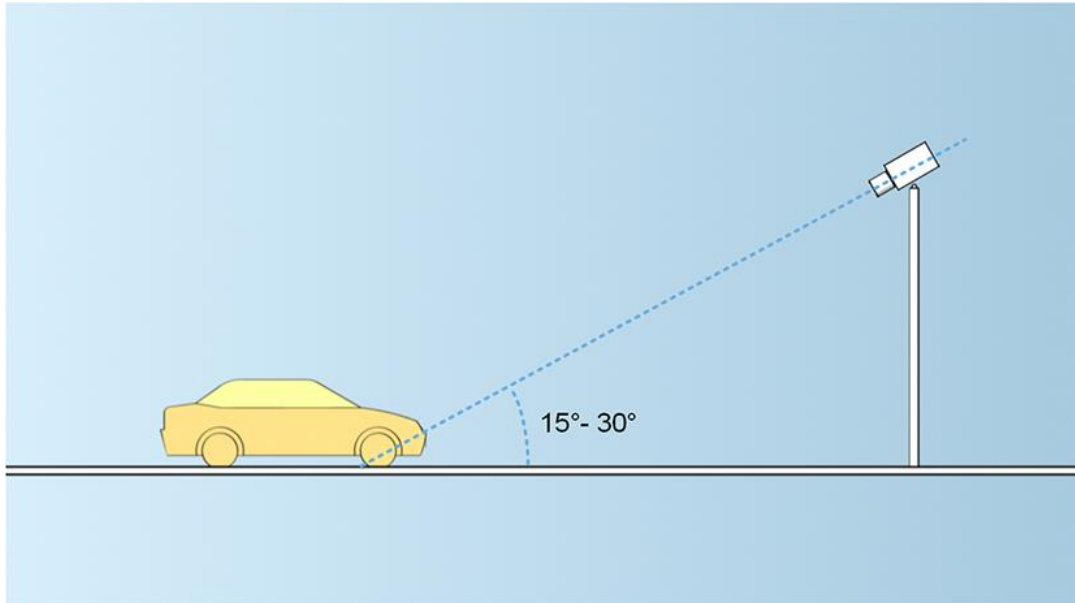
Camera angles

- **Single-line rule:** Mount the camera so that you can draw a horizontal line that crosses both the left and right edge of the license plate in the captured images. See the illustrations below for correct and incorrect angles for recognition.





- **Vertical angle:** The recommended vertical view angle of a camera used for LPR is between 15° - 30° .



- **Horizontal angle:** The recommended maximum horizontal view angle of a camera used for LPR is between 15° - 25° .

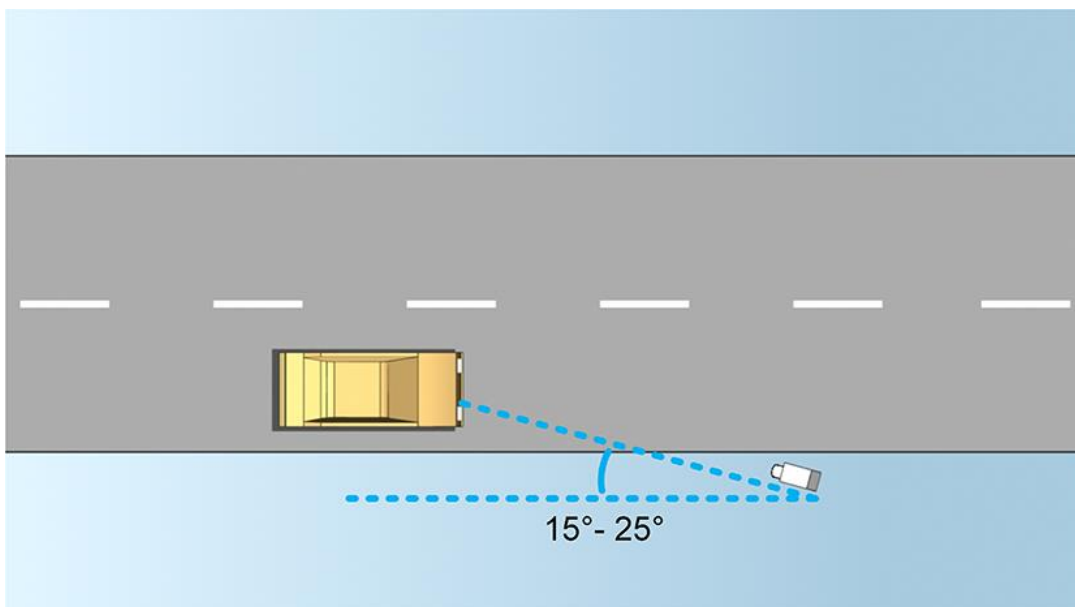
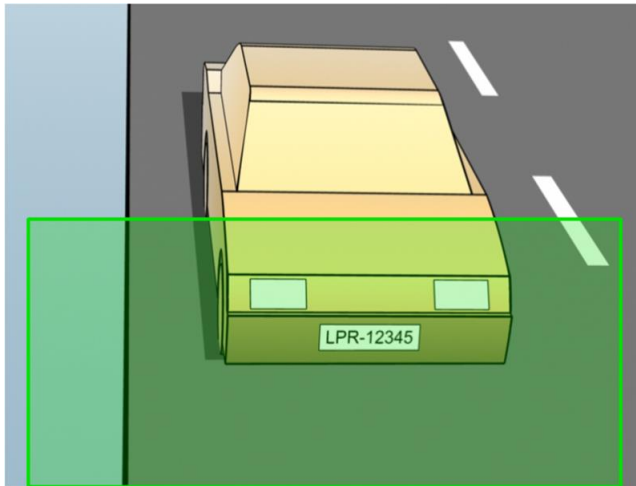




Plate width recommendations

Mount the camera so that the ideal snapshot of the license plate is captured when the license plate is in the center or lower half of the image:



Take a snapshot and make sure that the requirements to stroke width and plate width as described below are fulfilled. Use a standard graphics editor to measure the amount of pixels. When you start the process of reaching the minimum plate width, begin with a low resolution on the camera, and then work your way up in a higher resolution until you have the required plate width.

Stroke width

The term *pixels per stroke* is used to define a minimum requirement for fonts that should be recognized. The following illustration outlines what is meant by *stroke*:



Because the thickness of strokes depends on country and plate style, measurements like pixels/cm or pixels/inch are not used.

The resolution for best LPR performance should be at least 2.7 pixels/stroke.

Plate width

Plate type	Plate width	Setup	Minimum plate width (pixels)
Single line US plates	▶ plate width 12 inches ▶ stroke width around ¼ inches	vehicles stopped; no interlacing	130
		vehicles are moving; interlaced	215



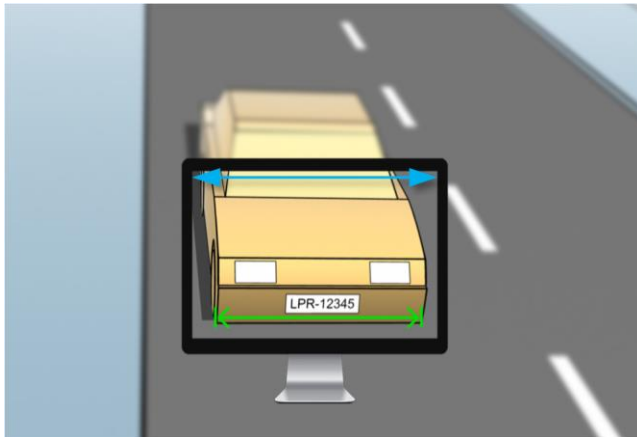
Plate type	Plate width	Setup	Minimum plate width (pixels)
Single line European plates	▶ plate width 52 cm ▶ stroke width around 1 cm	vehicles stopped; no interlacing	170
		vehicles are moving; interlaced	280

If vehicles are moving when recorded, and an interlaced camera is used, only a half of the image can be used (only the even lines) for recognition compared with a camera configured for stopped vehicles and no interlacing. This means that the resolution requirements are almost double as high.

Image resolution

Image quality and resolution is important for a successful license plate recognition. On the other hand, if the video resolution is too high, the CPU might be overloaded with the risk of skipped or faulty detections. The lower you can set the acceptable resolution, the better CPU-performance and the higher detection rate you get.

In this example we explain how to do a simple image quality calculation and find a suitable resolution for LPR. The calculation is based on the width of a car.



Example of a capture where we want to calculate a suitable resolution.

We estimate that the horizontal width is 200 cm/78 inches, as we assume the width of a standard car is 177 cm/70 inches, and besides that we add ~10% for the extra space. You can also do a physical measuring of the area of interest if you need to know the exact width.

The recommended resolution of the stroke thickness is 2.7 pixels/stroke, and the physical stroke thickness is 1 cm for a European plate and 0.27 inches for a US plate. This gives the following calculation:

Calculation for European plates in cm:

$$200 \times 2.7 \div 1 = 540 \text{ pixels}$$

Recommended resolution = VGA (640x480)



Calculation for US plates in inches:

$$78 \times 2.7 \div 0.27 = 780 \text{ pixels}$$

Recommended resolution = SVGA (800×600)

Because US plates use a font with a narrow stroke, a higher resolution is needed than for European plates.

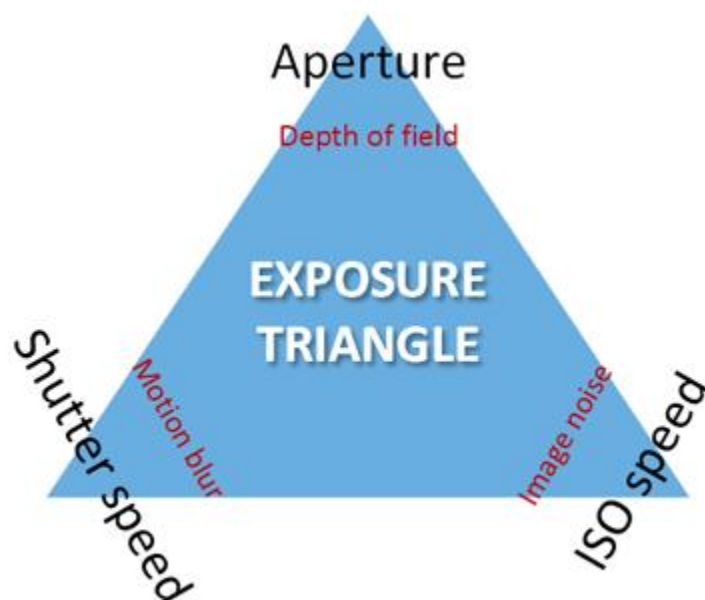
Common video resolutions

Name	Pixels (W×H)
QCIF	176×120
CIF	352×240
2CIF	704×240
VGA	640×480
4CIF	704×480
D1	720×576
SVGA	800×600
XGA	1024×768
720p	1280×1024



Understanding camera exposure

Camera exposure determines how light/dark and sharp/blurry an image appears when it has been captured. This is determined by three camera settings: aperture, shutter speed, and ISO speed. Understanding their use and interdependency can help you to set up the camera correctly for LPR.



Exposure triangle

You can use different combinations of the three settings to achieve the same exposure. The key is to know which trade-offs to make, since each setting also influences the other image settings:

Camera settings	Controls...	Affects...
Aperture	The adjustable opening that limits the amount of light to enter the camera	Depth of field
Shutter speed	The duration of the exposure	Motion blur
ISO speed	The sensitivity of the camera's sensor to a given amount of light	Image noise

The next sections describe how each setting is specified, what it looks like, and how a given camera exposure mode affects this combination:

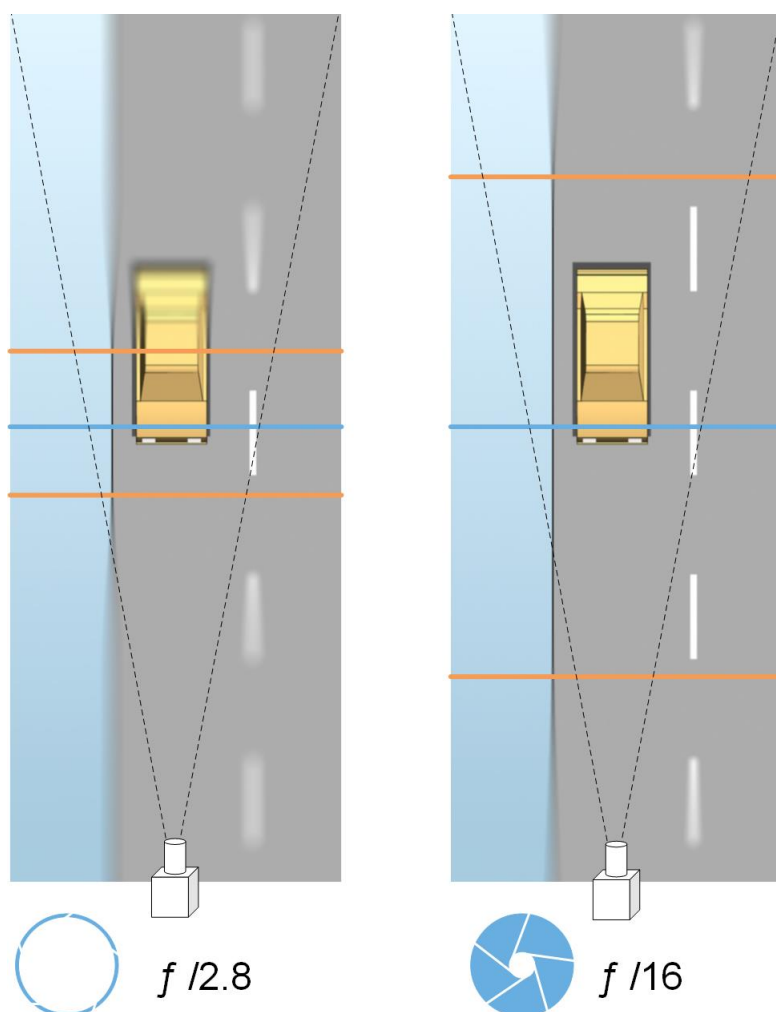
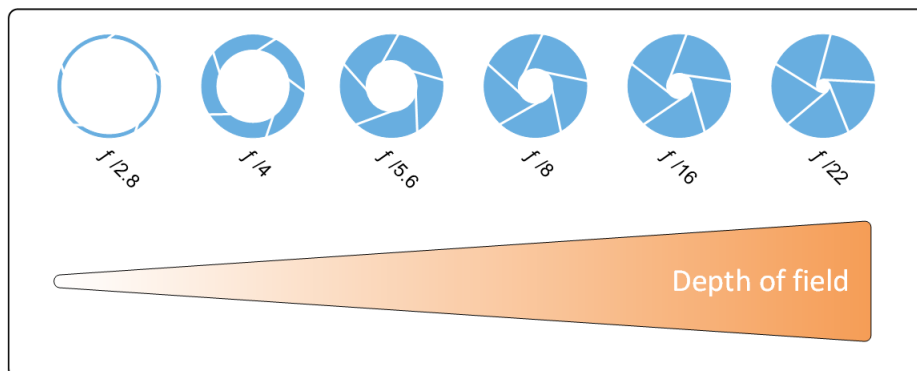
Aperture settings

The aperture setting controls the amount of light that enters your camera from the lens. It is specified in terms of an f-stop value, which can at times be counterintuitive, because the area of the opening increases as the f-stop decreases.

Low f-stop value/wide aperture = shallow depth of field



High f-stop value/narrow aperture = large depth of field



The example illustrates how the depth of field is affected by the f-stop value. The blue line indicates the focus point.

A high f-stop value makes it possible to have a longer distance where the license plate is in focus. Good light conditions are important for sufficient exposure. If lighting conditions are insufficient, the exposure time needs to be longer, which again increases the risk of getting blurry images.



A low f-stop value reduces the focus area and thereby the area used for recognition, but is suitable for conditions with low light. If it is possible to ensure that vehicles are passing the focus area at a low speed, a low f-stop value is suitable for a consistent recognition.

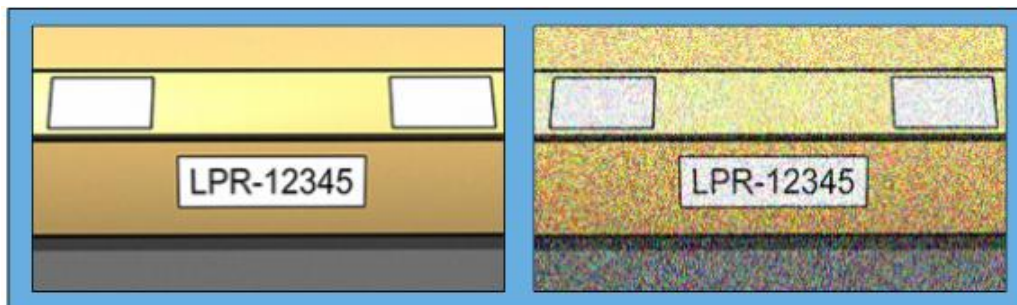
Shutter speed

A camera's shutter determines when the camera sensor is open or closed for incoming light from the camera lens. The shutter speed refers to the duration when the shutter is open and light can enter the camera. Shutter speed and exposure time refer to the same concept, and a faster shutter speed means a shorter exposure time.

Motion blur is undesired for license plate recognition and surveillance. In many occasions vehicles are in motion while license plates are detected which makes a correct shutter speed an important factor. The rule of thumb is to keep the shutter speed high enough to avoid motion blur, but not too high as this may cause under-exposed images depending on light and aperture.

ISO speed

The ISO speed determines how sensitive the camera is to incoming light. Similar to shutter speed, it also correlates 1:1 with how much the exposure increases or decreases. However, unlike aperture and shutter speed, a lower ISO speed is in general desirable, since higher ISO speeds dramatically increase image noise. As a result, ISO speed is usually only increased from its minimum value if the desired image quality is not obtainable by modifying the aperture and shutter speed settings solely.



Example of low and high ISO speed images. High ISO speed on the right image affects the level of image noise negatively.

Common ISO speeds include 100, 200, 400 and 800, although many cameras also permit lower or higher values. With digital single-lens reflex (DSLR) cameras, a range of 50-800 (or higher) is often acceptable.

Physical surroundings

When you mount and use cameras for LPR, note the following factors related to the surroundings:

- **Much light:** Too much light in the surroundings can lead to overexposure or smear.
 - **Overexposure** is when images are exposed to too much light, resulting in a burnt-out and overly white appearance. To avoid overexposure, Milestone recommends that you use a camera with a high dynamic range and/or use an auto-iris lens. **Iris** is the adjustable aperture. For that reason, iris has a significant effect on the exposure of images.



- **Smear** is an effect that leads to unwanted light vertical lines in images. It is often caused by slight imperfections in the cameras' charge-coupled device (CCD) imagers. The CCS imagers are the sensors used to digitally create the images.



License plate image with smear because of overexposure

- **Little light:** Too little light in the surroundings or too little external lighting can lead to underexposure.
 - **Underexposure** is when images are exposed to too little light, resulting in a dark image with hardly any contrast (on page 301). When auto-gain (see "Unwanted camera features" on page 301) cannot be disabled or when you are not able to configure a maximum allowed shutter time (see "Lens and shutter speed" on page 299) for capturing moving vehicles, too little light will initially lead to gain noise and motion blur in the images, and ultimately to underexposure. To avoid underexposure, use sufficient external lighting and/or use a camera that has sufficient sensitivity in low-light surroundings without using gain.
- **Infrared:** Another way to overcome difficult lighting conditions is to use artificial infrared lighting combined with an infrared-sensitive camera with an infrared pass filter. Retro-reflective license plates are particularly suitable for use with infrared lighting.
 - **Retro-reflectivity** is achieved by covering surfaces with a special reflective material which sends a large portion of the light from a light source straight back along the path it came from. Retro-reflective objects appear to shine much more brightly than other objects. This means that at night they can be seen clearly from considerable distances. Retro-reflectivity is frequently used for road signs, and is also used for different types of license plates.
- **Weather:** Snow or very bright sunlight may for example require special configuration of cameras.
- **Plate condition:** Vehicles may have damaged or dirty license plates. Sometimes this is done deliberately in an attempt to avoid recognition.

Lens and shutter speed

When configuring cameras' lenses and shutter speeds for LPR, note the following:

- **Focus:** Always make sure the license plate is in focus.



- **Auto-iris:** If using an auto-iris lens, always set the focus with the aperture as open as possible. In order to make the aperture open, you can use neutral density (ND) filters or—if the camera supports manual configuration of the shutter time—the shutter time can be set to a very short time.
 - **Neutral Density (ND)** filters or gray filters basically reduce the amount of light coming into a camera. They work as "sunglasses" for the camera. ND filters affect the exposure of images (see "Understanding camera exposure" on page 296).
- **Infrared:** If using an infrared light source, focus may change when switching between visible light and infrared light. You can avoid the change in focus by using an infrared compensated lens, or by using an infrared pass filter. Note that if you use an infrared pass filter, an infrared light source is required—also during daytime.
- **Vehicle speed:** When vehicles are moving, cameras' shutter time should be short enough to avoid motion blur. A formula for calculating the longest suitable shutter time is:
 - **Vehicle speed in km/h:** Shutter time in seconds = 1 second / (11 × max vehicle speed in kilometers per hour)
 - **Vehicle speed in mph:** Shutter time in seconds = 1 second / (18 × max vehicle speed in miles per hour)

where / denotes "divided by" and × denotes "multiplied by."

The following table provides guidelines for recommended camera shutter speeds for different vehicle speeds:

Shutter time in seconds	Max. vehicle speed in kilometers per hour	Max. vehicle speed in miles per hour
1/50	4	2
1/100	9	5
1/200	18	11
1/250	22	13
1/500	45	27
1/750	68	41
1/1000	90	55
1/1500	136	83
1/2000	181	111
1/3000	272	166
1/4000	363	222



Contrast

When you determine the right contrast for your LPR camera, consider the difference in gray value (when images are converted to 8-bit grayscale) between the license plate's characters and the license plate's background color:



Good contrast



Acceptable contrast; recognition is still possible

Pixels in an 8-bit grayscale image can have color values ranging from 0 to 255, where grayscale value 0 is absolute black and 255 is absolute white. When you convert your input image to an 8-bit grayscale image, the minimum pixel value difference between a pixel in the text and a pixel in the background should be at least 15.

Note that noise in the image (see "Unwanted camera features" on page 301), the use of compression (see "Unwanted camera features" on page 301), the light conditions, and similar can make it difficult to determine the colors of a license plate's characters and background.

Unwanted camera features

When you configure cameras for LPR, note the following:

- **Automatic gain adjustment:** One of the most common types of image interference caused by cameras is gain noise.
 - **Gain** is basically the way that a camera captures a picture of a scene and distributes light into it. If light is not distributed optimally in the image, the result is gain noise.

Controlling gain requires that complex algorithms are applied, and many cameras have features for automatically adjusting gain. Unfortunately, such features are rarely helpful in connection with LPR. Milestone recommends that you configure your cameras' auto-gain functionality to be as low as possible. Alternatively, disable the cameras's auto-gain functionality.



License plate image with gain noise

In dark surroundings, you can avoid gain noise by installing sufficient external lighting.

- **Automatic enhancement:** Some cameras use contour, edge or contrast enhancement algorithms to make images look better to the human eye. Such algorithms can interfere with the algorithms used in the LPR process. Milestone recommends that you disable the cameras' contour, edge and contrast enhancement algorithms whenever possible.



- **Automatic compression:** High compression rates can have a negative influence on the quality of license plate images. When a high compression rate is used, more resolution (see "Plate width recommendations" on page 293) is required in order to achieve optimal LPR performance. If a low JPEG compression is used, the negative impact on LPR is very low, as long as the images are saved with a JPEG quality level of 80% or above, and images have normal resolution, contrast and focus as well as a low noise level.



Left: License plate image saved with a JPEG quality level of 80% (i.e. low compression); acceptable

Right: License plate image saved with a JPEG quality level of 50% (i.e. high compression); unacceptable

LPR installation

Install XProtect LPR

To run XProtect LPR you must install:

- At least one LPR server.
- The LPR plug-in on all computers that run the Management Client and the event server.

In distributed systems, Milestone recommends that you do not install the LPR server on the same computer as your management server or recording servers.

Start installation:

1. Go to the download page on the Milestone website <http://www.milestonesys.com/downloads>.
2. Download the two installers:
 - *Milestone XProtect LPR Plug-in* installer to all computers that run the Management Client and the event server.
 - *Milestone XProtect LPR Server* installer to all computers allocated for this purpose. You can also create virtual servers for LPR on one computer.
3. First, run all the *Milestone XProtect LPR Plug-in* installers.
4. Then, run the *Milestone XProtect LPR Server* installer(s).

During installation, specify the IP address or hostname of the management server for XProtect Advanced VMS products or the image server for XProtect Professional VMS products



including the domain user name and password of a user account that has administrator rights to the surveillance system.

5. Launch the Management Client.

In the **Site Navigation pane**, your Management Client automatically lists the installed LPR servers in the **LPR Servers** list.

6. Make sure that you have the necessary licenses (see "LPR licenses" on page 288).
7. All country modules are automatically installed when you install your XProtect LPR product. However, the installed modules are by default disabled and you must enable the modules (see "Country modules tab" on page 313) that you want to use. You can only enable as many country modules as you have country module licenses for.

You cannot add LPR servers from the Management Client.

If you need to install more LPR servers after the initial installation, run the *Milestone XProtect LPR Server* installer on these servers.

Upgrade XProtect LPR

To upgrade XProtect LPR, you follow the same steps as for installation (see "Install XProtect LPR" on page 302).

If you upgrade from XProtect LPR 1.0 to XProtect LPR 2015, some recognition settings are not compatible with those from the previous configuration. To apply the new settings, you must save your configuration. The settings that previously allowed you to flip, rotate and invert the colors of the video have been removed. If you still need these functions, you must change the settings on the cameras themselves.

LPR configuration

View LPR server information

To check the state of your LPR servers:

1. In the **Site Navigation pane**, expand **Servers** and select **LPR servers**. Go to the Overview pane.

The **LPR server information** window opens with a summary of the server status:

- Name
- Host name
- Status

2. Select the relevant LPR server and review all details for this server (see "LPR server information properties" on page 304).



LPR server information properties

Field	Description
Name	Here you can change the name of the LPR server.
Host name	Shows the LPR server host name. The first part of the name of the LPR server consists of the name of the host computer for your LPR server installation. Example: <i>MYHOST.domainname.country</i> .
Status	Shows the status of the LPR server. If the server has just been added, the status is: <ul style="list-style-type: none">▶ <i>No LPR cameras configured.</i> If the system is running without problems, the status is: <ul style="list-style-type: none">▶ <i>All LPR cameras are running.</i> Alternatively the system returns: <ul style="list-style-type: none">▶ <i>Service not responding.</i>▶ <i>Not connected to surveillance system.</i>▶ <i>Service not running.</i>▶ <i>Event Server not connected.</i>▶ <i>Unknown error.</i>▶ <i>X of Y LPR cameras running.</i>
Service up time	Shows the up time since the LPR server was last down and the LPR server service started.
Computer CPU usage	Shows the current CPU usage on the entire computer with the LPR server(s) installed.
Memory available	Shows how much memory is available on the LPR server.
Recognized license plates	Shows the number of license plates that the LPR server has recognized in this session.
LPR cameras	Shows a list of enabled LPR cameras that run on the LPR server and their status.
LPR cameras available	Based on your license, this number shows how many additional LPR cameras you are allowed to add and use on all your LPR servers in total.
Country modules available	Based on your license, this number shows how many additional country modules you are allowed to use on all your LPR servers in total. It also lists the number of country modules already in use.



Configuring cameras for LPR

Prerequisites in the Management Client

Once cameras have been mounted and added in the Management Client, adjust each camera's settings so that they match the requirements for LPR. You adjust camera settings on the properties tabs for each camera device.

For the relevant cameras Milestone recommends to:

- Set the video codec to JPEG.

Note that if you use H.264 codec, only key frames are supported. This is usually only one frame per second which is not enough for LPR. For higher frame rates, always use a JPEG codec.

- Specify a frame rate of four frames per second.
- Avoid compression, so set a fine quality.
- If possible, specify a resolution below one megapixel.
- If possible, keep automatic sharpness at a low level.

To learn about LPR fundamentals, make yourself familiar with the information in About preparing cameras for LPR (on page 289).

About snapshots

The system uses snapshots to optimize the configuration automatically and to visualize the effect of the recognition settings as they are applied.

You need to provide at least one valid snapshot in order to complete the initial configuration of a camera.

As a guideline, capture snapshots of vehicles in the real physical surroundings and conditions, in which you want to be able to recognize license plates.

The list below illustrates examples of the situations that you should consider when you capture and select snapshots. Not all may be applicable for your surroundings.

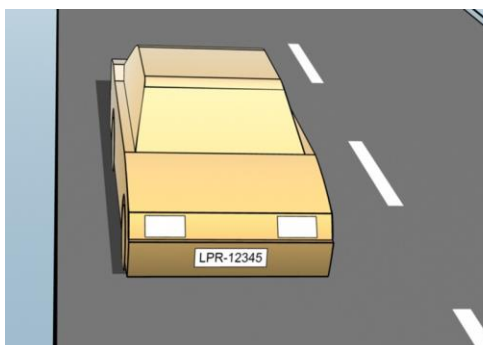
Milestone recommends that you select minimum 5-10 snapshots that represent typical conditions of:



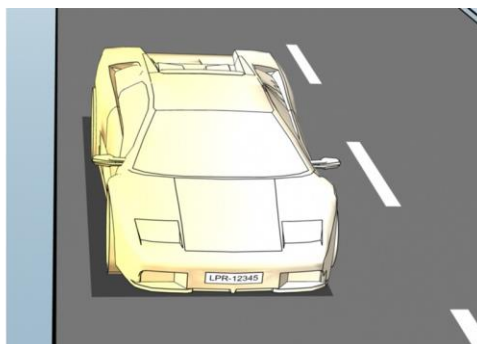
- **The weather; for example sunlight and rain**



- **The light; for example daylight and nighttime**

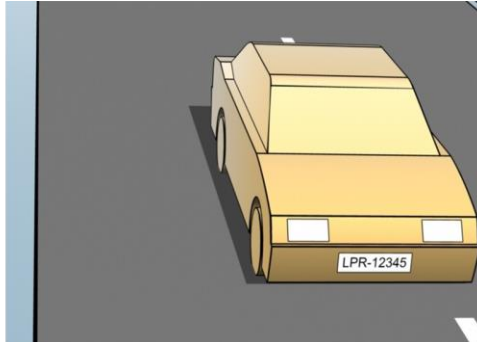
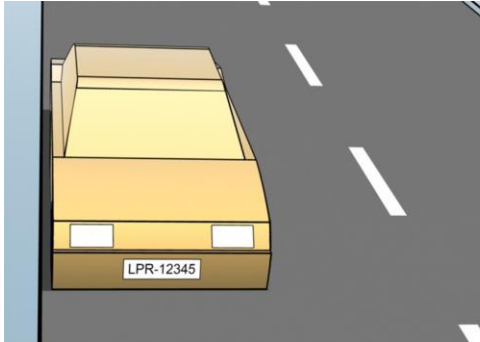


- **Vehicle types; to define the top and bottom of the recognition area**

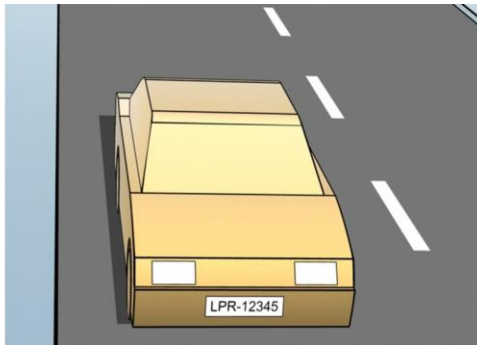
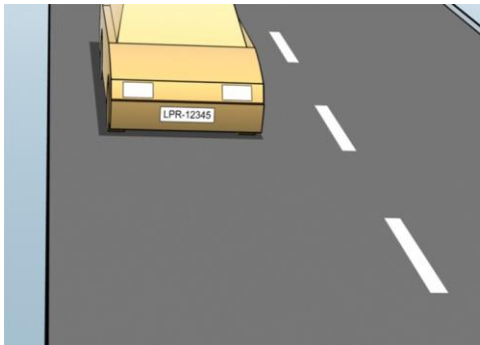




- **Position in the lane; to define the left and right of the recognition area**



- **Distance to the car; to define the area where LPR analyzes license plates**



Add LPR camera

To configure cameras for LPR, you initially run the **Add LPR camera** wizard. The wizard takes you through the main configuration steps and automatically optimizes the configuration.

To run the wizard:

1. In the **Site Navigation pane**, expand **Servers**, expand **LPR servers**, and select **LPR camera**.
2. Go to the Overview pane. Right-click **LPR camera**.
3. From the menu that appears, select **Add LPR camera** and follow the instructions in the wizard:
 - Select the camera you want to configure for LPR.
 - Select which country modules you want to use with your LPR camera (see "Country modules tab" on page 313).
 - Select snapshots to use for validating the configuration (see "About snapshots" on page 305).



- Validate the result of the snapshot analysis (see "Validate configuration" on page 315).
 - Select which license plate match lists to use (see "About license plate match lists" on page 316). Choose the default selection, if you have not yet created any lists.
4. On the last page, click **Close**.
- The LPR camera appears in the Management Client and based on your selections, the system has optimized the recognition settings for the camera (see "Recognition settings tab" on page 309).
5. Select the camera you have added and review its settings. You only need to change the configuration if the system does not recognize license plates as well as expected.
6. In the **Recognition settings** tab, click Validate configuration (on page 315).

Adjust settings for your LPR camera

The system automatically optimized the configuration of your LPR camera, when you added the LPR camera with the **Add LPR camera** wizard. If you want to make changes to the initial configuration, you can:

- Change the name of the server or change server (see "Info tab" on page 308).
- Adjust and validate the recognition settings (see "Recognition settings tab" on page 309).
- Add more license plate match lists (see "Match lists tab" on page 312).
- Enable additional country modules (see "Country modules tab" on page 313).

Info tab

This tab provides information about the selected camera:

Name	Description
Enable	LPR cameras are by default enabled after the initial configuration. Disable any camera that is not used in connection with LPR. Disabling an LPR camera does not stop it from performing normal recording in the surveillance system.
Camera	Shows the name of the selected camera as it appears in the XProtect Management Client and the clients.
Description	Use this field to enter a description (optional).
Change Server	Click to change LPR server. Changing the LPR server can be a good idea if you need to load balance. For example, if the CPU load is too high on an LPR server, Milestone recommends that you move one or more LPR cameras to another LPR server.



Recognition settings tab

Recognition settings are auto-configured and optimized by the system during the initial configuration of your LPR camera, primarily based on the snapshots you have provided.

Action buttons

Use these buttons to update and validate your settings after the initial configuration.

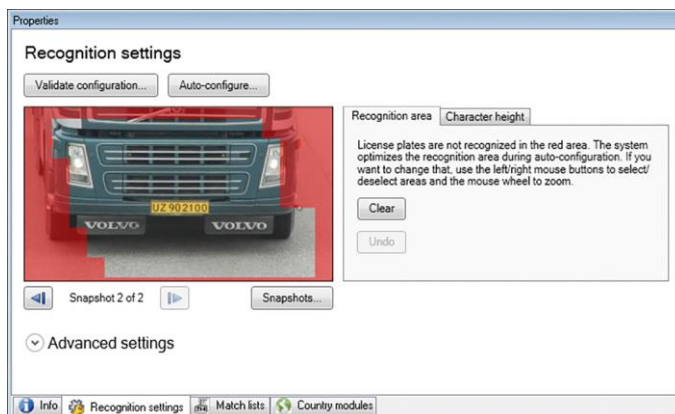
Name	Description
Snapshots	Add or delete snapshots (see "Select snapshots" on page 314).
Validate configuration	Test that license plates are recognized as expected (see "Validate configuration" on page 315).
Auto-configure	Disregard manual changes and optimize settings (see "Auto-configure" on page 316).

Recognition area

The system optimizes the recognition area during auto-configuration, but you can change it manually.

To ensure the best possible performance and low risk of false detection, Milestone recommends that you always select a clearly defined and "well-trimmed" recognition area. The area should cover **only** the part of the image where the license plate is visible as the vehicle moves in and out of the image. Avoid irrelevant moving objects such as people, trees, or traffic in the recognition area (see "Positioning the camera" on page 290).

License plates are not recognized in the red area.



When you specify an area of recognition, you have the following options:

Name	Description
Clear	Click to remove all selections, so no areas are used for LPR. Select new areas.
Undo	Click to revert to your latest saved configuration of the recognition area.



When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 315) to see if the system recognizes license plates as well as expected.

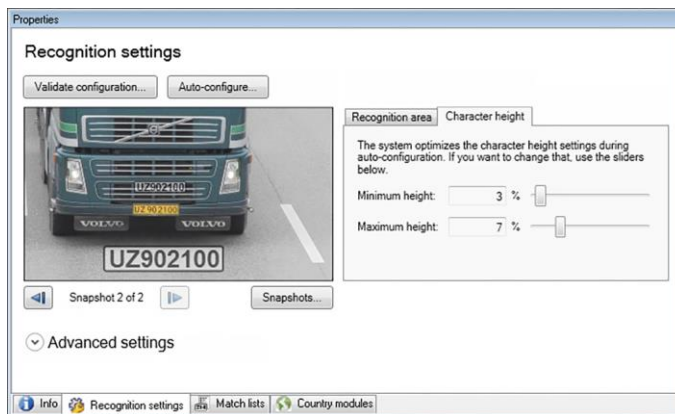
Character height

The system optimizes the character height during auto-configuration, but you can change it manually.

You define the minimum and maximum height of the license plate characters (in percent). Select character heights as close as possible to the height of the characters in the real license plate.

These character settings influence the recognition process as they partly determine the recognition time. As a rule, the larger the difference between the minimum and the maximum character height:

- The more complex the LPR process is.
- The higher the CPU load is.
- The longer you have to wait for the results.



The overlay in the snapshot displays the currently defined character height setting. The overlay grows and shrinks proportionally with the character height settings to the right. For easy comparison, you can drag the overlay on top of the real license plate in the snapshot. If needed, use the mouse wheel to zoom.

Name	Description
Minimum height	Use the sliders to set the minimum character height to be included in a recognition process. The system will not start the recognition process on license plates that contain characters below the specified value.
Maximum height	Use the sliders to set the maximum character height to be included in a recognition process. The system will not start the recognition process on license plates that contain characters above the specified value.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 315) to see if the system recognizes license plates as well as expected.



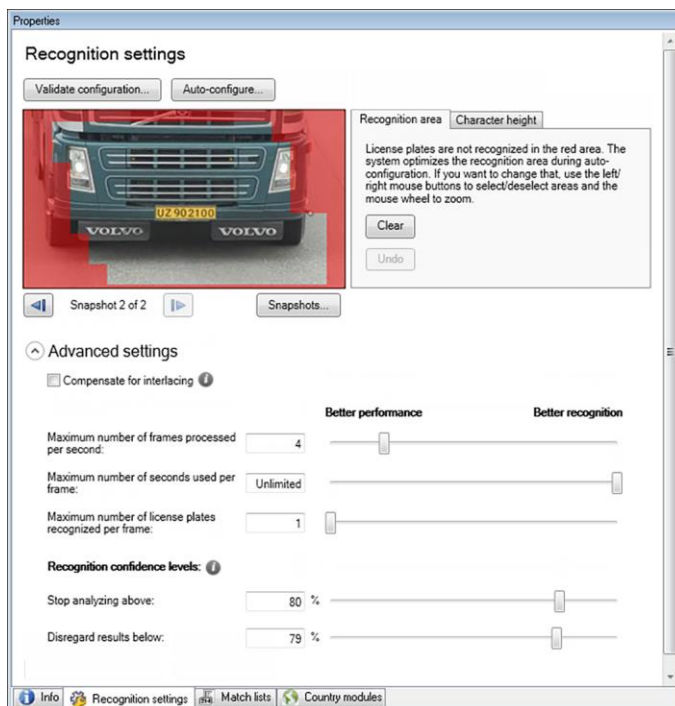
Advanced settings

The system optimizes the advanced settings during auto-configuration, but you can change them manually.

The recognition process can be divided into two steps: finding the plate(s) and recognizing the characters on the plates. The advanced settings allow you to define a trade-off between processing speed and recognition quality.

The general rule is that high recognition quality:

- needs the highest computational effort,
- results in higher CPU load,
- requires more time to return results.



By adjusting the advanced settings, you define the trade-off. The recognition process stops if any of the stop criteria are met and returns the license plate it recognized at that point.



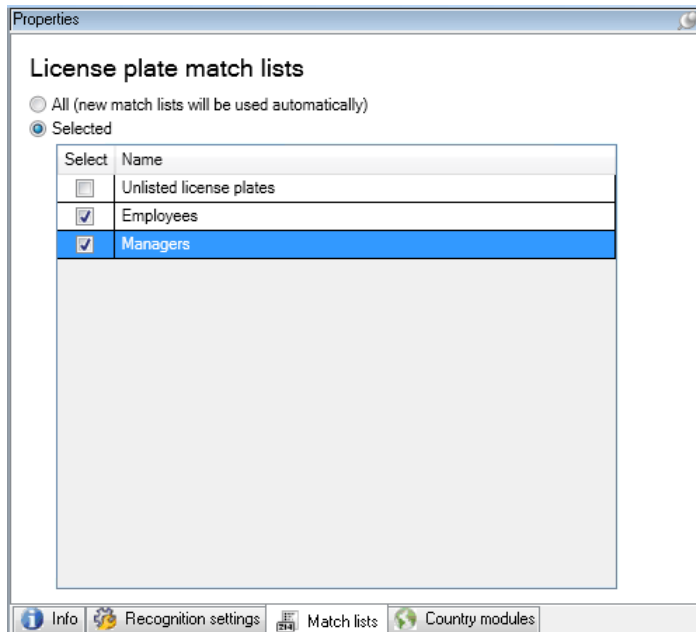
Name	Description
Compensate for interlacing	In case your LPR camera sends interlaced video and you observe combing effects in the de-interlaced image in LPR, you can enable this function. This may improve the quality of the image and thereby your recognition results.
Maximum number of frames processed per second	Specifies a limit to the number of frames that your LPR solution processes per second. If you keep the number of frames low for LPR processes, you can apply a higher frame rate on the camera for recording without adding unnecessary load to the LPR Server. Unlimited means that you have not defined a stop criterion for this setting.
Maximum number of seconds used per frame	Specifies a limit to the number of seconds that your LPR solution is allowed to spend on recognition of one frame. If adjusted, recommended value is 200 ms per frame. Unlimited means that you have not defined a stop criterion for this setting.
Maximum number of license plates recognized per frame	Specifies a limit to the number of recognized license plates returned per frame. Do only change this setting if really needed, for example, if you are detecting multiple lanes with one LPR camera. Unlimited means that you have not defined a stop criterion for this setting.
Stop analyzing above	Specifies a minimum confidence level (in percent). The recognition process continues until the system can return a license plate reading with a confidence level equal to or higher than the specified value.
Disregard results below	The system rejects license plate readings with a confidence level equal to or lower than the specified value. As a rule, the smaller you keep the difference between the Stop analyzing above and Disregard results below values, the lower is the CPU load and the system returns recognition results faster.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 315) to see if the system recognizes license plates as well as expected.

Match lists tab



On this tab you select which license plate match list(s) you want a specific LPR camera to match license plates against. You can create as many lists as you need (see "Add new license plate match lists" on page 317).



Name	Description
All	License plates are matched against all available and future lists.
Selected	License plates are matched against the selected lists only. Select one or more from the available lists.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 315) to see if the system recognizes license plates as well as expected.

Country modules tab

Here you select the country modules that you want to use with a specific LPR camera. The list that you can select from, depends on which modules you have installed and your licenses (see "LPR licenses" on page 288).

A country module is a set of rules that defines license plates of a certain type and form belonging to a certain country, state or region.



Already licensed modules appear with a check mark in the **Licensed** column. If the country module you are looking for is not on your list, contact your vendor.

Properties

Country modules

Select	Country module	Country code	Licensed
<input type="checkbox"/>	Croatia	HR	<input type="checkbox"/>
<input type="checkbox"/>	Czech Republic	CZ	<input type="checkbox"/>
<input type="checkbox"/>	Democratic Republic of Congo	RCB	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Denmark	DK	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ecuador	EC	<input type="checkbox"/>
<input type="checkbox"/>	Egypt	ET	<input type="checkbox"/>
<input type="checkbox"/>	Estonia	EST	<input type="checkbox"/>
<input checked="" type="checkbox"/>	EU	X_EU	<input type="checkbox"/>
<input type="checkbox"/>	Faroe Islands	FO	<input type="checkbox"/>
<input type="checkbox"/>	Finland	FIN	<input type="checkbox"/>
<input type="checkbox"/>	France	F	<input type="checkbox"/>
<input type="checkbox"/>	Generic	X_XX	<input type="checkbox"/>
<input type="checkbox"/>	Germany	D	<input type="checkbox"/>
<input type="checkbox"/>	Ghana	GH	<input type="checkbox"/>
<input type="checkbox"/>	Great Britain	GB	<input type="checkbox"/>
<input type="checkbox"/>	Greece	GR	<input type="checkbox"/>
<input type="checkbox"/>	Guyana	GUY	<input type="checkbox"/>
<input type="checkbox"/>	Honduras	HON	<input type="checkbox"/>
<input type="checkbox"/>	Hong Kong	HK	<input type="checkbox"/>
<input type="checkbox"/>	Hungary	H	<input type="checkbox"/>
<input type="checkbox"/>	Iceland	IS	<input type="checkbox"/>

7 free country module license(s) available.

Selected country modules:
Denmark (DK)
EU (X_EU)

Info Recognition settings Match lists Country modules

Name	Description
Select	Click to select or deselect a country module. The list of selected country modules on the right side updates automatically.
Country Module	Lists the installed country modules.
Country Code	Letters that identify a country module.
Licensed	Shows if a country module is already licensed. You can select a licensed country module for as many cameras as you like.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 315) to see if the system recognizes license plates as well as expected.

Select snapshots



When you configured the LPR initially with the **Add LPR camera** wizard, you also added snapshots (see "About snapshots" on page 305). You can always add additional representative snapshots to improve the optimization of the configuration.

1. Select the relevant camera.
2. In the **Recognition settings** tab, click **Snapshots**.
3. Capture snapshots from live video or import them from an external location. Click **Next**.

The system analyzes the snapshots you have selected for the camera.

4. On the next page, approve or reject each of the snapshots. If the system could not recognize any license plates, click **Previous** to add new snapshots in a better quality. If the system still cannot provide correct recognitions, you probably need to change your configuration. Check that the camera have been mounted and configured correctly (see "About preparing cameras for LPR" on page 289).
5. When you have approved all snapshots, click **Next** and close the wizard.
6. On the **Recognition settings** tab, click **Validate configuration** (on page 315).

Validate configuration

You can validate your current configuration to see if you need to change any settings or provide more snapshots. The validation function informs you about how many license plates your system recognizes, and if they are recognized correctly.

It can help you decide if your confidence level is set correctly and if your system configuration is optimal.

1. Select the relevant camera.
2. From the **Recognition settings** tab, click **Validate configuration**.

Based on the current settings, the system analyzes the snapshots you have selected for the camera and provides a result summary:

- **License plates detected:** The number of recognized license plates, for example, 3 of 3.
- **Average confidence:** The average percent of confidence with which the license plates have been recognized.
- **Average processing time:** The average time it took to analyze a snapshot and return a reading measured in ms.

License plates detected:	2 of 2
Average confidence:	91 %
Average processing time:	112 ms

3. If the current configuration meets your requirements, click **Close**.
4. If you want to investigate the results further, click **Next**, and you can review the results for each snapshot. This helps you to identify the situations that cause problems.



You can validate the configuration as many times as you like and on any LPR camera and with different settings.

Auto-configure

Auto-configuration of the LPR camera overwrites any manual changes you have made to the settings. You can select this option if, for example, you have made manual changes that have not given you good recognition results.

1. From the **Recognition settings** tab, click **Auto-configure**.

A new dialog box appears.

2. Confirm that you want to return to auto-configured settings by clicking **Next**.

The system optimizes the settings.

3. Click **Close**.

4. If prompted, confirm to save the configuration.

5. Review and validate (see "Validate configuration" on page 315) the new settings.

Working with license plate match lists

About license plate match lists

License plate lists are collections of license plates that you want your LPR solution to treat in a special way. License plate recognitions are compared with these lists and if there is a match, the system triggers an LPR event. The events are stored on the event server and can be searched for and viewed on the **LPR** tab in XProtect Smart Client.

By default, events are only stored for 24 hours. To change this, open the **Options** dialog box in the Management Client and on the **Event Server Settings** tab, in the **Keep events for** field, enter a new time frame.

When you have specified a license plate match list, you can set up additional events and alarms to be triggered on a match.

Examples:

- A company headquarter uses a list of executive management's company car license plates to grant executives access to a separate parking area. When executives' license plates are recognized, the LPR solution triggers an output signal that opens the gate to the parking area.
- A chain of gas stations creates a list of license plates from vehicles that have previously left gas stations without paying for their gas. When such license plates are recognized, the LPR solution triggers output signals that activate an alarm and temporarily block the gas supply to certain gas pumps.



Triggered events can also be used for making cameras record in high quality or similar. You can even use an event to trigger combinations of such actions.

About Unlisted license plates list

Often you would trigger an event when a license plate that is included in a list is recognized, but you can also trigger an event with a license plate, which is **not** included in a list.

Example: A private car park uses a list of license plates to grant residents' vehicles access to the car park. If a vehicle with a license plate that is not on the list approaches the car park, the LPR solution triggers an output signal which lights a sign telling the driver to obtain a temporary guest pass from the security office.

To trigger a surveillance system event, when a license plate that is **not** on a list is recognized, use the **Unlisted license plates** list. You select it for a camera like any other list (see "Match lists tab" on page 312) and set it up like any other list (see "Events triggered by LPR" on page 320).

Add new license plate match lists

1. In the **Site Navigation pane**, select **License plate match lists**, right-click and select **Add New**.

2. In the window that appears, give the list a name and click **OK**.

As soon as you have created a license plate list, it becomes visible in the **License plate match list** and on the **Match lists** tab for all your LPR cameras.

3. If you want to add columns to the match list, click **Custom field** and specify the columns in the dialog box that opens (see "Edit custom fields properties" on page 319).
4. To update the match list, use the **Add**, **Edit**, **Delete** buttons (see "Edit license plate match lists" on page 317).
5. Instead of defining the match list directly in the Management Client, you can import a file (see "Import/export license plate match lists" on page 318).
6. If prompted, confirm to save changes.

Edit license plate match lists

1. In the **Site Navigation pane**, select **License plate match lists**.
2. Go to the Overview pane. Click the relevant list.
3. The **License plate match list information** window opens.
4. To include new rows to your list, click **Add** and fill out the fields:

- Do not include any spaces.
- Always use capital letters.

Examples: *ABC123* (correct), *ABC 123* (incorrect), *abc123* (incorrect)

- You can use wildcards in your license plate match lists. Do this by defining plates with a number of ?'s and the letter(s) and/or number(s) which must appear at specific places.



Examples: ?????A, A?????, ???1??, 22??33, A?B?C? or similar.

5. If prompted, confirm to save changes.

Import/export license plate match lists

You can import a file with a list of license plates that you want to use in a license plate match list. You have the following import options:

- Add license plates to the existing list.
- Replace the existing list.

This is useful if, for example, the lists are managed from a central location. Then all local installations can be updated by distributing a file.

Similarly you can export the complete list of license plates from a match list to an external location.

Supported file formats are .txt or .csv.

To import:


1. In the **Site Navigation pane**, click **License plate match lists** and select the relevant list.
2. To import a file, click **Import**.
3. In the dialog box, specify the location of the import file and the import type. Click **Next**.
4. Await the confirmation and click **Close**.

To export:

1. To export a file, click **Export**.
2. In the dialog box, specify the location of the export file and click **Next**.
3. Click **Close**.
4. You can open and edit the exported file in, for example, Microsoft Excel.

License plate match list properties



Name	Description
Name	Shows the name of the list. If needed, you can change the name.
Custom fields	Click to specify which license plate entry columns that you or the client user can add additional information to. See Custom fields (properties) (see "Edit custom fields properties" on page 319).
Search	Search the list for specific license plates, numbers, patterns or similar. If needed, you can use ? as a single wildcard
Add	<p>Click to add a license plate.</p> <ul style="list-style-type: none">▶ Do not include any spaces.▶ Always use capital letters. <p>Examples: ABC123 (correct), ABC 123 (incorrect), abc123 (incorrect)</p> <ul style="list-style-type: none">▶ You can use wildcards in your license plate lists. Do this by defining plates with a number of ?'s and the letter(s) and/or number(s) which must appear at specific places. <p>Examples: ?????A, A?????, ???1??, 22???33, A?B?C? and similar.</p> <p>Some regional areas might have exceptions to these rules. For example, personalized plates with spaces. Plates with two sets of characters which must be recognized separately by an underscore character (_). Or plates from certain regions with letters on a different background color on parts of the license plate.</p> <p>Example: </p>
Edit	Click to edit a license plate. You can select multiple rows for editing.
Delete	Click to delete the selected license plate(s).
Import	Click to import license plates from any comma-separated file, for example a .txt-file or .csv-file (see "Import/export license plate match lists" on page 318).
Export	Click to export the entire license plate list to a comma-separated file, for example a .txt-file or .csv-file (see "Import/export license plate match lists" on page 318).
Rows per page	Select how many license plates to display in one page (one screen). You can choose between 50 to 1000 rows.
Events triggered by list match	Select which event(s) should be triggered by a list match (see "Events triggered by LPR" on page 320). You can choose between all available types of events defined in your system.

Edit custom fields properties



You can add columns to your license plate match lists for additional information. You define the name and number of columns as well as the field content.

The XProtect Smart Client users can update the information in the columns but not the columns themselves.

Name	Description
Add	Adds a column to the match list. Type a name for the column.
Edit	Click to edit the name of the column.
Delete	Deletes a column.
Up	Changes the order of the columns.
Down	Changes the order of the columns.

Events triggered by LPR

After you have created license plate match lists (see "Add new license plate match lists" on page 317), you can associate them with all types of events defined in your system.

The type of events available depends on the configuration of your system. In connection with LPR, events are used to trigger output signals for, for example, raising of parking barrier or making cameras record in high quality. You can also use an event to trigger combinations of such actions. See About license plate match lists (on page 316) for more examples.

Set up system events triggered by list matches

1. Expand **Servers**, click **License plate match list** and select the list to which you want to associate an event.
2. In the **License plate match list information** window, next to the **Events triggered by list match** selection field, click **Select**.
3. In the **Select triggered events** dialog box, select one or more events.
4. If prompted, confirm to save changes.
5. The event is now associated with recognitions on the selected license plate match list.

To trigger a surveillance system event, when a license plate that is **not** on a list is recognized, configure the **Unlisted license plates** list.

Alarms triggered by LPR

You can associate some types of alarms with events from XProtect LPR. Do the following:

1. Create the license plate match list (see "Add new license plate match lists" on page 317) you want to match license plates against.



2. Add and configure your LPR camera(s) (see "Add LPR camera" on page 307).
3. In the **Site Navigation pane**, expand **Alarms**, right-click **Alarm Definitions** and select to create a new alarm.
4. The **Alarm Definition Information** window appears. Select the relevant properties (see "Alarm Definitions for LPR" on page 321).
5. If prompted when done, confirm to save changes.
6. Configure the alarm data settings for LPR (see "Alarm Data Settings for LPR" on page 321).

Alarm Definitions for LPR

Except for defining **Triggering events**, the settings for **Alarm Definitions** are the same for LPR as for the remaining part of the system.

To define triggering events related to LPR, select the event message to use when the alarm is triggered:

- a) In the **Triggering events** field, in the top drop-down list, decide what type of event to use for the alarm. The list offers **License plate match lists** and **LPR server** events (see "Working with license plate match lists" on page 316).
- b) In the second drop-down list, select the specific event message to use. If you selected **License plate match lists** in the drop-down above, select a license plate list. If you selected **LPR server**, select the relevant LPR server event message:
 - LPR camera connection lost
 - LPR camera running
 - LPR server not responding
 - LPR server responding

For information about the remaining alarm definition settings, see the **Alarms** section.

Alarm Data Settings for LPR

In the Management Client, you must make two specific **Alarm List Configuration** elements available for selection in XProtect Smart Client.

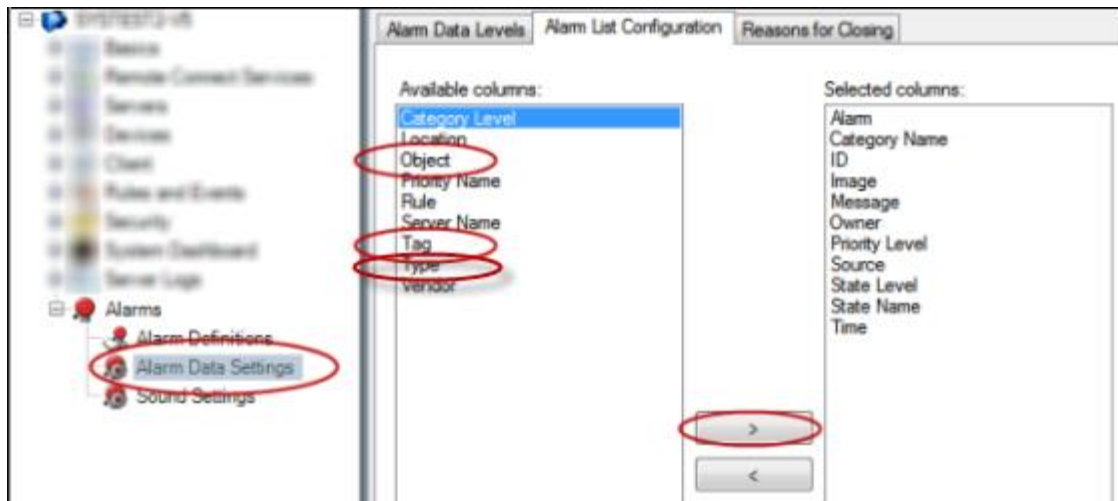
These two elements are used for configuring alarm lists in the **Alarm Manager** tab in XProtect Smart Client. The relevant elements are **Object**, **Tag**, and **Type**, which are essential for recognizing license plate numbers (Object) and country codes (Tag).

Do the following in the Management Client:

1. In the **Site Navigation pane**, expand **Alarms**, select **Alarm Data Settings**.



2. On the **Alarm List Configuration** tab, select **Object**, **Tag**, and **Type** and click **>**.



3. If prompted, confirm to save changes.

LPR maintenance

About LPR Server Manager

When you have installed an LPR server, you can check the state of its services with the XProtect LPR Server Manager. You can, for example, start and stop the LPR Server Service, view status messages, and read log files.

- You access LPR server state information via the **LPR Server Manager** icon in the notification area of the **computer running the LPR server**.



Example: LPR Server Manager
icon in notification area.

In the Management Client, you can get a full overview of the status of all your LPR servers (see "View LPR server information" on page 303).

Start and stop LPR Server Service

The LPR Server Service starts automatically after installation. If you have stopped the service manually, you can restart it manually.

1. Right-click the **LPR Server Manager** icon in the notification area.
2. From the menu that appears, select **Start LPR Server Service**.
3. If needed, select **Stop LPR Server Service** to stop the service again.



Show LPR server status

1. On your LPR server, right-click the **LPR Server Manager** icon in the notification area.
2. From the menu that appears, select **Show LPR server status**.

If the system is running without problems, the status will be: *All LPR cameras running*.

Other statuses are:

- *Service not responding*
- *Not connected to surveillance system*
- *Service not running*
- *Event Server not connected*
- *Unknown error*
- *X of Y LPR cameras running*

Show LPR server log

Log files are a useful tool for monitoring and troubleshooting the status of the LPR Server Service. All entries are time-stamped, with the most recent entries at the bottom.

1. In the notification area, right-click the **LPR Server Manager** icon.
2. From the menu that appears, select **Show LPR server Log File**.

A log-viewer lists the server activities with time stamps.

Change LPR server settings

The LPR server must be able to communicate with your management server. To enable this, you specify the IP address or hostname of the management server during the installation of the LPR server.

If you need to change the address of the management server, do the following:

1. Stop (see "Start and stop LPR Server Service" on page 322) the LPR Server Service.
2. In the notification area, right-click the **LPR Server Manager** icon.
3. From the menu that appears, select **Change settings**. The **LPR Server Service settings** window appears.
4. Specify the new values and click **OK**.
5. Restart the LPR Server Service.

Uninstall XProtect LPR

If you want to remove XProtect LPR from your system, uninstall the two components separately using the regular Windows removal procedure:



- On the computers where the LPR plug-in is installed, uninstall *Milestone XProtect LPR Plug-in*.
- On the computers where the LPR server is installed, uninstall *Milestone XProtect LPR Server*.



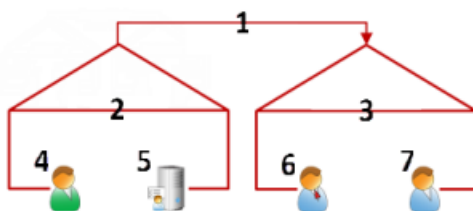
Multi-domain with one-way trust

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, **svcMilestone**.
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 XProtect 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. Milestone 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**.



XProtect Enterprise servers

About XProtect Enterprise servers

This section is only relevant if you use:

- XProtect Corporate
- your system does not use IPv6, and
- you have installations with XProtect Enterprise version 7 or later.

In all other cases, use Milestone Federated Architecture or Milestone Interconnect.

You can add XProtect Enterprise servers to your XProtect Corporate system. When added, the servers act as recording servers and their video can be viewed by the clients.

In the Management Client, you can see the status of added XProtect Enterprise servers. You must still define all XProtect Enterprise server settings (cameras, scheduling, user rights etc.) in XProtect Enterprise's Management Application. See the XProtect Enterprise documentation.

To give users access to video from XProtect Enterprise servers, you must match roles in XProtect Corporate with user rights defined on the XProtect Enterprise servers.

- Add XProtect Enterprise servers (on page 327)
- Define roles with access to XProtect Enterprise servers (on page 328)
- Edit XProtect Enterprise servers (on page 328)

Add XProtect Enterprise servers

Even if the XProtect Enterprise system has an internal master/slave setup, you cannot reuse it in your XProtect Corporate system. You must add each XProtect Enterprise server that you need device data from individually.

To add an existing XProtect Enterprise server to your system:

1. From the Management Client's **Tools** menu, select **Enterprise Servers**.
2. In the **Add/Remove Enterprise Servers** dialog box, click **Add**.
3. Enter the IP address or the host name of the XProtect Enterprise server.
4. Enter the port number used by the XProtect Enterprise server.

The default port number is 80. If in doubt, you can find the port number in XProtect Enterprise's Management Application under Server Access.

5. Enter the user credentials for the administrator of the XProtect Enterprise server to give yourself unlimited rights to the device data from it.
6. If the XProtect Corporate system accesses the XProtect Enterprise server through an Internet connection, click **Network** to specify the WAN address of XProtect Corporate's management server. You need only define the WAN address once.



Next step is to give your users access to devices from the XProtect Enterprise server.

Define roles with access to XProtect Enterprise servers

To give the users access to devices from the added XProtect Enterprise servers:

1. On the XProtect Enterprise server, open the Management Application to find an XProtect Enterprise user who has user rights you can reuse and match with a role in your XProtect Corporate system. If not, create a new XProtect Enterprise user that matches the role in your XProtect Corporate system.
2. Take careful note of the XProtect Enterprise user's user name, password and authentication type (basic or Windows). The XProtect Corporate system does not verify that the information you specify later in these steps corresponds to a defined user in XProtect Enterprise.
3. In the XProtect Corporate Management Client's **Site Navigation** pane, expand **Security**, and select **Roles**.
4. Select the role you want to use or define a new role.
5. At the bottom of the **Role Settings** pane, select the **Servers** tab and then the XProtect Enterprise server.
6. Select the XProtect Enterprise user with the user rights you want to match with your role.
7. Click **Save**.

Edit XProtect Enterprise servers

To edit an XProtect Enterprise server added to your system:

1. From the **Tools** menu, select **Enterprise Servers**.
2. Select the XProtect Enterprise server from the list, and click **Edit**.
3. Edit the relevant settings and 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.



Port number	Protocol	Used by	Purpose
20 and 21	FTP	Recording servers	Listening for event messages from devices.
25	SMTP	Recording servers	Listening for event messages from devices and for sending images to the surveillance system server via e-mail.
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.
5210	TCP	Recording servers and failover recording servers	Merging of databases after a failover recording server has been running.
5432	TCP	Recording servers	Listening for event messages from devices.
7563	TCP	Recording servers and XProtect Smart Client	Communication with the ImageServer interface. Also handling of PTZ camera control commands and for retrieving image streams from clients etc.



Port number	Protocol	Used by	Purpose
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.
8844	UDP	Failover recording servers	Communication between the servers.
8990	TCP	Management server	Monitoring the status of the Failover Server service.
9090	TCP	Event Server	Listening for analytics events from external systems or devices.
9993	TCP	Recording servers and management server	Communication between the two.
11000	TCP	Failover recording servers	Polling the state of recording servers.
12345	TCP	Management server and XProtect Smart Client	Communication between the system and Matrix recipients. You can change the port number in the Management Client.
22331	TCP	Event server, XProtect Smart Client and Management Client	Communication between the event server and the two others.
52111	TCP	XProtect 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

Milestone 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, Milestone 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 <http://www.support.microsoft.com> 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 manual back up

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 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 machine. 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

Milestone 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 332).

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.

Flush 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 support.microsoft.com <http://www.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
 - 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 scheduled backup

Prerequisite: To prevent configurational changes being made while you restore the system configuration database, stop the:

- Management Server service (see "About the Management Server service and Recording Server service" on page 344)
- Event Server Service (can be done from Windows **Services** (search for **services.msc** on your machine. Within **Services**, locate **Milestone XProtect Event Server**))
- World Wide Web Publishing Service, also known as the Internet Information Service (IIS). Learn how to stop the IIS at: [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx)
[http://www.technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://www.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 backup **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 initial license (.lic) file**, that is the one you used when initially installing your system, not the .lic file which is the result of your license activation. License activation is, among other things, based on the specific hardware on which the activation took place. Therefore an activated .lic 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 received a new initial .lic file together with your new Software License Code (SLC).
- **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 338)
- Copy log server database (see "Back up log server database" on page 332)



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.

Milestone 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 335).
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 (on page 336).

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%MilestoneXProtect 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%Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (with content) to temporary directory on the event server.
2. If:
 - o **a** and **b**, go to the notification area of the taskbar. Right-click the **Management Server** icon, select **Update SQL address**.
 - o **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.

Your system might be affected by license limitations. Using the **Activate Online** wizard, you must reactivate your licenses **after** replacing hardware devices. If the new number of cameras exceeds the old number of cameras, you might also have to buy new 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)**.

Address	Port	User Name	Password	Hardware Driver
10.100.10.10		root	****	Axis 216MFD Camera

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.

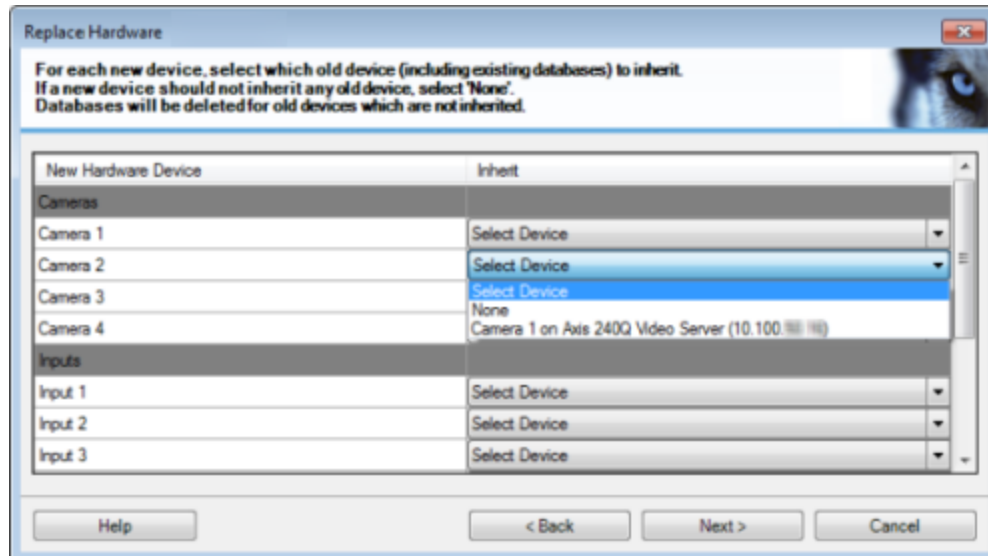
5. Do one of the following:
 - If you selected the required hardware device driver directly from the list, click **Next**.
 - If you selected **Auto Detect** in the list, click **Auto Detect**, wait for this process to be successful (marked by a ✓ to the far left), click **Next**.

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.

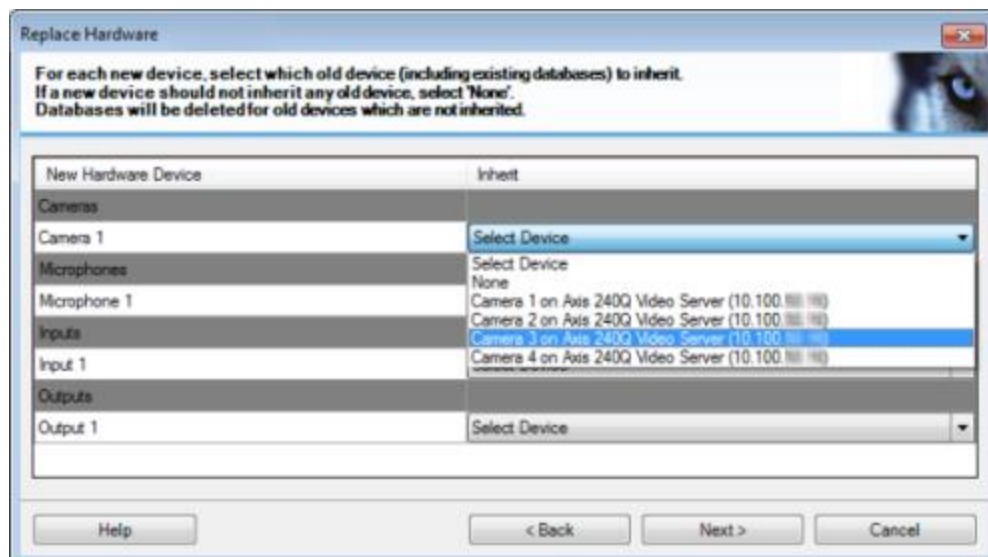
It is important to consider **how** to map databases from the old hardware device to databases of the new hardware device. You do the actual mapping of individual devices by selecting a corresponding camera, microphone, input, output or **None** in the right-side column.



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.



Example of the new hardware device having more individual devices than the old one.

Click **Next**.

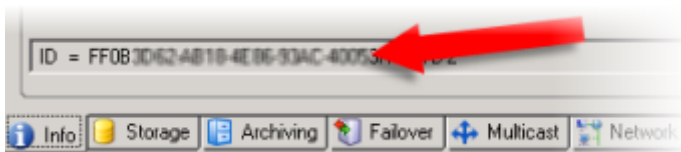
6. You are presented with a list of hardware to be added, replaced or removed. Click **Confirm**.
7. Final step is a summary of added, replaced and inherited devices and their settings. Click **Copy to Clipboard** to copy contents to the Windows clipboard or/and **Close** to end the wizard.



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:
 - a) Select **Recording Servers**, then in the **Overview** pane select the old recording server.
 - b) Select the **Storage** tab.
 - c) Press and hold down the CTRL key on your keyboard while selecting the **Info** tab.
 - d) 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:
 - a) 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.

- b) On the new recording server, open an explorer and go to *C:\ProgramData\Milestone\XProtect Recording Server* or the path where your recording server is located.
- c) Open the file *RecorderConfig.xml*.
- d) Delete the ID stated in between the tags `<id>` and `</id>`.

```
- <recorderconfig>
- <recorder>
  <id>ff0b3d62-4b18-4e06-93ac-400731f63742</id>
```

- e) Paste the copied recording server ID in between the tags `<id>` and `</id>`. Save the *RecorderConfig.xml* file.
- f) Go to the registry:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation.
- g) Open **RecorderIDOnMachine** and change the old recording server ID with the new ID.
- h) 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. Milestone releases new versions of video device drivers regularly and makes them available on the download page <http://www.milestonesys.com/downloads> 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.

Services

About the Management Server service and Recording Server service

You can check the state of the Management Server service or the Recording Server service by looking at the icon in the notification area of the computer running the management server or recording server.

In the notification area, you can start and stop the Management Server service/Recording Server service, view status messages, check version information and more. To do this, right-click the server service icon. Depending on server type, select the needed icon. If you use multiple instances of the Recording Server service, you select a particular instance or all instances from a sub-menu.

If you stop the recording server service at some point, your system cannot interact with devices connected to the recording server. This means you cannot view live video or record video. If you stop the management server service, you cannot use the Management Client at all.

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, the recording server might not be able to rename or move relevant media files, which might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server



service, close the program accessing the relevant media file(s) or folder(s), and restart the Recording Server service.

View status messages

1. Right-click the notification area's server service icon.
2. Depending on server type, select the relevant icon.
3. Select **Show Status Messages**. Depending on the current server type, either the **Management Server Status Messages** or **Recording Server Status Messages** window appears, listing time-stamped status messages:



Example from Management Server service

Read server service icons - management, recording and failover

The following notification area icons represent the possible states of the Management Server service, Recording Server and Failover Recording Server services. They are all visible on the computers where the service is installed, not in the Management Client:



Management Server service icon	Recording Server service icon	Failover Recording Server service icon	Description
			Running Reg. failover recording server, it is enabled and started and can take over from standard recording servers.
			Stopped Reg. failover recording server, it is stopped and no longer taking over from standard recording servers.
			Starting Appears when a server service is in the process of starting. Under normal circumstances, the icon changes after a short while to Running .
		Management and Recording Server service only	Stopping Appears when a server service is in the process of stopping. Under normal circumstances, the icon changes after a short while to Stopped .
Recording Server service only		Recording Server service only	In indeterminate state Appears when the Recording Server service is initially loaded and until the first information is received, upon which the icon, under normal circumstances, changes to Starting and afterwards to Running .
			Running offline Typically appears when the Recording Server or Failover recording service is running but the Management Server service is not.
		Recording Server service only	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 recording server settings

To change basic settings for the Recording Server service, such as which port numbers to use:



You must stop the Recording Server service to change settings. 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. Right-click the server service icon.
2. Depending on server type, select the needed icon.
3. Select **Stop Recording Server service**.
4. Right-click the notification area's recording server icon.
5. Select **Change Settings**. The **Recording Server Settings** window appears. Change the appropriate settings.

Recording server properties

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 XProtect 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. Also, some devices use SMTP (e-mail) for sending event messages and/or for sending images to the surveillance system server via e-mail. SMTP is a standard for sending e-mail messages between servers. Default is port 25. You can change this if you need to.
FTP server port	Port number to be used when the recording server listens for FTP information (some devices use FTP for sending event messages). Default is port 21. You can change this if you need to.



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 XProtect Smart Client is time-synchronized with the computer running the Service Channel service. If an XProtect Smart Client is not time-synchronized with the management server and the computer running the Service Channel service, the XProtect Smart Client is not updated with information about configuration changes made by other users in XProtect Smart Client. This means that users risk overwriting each others' configuration changes. If your XProtect 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	<p>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 <i>http://</i> or <i>https://</i> and must not contain any of the following characters: <code>< > & ' " * ? []</code>.</p> <p>Example of a typical URL format: <i>http://ipaddress:port/directory</i> (where port and directory are optional). Note that you can add more than one URL if required.</p>
Trusted	<p>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).</p> <p>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.</p>
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, <i>http</i> , <i>https</i> , <i>tcp</i> or <i>udp</i>) 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

3

360° Lens tab (devices) • 123

A

A distributed system setup • 15

About access control integration • 265

About actions and stop actions • 109, 145, 266

About alarm configuration • 219

About alarms • 219

About analytics events • 173

About archive structure • 69

About back up/restore fail and problem
scenarios • 318

About backing up and restoring the event
server configuration • 318

About backing up and restoring your system
configuration • 53, 317

About basic users • 211

About camera devices • 38, 91

About camera settings • 101

About clients • 135

About configuration reports • 214

About current tasks • 214

About day length time profiles • 165, 167

About daylight saving time • 49

About default rules • 159

About device groups • 87

About devices • 87, 90

About dynamic sensitivity • 132

About evidence lock • 213

About failover recording server functionality •
236

About failover recording server services • 240

About failover recording servers • 74, 157, 234

About failover steps • 235

About generate motion data for smart search •
134

About generic events • 176, 232

About hardware • 78

About input devices • 93

About IPv6 and IPv4 • 23

About license plate match lists • 294, 302, 306

About licenses • 21

About local IP address ranges • 23

About login authorization • 50

About logs • 215, 226

About LPR Server Manager • 308

About Management Client profiles • 139, 183

About manually backing up your system
configuration • 318

About Matrix • 142

About metadata devices • 93

About microphone devices • 91

About Milestone Federated Architecture • 210,
247



- About Milestone Interconnect • 255
- About Milestone Mobile client • 19
- About moving the management server • 322
- About multicasting • 75, 126
- About multiple management servers (clustering) • 241
- About multi-streaming • 101, 103
- About notification profiles • 168, 227
- About output devices • 94
- About possible Milestone Interconnect setups • 257
- About pre-buffering • 107
- About preparing cameras for LPR • 275, 291, 301
- About recording servers • 61
- About remote connect services • 244
- About remote recording • 110
- About removing video device drivers • 329
- About rights of a role • 183
- About roles • 38, 182
- About rule complexity • 162
- About rules • 158
- About rules and events • 38, 144
- About scheduled backup and restore of system configuration • 320
- About selecting Milestone Interconnect or Milestone Federated Architecture • 247, 254
- About setting up alarms using Enterprise slaves • 224
- About Smart Client profiles • 136
- About snapshots • 291, 293, 301
- About SNMP support • 312
- About speaker devices • 92
- About storage • 109
- About storage and archiving • 38, 65, 110
- About system dashboard • 212
- About system monitor • 212
- About the 360° Lens tab • 123
- About the Client tab • 126
- About the Events tab • 124
- About the Info tab • 98
- About the Management Client • 18
- About the Management Server service and Recording Server service • 321, 329
- About the Motion tab • 131
- About the Patrolling tab • 117
- About the Presets tab • 112
- About the Privacy Mask tab • 128
- About the Record tab • 105
- About the service channel • 54, 333
- About the Settings tab • 100
- About the Streams tab • 102
- About time profiles • 164
- About time servers • 49



- About unavailable management servers • 323
- About Unlisted license plates list • 303
- About updating the SQL server address • 324
- About upgrade • 26, 45
- About user-defined events • 156, 171
- About using rules with Smart Wall presets • 262, 263
- About using the system with IPv6 • 23
- About validating rules • 161
- About video device drivers • 329
- About view groups • 135
- About view groups and roles • 136
- About virus scanning • 28
- About writing IPv6 addresses • 24
- About XProtect Enterprise servers • 54, 210, 313
- About XProtect LPR • 272
- About XProtect Smart Client • 19
- About XProtect Smart Wall • 135, 259
- About XProtect Web Client • 21
- Accept inclusion in the hierarchy • 251, 252
- Access Control Events tab (Access Control) • 158, 269
- Access control properties • 266, 268
- Access Control Settings tab (options) • 225, 230, 266
- Access Control tab (roles) • 211, 266
- Access Request Notification tab (Access Control) • 266, 271
- Activate input manually for test • 94
- Activate licenses after grace period • 60
- Activate licenses offline • 38, 59
- Activate licenses online • 38, 58
- Activate output manually for test • 95
- Active Directory • 18, 28
- Add a configuration report • 214
- Add a device group • 88
- Add a generic event • 177
- Add a new recording storage • 67
- Add a patrolling profile • 84, 118
- Add a preset position (type 1) • 84, 113
- Add a rule • 163, 262
- Add a stream • 103
- Add a user-defined event • 173
- Add a view group • 136
- Add an event • 124
- Add and configure a Management Client profile • 139
- Add and configure a Smart Client profile • 137
- Add and edit an analytics event • 174
- Add and edit registered services • 333
- Add and manage a role • 183, 184
- Add hardware • 38, 78, 257
- Add LPR camera • 293, 306



Add Matrix recipients • 143

Add new license plate match lists • 299, 303, 306

Add notification profiles • 169

Add site to hierarchy • 251

Add XProtect Enterprise servers • 313

Add/edit STSs • 245

Add/publish Download Manager installer components • 43

Adjust settings for your LPR camera • 294

Alarm Data Settings • 222

Alarm Data Settings for LPR • 307

Alarm Definitions • 220

Alarm Definitions (properties) • 221

Alarm Definitions for LPR • 307

Alarms • 219

Alarms tab (roles) • 210

Alarms triggered by LPR • 306

Alternative upgrade for workgroup • 34, 46

Analytics events • 173

Analytics Events tab (options) • 225, 230

Archive Settings properties • 38, 68, 73

Assign a default preset position • 115

Assign failover recording servers • 238

Assign IP address range • 75

Assign local IP ranges • 77

Assign/remove users and groups to/from roles • 38, 183, 184, 185

Associated cameras • 267

Associated Cameras tab (Access Control) • 269

Attach a device or group of devices to a storage • 38, 66, 68

Audit log (properties) • 217

Authorize a recording server • 38, 62

Auto-configure • 295, 302

AVI Generation tab (options) • 225, 228

Axis One-Click Camera connection properties • 246

B

Back up archived recordings • 68

Back up log server database • 317, 323

Back up system configuration manually • 318

Back up system configuration with scheduled backup • 320, 323

Backing up and restoring system configuration • 69, 317

Backup and restore event server configuration • 321

Basic users • 211

Basics • 56

Before you start • 12

Best practices • 48

Bookmark tab (options) • 225, 229

C

Camera angles • 276, 277

Cardholders tab (Access Control) • 271



Change log language • 216

Change LPR server settings • 309

Change recording server settings • 331

Change Software License Code • 38, 39

Change the management server address • 241

Change/verify the basic configuration of a recording server • 62

Client • 135

Client tab (devices) • 126

Client tab properties • 126

Clients • 18

Compatibility • 274

Configure an integrated access control system • 266

Configure report details • 215

Configure Smart Walls • 249, 260

Configure SNMP service • 312

Configure the system in Management Client • 31, 34, 37

Configuring cameras for LPR • 291

Connect to another site in hierarchy • 252

Connecting to the access control system • 267

Contrast • 276, 285, 287

Copy a Management Client profile • 140

Copy a Smart Client profile • 137

Copy, rename or delete a role • 184

Copyright, trademarks and disclaimer • 11

Country modules tab • 275, 289, 293, 294, 299

Create a day length time profile • 167

Create access control system integration • 267

Create an archive within a storage • 67

Create and set up Smart Client profiles, roles and time profiles • 136, 137

Create basic users • 188, 211

Customize IIS • 28

Customize transitions • 120

D

Day length time profile properties • 168

Deactivate and activate a rule • 164

Define public address and port • 77

Define roles with access to XProtect Enterprise servers • 313, 314

Define rules sending video to Matrix recipients • 143

Delete all hardware on a recording server • 87

Delete an archive from a storage area • 70

Delete an entire storage area • 70

Detach a site from the hierarchy • 253

Determine installation method • 26

Determine SQL server type • 26

Device pack installer - must be downloaded • 43, 45

Device tab (roles) • 203, 214, 229, 230

Devices • 87

Devices which require a license • 58

Disable/enable hardware • 79



Download Manager/download web page • 40
Download Manager's default configuration • 42
Download Manager's standard installers (user)
• 43

E

Edit a preset position (type 1 only) • 115
Edit a time profile • 167
Edit analytics events settings • 176
Edit basic hardware settings • 79
Edit custom fields properties • 303, 304, 305
Edit license plate match lists • 303
Edit settings for a selected storage or archive •
68
Edit XProtect Enterprise servers • 313, 314
Edit, copy and rename a rule • 164
Enable and disable motion detection • 131,
132
Enable and disable panomorph support • 123
Enable keyframe recording • 109
Enable manual sensitivity • 132
Enable multicasting • 75
Enable multicasting for individual cameras • 76
Enable playback directly from remote site
camera • 107, 258
Enable PTZ on a video encoder • 83
Enable recording on related devices • 107, 126
Enable/disable devices via device groups • 91,
92, 93, 94, 95, 96

Enable/disable individual devices • 80
Enable/disable privacy masking • 128
Enable/disable recording • 107
Establish remote desktop connection to remote
system • 258
Event server • 17
Event Server tab (options) • 225, 231
Event tab (properties) • 125
Events overview • 145, 152, 266
Events tab (devices) • 92, 94, 124
Events tab (remote server) • 85
Events triggered by LPR • 303, 305, 306
Evidence Lock tab (options) • 225, 229

Example

Create and test a basic generic event • 178
Export logs • 216
External Event tab (roles) • 209

F

Failover group properties • 240
Failover management server • 16
Failover management servers • 241
Failover recording server • 16
Failover recording server properties • 239
Failover recording servers (regular and hot
standby) • 234
Failover tab (recording server) • 74
Failover tab properties • 74
Feature configuration • 12, 234



Federated site properties • 253

Final summary • 267

First time use • 12, 48

Flush SQL server transaction log • 320

G

General Settings tab (Access Control) • 268

General tab • 253

General tab (options) • 224, 225

Generic event (properties) • 177, 178

Generic event data source (properties) • 180,
181

Generic event test (properties) • 177, 180

Generic events • 176

Generic Events tab (options) • 180, 225, 232

Get additional licenses • 58, 60

Group failover recording servers • 239

H

Hard disk failure

protect your drives • 48

Hardware and remote servers • 78

Hide/remove Download Manager installer
components • 44

I

Image resolution • 276, 280

Import/export license plate match lists • 303,
304, 305

Info tab • 294

Info tab (devices) • 92, 93, 94, 95, 98

Info tab (hardware) • 82

Info tab (Management Client Profiles) • 140

Info tab (monitor properties) • 263

Info tab (recording server) • 64

Info tab (remote server) • 82, 85

Info tab (roles) • 139, 186, 214

Info tab (Smart Wall properties) • 262

Info tab properties • 64, 98

Install a failover recording server • 33, 237

Install clients • 39

Install in a cluster • 242, 244

Install Milestone Mobile server • 40

Install SNMP service • 312

Install STS environment for One-click camera
connection • 245

Install the recording server • 32, 33

Install the system • 30, 38, 46

Install XProtect LPR • 288, 289

Install XProtect Smart Client silently • 39

Install your system - Custom option • 30, 32

Install your system - Distributed option • 30, 31

Install your system - Single Server option • 30

Installation • 12, 26

Installation for workgroups • 28, 34, 47

Installation preconditions • 26

Installation troubleshooting • 34

Introduction to the help • 12

Issue



- Automatic installation of IIS failed • 36
- Changes to SQL server location prevents database access • 37
- Recording server startup fails due to port conflict • 35

L

- Layout tab (Smart Wall properties) • 263
- Lens and shutter speed • 276, 285
- License information • 56
- License plate match list properties • 304
- Licenses and hardware device replacement • 60
- Log server • 17
- LPR configuration • 289
- LPR installation • 288
- LPR licenses • 274, 289, 299
- LPR maintenance • 308
- LPR server information properties • 289, 290
- LPR system architecture • 273
- LPR system overview • 272

M

- Mail Server tab (options) • 225, 227
- Manage hardware • 82
- Manage manual recording • 108
- Manage network configuration • 333
- Manage pre-buffering • 108, 229
- Manage remote servers • 85
- Manage roles with Smart Walls • 261
- Management Client elements • 12, 54, 56

- Management Client overview • 18, 50
 - Management Client profile properties • 140
 - Management Client profiles • 139
 - Management Client window overview • 50
 - Management server • 15
 - Managing the SQL server • 324
 - Manual backup and restore of system configuration • 318, 320
 - Match lists tab • 294, 298, 303
 - Matrix • 142
 - Matrix tab (roles) • 210
 - Menu overview • 53
 - Milestone Federated Architecture • 247
 - Milestone Interconnect • 254
 - Milestone Interconnect and licensing • 258
 - Minimum system requirements • 274
 - MIP tab (roles) • 211
 - Monitor properties • 263
 - Motion tab (devices) • 91, 131
 - Move non-archived recordings from one storage to another • 71
 - Move the system configuration • 323
 - Moving the management server • 322
 - Multicast tab (recording server) • 74
 - Multi-domain with one-way trust • 311
- ## **N**
- Navigate the built-in help system • 12
 - Network tab (options) • 225, 229



Network tab (recording server) • 77

Notification profile (properties) • 170

Notification profiles • 168

O

Options dialog box • 224

Overall Security tab (roles) • 139, 188

P

Panes overview • 52

Parent Site tab • 254

Patrolling tab (devices) • 117

Physical surroundings • 276, 284

Plate width recommendations • 276, 279, 288

Ports used by the system • 315

Positioning the camera • 276, 295

Power outages

 use a UPS • 48

Prerequisites • 168

Prerequisites for clustering • 242

Prerequisites for offline installation • 30

Prerequisites in the Management Client • 291

Presets tab (devices) • 112

Presets tab (monitor properties) • 264

Presets tab (Smart Wall properties) • 262

Privacy mask tab (devices) • 128

Privacy mask tab (properties) • 129

Product comparison chart • 22, 71, 74, 135,
136, 139, 140, 183, 186, 188, 203, 212, 213,
224, 229, 234, 244, 247, 255, 259

Product overview • 14

Profile tab (Management Client Profiles) • 140

Protect recording databases from corruption •
48, 63

PTZ tab (roles) • 208

PTZ tab (video encoders) • 83

R

Read failover recording server status icons •
239

Read server service icons - management,
recording and failover • 330

Recognition settings tab • 294

Record tab (devices) • 91, 92, 93, 105

Recording server • 16

Recording server properties • 332

Recording server status icons • 63

Recording servers • 61

Refresh site hierarchy • 252

Register new Axis One-click camera • 245

Register Software License Code • 29, 39

Registered services • 332

Registered services properties • 334

Remote connect services • 244

Remote Recordings tab (roles) • 209

Remote Retrieval tab • 86

Remove a recording server • 86

Rename a user-defined event • 173

Replace a recording server • 328



Replace hardware • 60, 325

Restart Data Collector Server service • 213

Restore system configuration from manual
back up • 319

Restore system configuration from scheduled
backup • 321, 323

Retrieve remote recordings from remote site
camera • 259

Roles • 182

Roles settings • 184, 186

Rule log (properties) • 218

Rules • 158

Rules and events • 144

S

Scheduled backup and restore • 320

Search logs • 216

Security • 182

Select image processing interval • 133

Select keyframes settings • 133

Select service account • 27

Select shared backup folder • 319

Select snapshots • 295, 300

Send the same video to several XProtect
Smart Client views • 144

Server logs • 215

Server Logs tab (options) • 215, 225, 226

Servers and hardware • 61

Servers tab (roles) • 210

Services • 329

Set up a secure connection to the hardware •
80

Set up and enable failover recording servers •
237

Set up your system to run federated sites • 250

Settings tab (devices) • 91, 92, 93, 94, 95, 100

Settings tab (hardware) • 82

Settings tab (remote server) • 83, 85

Setup with one-way trust • 311

Show LPR server log • 309

Show LPR server status • 309

Site information • 60

Smart Client profile properties • 138, 266

Smart Client profiles • 136

Smart Wall properties • 262

Smart Wall tab (roles) • 209, 262

SNMP • 312

Sound Settings • 223

Specify a time profile • 165

Specify an end position • 121

Specify common properties for all devices in a
device group • 88, 90

Specify datagram options • 76

Specify detection method • 133

Specify event properties • 124, 125

Specify exclude regions • 134

Specify manual PTZ session timeout • 121



Specify motion detection settings • 132

Specify Panomorph settings • 123

Specify preset positions in a patrolling profile • 119

Specify privacy mask settings • 129

Specify recording frame rate • 109

Specify the time at each preset position • 119

Specify threshold • 133

Specify which devices to include in a device group • 88, 89

Speech tab (roles) • 208

SQL server • 17

Start and stop LPR Server Service • 308, 309

Status icons of devices • 96

Storage and Recording Settings properties • 67, 71

Storage tab (recording server) • 65

Streams tab (devices) • 91, 102

System components • 15

System dashboard • 212

System log (properties) • 217

System maintenance • 12, 315

System overview • 12, 14

System requirements • 25

T

Test a generic event • 177

Test a preset position (type 1 only) • 116

Test analytics event • 174

Time profiles • 164

U

Understanding camera exposure • 276, 282, 286

Uninstall XProtect LPR • 309

Unwanted camera features • 276, 285, 287

Update remote site hardware • 258

Update site information • 61

Update the log server's SQL address • 324

Update the management server or event server SQL server address • 325

Upgrade • 45

Upgrade in a cluster • 244

Upgrade prerequisites • 46

Upgrade XProtect LPR • 289

Use preset positions from the camera (type 2) • 114

Use rules to trigger email notifications • 169, 228

Use several instances of an event • 124, 125

User and Groups tab (roles) • 187, 211

User Settings tab (options) • 225, 230

User-defined events • 171

V

Validate configuration • 293, 294, 295, 296, 298, 299, 300, 301, 302

Video device drivers • 329

View effective roles • 186

View Group tab (roles) • 210



View groups • 135

View license overview • 58

View LPR server information • 275, 289, 308

View status messages • 241, 330

View version information • 241

Virtual servers • 18

W

Why use a public address? • 77

Windows Task Manager

- be careful when you end processes • 48

Wizard for access control system integration •
266

Working with device groups • 87

Working with devices • 38, 90

Working with license plate match lists • 302,
307

X

XProtect Access Control Module • 265

XProtect Enterprise servers • 313

XProtect LPR • 272

XProtect Smart Wall • 259



About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit:

www.milestonesys.com.