

Milestone Systems

XProtect® Corporate 5.0b

Administrator's Manual



The Open Platform Company



Contents

INTRODUCTIONS	13
PRODUCT OVERVIEW XPROTECT CORPORATE	13
A Typical XProtect Corporate Setup	13
About Updates	14
The Management Server	14
The Recording Server	15
The Management Client	15
The Download Manager	15
The XProtect Smart Client and Remote Client	15
SYSTEM REQUIREMENTS.....	16
Computer running Management Server.....	16
Computer running Recording Server or Failover Server	16
Computer running Management Client.....	17
Computer running Event Server	17
Computer running Log Server	17
Computer running Service Channel	18
Computer running XProtect Smart Client.....	19
Computer accessing Remote Client.....	19
Active Directory.....	20
CLIENTS OVERVIEW.....	20
Working with clients	20
Installing the XProtect Smart Client	22
Remote Client	24
Navigating the Built-in Help System (online)	25
INSTALLATION AND REMOVAL	27
INSTALLATION OVERVIEW.....	27



Installing XProtect Corporate on virtual servers	27
INSTALL MANAGEMENT SERVER	28
Alternative for workgroups	30
Step 1: Internet Information Services	30
Step 2: XProtect Corporate management server database	31
Step 3: XProtect Corporate management server	32
What's next?	34
INSTALL SYSTEM COMPONENTS.....	34
Part I—Downloading the installer	35
Part II—Installing the component	36
Recording servers.....	36
Failover servers.....	38
Management client	40
Specify recording server setup parameters	40
INSTALL EVENT SERVER AND LOG SERVER (CUSTOM).....	40
Installing event server and log server.....	41
INSTALL THE SERVICE CHANNEL	42
Install Service Channel (typical)	44
Install Service Channel (custom).....	45
PORT NUMBERS OF SPECIAL INTEREST	46
Ports used by XProtect Corporate	46
MULTIPLE MANAGEMENT SERVERS (CLUSTERING)	47
Prerequisites for installing XProtect Corporate in a cluster.....	48
Installing XProtect Corporate in a cluster	48
Upgrading XProtect Corporate in a cluster	50
MULTIPLE RECORDING SERVER INSTANCES.....	50
Installing multiple recording server instances	50
REMOVE SYSTEM COMPONENTS	51



Removing Management Server.....	51
Removing Download Manager, Event Server and Log Server	51
Removing Management Client or Service Channel	51
Removing Recording Server	52
Removing non-required components from Management Server.....	52
UPGRADE FROM PREVIOUS VERSION.....	52
Prerequisites.....	53
Upgrading the Management Server.....	53
Upgrading Recording Servers	54
Upgrading a Management Client	54
Upgrading the XProtect Smart Client.....	54
Upgrading Video Device Drivers	55
INSTALLATION TROUBLESHOOTING	55
Issue: Automatic IIS installation for Management or Event Server fails	55
Issue: Recording Server startup fails due to port conflict.....	56
Issue: Changes to SQL Server location prevents database access	58
Issue: Insufficient continuous virtual memory fails installation	58
Issue: Multi-domain environments; one-way trusts not working	59
USE DOWNLOAD MANAGER.....	60
Access Download Manager.....	60
Make new components available.....	60
Move components between web page versions	61
Hide and remove components.....	62
Download Manager is not user rights management tool	62
Default configuration of Download Manager and web page.....	63
Components controllable through the Download Manager.....	65
Virus scanning on the Management Server not recommended	65
MANAGEMENT CLIENT	66
MANAGEMENT CLIENT OVERVIEW	66



Management Client's Elements	66
Site Navigation Pane and Federated Hierarchy Pane.....	67
Menu Bar	68
Toolbar	68
Memory Indicator	69
PANES OVERVIEW	70
Menu and tool bars	70
Overview Pane.....	70
Preview Pane	70
Properties Pane	71
Site Navigation Pane and Federated Hierarchy Pane.....	71
BASICS	72
Get started	72
Log in to the Management Client.....	74
Management Client menu overview	75
Customize the Management Client's Layout.....	76
Activate Licenses	81
Manage Licenses.....	84
Manage Software License Codes (SLC).....	86
REMOTE CONNECT SERVICES.....	88
About Remote Connect Services	88
Axis One-Click Camera Connection Properties	90
SERVERS	90
Add Hardware (Cameras, etc.)	90
Manage Hardware.....	95
About Storage and Archiving	101
Manage Recording Servers.....	106
Manage Multicasting	120
Manage Public Addresses.....	122
Servers and Clients Require Time-Synchronization	123



DEVICES	125
About Devices	125
CLIENT	179
About clients.....	179
Manage View Groups	179
Manage Smart Client Profiles	182
Manage XProtect Matrix Recipients	185
RULES AND EVENTS.....	187
About Rules and Events	187
Actions and Stop Actions Overview	188
Create Typical Rules	194
Default Rules	214
Events Overview.....	216
Manage Rules	221
Manage Time Profiles	229
Manage Day Length Time Profiles.....	232
Manage Notification Profiles	233
Manage User-defined Events	238
Managing Analytics Events.....	239
Manage Generic Events.....	242
SECURITY	248
About Security.....	248
About Roles	249
Manage Roles	251
Manage View Groups	262
SYSTEM DASHBOARD	264
About System Dashboard	264
About System Monitor	264
About Current Task.....	266
About configuration report	266



SERVER LOGS.....	267
Manage Logs	267
ALARMS.....	273
Manage Alarms	273
ENTERPRISE.....	279
Manage XProtect Enterprise Servers	279
REGISTERED SERVICES.....	282
Manage Network Configuration	282
Manage Registered Services	283
OPTIONS.....	285
Options	285
AVI Compression Settings	290
Outgoing SMTP Mail Server Settings.....	291
Manage local IP address ranges.....	292
MILESTONE FEDERATED ARCHITECTURE.....	293
MILESTONE FEDERATED ARCHITECTURE OVERVIEW	293
Important Prerequisites When Running Federated Sites	293
Licensing of Milestone Federated Architecture	295
Basic Rules of Federated Sites.....	295
Principles for Setting Up Federated Sites	296
The Administrator Role and Federated Sites	296
Possibilities and Constrains of Federated Sites.....	297
Frequently Asked Questions to Federated Sites	297
Federated Sites Example Scenario—Limestone City	299
ILLUSTRATION OF MILESTONE FEDERATED ARCHITECTURE	301
MANAGE MILESTONE FEDERATED ARCHITECTURE	302
Federated Icons.....	302
Expand/Collapse	303



Site Navigation Pane	303
Right-clicking is not Selecting!	303
Context Menu	303
Adding a Site to the Hierarchy	303
Accepting Inclusion in the Hierarchy	304
Connecting to Another Site in the Hierarchy	305
Detaching a Site from the Hierarchy	305
Refreshing the Site Hierarchy	306
Renaming a Site	307
Setting the Site Properties	307
BACKUP, RESTORE AND MOVE SYSTEM CONFIGURATION ..	309
SCHEDULED BACKUP & RESTORE OF SYSTEM CONFIGURATION.....	309
Flushing the SQL Server Transaction Log	309
Prerequisites	309
Scheduled Back Up of System Configuration	309
Backup and Restore Event Server Configuration	310
Backing Up Log Server Database	310
Restoring System Configuration (From Scheduled Back Up)	311
MANUAL BACKUP & RESTORE OF SYSTEM CONFIGURATION	311
Select Shared Backup Folder	312
Manual Back Up of System Configuration	312
Restoring System Configuration (From Manual Back Up)	313
Back Up/Restore Fail & Problem Scenarios	313
MOVE SYSTEM CONFIGURATION TO NEW MANAGEMENT SERVER.....	313
Copying System Configuration from Old Server (Step 1)	315
What Happens while the Management Server Is Unavailable?	315
Copying Log Server Database	315
Installing New Management Server on New Server (Step 2)	316
Copying/Restoring System Configuration to New Server (Step 3)	316



DEVICE DRIVERS.....	317
MANAGE AND REMOVE VIDEO DEVICE DRIVERS.....	317
Making New Video Device Driver Versions Available for Installation	317
Installing Video Device Drivers.....	317
Removing Video Device Drivers	318
FAILOVER SERVERS.....	319
FAILOVER SERVER SERVICE ADMINISTRATION	319
Starting and Stopping the Failover Server Service	319
Changing the Management Server Address	319
Viewing Status Messages	319
Viewing Version Information.....	320
Read Failover Server Service State Icons	320
MANAGE FAILOVER SERVERS.....	321
Installing Failover Servers	322
Adding and Grouping Failover Servers	322
Enabling Failover Servers	324
Editing Failover Server properties	324
Assigning Failover Servers to Recording Servers	326
Frequently Asked Questions	326
Failover-Related Events	327
MAP	328
ABOUT MAPS.....	328
DATABASE CORRUPTION	329
PROTECT DATABASES FROM CORRUPTION.....	329
Power outages: use a UPS.....	329
Windows Task Manager: Be Careful when Ending Processes	329
Hard Disk Failure: Protect Your Drives.....	329



SERVICES ADMINISTRATION	330
ABOUT THE SERVICE CHANNEL	330
MANAGEMENT SERVER SERVICE AND RECORDING SERVER SERVICE	330
Accessing the Server Service	331
Starting the Server Service	331
Stopping the Server Service	331
Changing Recording Server Settings	331
Viewing Status Messages	331
Viewing Version Information.....	332
Work with Recording Server Settings in details	332
Read Server Service State Icons	333
VIRUS SCANNING	334
VIRUS SCANNING INFORMATION.....	334
SNMP	335
SNMP SUPPORT	335
Installing the SNMP Service	335
Configuring the SNMP Service	335
DAYLIGHT SAVING TIME.....	336
DAYLIGHT SAVING TIME	336
Spring: Switch from Standard Time to DST	336
Fall: Switch from DST to Standard Time.....	336
IPv6	338
IPv6 (vs. IPv4).....	338
Important Information if Using XProtect Corporate with IPv6.....	338
How to Write IPv6 Addresses	339
MULTI-DOMAIN WITH ONE-WAY TRUST	341



SETUP WITH ONE-WAY TRUST	341
APPENDIX.....	343
PORTS USED BY XPROTECT CORPORATE	343
INDEX.....	344
ANALYTICS EVENTS • 243, 244, 289.....	ERROR! BOOKMARK NOT DEFINED.



Copyright, trademarks and disclaimer

Copyright

© 2012 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.



Introductions

Product overview XProtect Corporate

XProtect Corporate 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.

XProtect Corporate consists of the following main elements:

- The **management server** - the center of your installation
- One or more **recording servers**
- One or more **Management Clients**, which are unlicensed and can be downloaded and installed for free (as many times as needed).
- A **Download Manager**
- One or more **XProtect Smart Client's** and **Remote Clients**, which are both unlicensed and can be downloaded and installed for free (as many times as needed).

Furthermore, XProtect Corporate includes fully integrated Matrix functionality for distributed viewing of video from any camera on your surveillance system to any computer with an XProtect Smart Client installed.

The system also offers the possibility of including the standalone XProtect Smart Client – Player when exporting video evidence from the XProtect Smart Client. The 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.

Finally, XProtect Corporate handles an unlimited number of cameras, servers, and users—across multiple sites if required. XProtect Corporate is capable of handling IPv4 as well as IPv6 (see "IPv6 (vs. IPv4)" on page 338).

A Typical XProtect Corporate Setup



Example of an XProtect Corporate solution. The number of cameras and recording servers, as well as the number of connected clients, can be as high as you require.

Legend:

1. Management Client(s)
2. Event Server
3. Microsoft Cluster
4. Management Server
5. Management Failover Server



6. SQL Server
7. Failover Recording Server
8. Recording Server(s)
9. XProtect Smart Client
10. IP Video Cameras
11. Video Server
12. Analog Cameras
13. PTZ IP Camera
14. Camera Network
15. Server Network

About Updates

Milestone regularly release service updates for our products, offering improved functionality and support for new devices.

If you are an XProtect Corporate system administrator, it is recommended that you check the Milestone website www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) for updates at regular intervals in order to make sure you are using the most recent version of XProtect Corporate.

The Management Server

What? Stores the surveillance system's configuration in a relational database, either on the management server computer itself or on a separate SQL Server on the network. Also handles user authentication, user rights, etc. To enhance system performance, several management servers can be run as a Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293).

Where? Runs as a service, and is typically installed on a dedicated server.

- **What comes along with the management server?** Furthermore, when installing the management server, you get the following integrated components as well (if you select Typical Management Server Installation (see "Typical" on page 32)):

The event server

- **What?** Stores and handles incoming alarms and map functionality, and receives analytic and generic events from XProtect Corporate servers (and any XProtect Enterprise servers if such are present in a possible federated hierarchy). This enables powerful monitoring and instant overview of alarms and maps and possible technical problems within your systems. If your setup does not have an event server installed, neither of the features mentioned under this bullet will work.
- **Where?** Usually installed on the same server as the management server and runs as a service.

The log server

- **What?** Provides the necessary functionality for logging information from your XProtect Corporate installation.
- **Where?** Usually installed on the same server as the management server and runs as a service.

The service channel

- **What?** Enables automatic and transparent configuration communication between servers and clients in your XProtect Corporate installation.



- **Where?** Usually installed on the same server as the management server and runs as a service.

The Recording Server

What? Used for recording video and for communicating with cameras and other devices. In large installations, more than one recording server is often used on the surveillance system. Failover servers can be set up to take over if a recording server becomes temporarily unavailable.

Where? Recording servers as well as failover servers run as services, and are typically installed on separate servers rather than on the management server itself.

The Management Client

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

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

The Download Manager

What? Lets surveillance system administrators manage which XProtect Corporate -related components (e.g. particular language versions of clients) your organization's users will be able to access from a targeted web page generated by the management server.

Where? Automatically installed on the management server during XProtect Corporate installation process.

The XProtect Smart Client and Remote Client

What? Clients enabling access to live and recorded video as well as other key surveillance system features, such as export of recordings for use as evidence.

Where? Depends on type of client. The very feature-rich XProtect Smart Client must be installed on users' computers. The more basic Remote Client is accessed through a browser, and run directly from the XProtect Corporate management server without the need for any installation.

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



System requirements

IMPORTANT: XProtect Corporate no longer supports Microsoft® Windows® XP (however, clients can still be run/accessed from computers with Windows XP Professional).

For easy user/group management (see "Manage Users and Groups" on page 249), it is recommended to have Microsoft Active Directory® in place before you install XProtect Corporate. If you add the management server to the Active Directory after installing XProtect Corporate, you must re-install the management server, and replace users with new users defined in the Active Directory.

The following are **minimum** requirements for the computers used in an XProtect Corporate solution:

Computer running Management Server

- **CPU:** Intel® Xeon®, minimum 2.0 GHz (Dual Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)
- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 50 GB free (depends on number of servers, cameras, rules, and logging settings)
- **Operating System:** Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Server 2003 (32 or 64 bit).

Furthermore, to run clustering/failover servers, a Microsoft® Windows® Server 2003/2008 Enterprise or Data Center edition is needed.

- **Software:** Microsoft .NET 3.5 SP1 and .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Computer running Recording Server or Failover Server

- **CPU:** Dual Core Intel Xeon, minimum 2.0 GHz (Quad Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)
- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP, or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 100 GB free (depends on number of cameras and recording settings)
- **Operating System:** Microsoft® Windows® 7 Ultimate (32 bit or 64 bit), Microsoft® Windows® 7 Enterprise (32 bit or 64 bit), Microsoft® Windows® 7 Professional (32 bit or 64 bit), Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Vista® Business (32 or 64 bit), Microsoft® Windows® Vista Enterprise (32 or 64 bit), Microsoft® Windows® Vista Ultimate (32 or 64 bit) or Microsoft® Windows® Server 2003 (32 or 64 bit).
- **Software:** Microsoft .NET 4.0 Framework.



IMPORTANT: When formatting the hard disk of a recording/failover server device, 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> (see <http://support.microsoft.com/kb/140365/en-us> - <http://support.microsoft.com/kb/140365/en-us>).

Computer running Management Client

- **CPU:** Intel Core2TM™ Duo, minimum 2.0 GHz
 - **RAM:** Minimum 1 GB
 - **Network:** Ethernet (100 Mbit or higher recommended)
 - **Graphics Adapter:** AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit color
 - **Hard Disk Space:** Minimum 100 MB free
 - **Operating System:** Microsoft® Windows® 7 Professional (32 bit or 64 bit*), Microsoft® Windows® 7 Enterprise (32 bit or 64 bit*), Microsoft® Windows® 7 Ultimate (32 bit or 64 bit*), Microsoft® Windows® Vista Ultimate (32 bit or 64 bit*), Microsoft® Windows® Vista Enterprise (32 bit or 64 bit*), Microsoft® Windows® Vista Business (32 bit or 64 bit*), Microsoft® Windows® Server 2008 (32 bit or 64 bit*), Microsoft® Windows® Server 2008 R2 (64 bit) or Microsoft® Windows® Server 2003 (32 bit or 64 bit*).
- * Running as a 32 bit service/application
- **Software:** Microsoft .NET 4.0 Framework, DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from [http:// www.microsoft.com/downloads/](http://www.microsoft.com/downloads/) (see <http://www.microsoft.com/downloads/> - <http://www.microsoft.com/downloads/>).

Computer running Event Server

- **CPU:** Intel® Xeon®, minimum 2.0 GHz (Dual Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)
- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)
- **Operating System:** Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Server 2003 (32 or 64 bit)
- **Software:** Microsoft .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Computer running Log Server

- **CPU:** Intel® Xeon®, minimum 2.0 GHz (Dual Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)



- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)
- **Operating System:** Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Server 2003 (32 or 64 bit)
- **Software:** Microsoft .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Computer running Service Channel

- **CPU:** Intel® Xeon®, minimum 2.0 GHz (Dual Core recommended)
 - **RAM:** Minimum 1 GB (2 GB or more recommended)
 - **Network:** Ethernet (1 Gbit recommended)
 - **Graphics Adapter:** Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
 - **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
 - **Hard Disk Space:** Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)
 - **Operating System:** Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit)*, Microsoft® Windows® Server 2003 (32 or 64 bit)*
- * Limited by Windows operating system to ten concurrent, incomplete outbound TCP connection attempts
- **Software:** Microsoft .NET 4.0 Framework, and Internet Information Services (IIS) 5.1 or newer

If installing on Windows Server 2008, a standard IIS installation must furthermore be customized:

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**.

Computer running XProtect Smart Client

- **CPU:** Intel Core2 Duo, minimum 2.0 GHz (Quad Core recommended for larger views)
- **RAM:** Minimum 512 MB (1 GB recommended for larger views, 1 GB recommended on Microsoft Windows Vista®)
- **Network:** Ethernet (100 Mbit or higher recommended)
- **Graphics Adapter:** AGP or PCI-Express, minimum 1280 x 1024, 16 bit colors
- **Hard Disk Space:** Minimum 500 MB free
- **Operating System:** Microsoft® Windows® 7 Professional (32 bit or 64 bit*), Microsoft® Windows® 7 Enterprise (32 bit or 64 bit*), Microsoft® Windows® 7 Ultimate (32 bit or 64 bit*), Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Vista Ultimate (32 bit or 64 -bit*), Microsoft® Windows® Vista Enterprise (32 bit or 64 bit*), Microsoft® Windows® Vista Business (32 bit or 64 bit*), Microsoft® Windows® Server 2008, Microsoft® Windows® Server 2003 (32 bit or 64 bit*), and Microsoft® Windows® XP Professional (32 bit or 64 bit*).

*Running as a 32 bit service/application

- **Software:** Microsoft .NET 4.0 Framework, DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from [http:// www.microsoft.com/downloads/](http://www.microsoft.com/downloads/) (see <http://www.microsoft.com/downloads/> - <http://www.microsoft.com/downloads/>).

Computer accessing Remote Client

- **CPU:** Intel Pentium® 4, minimum 2.4 GHz
- **RAM:** Minimum 256 MB (512 MB recommended for larger views, 1 GB recommended on Microsoft Windows Vista)
- **Network:** Ethernet (100 Mbit or higher recommended)
- **Graphics Adapter:** AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit color
- **Hard Disk Space:** Minimum 10 MB free
- **Operating System:** Microsoft® Windows® 7 Professional (32 bit or 64 bit*), Microsoft® Windows® 7 Enterprise (32 bit or 64 bit*), Microsoft® Windows® 7 Ultimate (32 bit or 64 bit*), Windows Vista Ultimate (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*), Windows Vista Business (32 bit or 64 bit*), Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008, Windows Server 2003 (32 bit or 64 bit*), and Microsoft Windows® XP Professional (32 bit or 64 bit*)

* Running as a 32 bit service/application

- **Software:** DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from [http:// www.microsoft.com/downloads/](http://www.microsoft.com/downloads/) (see <http://www.microsoft.com/downloads/> - <http://www.microsoft.com/downloads/>).



Active Directory

XProtect Corporate users are normally added from Active Directory, although users can also be added 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.

If wishing 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.

Clients overview

Working with clients

Users can access an XProtect Corporate surveillance system with two different clients. Both clients are unlicensed and can be downloaded and installed (a many times as needed) for free:

- The Smart Client is very feature-rich and flexible for future integration of plugins, etc. The Smart Client must be installed on users' computers.
- The Remote Client has a more basic feature set. Its main benefit is that it is accessed through a browser, and run directly from the XProtect Corporate management server without the need for any client installation on the user's computer.

Both clients are included in the XProtect Corporate solution.

View examples of the two clients



Examples of user interfaces: XProtect Smart Client (left) and Remote Client (right)

Which client should I choose?

Which clients to use in your organization depends on your organization's needs. Note, however, that the two clients can easily be used alongside each other: There is no problem in some of your users using the XProtect Smart Client and others using the Remote Client.

Both clients provide access (user rights permitting) to key surveillance system features such as live and recorded video, control of PTZ cameras and export of recordings for use as evidence. But if you want support for multiple screens, audio, digital zoom, intelligent browsing of recordings, etc., the XProtect Smart Client should be your choice.

The following table outlines the main differences between the two clients:



Clients at a Glance	Smart Client	Remote Client
User's Installation	Client must be installed on user's computer.	None; client is accessed from server through a browser.
User's Feature Set	Very feature-rich.	Basic features.
User's Ease of Use	Very easy to use. Setup of views can be handled locally as well as centrally. With central views handling, remote users can begin using their client upon first login.	
System Administrator's Installation	None required, although the administrator would in most cases install an XProtect Smart Client on his/her workstation.	None.
System Administrator's Feature Set	Very flexible configuration through the Management Client; options include handling of local IP address ranges, NAT, multicasting, etc.	Configuration through the Management Client.
System Administrator's Access Control Options	Users and their access rights are set up as part of roles definition process in the Management Client.	
Flexibility re. Future Features and Plugins	Offers a high degree of flexibility for integration of new features, plugins, etc.	Limited.
Recommended Use	Users who require audio. Users who require access to the latest features. Users who demand a high degree of flexibility re. use of plugins. Users who do not wish to install client software.	Users who find that a .NET-based client solution is not desirable.

How to connect to the surveillance system?

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

How do I set up users and their rights?

You set up your surveillance system's users, and their access rights, as part of the roles (see "Manage Roles" on page 251) definition process in the XProtect Corporate Management Client.

Where can I find more information?

See XProtect Smart Client Introduction (see "Installing the XProtect Smart Client" on page 22) and Remote Client Introduction (see "Remote Client" on page 24) respectively.



Installing the XProtect Smart Client

The XProtect Smart Client provides remote users with extremely feature-rich access to the surveillance system and enables them to view live and recorded video and to access other features from the system. Like XProtect Corporate, the XProtect Smart Client supports IPv6 (see "IPv6 (vs. IPv4)" on page 338).



Example of the XProtect Smart Client, in this case displaying live video

Where can I find more information about the XProtect Smart Client? Once installed, the XProtect Smart Client has its own built-in help system. Alternatively, refer to the XProtect Smart Client User's Manual, available on the XProtect Corporate software DVD as well as from www.milestonesys.com.

The XProtect Smart Client must be installed locally on the remote user's computer, which can be done in three different ways. Naturally it can also subsequently be removed.

Installing the XProtect Smart Client from server or DVD

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements (on page 16).

Downloading and Installing from the Surveillance System Server (Typical Method)

1. Open an Internet Explorer browser (version 6.0 or later), and connect to surveillance system server at the URL or IP address specified by your system administrator. The address is typically:

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

When you are connected to the surveillance system server, you will see a welcome page.

2. On the welcome page, click the required language link for the XProtect Smart Client.

Installing from the XProtect Corporate software DVD (Alternative Method)

3. Insert the surveillance system software DVD, wait for a short while, select required language, then click the **Install Milestone XProtect Smart Client** link.

Tip: Depending on your security settings, you may receive one or more security warnings (**Do you want to run or save this file?**, **Do you want to run this software?** or similar; exact wording depends on your browser version). When this is the case, accept the security warnings (by clicking **Run** or similar; exact button names depend on your browser version).

2. The **XProtect Smart Client Setup** wizard begins. In the wizard, click **Next**, and follow the installation instructions.



Installing the XProtect Smart Client silently

For surveillance system administrators, it is possible to deploy the XProtect Smart Client to users' computers using tools such as Microsoft Systems Management Server (SMS). Such tools let administrators 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 the XProtect Smart Client, over local networks.

In order to be able to deploy the XProtect Smart Client this way, it is necessary to make an installation package for a so-called silent installation, i.e. an installation which does not require end users to be actively involved. To make the installation package, do the following:

You cannot complete the following procedure if you already have an XProtect Smart Client installed; in that case, remove your existing XProtect Smart Client before completing this step.

1. Locate the self-extracting XProtect Smart Client installation file **MilestoneXProtectSmartClient.exe**.

You find the file in a folder located under the Milestone surveillance software installation folder (typically **C:\Program Files\Milestone\XProtect Corporate Management Server\Clients\Binary\Client**).

2. With an extraction tool, such as WinZip® or similar, extract the files contained in **MilestoneXProtectSmartClient.exe** to a folder of your choice.
3. Make a response file for the silent installation:
 - a) Open a command prompt.
 - b) With the command prompt, call the file **setup.exe** (located in the folder to which you extracted **MilestoneXProtectSmartClient.exe**) with the parameter **/r**.

This will start the XProtect Smart Client installation and record your subsequent actions in a response file, which you will later use when deploying the XProtect Smart Client to end users.

- c) Go through the entire XProtect Smart Client installation.
 - d) Exit the command prompt.
4. The response file, called **Setup.iss** will be stored in your computer's Windows folder (example: **C:\WINDOWS** (or **C:\WINNT** if running Windows NT)). Copy the response file to the folder to which you extracted **MilestoneXProtectSmartClient.exe**.
 5. Based on the content of the folder to which you extracted **MilestoneXProtectSmartClient.exe** (i.e. all the original files as well as the newly created response file **Setup.iss**), create a new self-extracting file.

The new self-extracting file should use the following command after unzip: **Setup.exe /s**

6. Use the new self-extracting file when deploying the XProtect Smart Client through your systems management tool.

Removing the XProtect Smart Client

To remove an XProtect Smart Client, do the following on the computer where it is installed:

1. In Windows' **Start** menu, select **Control Panel**, and select **Add or Remove Programs**. This will open the **Add or Remove Programs** window.
2. In the **Add or Remove Programs** window's list of currently installed programs, select **Milestone XProtect Smart Client x.x** (where x.x refers to the version number).
3. Click **Remove**, and follow the removal instructions.



Remote Client

The Remote Client provides users with basic access to the surveillance system. The Remote Client does not offer nearly as many features as the XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22). The main benefit of the Remote Client is that it is installed on (see "System requirements" on page 16), and runs directly from, the XProtect Corporate management server, and is accessed through a browser. This eliminates the need for installing any client software on the user's computer.



Example of the Remote Client, in this case displaying video from 16 cameras

Where can I find more information about the Remote Client? Refer to the Remote Client User's Manual, available on the XProtect Corporate software DVD as well as from www.milestonesys.com.

Accessing the Remote Client

1. Open an Internet Explorer browser (version 6.0 or later), and connect to the surveillance system server at the URL or IP address specified by your system administrator. The address is typically:

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

2. When you connect to the management server, you will see a welcome page. On the welcome page, click the Remote Client link in order to view the Remote Client login dialog.
3. To log in, specify information in the fields:

- **Previous Logins:** Only available if you have logged in before. Lets you reuse previously specified login details (except any password, which you must always type yourself). This can greatly speed up the login process.
- **Address:** Type the URL or IP address of the management server, as specified by your system administrator.



- **Port:** Internet connections may use different ports for different purposes. Specify the port number to use when logging in to the Remote Client. In most circumstances, port 80 is used.
- **Authentication:** Select required authentication method.

Windows (current user), with which you will be authenticated through your current Windows login, and do not have to specify any user name or password. This is the default authentication method, i.e. the method which is automatically used unless you select another method.

Windows, with which you will be authenticated through your Windows login, but you will need to type your Windows user name and password.

Basic, not used when connecting to an XProtect Corporate surveillance system.

- **User name:** Type your user name. The user name is case-sensitive, i.e. there is a difference between typing, for example, amanda and Amanda.
 - **Password:** Type your password. The password is case-sensitive.
4. Click the **Login** link. After a short wait, you get access to the Remote Client. Content in the Remote Client is grouped on three tabs: **Live**, **Browse** and **Setup**.



The **Live** tab is used for viewing live video from cameras, the **Browse** tab is used for finding and playing back recorded video, and the **Setup** tab is used for configuring the Remote Client.

Navigating the Built-in Help System (online)

You are always able to freely navigate between the help system's contents. To do this, simply use the help window's three tabs: **Contents**, **Search**, and **Glossary**, or use the links inside the help topics.



- **Contents Tab:** Lets you navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer. To go straight to the help system's **Contents** tab, click **Contents...** button in the Management Client's toolbar.
- **Search Tab:** Lets you search for help topics containing particular terms of interest. For example, you can search for the term **zoom** and every help topic containing the term **zoom** will be listed in the search results. Clicking a help topic title in the search results list will open the required topic. To go straight to the help system's **Search** tab, click the **Search...** button in the Management Client's toolbar.
- **Glossary Tab:** What is a video encoder? What does PTZ mean? The **Glossary** tab provides a glossary of common surveillance and network-related terms. Simply select a term to view a corresponding definition in the small window below the list of terms.

Links in Help Topics

The actual content of each help topic is displayed in the right pane of the help window. Help topic texts may contain various types of links, notably so-called expanding drop-down links.

Clicking an expanding drop-down link will display detailed information. The detailed information will be displayed immediately below the link itself; the content on the page simply expands. Expanding drop-down links thus help save space.



Example This is an example of text shown below an expanding drop-down link. To hide this text, simply click the expanding drop-down link again.

Printing Help Topics



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

Tip: When printing a selected help topic, the topic will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links, click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you require.

Browsers supported

The following browsers support the built-in help system (recent versions only):

- Internet Explorer
- Mozilla Firefox
- Safari.



Installation and removal

Installation Overview

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from previous version" on page 52).

If you plan to run **Milestone Federated Architecture** (on page 293), make sure to read about important prerequisites for running Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293).

Your XProtect Corporate installation process begins with the installation of the management server software.

- The **management server** is the center of your XProtect Corporate installation. It is typically installed on a dedicated server. See Management Server Installation (see "Install management server" on page 28).

Once the management server is installed, you are able to install key components required by the management server:

- The **recording server**, which is used for recording video feeds, and for communicating with cameras (via video device drivers (see "Manage and Remove Video Device Drivers" on page 317)) and other devices. The recording server is typically installed on one or more separate computers, rather than on the management server itself. See Install System Components (on page 34).
- The **Management Client**, which is used for configuration and day-to-day management of the system. The Management Client is typically installed on the system administrator's workstation or similar. See Management Client Installation (see "Management client" on page 40).

Finally, you are able to install client software for access to the XProtect Corporate system:

- The XProtect Smart Client is the feature-rich client used for access to live and recorded video and other features from the surveillance system. The XProtect Smart Client client software must be installed on users' computers. See Install and Remove XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22) for more information.
- Alternatively, the Remote Client lets you avoid installing client software, as the Remote Client is run straight from the XProtect Corporate system through a browser. It does, however, have significantly fewer features than the XProtect Smart Client. See Remote Client Introduction (see "Remote Client" on page 24).

Tip: Video device drivers are small programs used for controlling/communicating with the cameras connected to a recording server. You get the drivers automatically during the initial installation of your XProtect Corporate system. However, new versions of the drivers are released from time to time.

As well on traditional servers, installation can also take place on virtualized servers.

Installing XProtect Corporate on virtual servers

As mentioned, it is possible to run all XProtect Corporate components on virtualized Windows® servers, such as - for example - VMware® and Microsoft Hyper-V®. Contact your IT department for more information.

Tip: 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, XProtect Corporate recording servers record all cameras and streaming video. This puts high load on CPU, memory, network, and storage system. Thus when run on a virtual server, the normal gain of virtualization disappears to a large extent, since - in many cases - it will use 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.

Install management server

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from previous version" on page 52).

If you plan to run **Milestone Federated Architecture**, make sure to read about important prerequisites for running Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293).

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of XProtect Corporate.

Note that if you run workgroups you should ignore the normal installation guidelines and use the alternative method indicated below.

Alternative method for installing management server in workgroups

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, 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 XProtect Corporate systems you want to connect. They must all be installed using a common administrator account.

Your XProtect Corporate installation process begins with the installation of the XProtect Corporate management server software. The management server is the center of your XProtect Corporate installation.

Prerequisites

- **Windows Installer 4.5 - only on Windows Server 2003**

Before installing XProtect Corporate, it is important that you install Windows Installer 4.5. You can download the Windows Installer 4.5 (see <http://www.microsoft.com/downloads> - <http://www.microsoft.com/downloads>) from this link: <http://www.microsoft.com/downloads> (see <http://www.microsoft.com/downloads/> - <http://www.microsoft.com/downloads/>).

- **SQL Server**

The management server requires access to a relational database. Later in this installation process you must choose between using an existing SQL Server on the network (**Administrator rights** on the SQL Server are required) or setting up a SQL Server Express Edition (a lightweight, yet powerful, version of a full SQL server) on the management server computer itself.

Whatever SQL solution you choose, make sure to have Microsoft .NET Framework 3.5 Service Pack 1 installed on the management server computer running the SQL Server Express Edition (even though Microsoft .NET Framework 4.0 is already installed) or the separate server running the existing SQL Server. See also System Requirements (on page 16).



Which SQL Server type is right for our organization? The SQL Server Express Edition is easy to install and prepare for use, and will often suffice for systems with less than 500 cameras. However, if you plan to perform frequent/regular backups of your database, using an existing SQL Server on the network is recommended (**Administrator rights** on the SQL Server are required). For large installations, such as installations with 500 cameras or more, using an existing SQL Server on the network is always recommended.

- **Windows Server 2003 Fix**

If you use Windows Server 2003 it is recommended to install this supported fix (see <http://support.microsoft.com/kb/925336> - <http://support.microsoft.com/kb/925336>) for Windows Server 2003 before starting: <http://support.microsoft.com/kb/925336> (see <http://support.microsoft.com/kb/925336> - <http://support.microsoft.com/kb/925336>). Otherwise, the installation of your management server might fail due to Microsoft Windows Installer process having insufficient contiguous virtual memory to verify that the .msi package or the .msp package is correctly signed.

Installing

1. Shut down any Milestone software running. If upgrading, it is highly recommended that you remove any previous versions of the management server before upgrading. Note, however, that you may not want to remove the management server database, as it contains your XProtect Corporate configuration.
2. Insert the XProtect Corporate software DVD. If the **XProtect Corporate Management Server Installation** window does not open automatically upon inserting the DVD, run the following file from the DVD:

setup.exe

Tip: Alternatively, if you are installing a version downloaded from the internet, run the **setup.exe** file from the location you have saved it to.

3. A window will open, listing the steps involved in the installation:



4. Complete the steps outlined in the window.

Tip: Depending on what is already installed on the computer which is going to act as management server, you may not need to complete all of the window's three steps. The step that currently requires your attention will be highlighted.

Tip: When the management server software is installed, you are able to check the state of the management server by looking at the management server icon in the management server computer's notification area.

See Management Server Service and Recording Server Service (on page 330) for more information.



Alternative for workgroups

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, 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 XProtect Corporate systems you want to connect. They must all be installed using a common administrator account.

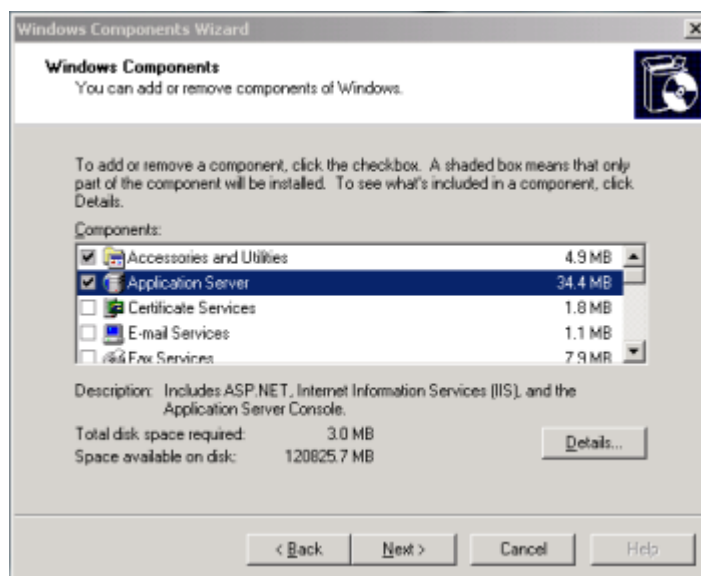
Step 1: Internet Information Services

XProtect Corporate Management Server Installation automatically detects if Internet Information Services (IIS) is already installed. If this step is not available, it is simply because IIS is already installed.

Internet Information Services includes a range of administrative features for managing web servers and web applications, and is required in order to run an XProtect Corporate management server.

If installing on a server running Windows 2008 Server, IIS is automatically installed once you click the **Internet Information Services** step (should automatic installation fail, it is possible to do installation troubleshooting (on page 55)).

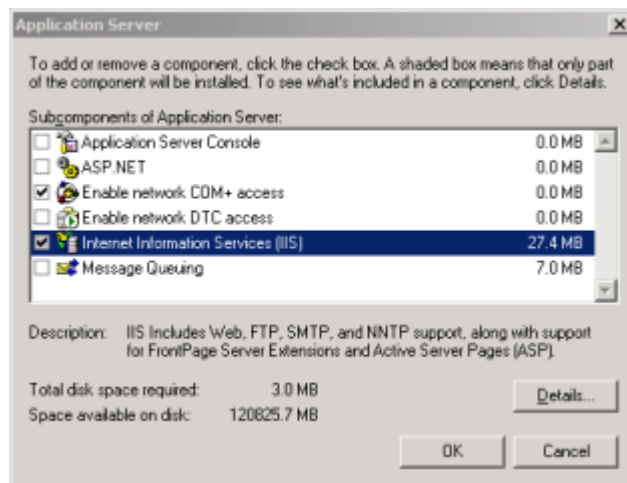
1. On Windows Server 2003, clicking the **Internet Information Services** step opens Windows' built-in **Windows Components** wizard:



2. In the wizard's **Components** list, select **Application Server**.



Click **Details...** and select **Internet Information Services (IIS)**.



3. Click **Details...** and verify that all IIS subcomponents are selected. Click **OK** to return to the **Windows Components** wizard.
4. In the **Windows Components** wizard, click **Next** and follow the wizard.

Tip: It is a good idea to have your Windows installation DVD ready; it may be required during the process.

When IIS is installed, you will be returned to the **XProtect Corporate Management Server Installation** window for the next step of the installation.

Step 2: XProtect Corporate management server database

Before completing this step, click the **View Microsoft SQL Server 2008 Express End-user License Agreement** link to read the license agreement for the software.

This step opens the **Database Setup** wizard, which will guide you through the process of preparing a database for use with the management server.

In the **Database Setup** wizard you will get the choice of using an existing SQL Server on the network or setting up a SQL Server Express Edition (a lightweight, yet powerful, version of a full SQL server) on the management server computer itself.

Follow the wizard's steps by clicking **Next**.

IMPORTANT: We recommend 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 will prevent low disk performance.

IMPORTANT: During the database preparation process, you will be asked whether you want to create a new database, use an existing database, or overwrite an existing database. For a new installation, you would typically select the default option **Create new database**. However, if you are installing the database as part of upgrading to a newer version of XProtect Corporate, and you want to use your existing database, make sure you select **Use existing database**.

When you have prepared the database, you will be returned to the **Milestone XProtect Corporate Management Server Installation** window for the last step in the management server installation.



Step 3: XProtect Corporate management server

This step opens a wizard, which will guide you through the process of installing the management server software itself.



Opening page in Management Server Setup wizard

Follow the wizard's steps by clicking **Next**.

Tip: The wizard will ask you to specify the location of your temporary license (.lic) file. The system will verify your license file before you are able to continue. Therefore, have your license file ready.

On one of the wizard's steps, you will be asked to select between two installation options:

Typical (on page 32)

- or -

Custom (on page 32)

You install the XProtect service channel, XProtect event server and XProtect log server as part of the management server installation. But if required you can just as well install these on another server in your surveillance system:

- Installing the XProtect service channel (see "Install the Service Channel" on page 42) enables automatic and transparent configuration communication between servers and clients in your XProtect Corporate installation.
- Installing the XProtect event server (see "Install event server and log server (custom)" on page 40) enables handling alarms and maps. Maps provide a physical overview of your surveillance system: Which cameras are placed where, and in what direction are they pointing? As mentioned it does not necessarily have to be installed on the management server - in fact, you can often achieve better performance by installing the event server on another server.
- Installing the XProtect log server (see "Install event server and log server (custom)" on page 40) provides the necessary functionality for logging information from your XProtect Corporate installation.

Typical

If you select **Typical** installation, the wizard will install all the management server components at their default location and with other default settings. A Typical installation is recommended for most users.

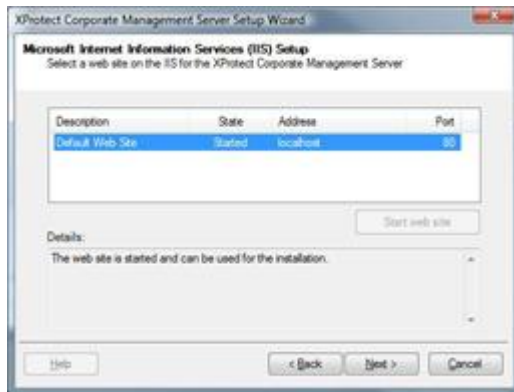
Custom

If you select **Custom** installation, you get the option to select where to install each individual management server component. A **Custom** installation is recommended for advanced users.



Only relevant if selecting **Custom** installation:

On one of the wizard's steps you will be asked to select an IIS (Internet Information Services) web site for the Management Server service:



Select one of the listed web sites, and make sure the selected web site is started, then click **Next**. If the selected web site is not started, **Next** is disabled.

Tip: You may find that only a single IIS web site—the Default Web Site—is listed. In that case simply make sure that the web site is started, then click **Next**.

Towards the end of the wizard, in the **Service Log On Setup** window, you will be asked to select a user account under which the Management Server service will run:



You will be able to select either a:

- predefined Network Service account (see "Select a Predefined Account; Network Service" on page 33) (in which case the service will run whenever the computer acting as management server is running).
- or -
- particular user account (see "Select a Particular User Account" on page 34) (in which case the service will use the specified user account to log in to the computer acting as management server).

Tip: If the computer acting as management server is a member of a domain, you should either select **Network Service**, or make sure that you specify a user account which belongs to the domain in question.

Select a Predefined Account; Network Service

1. Select **This predefined account**.
2. Select **Network Service**.
3. Click **OK**.



Select a Particular User Account

1. Select **This account**.
2. Click **Browse....** This will open the **Select User** window.
3. In the **Select User** window, verify that the required domain is specified in the **From this location** field. If not, click **Locations...** to browse for the required domain.
4. In the **Enter the object names to select** box, type the required user name.

Tip: Typing part of a name is often enough. Use the **Check Names** feature to verify that the name you have entered is recognized.

5. Click **OK**.
6. Specify the password for the user account in the **Password** field, and confirm the password in the **Confirm password** field.

The password fields must not be empty; the password for the account must contain one or more characters and/or digits.

7. Click **OK**.

What's next?

Upon installation of the management server software, the management server's built-in web page automatically opens in a browser. The web page lets you install key components required by the management server, among these:

- One or more **recording servers** (for recording video feeds and for communicating with cameras and other devices)
- A **Management Client** (for configuration and day-to-day management of the system)

Even though the web page opens automatically on the management server computer, you will in most cases want to install the key components on other computers than the management server itself. This is no problem since installation takes place through the web page, which can easily be accessed from other computers. See *Install System Components* (on page 34) for further information.

Install system components

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from previous version" on page 52).

Installation of the following components is **not** covered in this section: XProtect event server, XProtect log server (see "Install event server and log server (custom)" on page 40), management server (see "Install management server" on page 28) and XProtect service channel (see "Install the Service Channel" on page 42). See installation details for each.

Read the **End User License Agreement** on the Product License Sheet (enclosed with the software DVD) before installing any part of Milestone XProtect Corporate.

IMPORTANT: As a prerequisite make sure of the following. During the installation process you will be asked to specify a user account under which the **Failover Server service** will run. For the failover solution to work, the failover server has to use the same user account as the recording server. Furthermore, the user account you specify must have access to your XProtect Corporate system with administrator rights. **Do the following to make sure of this...**



To verify whether the user account has administrator access to your XProtect Corporate system, do the following:

1. In the Management Client's Site Navigation pane, expand Security and select **Roles**. In the overview pane's roles list, select the **Administrators** role.
2. In the properties pane's role settings list, verify that the required user is listed.
3. If the user is not listed, add the required user (see "Assign and Remove Users and Groups to/from Roles" on page 254) to the Administrators role by clicking **Add...** below the role settings list.

Note that if you run workgroups you should ignore the normal installation guidelines for installing recording servers and use the alternative method indicated below.

Alternative method for installing recording server(s) in workgroups

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, 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 XProtect Corporate systems you want to connect. They must all be installed using a common administrator account.

Part I—Downloading the installer

The following describes the installation process. The process is more or less similar for the component types mentioned, so replace **the component** with **the XProtect Corporate recording server**, **failover server** or **the Management Client**, depending on your needs.

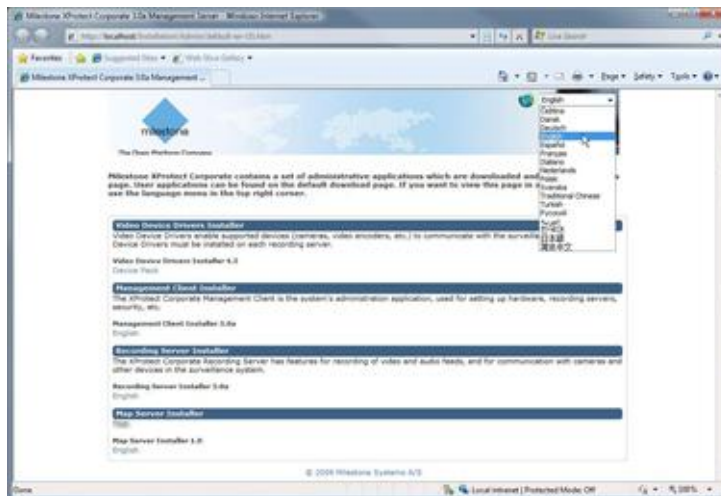
1. On the computer on which you will install the component, shut down any Milestone software running. If upgrading, it is highly recommended that you remove (see "Remove system components" on page 51) any previous versions of the component before upgrading.
2. With an Internet Explorer browser, connect to the XProtect Corporate management server at the following address:

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.



This will open the management server's built-in web page. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.



3. The web page is available in a number of different languages. In this example, we assume that you view the web page in English, and that you want to install English versions of the Milestone XProtect Corporate components.

On the web page find the relevant component's installer section, and then click the **English** link under the required recording server version (often, only one version will be available).

Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking **Run** or similar (exact button text depends on your browser version).

Part II—Installing the component

Select the relevant component for a description of the process (if required, repeat the process on other computers where the component should be installed):

Recording servers

1. This will open the XProtect Corporate **Recording Server Setup** wizard, which will guide you through the installation.

On the first step of the wizard, click **Next**.

2. Select installation method:

Typical (see "Recording servers (Typical)" on page 37)

- or -

Custom (see "Recording servers (Custom)" on page 37)

3. Click **Install**.
4. On the last step of the wizard, click **Finish**. The recording server is now installed. The recording server has no user interface as such; it is accessed and managed through the Management Client.

Tip: When the recording server software is installed, you are able to check its state.



See Management Server Service and Recording Server Service (on page 330) for more information.

Recording servers (Typical)

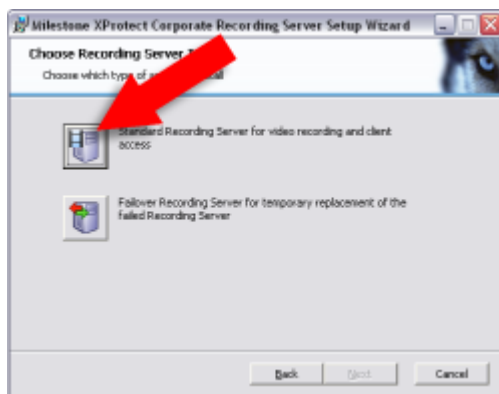
The **Typical** option installs the XProtect Corporate recording server with default settings. A **Typical** installation is recommended for most users.

1. Specify recording server setup parameters (see "Specify recording server setup parameters" on page 40).
2. Click **Next**.

Recording servers (Custom)

The **Custom** option lets you select where to install the XProtect Corporate recording server components. A **Custom** installation is recommended for advanced users.

1. Select required installation folder, then click **Next**.
2. When asked which type of server to install, click the **Standard recording server [...]** icon. This lets you install a regular recording server.



3. Specify recording server setup parameters.
4. Click **Next**.
5. The wizard will ask you to select a user account under which the Recording Server service will run.

You must select between:

- a predefined system account (see "Select a Predefined System Account" on page 38)
- or -
- a particular user account (see "Select a Particular User Account" on page 38) (in which case the service will use the specified user account to log in to the computer acting as recording server).

Tip: If the computer acting as recording server is a member of a domain, select the predefined account Local System or make sure you specify a user account which belongs to the domain in question.

If using network drives, you should always specify a particular user account (which has access to the network drives in question), as the Recording Server service will not be able handle the network drives otherwise.



6. Click **Next**.
7. In some cases it can be advantageous to install more than one instance of the recording server on the same physical server (see "Multiple recording server instances" on page 50). Specify the required number of instances (default is 1), then click **Next**.
 - Only relevant if installing more than one instance of the recording server on the same physical server: For each instance, specify the IP address to use for the instance in question.

IMPORTANT: Note that the IP addresses you specify must be assigned to the physical server in question. Furthermore, even though your organization will not use IPv6 addresses, make sure to assign both IPv6 and IPv4 on the server as these are needed by the software.

Tip: Provided enough IP addresses are assigned to the server, the fields will be pre-filled.

8. Click **Next**.

Select a Predefined System Account

1. Select **This predefined account**.
2. Select **Local System**, **Local Service**, or **Network Service** as applicable.
3. Click **OK**.

Select a Particular User Account

1. Select **This account**.
2. Click **Browse....** This will open the **Select User** window.
3. In the **Select User** window, verify that the required domain is specified in the **From this location** field. If not, click **Locations...** to browse for the required domain.
4. In the **Enter the object names to select** box, type the required user name.

Tip: Typing part of a name is often enough. Use the **Check Names** feature to verify that the name you have entered is recognized.

5. Click **OK**.
6. Specify the password for the user account in the **Password** field, and confirm the password in the **Confirm password** field.

The password must contain one or more characters and/or digits.

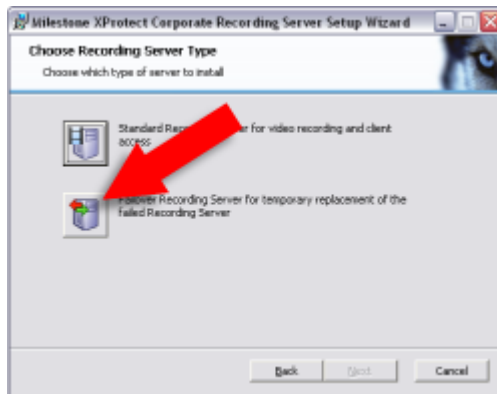
7. Click **OK**.

Failover servers

1. This will open the XProtect Corporate **Recording Server Setup** wizard, which will guide you through the installation
On the first step of the wizard, click **Next**.
2. Select installation method **Custom**.
3. Select required installation folder, and then click **Next**.

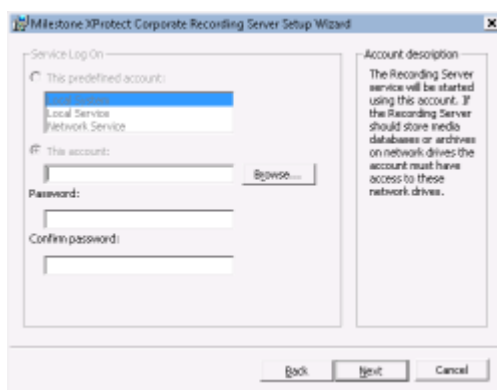


4. When asked which type of server to install, click the **Failover recording server for temporary** [...] icon.



5. Specify failover server setup parameters (see "Specify recording server setup parameters" on page 40).
6. Click **Next**.
7. A failover server has two services:
 - A Failover Server service, which handles the processes of taking over from the regular recording server.
 - A Recording Server service, which enables the failover server to act as a recording server while the regular recording server is unavailable.

The wizard will ask you to select a particular user account under which the services will run. Make your selection.



See Select a Particular User Account... (see "Select a Particular User Account" on page 38) for how to select.

For the failover solution to work, the user account you specify must have access to your XProtect Corporate system with administrator rights. If the computer acting as failover server is a member of a domain, make sure you specify a user account which belongs to the domain in question. If using network drives, always specify a user account which has access to the network drives in question.

8. Click **Install**.
9. On the last step of the wizard, click **Finish**. The failover server is now installed. The failover server has no user interface as such; it is accessed and managed through the Management Client.

When the failover server software is installed, you are able to check its state. See Management Server Service and Recording Server Service (on page 330) for more information.



Management client

1. In the **Select installer language** drop down box, select language to use during the installation. In this example, we assume that you prefer English.
2. Next to appear is the XProtect Corporate **Management Client Setup** wizard, which will guide you through the installation process. On the first step of the wizard, click **Next**.
3. Select required installation folder, then click **Next**.
4. Click **Install** to begin installation; wait while the required components are installed.
5. When ready, click **Finish**.
6. To get an overview of the Management Client (see "Management Client Overview" on page 66), select **Launch XProtect Corporate Management Client**. This will start the Management Client right away.

Specify recording server setup parameters

- **Name:** A name for the server in question. If required, you can later change the name through the XProtect Corporate Management Client.
- **Milestone XProtect Corporate management server:** The IP address (example: 123.123.123.123) or host name (example: ourserver) of the management server to which the server in question should be connected. If required, you can later change the management server IP address/host name as part of the basic administration on the Recording or Failover Server service.
- **MediaDB:** The path to the server in question's media database. The media database is the recording server's default storage area, i.e. the default location in which recordings from connected cameras are stored in individual camera databases. If required, you can later change the path, and/or add paths to more storage area locations, from the XProtect Corporate Management Client.

When should I choose a particular user account instead of a predefined? If using network drives you should always specify a particular user account (with access to the network drives in question). Otherwise the service in question is unable to handle the required network drives.

Install event server and log server (custom)

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from previous version" on page 52).

Installation of the following components are **not** covered in this section: recording servers, failover servers, Management Client (see "Install system components" on page 34), management server (see "Install management server" on page 28) and XProtect service channel (see "Install the Service Channel" on page 42). See installation details for each.

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of XProtect Corporate.

Learn more about the event server and the log server (see "The Management Server" on page 14).

Normally, the XProtect event server and XProtect log server are both installed as part of the Management Server Installation (see "Install management server" on page 28), when installed with the **Typical** option. The following describes how to make a custom installation of the XProtect event server and/or the XProtect log server, when these are not installed as part of the **Typical** management server installation.

The XProtect event server and the XProtect log server can be installed either on the management server or on any other computer.



Make sure that user rights are set up correctly in the operating system. You can read about user rights in the operating system on Microsoft's web site_ ([http://technet.microsoft.com/en-us/library/cc794944\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc794944(WS.10).aspx)) (see [http://technet.microsoft.com/en-us/library/cc794944\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc794944(WS.10).aspx) - [http://technet.microsoft.com/en-us/library/cc794944\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc794944(WS.10).aspx)).

Installing event server and log server

The following describes the installation process (custom Installation). The process is more or less similar for the two server types, so replace the server with XProtect event server or XProtect log server depending on your needs.

1. On the computer on which you will install the server, shut down any Milestone software running. If upgrading, it is highly recommended that you remove (see "Remove system components" on page 51) any previous versions of the server before upgrading.
2. Download the relevant server's installer from the management server's built-in web page at the address

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

On the web page find the servers' installer section, and then click the **English** link. Note that depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking **Run** or similar (exact button text depends on your browser version).

3. Run the installation file, either directly or from the location you saved it to. Follow the on-screen installation guide.
4. Verify/specify the required installation path and click **Next**.
5. Select the relevant server type:

Event Server

- Specify the URL address of the XProtect Corporate management server (example: <http://123.123.123.123>). If installing the server on the management server itself, simply specify localhost and click **Next**.
- Select the database to be used and click **Next**.
- Select the web site on which you want to install and click **Next**.

Log Server

- Select the database to be used by the log server and click **Next**.
 - Select the web site on which you want to install and click **Next**.
 - Specify the URL address of the XProtect Corporate management server (example: <http://123.123.123.123>). If installing the server on the management server itself, simply specify localhost and click **Next**.
6. Specify a user account under which the server's service will run. The specified user is automatically granted administrator rights in XProtect Corporate, see Specify the Rights of a Role (see "Specify Rights of a Role" on page 256).

You must select between:



- a predefined Network Service account (see "Select a predefined network service account" on page 42)(in which case the service will run whenever the computer acting as management server is running).

-or -

- a particular user account (see "Select a particular user account" on page 42) (in which case the service will use the specified user account to log in to the computer acting as recording server).

When should I choose a particular user account instead of a predefined? If using network drives you should always specify a particular user account (with access to the network drives in question). Otherwise the service in question is unable to handle the required network drives.

7. Click **Install**. When installation is complete, click **Finish**.

Select a predefined network service account

1. The Network Service account is selected by default.
2. Click **OK**.

The Network Service account must be added as a Windows user on the relevant recording server computers in your surveillance system in order to retrieve status information from these recording servers.

Select a particular user account

1. Select **This account**.
2. Click **Browse....** This will open the **Select User** window.
3. In the **Select User** window, verify that the required domain is specified in the **From this location** field. If not, click **Locations...** to browse for the required domain.
4. In the **Enter the object names to select** box, type the required user name.

Tip: Typing part of a name is often enough. Use the **Check Names** feature to verify that the name you have entered is recognized.

5. Click **OK**.
6. Specify the password for the user account in the **Password** field, and confirm the password in the **Confirm password** field.

The password must contain one or more characters and/or digits.

7. Click **OK**.

Install the Service Channel

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from previous version" on page 52).

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of XProtect Corporate.

The XProtect service channel is installed as part of the Management Server Installation (see "Install management server" on page 28), when the management server is installed with the **Typical** option. The following describes how to make a custom installation of the service channel, when the service channel is not installed as part of the



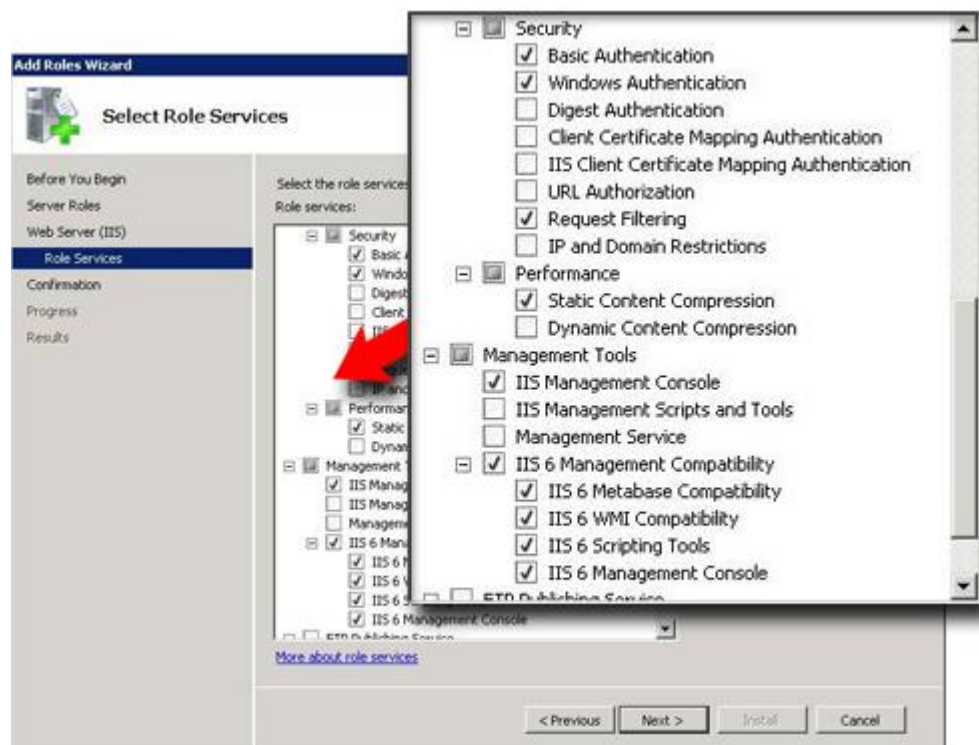
management server installation. This allows you to install the service channel on another server in your surveillance system, if required.

When you install the service channel on another computer, you must first **manually install the IIS**.

To manually install the IIS, use the following procedure:

1. On the computer you want to install the service channel on, select **Server Manager** from Windows' **Start** menu.
2. 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 will 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.

1. when the IIS is in place, on the computer on which you want to install the service channel, shut down any Milestone software running. If upgrading, it is highly recommended that you remove (see "Remove system components" on page 51) any previous versions of the service channel before upgrading.
2. If you want to install the service channel elsewhere, download the service channel installer from the management server's built-in web page at the address



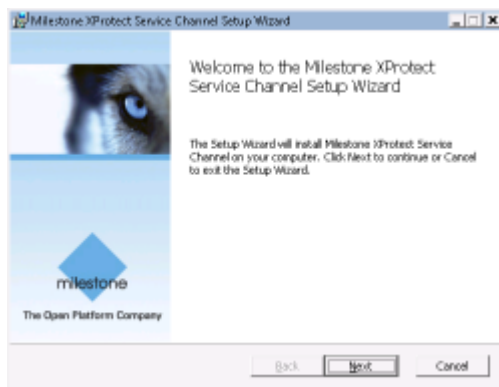
[http://\[management server address\]:\[port\]/installation/admin/](http://[management server address]:[port]/installation/admin/)

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server. On the web page find the **Service Channel Installer** section, and then click the **English** link. Note that depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking **Run** or similar (exact button text depends on your browser version).

When installing the service channel, you must be logged on to the computer with a user that has administrator rights in XProtect Corporate for the installation to be successful.

When the **Service Channel Setup** wizard opens:

- Click **Next** on the wizard's opening page.



- Select between:

Typical installation (see "Install Service Channel (typical)" on page 44)

- or -

Custom installation (see "Install Service Channel (custom)" on page 45).

If you select **Custom**, next select between:

A Predefined Network Service Account (see "Select a predefined network service account" on page 45)

- or -

A Particular User Account (see "Select a particular user account" on page 42)

When should I choose a particular user account instead of a predefined? If using network drives you should always specify a particular user account (with access to the network drives in question). Otherwise the service in question is unable to handle the required network drives.

- Click **Install**. When installation is complete, click **Finish** to exit wizard.

Install Service Channel (typical)

The **Typical** option installs the service channel with default settings. A **Typical** installation is recommended for most users.

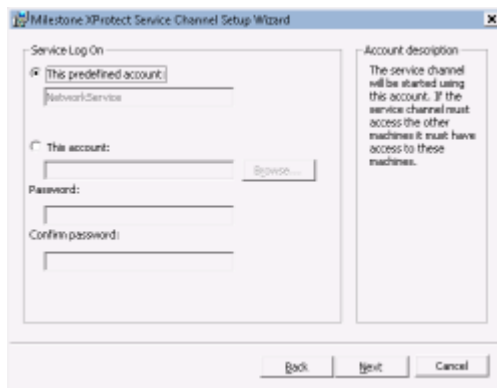


- Choose **Management Server**; specify the URL address of the management server (including the **http://** prefix, example: <http://123.123.123.123>), or host name including domain name of the management server computer, example: <http://myhost.mydomain.com>, then click **Next**.

Install Service Channel (custom)

The **Custom** option lets you select where to install the service channel components. A **Custom** installation is recommended for advanced users.

- Verify/specify the required installation path, and click **Next**.
- Verify/specify web site, and click **Next**.
- Choose **Management Server**; specify the URL address of the management server (including the **http://** prefix, example: <http://123.123.123.123>), or host name including domain name of the management server computer, example: <http://myhost.mydomain.com>, then click **Next**.
- Specify a user account under which the service channel will run. The specified user is automatically granted administrator rights in XProtect Corporate, see Specifying the Rights of a Role (see "Specify Rights of a Role" on page 256).



You are able to select either a particular user account or Network Service.

Tip: If the computer acting as management server is a member of a domain, you should either select **Network Service**, or make sure that you specify a user account which belongs to the domain in question.

You must select between:

- a predefined Network Service account (see "Select a predefined network service account" on page 45).
- or -
- a particular user account (see "Select a particular user account" on page 42) (in which case the service will use the specified user account to log in to the computer acting as management server).

- Click **Next**.

Select a predefined network service account

1. Select **This predefined account**.
2. Select **Network Service account**.
3. Click **OK**.



Select a particular user account

1. Select **This account**.
2. Click **Browse....** This will open the **Select User** window.
3. In the **Select User** window, verify that the required domain is specified in the **From this location** field. If not, click **Locations...** to browse for the required domain.
4. In the **Enter the object names to select** box, type the required user name.

Tip: Typing part of a name is often enough. Use the **Check Names** feature to verify that the name you have entered is recognized.

5. Click **OK**.
6. Specify the password for the user account in the **Password** field, and confirm the password in the **Confirm password** field.

The password must contain one or more characters and/or digits.

7. Click **OK**.

Port numbers of special interest

XProtect Corporate uses particular ports when communicating with other computers, cameras, etc.

What is a port? A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic which is used when viewing web pages.

When using XProtect Corporate, you must therefore make sure that certain ports are open for data traffic on your network.

The port numbers can be changed. Different port numbers may therefore be used in your organization. See Management Server Service and Recording Server Service (on page 330) for information about changing the recording server-related port numbers.

Tip: Consult the administrator of your organization's firewall if in doubt about how to open ports for traffic.

Ports used by XProtect Corporate

If nothing else is stated, ports are both inbound and outbound.

Port 20 and 21: Used by **recording servers** to listen for FTP information; some devices use FTP for sending event messages. FTP (File Transfer Protocol) is a standard for exchanging files across networks.

Port 25: Used by **recording servers** to listen for 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 (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers.

Port 80: While not directly used by XProtect Corporate, but by **management servers**, port 80 is typically used by the IIS (Internet Information Services) Default Web Site for running the XProtect Corporate Management Server service.

Port 554: Used by **recording servers** for RTSP traffic in connection with H.264 video streaming.



Port 1024 and above (outbound only (except ports listed in the following)): Used by **recording servers** for HTTP traffic between cameras and servers.

Port 1249: Used for communication between **event server** and **Management Client**.

Port 5210: Used for communication between **recording servers** and **failover servers** when databases are merged after a failover server has been running.

Port 5432: Used by **recording servers** to listen for TCP information; some devices use TCP for sending event messages.

Port 7563: Used by **recording servers** and **XProtect Smart Client** for handling PTZ camera control commands and for communicating.

Port 7609: Used by the **Data Collector Server service** to communicate with the server.

Port 8080: Used for internal system communication.

Port 8844: Used for communication between **failover servers**.

Port 9000: Used by **management servers** for communication between XProtect Corporate and XProtect Transact.

Port 9993: Used for communication between **recording servers** and **management servers**.

Port 11000: Used by **failover servers** for polling (i.e. regularly checking) the state of **recording servers**.

Port 12345: Used by **management servers** and **XProtect Smart Client** for communicating between XProtect Corporate and Matrix recipients.

Port 22331: Used for communication between Event Server and XProtect Smart Client.

Port 65101: Used by **recording servers** for communication between recording servers and drivers (internally, used for example when SMTP events are received).

Any other port numbers you may have selected to use. Examples: If you have changed the IIS Default Web Site port from its default port number (80) to another port number, or if you have integrated XProtect Enterprise servers into your XProtect Corporate solution, in which case a port must be allocated for use by XProtect Enterprise's Image Server service.

Multiple management servers (clustering)

The XProtect Corporate management server can be installed on multiple servers within a cluster of servers. This ensures that XProtect Corporate has very little down-time: if a server in the cluster fails, another server in the cluster will automatically take over the failed server's job running the XProtect Corporate management server. The automatic process of switching over the XProtect Corporate server service to run on another server in the cluster only takes a very short time (up to 30 seconds).

Note that 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> (see [http://technet.microsoft.com/en-us/library/cc787861\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc787861(WS.10).aspx) - [http://technet.microsoft.com/en-us/library/cc787861\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc787861(WS.10).aspx)) for details on how to do this.

Is clustering the same as federated architecture? No, clustering is not the same as federated architecture. Clustering is a method to obtain failover support for a management server on a site. With clustering, 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. On the other hand, federated architecture, is a method to combine multiple independent corporate sites into one large setup, offering flexibility and unlimited possibilities.

Click here to read more about federated architecture (see "Milestone Federated Architecture Overview" on page 293).



Prerequisites for installing XProtect Corporate in a cluster

- Two or more servers installed in a cluster.

Tip: You can find information about failover clusters on Microsoft's web site.

-Regarding clusters in Windows 2003, see Deploying Exchange Server 2003 in a Cluster (see [http://technet.microsoft.com/en-us/library/bb123612\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/bb123612(EXCHG.65).aspx) - [http://technet.microsoft.com/en-us/library/bb123612\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/bb123612(EXCHG.65).aspx)).

-Regarding clusters in Windows 2008, see Failover Clusters (see [http://technet.microsoft.com/en-us/library/cc732488\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx) - [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 will require the use of SQL Server Standard or a greater version which is capable of working as a clustered SQL Server).
- A Microsoft® Windows® Server 2003/2008 Enterprise or Data Center edition.

Installing XProtect Corporate in a cluster

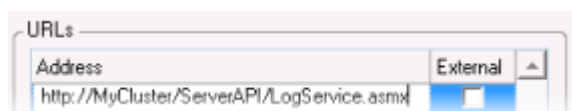
The section is based on Windows 2008. So, if you are using Windows 2003, descriptions and illustrations might differ from what you see on your screen.

1. Install the XProtect Corporate management server and all its subcomponents on the first server in the cluster by following the procedures described in Install Management Server (on page 28).

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, see Install Management Server, step 3 (see "Install management server" on page 28), for details. Furthermore, the specific user must have access to the shared network drive and preferably a nonexpiry password.

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

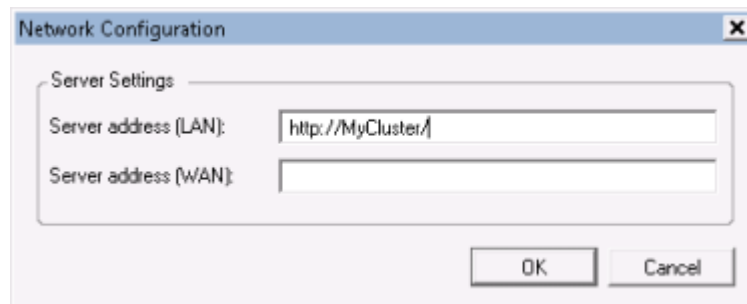
2. After you have installed the management server and the Management Client on the first server in the cluster, open the Management Client, then from the **Tools** menu select **Registered Services...**
 - a) In the **Add/Remove Registered Services** window, select the **Log Service** in the list, then 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.
- d) In the **Add/Remove Registered Services** window, click **Network...**



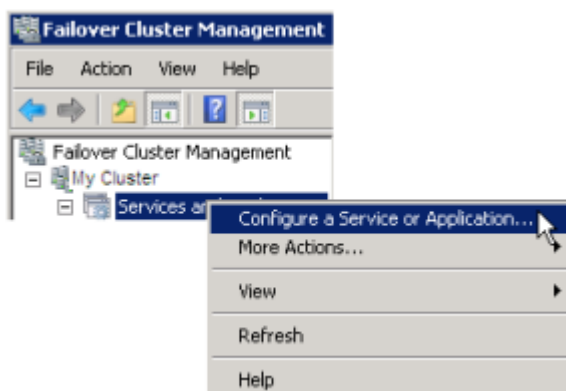
- e) In the **Network Configuration** window, change the URL address of the server to the URL address of the cluster. (This step only applies to the first server in the cluster.) Click **OK**.



3. Click **Close** in the **Add/Remove Registered Services** window, then exit the Management Client.
4. Stop the management server service (see "Management Server Service and Recording Server Service" on page 330) and the Internet Information Service (IIS). You can 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) (see [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx) - [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, but for the **last** server in the cluster you install the management server on, do not stop the management server service.

The management server service must be configured as a generic service in the failover cluster in order to take effect:

1. On the last server you have installed the management server on, open Windows' **Failover Cluster Management**, found under **Administrative Tools** in the **Start** menu.
2. In the **Failover Cluster Management** window, expand your cluster, right-click **Services and Applications**, then select **Configure a Service or Application...**



3. On the first page of the **High Availability** wizard click **Next**, then on the second page of the wizard select **Generic Service** in the list, and click **Next**.
4. Do not specify anything on the third page of the wizard, click **Next**.
5. Select the **Milestone XProtect Corporate Management Server** service from the list, then click **Next**.
6. Specify the name (host name of the cluster), that clients will use when accessing the service, then click **Next**.
7. No storage is required for the service, click **Next**.



8. No registry settings should be replicated, click **Next**.
9. Verify that the cluster service is configured according to your needs, then click **Next**.
10. The XProtect Corporate management server has now been configured as a generic service in the failover cluster. Click **Finish** to exit.
11. The Event Server and the Data Collector should be set as a dependent service of the management server in the cluster setup, so the Event Server will stop when the management server is stopped.
12. To add the **Milestone XProtect Event Server** service as a resource to the **Milestone XProtect Corporate Management Server Cluster** service, right click the cluster service and click **Add a resource > 4 - Generic Service** and select **Milestone XProtect Event Server**.
13. Repeat step 12, but instead of the Event Server, select to add **Milestone XProtect Corporate Data Collector Server**.

Upgrading XProtect Corporate in a cluster

Prerequisite

Make sure to have a backup of the database in question before updating the cluster.

How To Update...

1. Stop Management Server services (see "Management Server Service and Recording Server Service" on page 330) on all management servers in the cluster.
2. Uninstall the management server on all servers in the cluster. See Remove System Components (on page 51).
3. Use the procedure for installing multiple management servers in a cluster as described in Installing XProtect Corporate in a Cluster (on page 48).

IMPORTANT: When installing, make sure to reuse the existing SQL configuration database (which will automatically be upgraded from the old existing database version to the new one).

Multiple recording server instances

It is only recommended to install multiple instances of the Recording Server service on the same server under the following conditions.

If you:

- are upgrading from XProtect Corporate 4.1 or older
—and—
- are already running more 32-bit Recording Server service instances on the same server.

Since it is not possible to move devices/cameras from one recording server to another, setups running more than one 32-bit Recording Server service instances on the same server, will need to maintain this structure.

For all other setups, the newer 64-bit recording server eliminates the need for running more 32-bit instances on the same server.

Installing multiple recording server instances

During the recording server installation (see "Install system components" on page 34), you simply select the required number of instances. A maximum of 99 recording server instances is allowed on a single server.



Using multiple recording server instances does not require additional licenses.

In the Management Client, each recording server instance will be displayed separately, allowing you to configure each instance separately.

When managing the Recording Server service (see "Management Server Service and Recording Server Service" on page 330) by right-clicking its icon in the notification area on the server itself, you can:

- Stop and start each instance individually
- View status messages for each instance individually, grouped on tabs.

Remove system components

If you are not an XProtect Corporate system administrator, do not attempt to remove the management software.

The following procedure describes standard system component removal in recent Windows versions; the procedure may be slightly different in older Windows versions:

1. In Windows' **Start** menu, select **Control Panel**, and then...
 - If using **Category** view, find the **Programs** category, and click **Uninstall** a program.
 - If using **Small icons** or **Large icons** view, select **Programs and Features**.

In the list of currently installed programs, right-click the required program or service, select **Uninstall**, and follow the removal instructions.

Removing Management Server (see "Removing Download Manager, Event Server and Log Server" on page 51)

Removing Download Manager, Event Server and Log Server (on page 51)

Removing Management Client or Service Channel (on page 51)

Removing Recording Server (on page 52)

Removing Non-Required Components from Management Server (on page 52)

Removing Management Server

XProtect Corporate management servers are most likely installed on a dedicated server.

To remove, follow the general removal procedure (see "Remove system components" on page 51).

Removing Download Manager, Event Server and Log Server

The **Download Manager**, **XProtect event server** and **XProtect log server**, which are all installed on the management server, are removed separately from the management server software.

To remove, follow the general removal procedure (see "Remove system components" on page 51).

Removing Management Client or Service Channel

XProtect Corporate Management Client and **XProtect service channel** are all removed at the computer on which the program or service is installed.

To remove, follow the general removal procedure (see "Remove system components" on page 51).



Removing Recording Server

To remove an **XProtect Corporate recording server**, use the following procedure on the computer on which the recording server is installed:

What happens to the recording server's recordings? During the removal process, you will be asked whether you want to keep the recording server's recordings.

1. Stop the recording server service by right-clicking the recording server icon in the computer's notification area (also known as the **system tray**), then selecting **Stop Recording Server Service**.



Example: recording server notification area icon

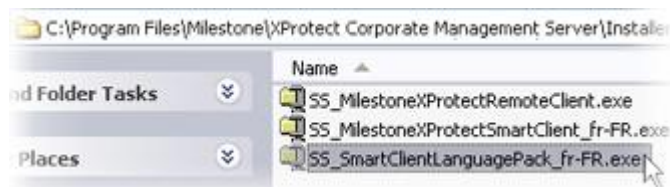
2. To remove, follow the general removal procedure (see "Remove system components" on page 51). Right-click the **XProtect Corporate Recording Server** in step 2 of the process.

Removing non-required components from Management Server

Upon installation, your management server by default contains installation files for a number of components, such as additional language versions of the XProtect Smart Client. The installation files lets you install the components on the management server, and make them available to your organization's users through the Download Manager.

You can remove installation files for non-required features from the management server. This can help you save disk space on the server if you know that your organization is not going to use certain features, for example non-relevant language versions.

1. Open the Installers folder located in the management server software installation folder, typically at **C:\Program Files\Milestone\XProtect Corporate Management Server\Installers**.
2. You may - depending on the type of component - need to select the required language sub-folder. Then you delete the unwanted installation (.exe) file. In this example, we are about to delete a French XProtect Smart Client language pack installation file from the management server:



Upgrade from previous version

This information is only relevant if you are upgrading a previous installation of XProtect Corporate.

IMPORTANT: XProtect Corporate no longer supports Microsoft® Windows® XP. See System Requirements (on page 16).

The process of upgrading XProtect Corporate involves removing all of its components **except** the Database Server. The Database Server is one of the management server's components, it contains the entire system configuration (recording server configurations, camera configurations, rules, etc.). As long as you do not remove the Database Server, you will not need to reconfigure your surveillance system configuration in any way (although you may of course want to configure some of the new features in the new version).



Backward compatibility with recording servers from XProtect Corporate versions older than this current version is limited. You can still access recordings on such older recording servers; but in order for you to be able to change their configuration, they must be of the same XProtect Corporate version as this current one. It is thus highly recommended that you upgrade all recording servers in your XProtect Corporate system.

When doing an update which includes updating your recording servers, you automatically update your Video Device Drivers as well. In this case, after restarting your system, it might take several minutes for your hardware devices to make contact with the new Video Device Drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Prerequisites

- Have your **temporary license (.lic) file** ready. The license file will change when your SLC changes, so you are likely to have received a new license file when purchasing the new version. When you install the management server, the wizard will ask you to specify the location of your license (.lic) file, which the system will verify before you will be able to continue.

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

- Have your **new XProtect Corporate version** ready. If you have not purchased the software on a DVD, you can download it from www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf). Note that although you can download any version, you will only be able to install a version for which your license file is valid.
- The management server stores your XProtect Corporate 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, or 2) in a database on an existing SQL Server on your network. If using 2), **Administrator rights on the SQL Server** are required whenever you need 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 database owner of the management server's system configuration database on the SQL Server will suffice.

Upgrading the Management Server

The management server has several components. This describes removing old components—except the Database Server—and installing the new ones:

1. First remove the management server itself. See Remove System Components (on page 51).
2. Next, remove the XProtect Corporate Windows components.
3. If the XProtect Corporate Management Client is installed on the management server itself, remove the Management Client too. See Remove System Components (on page 51).
4. Run the installation file for the new version of XProtect Corporate. After a short while, the installation window will open. Out of the three installation steps for the management server, you will be asked to address step 3 (XProtect Corporate management server).
5. Click the installation window's step 3, and complete the XProtect Corporate management server installation. During this process you will be asked to specify the path to your license (.lic) file.
6. When the management server is installed, the management server's web page will appear in a browser. If you want to install the Management Client software on the management server itself, you can do it from the management server's web page.



Upgrading Recording Servers

Once the new management server is installed, you can remove the old recording server version, and install the new one:

What happens to the recording server's recordings? During the removal process, you will be asked whether you want to keep the recording server's recordings.

1. See Remove System Components (on page 51) for how to remove a recording server.
2. When the recording server has been removed, open a browser and connect to the management server's web page at the following address:

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up 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.

3. From the web page, install the new version of the recording server software.
4. Repeat for each recording server on your XProtect Corporate system.

When updating your recording servers, you automatically update your Video Device Drivers as well. After restarting your recording servers, it might take several minutes for your hardware devices to make contact with the new Video Device Drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Upgrading a Management Client

If the Management Client is installed on separate computers, such as the surveillance system administrator's workstation or similar, you should now remove the old version and install the new one:

1. See Remove System Components (on page 51) for details on removing a Management Client.
2. When the Management Client has been removed, open a browser and connect to the management server's web page at the following address:

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up 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.

3. From the web page, install the new version of the Management Client.

Upgrading the XProtect Smart Client

XProtect Smart Client users should now remove their old XProtect Smart Client versions and install the new one:

1. See Installing the XProtect Smart Client (on page 22) for how to remove an XProtect Smart Client.
2. When the XProtect Smart Client has been removed, open a browser and connect to the management server's web page at the following address:

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



where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

3. From the web page, install the new version of the XProtect Smart Client.

Upgrading Video Device Drivers

Before upgrading Video Device Drivers, you must remove old Video Device Drives.

For information on how to remove/upgrade/install Video Device Drivers, see Manage and Remove Video Device Drivers (on page 317).

Installation troubleshooting

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

Issue: Automatic IIS installation for Management or Event Server fails

If installing the management server or the Event Server (custom installation) (see "Install event server and log server (custom)" on page 40) on a server running Windows 2008 Server, Internet Information Services (IIS) is under normal circumstances automatically installed.

- For the management server, this happens when you click the Internet Information Services step in the XProtect Corporate Management Server Installation window.
- For the event server, this is only a problem if the event server is installed on a different server than the management server.

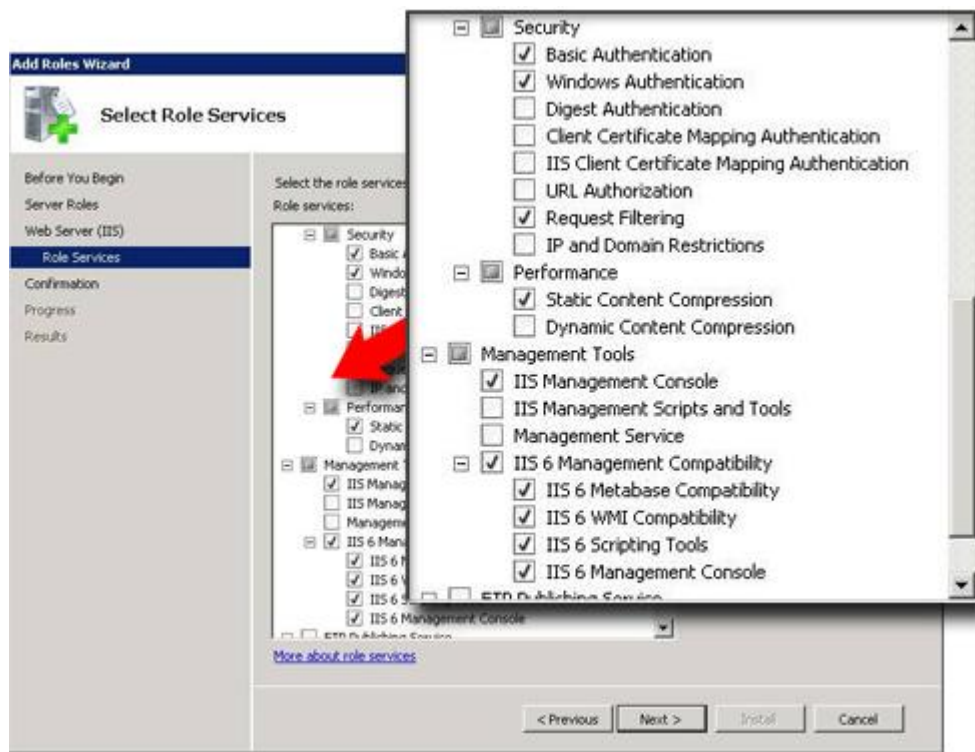
If the automatic installation fails, you can install IIS manually.

Solution: Install IIS Manually

1. If automatic IIS installation fails, you will see an error message asking you to install IIS manually. In the error message box, click **Install IIS Manually**.
2. You will now see the **Server Manager** window. In the left side of the 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 will 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 6 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:



- Complete the wizard by following the remaining steps.

Issue: Recording Server startup fails due to port conflict

This is an issue if either the Simple Mail Transfer Protocol (SMTP) Service or an existing installation of XProtect Enterprise is running.

Both use port 25. If port 25 is already in use, it may not be possible to start the XProtect Corporate Recording Server service. It is important that port number 25 is available for the recording server's SMTP service since many cameras are only capable of communicating via this port.

SMTP Service: Verification and solutions

To verify whether SMTP Service is installed, do the following:

- From Windows' **Start** menu, select **Control Panel**.
- In the **Control Panel**, double-click **Add or Remove Programs**.
- In the left side of the **Add or Remove Programs** window, click **Add/Remove Windows Components**.
- In the **Windows Components** wizard, select the **Internet Information Services (IIS)** item, and click **Details....**
- In the **Internet Information Services (IIS)** window, verify whether the **SMTP Service** check box is selected. If it is, 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 the **Simple Mail Transfer Protocol (SMTP)** item.
5. In the **SMTP Properties** window, click **Stop**, then set **Startup type** to either **Manual** or **Disabled**.

Tip: 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

Note that 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**, 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**.

XProtect Enterprise: Verification and solutions

To verify whether XProtect Enterprise is installed, do the following:

1. From Windows' **Start** menu, select **Control Panel**.
2. In the **Control Panel**, double-click **Add or Remove Programs**.
3. In the **Add or Remove Programs** window, verify whether XProtect Enterprise appears in the list. If it does, XProtect Enterprise is installed.

If XProtect Enterprise is installed, select one of the following solutions:

Solution 1: Remove XProtect Enterprise

1. From Windows' **Start** menu, select **Control Panel**.
2. In the **Control Panel**, double-click **Add or Remove Programs**.
3. In the **Add or Remove Programs** window, select XProtect Enterprise, click **Uninstall/Change**, and then **OK**.

Solution 2: Set XProtect Enterprise services to manual startup

This solution lets you start the recording server without having to stop the XProtect Enterprise Services 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, repeat steps a-c for these items: **Milestone ImageImportService**, **Milestone ImageServer**, **Milestone LogCheckService**, **Milestone Recording Server**.
5. Double-click the item.
6. In the **<item> Properties** window, click **Stop**, then set **Startup type** to **Manual**.
7. Click **Close**.

Tip: With the startup type **Manual**, you can start and stop the XProtect Enterprise Services from a command file:

To start the XProtect Enterprise Services from a command file, create a file named e.g. **startx.cmd** with the following content:

```
net start "Milestone ImageImportService"
net start "Milestone ImageServer"
net start "Milestone LogCheckService"
net start "RecordingServer"
```

To stop the XProtect EnterpriseServices from a command file create a file named e.g. **stopx.cmd** with the following content:

```
net stop "Milestone ImageImportService"
net stop "Milestone ImageServer"
net stop "Milestone LogCheckService"
net stop "RecordingServer"
```

Issue: Changes to SQL Server location prevents database access

This is an issue if using an MS SQL Server database as the XProtect Corporate management server database: If the location of the SQL Server is changed, for example by changing the host name of the computer running the SQL Server, access to the database will be lost.

Solution: Run Management Server database installation step again

See Management Server Installation (see "Install management server" on page 28). When running the database installation, you will - during the database preparation process - be asked whether you want to create a new database, use an existing database, or overwrite an existing database: Pointing to the new location of the SQL Server, select to use an existing database. This will update the SQL connection string used by the management server, and it will again be possible to access the database.

Issue: Insufficient continuous virtual memory fails installation

The following is only relevant if you use **Windows Server 2003**.

If you try to install a large Windows Installer package or patch package in Windows Server 2003, this problem might occur if the Windows Installer process has insufficient continuous virtual memory to verify that the .msi package or the .msp package is correctly signed.

Solution: A supported fix (see <http://support.microsoft.com/kb/925336> - <http://support.microsoft.com/kb/925336>) is available for Windows Server 2003. See <http://support.microsoft.com/kb/925336> (see <http://support.microsoft.com/kb/925336> - <http://support.microsoft.com/kb/925336>).



Issue: Multi-domain environments; one-way trusts not working

See Multi-domain Environments, One-way Trust (see "Setup with one-way trust" on page 341).



Use Download Manager

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

The web page is capable of displaying two sets of content:

- One targeted at system administrators, enabling them to download and install key XProtect Corporate components, such as recording servers (see "Install system components" on page 34) and the Management Client (see "Install system components" on page 34). This is the content you see during the XProtect Corporate installation process.
- One targeted at end users, providing them with access to client applications, such as the XProtect Smart Client and Remote Client, as well as various drivers, plugins, language packs, etc.



The example to the right shows the web page displaying content targeted at system administrators.

The web page automatically has some content; this is why you can use it straight away during the XProtect Corporate installation process. However, as a system administrator, you can customize what should be displayed on the web page, for example if particular language versions of the XProtect Smart Client are required in your organization. For this purpose you use the Download Manager.

Virus Scanning Information (see "Virus scanning on the Management Server not recommended" on page 65)

Access Download Manager

You access the Download Manager on the server running the management server software: In Windows' **Start** menu, select **All Programs > Download Manager > Download Manager**.

Make new components available

Making new components—including new language versions—available to your organization's users involves two procedures: First you install the required components on the management server. You then use the Download Manager to fine-tune which components should be available in the various language versions of the web page.

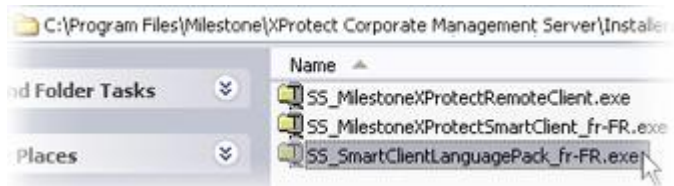
Installing new components on Management Server

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

Installation files for additional components, for example XProtect Smart Client language versions, language packs, etc., are by default available on your management server in a folder called **Installers**. The Installers folder is located in the management server software installation folder, typically at **C:\Program Files\Milestone\XProtect Corporate Management Server\Installers**.



To install a component from the **Installers** folder you may - depending on the type of component - need to select the required language sub-folder. Then you double-click the required installation (.exe) file. In the following example, we are about to install a French XProtect Smart Client language pack on the management server:



Tip: You can find more language versions of the XProtect Smart Client installer—and additional language packs - on the XProtect Corporate software DVD as well as on www.milestonesys.com.

When a new component has been installed on the management server, you will see a confirmation dialog. If required, you can open the Download Manager from the dialog:

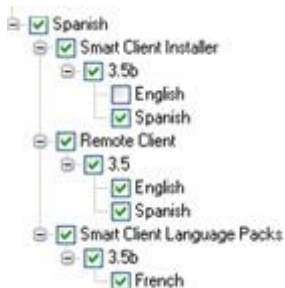


Making new components available through the Download Manager

When you have installed new components - such as XProtect Smart Client language versions, language packs, etc. - they will by default be selected in the Download Manager, and thus immediately be 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.

In the following example, we have specified that users who select the Spanish-language version of the **Default** web page version should have access to a Spanish version of the XProtect Smart Client, English and Spanish versions of the Remote Client, and a French language pack for the XProtect Smart Client:



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

Move components between web page versions

You are able to move components between the two versions of the web page, i.e. between the one targeted at system administrators and the one targeted at end users.



To move a component, simply right-click it, and select the web page version you want to move the component to. In this example we want to move the Remote Client, which is by default displayed on the end-user (**Default**) version of the web page, to the administrator version (**Admin**):



Hide and remove components

You have three options:

- You can **hide components** from the web page by clearing check boxes in the Download Manager's tree structure. In that case, the components will still be 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.
 - You can **remove components** which have previously been made available through the Download Manager. This will remove the installation of the components on the management server. The components will disappear from the Download Manager, but installation files for the components will be kept in the Management Server's **Installers** folder, so you can re-install them later if required.
- In the Download Manager, click **Remove features...**
 - In the **Remove Features** window, select the features you want to remove. In this example, we have selected to remove a Spanish XProtect Smart Client installer and a Spanish Remote Client.



- Click **OK**. You will be asked to confirm that you want to remove the selected features. If you are sure, click **Yes**.
- You can **remove installation files for non-required features** from the management server. This can help you save disk space on the server if you know that your organization is not going to use certain features - typically non-relevant language versions. See Remove System Components (on page 51) for more information.

Download Manager is not user rights management tool

The Download Manager lets you control which components users are able to download and install (or - in the case of the Remote Client - run straight from the web page). However, it is important to know that the Download Manager cannot be used for managing users' rights to use the components. Such rights are determined by roles (see "About Roles" on page 249); you define roles in the Management Client.



Default configuration of Download Manager and web page

The Download Manager has a default configuration. This ensures that your organization's users can access standard features without you having to set up anything.

- The default configuration provides **administrators** with access to downloading recording servers (see "Install system components" on page 34), the Management Client (see "Install system components" on page 34), the Event Server service (see "Install event server and log server (custom)" on page 40), as well as video device drivers (see "Manage and Remove Video Device Drivers" on page 317). This content is displayed when the web page is automatically loaded at the end of the management server installation as well as when the web page is accessed by entering the URL

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up 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.

- The default configuration provides **end users** with access to downloading an XProtect Smart Client as well as to running a Remote Client (which does not need to be downloaded). Both applications will by default be available in a language version matching the language version of your XProtect Corporate installation. This content is displayed when the web page is accessed by entering the URL

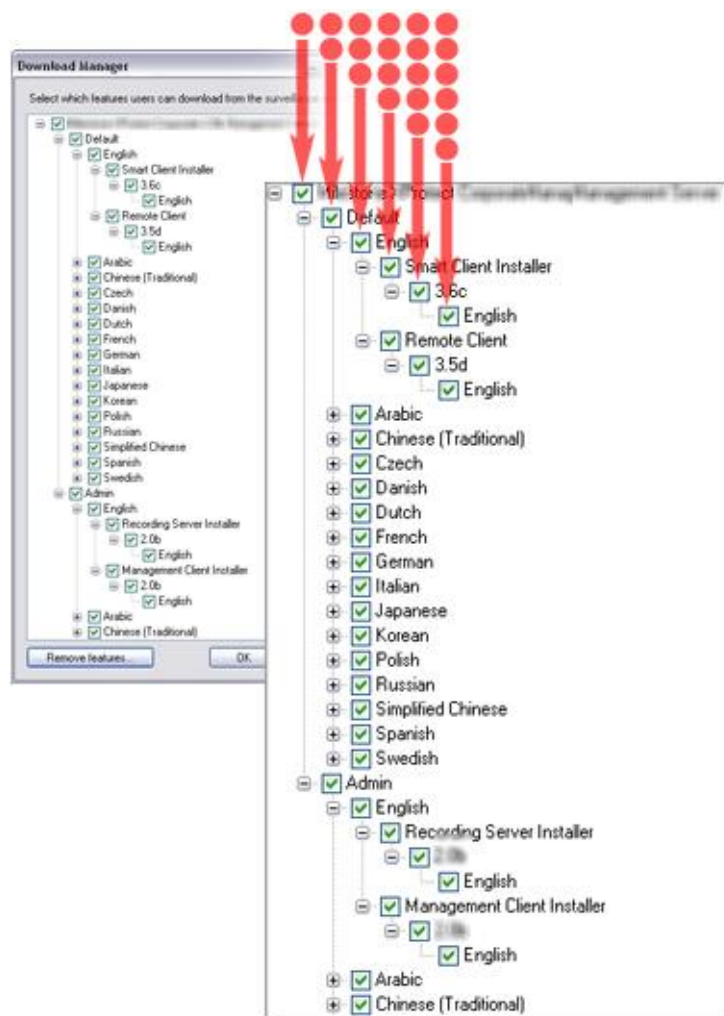
[http://\[management server address\]:\[port\]/installation/](http://[management server address]:[port]/installation/)

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

The Download Manager's configuration is represented in a tree structure.



Example: With an English version of XProtect Corporate, the Download Manager's default configuration would be represented in a tree structure like this:



Download Manager's Tree Structure Explained

The first level of the tree structure (one red dot in the example illustration) simply indicates that you are working with XProtect Corporate.

The second level (two red dots) refers to the two targeted versions of the web page. **Default** refers to the web page version viewed by end users. **Admin** refers to the web page version viewed by surveillance system administrators.

The third level (three red dots) refers to the languages in which the web page is available. In the example, the welcome page is available in a dozen languages (English, Arabic, Chinese, Czech, Danish, etc.).

The fourth level (four red dots) refers to the components which are - or can be made - available to users. In the example, these components include the XProtect Smart Client and Remote Client for end users. For system administrators, the components include recording server and Management Client.

The fifth level (five red dots) refers to particular versions of each component, which are - or can be made - available to users.

Example: version 3.5d of the Remote Client



The sixth level (six red dots) refers to the language versions of the components which are - or can be made - available to users.

In the example, XProtect Corporate has been installed in an English-language version. If we expand one of the other languages in the tree structure's third level, for example Arabic, we will see that users who select the Arabic version of the web page will initially also only have access to English versions of the XProtect Smart Client and, potentially, the Remote Client.

The fact that only standard components are initially available - and only in the same language version as the surveillance 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 is going to use it.

You can, however, make more components and/or languages available as required. See *Make New Components Available* (on page 60). Likewise, you can hide or remove unwanted components and/or languages; see *Hide and Remove Components* (on page 62).

Components controllable through the Download Manager

- Recording servers (including failover servers; failover servers are initially downloaded and installed as recording servers, during the installation process you specify that you want a failover server)
- Management Client
- Video device drivers (for use on recording servers)
- XProtect Smart Client
- Remote Client
- Language packs for XProtect Smart Clients (allowing users to add additional languages to their XProtect Smart Clients)
- Event Server; the service used in connection with map functionality (see "About maps" on page 328) in XProtect Smart Clients
- Various plugins (downloading such plugins can be relevant if your organization uses add-on products such as video analytics or transaction management solutions with XProtect Corporate)
- More options may be available in your organization

Virus scanning on the Management Server not recommended

If you are using virus scanning (see "Virus Scanning Information" on page 334) software on the management server, it is likely that the virus scanning will use a considerable amount of system resources on scanning data from the Download Manager. If allowed in your organization, disable virus scanning on the management server.



Management Client

Management Client Overview

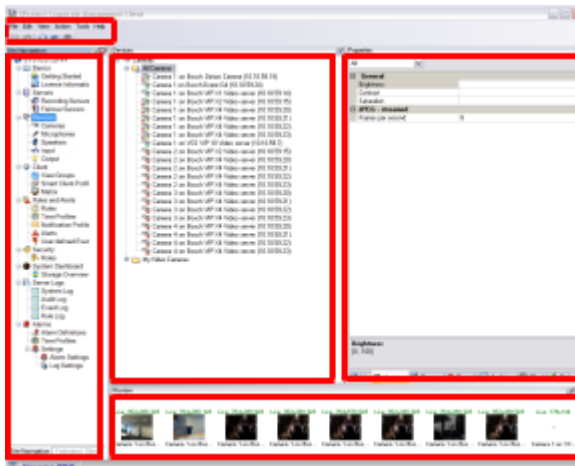
The Management Client is the feature-rich administration client used for configuration and day-to-day administration of your XProtect Corporate system. The Management Client software is typically installed (see "Install system components" on page 34) on the surveillance system administrator's workstation or similar.

Management Client's Elements

The Management Client window is divided into a number of panes. The number of panes will change depending on your task:

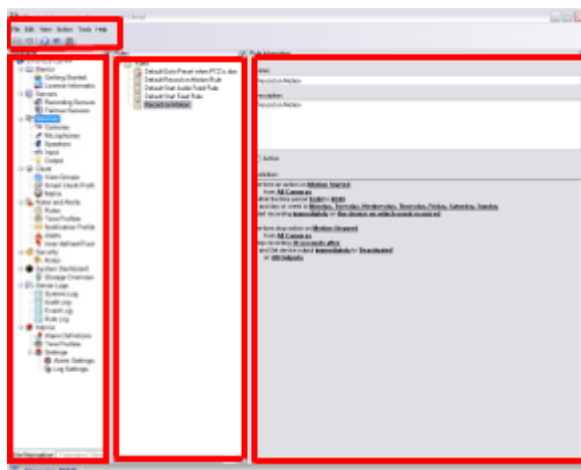
The following illustrations outline the Management Client window's default layout; the window layout can be customized (see "Customize the Management Client's Layout" on page 76), and may therefore be different on your computer.

- When working with recording servers and devices (cameras, inputs, outputs), the Management Client window contains a menu bar (on page 68) and four panes (see "Panels overview" on page 70):

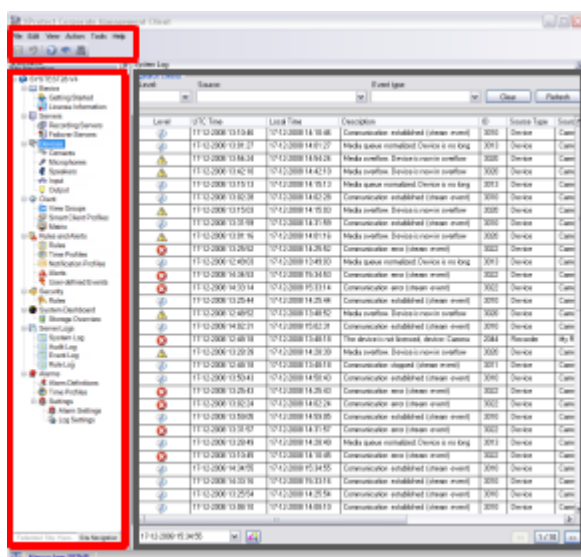




- When working with rules, time and notification profiles, users, roles, etc., the Management Client window typically contains a menu bar (on page 68) and three panes (see "Panes overview" on page 70):



- When viewing logs, the Management Client window typically contains only the menu bar (on page 68), the Site Navigation and Federated Sites Hierarchy Pane (see "Site Navigation Pane and Federated Hierarchy Pane" on page 67) and an overview area (marked in gray):



Site Navigation Pane and Federated Hierarchy Pane

The Management Client is the feature-rich administration client used for configuration and day-to-day administration of your XProtect Corporate system. The Management Client software is typically installed on the surveillance system administrator's workstation or similar.

Site Navigation Pane

Your main navigation element in the Management Client. Name, settings and configurations of the site you are logged into are reflected (see "Manage Milestone Federated Architecture" on page 302) here (site-name is visible at the top of the pane). The Management Client's features are grouped into the following categories:

- Basics:** General information, for example about licenses in your XProtect Corporate system



- **Servers:** Management of recording servers and failover servers (spare recording servers) connected to your XProtect Corporate system
- **Devices:** Management of cameras, microphones, speakers, input, and output
- **Client:** Management of view groups, Smart Client profiles and Matrix recipients
- **Rules and Events:** Management of rules, time profiles, notification profiles, events and events settings.
- **Security:** Management of users, groups, and roles
- **System Dashboard:** System reporting functionality and overview of recording servers' databases and archives.
- **Server Logs:** Access to the various logs of your XProtect Corporate system
- **Alarms:** Management of alarm definitions and alarm configuration.

Tip: Right-clicking items in the Site Navigation pane gives you quick access to management features.

Federated Site Hierarchy Pane

Your navigation element dedicated to displaying Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293) sites and their parent/child links.

The parent server you are logged in to, a.k.a your home site, will always be at top, and adopting its point of view, you can view all its linked children and downwards in the parent/child hierarchy.

What if I only have one server and don't run Milestone Federated Architecture? Your user interface looks the same, but you will only see the one server in your setup.

Menu Bar

The Management Client's menu bar features the following menus (see "Management Client menu overview" on page 75):

File Menu, **Edit** Menu, **View** Menu, **Action** Menu, **Tools** Menu and **Help** Menu.

Toolbar

The Management Client's toolbar features the following options:



Save: Save changes to your settings.



Undo: Undo your latest change.



Help...: Access a help topic relevant to your task



Contents...: Access the help system's table of contents.



Search...: Access the help system's search feature.

Read more about the Management Client's built-in help system (see "Navigating the Built-in Help System (online)" on page 25) here.

Memory Indicator

The memory indicator located in the lower left corner of the Management Client states how much memory is available for working with the Management Client.



When you expand items in the Site Navigation pane the Management Client uses memory to treat data stored in the individual items. Expanded items keep processing even when you expand other items in the Site Navigation pane, thus letting you access already-expanded items faster.

When available memory drops to 300 MB the memory indicator numbers turn red:



When the memory indicator drops to 0 MB, meaning there is no more memory available for the Management Client, you cannot expand any more items and you will see the following dialog.



To free up memory, refresh the Management Client: Click **OK** to exit the dialog, then press F5 on your keyboard or select **Refresh** from the **Action** menu.



Panes overview

The Management Client window may contain up to four panes:



1. Site Navigation Pane and Federated Sites Hierarchy Pane (see "Site Navigation Pane and Federated Hierarchy Pane" on page 67)
2. Overview Pane (on page 70)
3. Properties Pane (on page 71)
4. Preview Pane (on page 70)

The illustration outlines the Management Client window's default layout; the window layout can be customized (see "Customize the Management Client's Layout" on page 76), and may therefore be different on your computer.

Menu and tool bars

Provide quick access to often-used features.

Overview Pane

Provides an overview of the item you have selected in the navigation pane, typically in the form of a detailed list.

Selecting a particular item in the overview pane will typically display the item's properties in the properties pane. Right-clicking items in the overview pane gives you access to management features.

Preview Pane

Live: 640x480 88kB



Camera 5

Displays preview images from selected cameras or state information from selected microphones, speakers, inputs and outputs. The example to the left shows a camera preview image with information about the resolution and data rate of the camera's live stream.



Tip: By default, information shown with camera preview images will concern live streams (shown in green text). If you want recording stream information instead (shown in red text), select **View > Show Recording Streams** from the Management Client's menu.

You will see the preview pane when you deal with recording servers and devices. You can toggle the preview pane on and off in the **View** menu. To resize the preview pane, drag its borders. The larger the preview pane, the larger preview images and state information will appear.

Tip: 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** from the **Tools** menu.

Properties Pane

Displays properties of the item selected in the overview pane. In many cases, properties are displayed across a number of tabs:



Example of properties displayed on tabs

Site Navigation Pane and Federated Hierarchy Pane

The Management Client is the feature-rich administration client used for configuration and day-to-day administration of your XProtect Corporate system. The Management Client software is typically installed on the surveillance system administrator's workstation or similar.

Site Navigation Pane

Your main navigation element in the Management Client. Name, settings and configurations of the site you are logged into are reflected (see "Manage Milestone Federated Architecture" on page 302) here (site-name is visible at the top of the pane). The Management Client's features are grouped into the following categories:

- **Basics:** General information, for example about licenses in your XProtect Corporate system
- **Servers:** Management of recording servers and failover servers (spare recording servers) connected to your XProtect Corporate system
- **Devices:** Management of cameras, microphones, speakers, input, and output
- **Client:** Management of view groups, Smart Client profiles and Matrix recipients
- **Rules and Events:** Management of rules, time profiles, notification profiles, events and events settings.
- **Security:** Management of users, groups, and roles
- **System Dashboard:** System reporting functionality and overview of recording servers' databases and archives.
- **Server Logs:** Access to the various logs of your XProtect Corporate system
- **Alarms:** Management of alarm definitions and alarm configuration.

Tip: Right-clicking items in the Site Navigation pane gives you quick access to management features.

Federated Site Hierarchy Pane

Your navigation element dedicated to displaying Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293) sites and their parent/child links.



The parent server you are logged in to, a.k.a your home site, will always be at top, and adopting its point of view, you can view all its linked children and downwards in the parent/child hierarchy.

What if I only have one server and don't run Milestone Federated Architecture? Your user interface looks the same, but you will only see the one server in your setup.

Basics

Get started

Here the tasks typically involved in setting up an XProtect Corporate system are listed.

Note that although information is presented as a checklist, a completed checklist does not in itself guarantee that the XProtect Corporate system will match the exact requirements of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a good idea to spend time on testing and adjusting the motion detection sensitivity settings of individual cameras under different physical conditions (day/night, windy calm weather, etc.) once the system is running. The setup of rules, which determine most of the actions performed by the XProtect Corporate system (including when to record video), is another example of configuration which to a very large extent depends on your organization's needs.

- ☒ Install the various components of your XProtect Corporate system. See Installation Overview (on page 27).
- ☒ Log in to the Management Client. See Log in to the Management Client (on page 74).
- ☐ Authorize use of your XProtect Corporate system's recording servers. See Manage Recording Servers (on page 106).

Why must I authorize recording servers? By authorizing recording servers before they can be used, surveillance system administrators have full control over which recording servers are able to send information to their XProtect Corporate management server.

- ☐ Detect the hardware devices (i.e. cameras and video encoders) which should be added to each recording server. See the wizard Add Hardware (see "Add Hardware (Cameras, etc.)" on page 90).

What is the Add Hardware wizard? Add Hardware helps you detect IP hardware devices, such as cameras and video encoders, on your network and add them to your XProtect Corporate system. The wizard offers you two ways of detecting and adding hardware devices: With **automatic hardware detection**, XProtect Corporate automatically scans for available hardware within one or more specified IP address ranges. With **assisted hardware detection**, you manually specify the IP address of each required device. Both options offer the possibility of automatically detecting the correct hardware drivers.

- ☐ Verify that each recording server's storage areas will meet your needs. See About Storage and Archiving (on page 101).

What is a storage area? A storage area is a directory in which the databases containing recordings from the cameras connected to the recording server are stored— each individual camera database by default has a maximum size of 5 GB. A default storage area is automatically created for each recording server when the recording server is installed on the system. Connected cameras' databases are stored in the recording server's default storage area unless you specifically define that another storage area should be used for storing the databases of particular cameras. If required, a wizard lets you add further storage areas (on the recording server computer itself, or at another location, for example on a network drive), edit which storage area should be the default area, etc.

- ☐ Verify that each recording server's archiving settings will meet your needs. See About Storage and Archiving (on page 101).



What is archiving? Archiving is the automatic transfer of recordings from a camera's default database to another location. This way, the amount of recordings you are able to store will not be limited by the size of the camera's default database. Archiving also makes it possible to back up your recordings on backup media of your choice. Archiving is configured on a per-recording server basis. Once you have configured the archiving settings for a recording server (where to store archives, how often to transfer recordings to the archives, etc.), you can enable archiving for individual cameras. When archiving is enabled for a camera, the contents of the camera's database will automatically be moved to an archive at regular intervals.

☐ Configure any required failover servers. A failover server is a spare recording server which can take over if a regular recording server becomes unavailable. See About Failover Servers (see "Manage Failover Servers" on page 321).

☐ Configure each recording server's individual cameras. See Manage Cameras (on page 125).

Tip: You are able to group cameras, and configure common properties for all cameras within a group in one go.

Tip: Motion detection, a vital setting on most IP surveillance systems, is enabled by default. However, you may want to fine-tune motion detection settings, or disable motion detection for particular cameras.

☐ Enable and configure microphones— if any. See Manage Microphones (on page 144).

☐ Enable and configure speakers— if any. See Manage Speakers (on page 147).

☐ Enable and configure input— if any. See Manage Inputs (see "Manage Input" on page 149).

☐ Enable and configure output— if any. See Manage Outputs (see "Manage Output" on page 154).

☐ Create rules. See Manage Rules (on page 221).

What is a rule? Rules are a central element in XProtect Corporate. The behavior of an XProtect Corporate system is to a very large extent determined by rules. Rules determine highly important settings, such as when cameras should record, when PTZ (Pan/Tilt/Zoom) cameras should patrol, when notifications should be sent, etc.

When creating rules, you may also want to use time profiles (see "Manage Time Profiles" on page 229) (for quickly making rules apply within or outside predefined periods of time) or notification profiles (see "Manage Notification Profiles" on page 233) (for quickly making rules send pre-configured e-mails— with video clips, if required— to selected recipients).

☐ Add roles. See About Roles (on page 249).

What is a role? Roles determine which XProtect Corporate features users and groups are able to use. In other words, roles determine rights.

☐ Add users and/or groups of users. See About Users and Groups (see "Manage Users and Groups" on page 249).

Tip: If you have a server with Active Directory installed, and acting as domain controller on your network, XProtect Corporate lets you quickly add users and/or groups from Active Directory.

☐ Activate licenses. See About Licensing (see "Manage Licenses" on page 84).

Why must licenses be activated? When installing the system, you used a single temporary license. The temporary license is only valid for a certain number of days. After this initial period ends, all recording servers and cameras on your system will require activation of their individual licenses. You must therefore activate your licenses before the initial period ends, since all recording servers and cameras for which no licenses have been activated will otherwise stop sending data to the surveillance system.

☐ Use the Download Manager to make additional components available to users—if required. See Use the Download Manager (see "Use Download Manager" on page 60).

What is the Download Manager? An application which lets surveillance system administrators manage which system-related components (e.g. particular language versions of clients) surveillance system users will be able to access from a targeted web page generated by the management server.



Tip: The default configuration of the Download Manager ensures that end users have access to the XProtect Smart Client and Remote Client in language versions matching the language of your XProtect Corporate system. Basically, you only have to use the Download Manager if you want to make additional language versions, plug-ins or similar available to your organization's users.

Log in to the Management Client

Access to the XProtect Corporate Management Client requires certain user rights. Consult your surveillance system administrator if in doubt.

1. Click the XProtect Corporate Management Client desktop icon or—in Windows' **Start** menu—select **All Programs** > XProtect Corporate > **Management Client**. This will make the login window appear:



Management Client login window

2. The login window's **Server type** field will in many cases appear dimmed and pre-filled with the required information. If not, select XProtect Corporate.
3. In the **Server address** field, type the IP address or host name of the computer running the XProtect Corporate management server.

Tip: If you have logged in before, you can select previously used server IP addresses or host names from the list.

4. By default, you will log in to the management server with your active Windows account. This means that if you are currently logged in as, for example, **JohnSmith**, you will by default log in to the management server as **JohnSmith** as well.
 - If you wish to log in to the management server with your active Windows account (this is the default login option), select **Windows Authentication (current user)** in the **Authentication** field.
 - If you wish to log in to the management server with a different Windows account, select **Windows Authentication** in the **Authentication** field, then type the required user name and password in the **User name** and **Password** fields respectively.

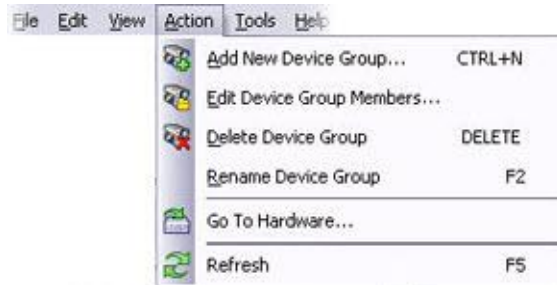
Tip: If you have logged in with **Windows Authentication** before, you can select previously entered user names from the list.

Tip: When using **Windows Authentication**, you have the option of selecting **Remember password**, in which case you will not have to type the password at subsequent logins.

5. Click **Connect** to open Management Client.



Management Client menu overview



Example only; Some menus changes depending on context.

Action Menu items

(Depending on context)

- **Refresh** is always available and reloads the requested information from the management server.
- **Expand** (or **Collapse**) is available when working with **Federated architecture**, **Servers**, **Devices**, **Client**, **Rules** and **Events** and **System Dashboard**.
- A number of context specific items.

Be aware of the following when working with the **Action** menu concerning Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293): To be able to delete a site without being connected to it, **right-clicking a site does not select it, but offers a context menu**. Because of this, some context menu items may be disabled if you are not connected to the site and some are only available on the home-site, i.e. the site you are logged in to. For more details see Manage Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293).

Edit Menu items

- **Undo** lets you cancel your latest action.
- Tip:** As an alternative to selecting **Edit > Undo**, press CTRL+Z on your keyboard.

File Menu items

- **Save:** Lets you save your current configuration.
- Tip:** As an alternative to selecting **File > Save**, press CTRL+S on your keyboard.
- **Logoff...:** Lets you log out of the Management Client, and log in with another user account if necessary.
 - **Exit:** Lets you close down and exit the Management Client.

Help Menu items

- **Help...** lets you access a help topic relevant to your task.
- **Contents...** lets you access the help system's table of contents.
- **Search...** lets you access the help system's search feature.



- **About...** opens a dialog displaying information about the version of your Management Client.

Tools Menu items

- **Registered Services...** lets you add trusted servers. See Manage Trusted Servers for details.
- **Enterprise Servers...** lets you add XProtect Enterprise servers specifically. See Manage XProtect Enterprise Servers (on page 279) for details.
- **Effective Roles...** lets you view all roles of a selected user or group (see "Manage Users and Groups" on page 249). For more information, see Manage Roles (on page 251).
- **Options...** opens the Options dialog (see "Options" on page 285), which lets you define and edit several global XProtect Corporate settings.

View Menu items

(Depending on context)

- **Reset Application Layout:** Lets you reset the layout of the different panes in the Management Client to their default settings. See Customize the Management Client's Layout (see "Customize the Management Client's Layout" on page 76) for details.
- **Preview Window:** Lets you toggle the preview pane (see "Panels overview" on page 70) on and off when working with recording servers and devices.

Tip: If the preview pane displays images from many cameras at a high frame rate, it may slow down performance. To specify the number of preview images you want in your preview pane, as well as their frame rate, select **Options > General** from the **Tools** menu.

- **Show Recording Streams:** By default, the information shown with preview images in the preview pane will concern cameras' live streams (shown in **green** text). If you want information about recording streams instead, select **Show Recording Streams**. Recording stream information will be shown in **red** text.
- **Federated Site Hierarchy:** By default, the is enabled, and this command lets you toggle it on and off.
- **Site Navigation:** By default, the Site Navigation pane (see "Panels overview" on page 70) is enabled, and this command lets you toggle it on and off.

Customize the Management Client's Layout

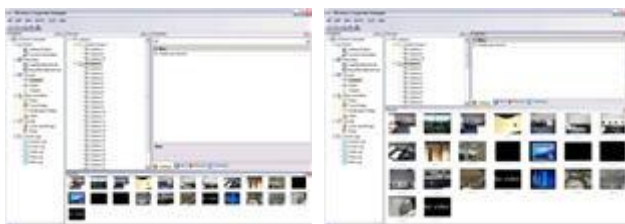
You can rearrange panes in the Management Client, and thus customize its look to suit your needs. If you rearrange the panes, you can always reset the entire layout to the Management Client's default layout.

Resizing Panes

You can resize panes by dragging the borders of the panes:

1. Place your mouse pointer over a border.
2. When the pointer becomes a double-headed arrow, drag the border in the required direction.

The size of the content inside the panes stays the same regardless of the size of the panes, with one exception: the larger the preview pane is, the larger preview images and state information will appear.



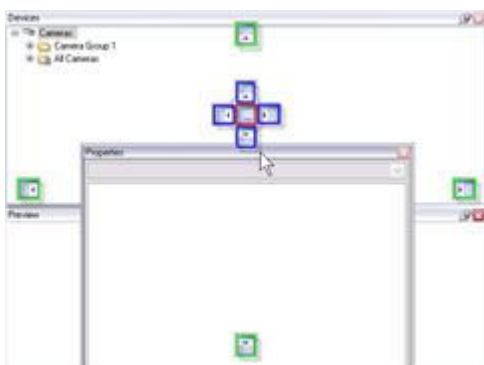
Moving Panes

You can move a pane to a different position either as a floating pane or to a docked position, by clicking on a pane's title bar and dragging it with the mouse.

The position and whether the pane becomes a floating pane or docked depend on where you release the mouse button. See the following topics for more information.



The Management Client offers some layout elements that help you control the new position of the pane. The layout elements



Outer layout elements illustrated with **green**

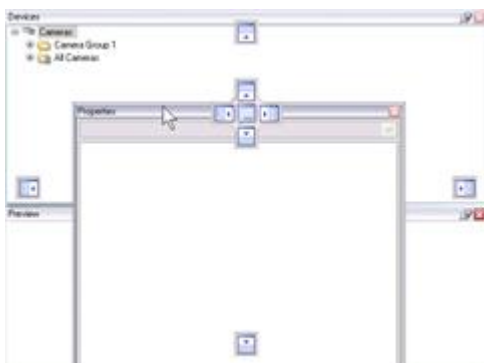
Inner layout elements illustrated with **blue**

Center layout element illustrated with **red**

For more information about how you use the layout elements when moving panes see these topics:

Floating Panes

To move a pane to a floating pane, drag the pane to its new position **without** using one of the layout elements.





Dragging a pane to a position without using a layout element



Result: A floating pane

Moving a Pane to a Docked Outer Position

If you move a pane to a docked outer position, it fills the area with a horizontal or vertical split that goes from top to bottom or left to right.

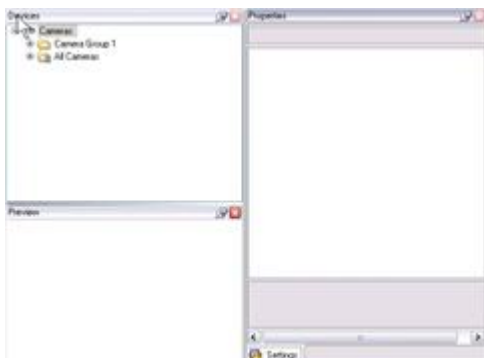
1. Drag the pane to one of the outer layout elements.

Tip: Before you release the mouse, the pane's new position is indicated by a gray area.

2. Release the mouse to dock the pane at its current position.



Dragging a pane to the right outer layout element



Result: The pane is docked to the right

Moving a Pane to a Docked Inner Position

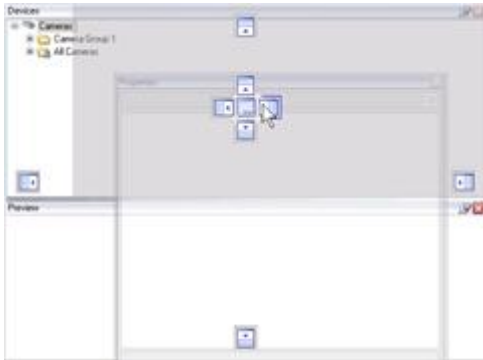
If you drag the pane to one of the inner layout elements, the pane will be positioned along one side of one of the other panes.



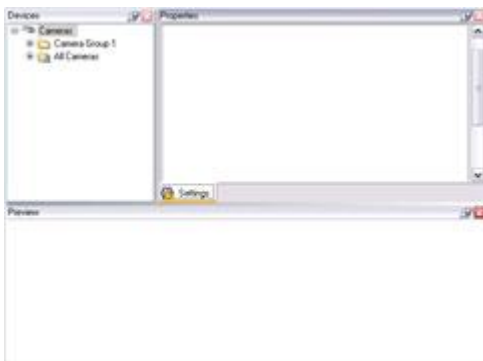
1. Drag the pane to one of the inner layout elements.

Tip: Before you release the mouse, the pane's new position is indicated by a gray area.

2. Release the mouse to dock the pane at its current position.



Dragging a pane to the right inner layout element of the overview pane



Result: The pane is docked to the right of the overview pane

Moving a Pane to a Shared Position

You can move a pane into another pane's position so two or more panes share the same position:

1. Drag the pane to the center layout element of the pane which position you want to share.



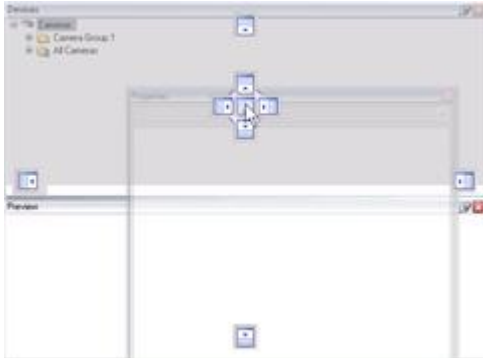
The center layout element

Tip: Before you release the mouse, the pane's new position is indicated by a gray area.

2. Release the mouse to dock the pane at its current position.



Tip: To view the content of the panes, click the tabs on the bottom of the shared position.



Dragging a pane to the inner center layout element of another pane



Result: The pane shares the same position as the other pane

Splitting Shared Positions

If you do not want a pane to share a position with another pane, do this:

1. Click the tab of the relevant pane and drag it to a new position.
The pane's new position can be a docked position or a floating pane.
2. Release the mouse to place the pane at its current position.

Using Auto-Hide

You can auto-hide panes. An auto-hidden pane is available as a tab to the right or left of the previous position of the pane. When you place your mouse pointer over the tab, the content of the pane slides out. As soon the cursor is positioned outside the pane, it slides back.

To auto-hide a pane click the **Auto Hide** pushpin in the title bar of the pane you want to auto-hide.





Default appearance and position of the overview pane.



The overview pane is hidden and available through a tab to the left.

Do the following to show and open an auto-hidden pane again:

1. Place your mouse pointer over the tab of the auto-hidden pane to show the pane.
2. Click the **Auto Hide** pushpin in the title bar of the pane to dock the pane.



Resetting to Default Layout

If you have moved, resized and auto-hidden panes and now want to reset the entire layout of the panes in the Management Client to their default settings, do the following:

1. From the Management Client's **View** menu, select **Reset Application Layout**.
2. Restart the application.

Toggling Preview Pane On and Off

You can close the preview pane when working with recorders and devices by clicking **Close** in the right side of the Preview pane's title bar.

To reopen the Preview pane (see "Panels overview" on page 70) select **Preview Window** from the Management Client's **View** menu.

Tip: If the preview pane displays images from many cameras at a high frame rate, it may slow down performance. To specify the number of preview images you want in your preview pane, as well as their frame rate, select **Options > General** from the **Tools** menu.

Tip: When the preview pane is closed, it uses no resources and improves therefore the computer's performance.

Activate Licenses

You can activate your licenses in two ways: online or offline.

Tip: If the computer running the Management Client has internet access, use online activation for a quick and convenient activation procedure.

You cannot activate more licenses than you have bought. To view your total number of licenses, expand **Basics** in the Management Client's Site Navigation pane, and select License Information. If you have added more cameras than you have licenses for, you must get additional licenses before you can activate them.



Activate Licenses Online

In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Basics**, right-click **License Information**, and select **Activate Licenses Online**.

1. **Activate Online** opens.
 - If you are an **existing user**, enter your user name and password to log into the Software Registration Service Center.
 - If you are a **new user**, click the **Create new user...** link to set up a new user account in the Software Registration Service Center and then follow the registration procedure. If you have not yet registered your SLC, you must do so, see earlier.
2. If you select **Save password**, the password will be saved on the computer, and can be accessed by other users of the computer.
3. Click **Next**, and follow the wizard's remaining steps to activate your licenses. When your licenses have been activated, you will see a confirmation.
4. Click **Finish** to end the activation.

If You Receive an Online Activation Error Message: (see "If You Receive an Online Activation Error Message" on page 82)

If You Receive an Online Activation Error Message

Under rare circumstances you may receive an error message during online activation. Often, such error messages will simply inform you that you forgot to include certain required information.

Should you receive an error message which refers to a slightly more complicated problem, the following list of selected error messages will help you identify the problem and find out what to do:

- ▶ **Could not acquire a new license.**
- ▶ **Could not acquire a new license. An error occurred on the activation server. Please try later.**
- ▶ **Could not acquire a new license. Access was denied.**
- ▶ **Could not acquire a new license. The format of the activation request was invalid.**
- ▶ **Could not acquire a new license. The requested license could not be granted. Please contact the software support to correct this problem.**

Could not acquire a new license. Unable to communicate with the license activation server.

Problem: Online activation was not possible, either due to a problem on the online activation server itself, due to a problem with your connection to the online activation server, or due to a problem with the specified information.

What to do: Contact Milestone Support (<mailto:support@milestonesys.com>), who will investigate the issue for you.

-
- ▶ **Could not acquire a new license. The license has already been activated on another system.**

Problem: License activation has already taken place on another XProtect Corporate system; you cannot activate licenses on more than one system.

What to do: Activation should not be necessary, as another system already runs with your licenses activated. If you believe that this is wrong, contact Milestone Support (<mailto:support@milestonesys.com>), who will investigate the issue for you.



► **Could not acquire a new license. The SLC was not registered.**

Problem: Activation cannot take place before the SLC (Software License Code) for your XProtect Corporate system has not been registered.

What to do: Register the SLC (see Manage Software License Codes (SLC), **Registering Your Software License Code (SLC)** section, for a step-by-step description of the brief and easy registration process). When the SLC is registered, use XProtect Corporate's **Activate Online** again, remembering to log in with the same user name and password as you used when registering the SLC.

► **Could not acquire a new license. The specified user is not allowed to activate this system.**

Problem: The SLC (Software License Code) for your system has been registered by another user name than the user name (e-mail address) you have specified on **Activate Online's Enter new user information** step. Online activation must take place with the user name under which the SLC was registered.

What to do: Find out under which user name the SLC was registered, then activate as an existing user (selectable on **Activate Online's** first step). If in doubt about which user name was used for registering the SLC, contact Milestone Support (mailto:support@milestonesys.com), quoting your SLC.

► **Could not acquire a new license. The specified user name or password was not correct.**

Problem: License activation was not possible due to a problem with the user name or password you have specified on **Activate Online's Enter new user information** step.

What to do: Verify that you have typed user name and password exactly as they were specified when you registered the SLC (Software License Code) for your XProtect Corporate system. If in doubt about which user name was used for registering the SLC, contact Milestone Support (mailto:support@milestonesys.com), quoting your SLC.

► **Could not acquire a new license. Too many licenses for camera feeds requested.**

Problem: If you have added more camera feeds to your XProtect Corporate system than you currently have licenses for, you must purchase additional licenses for these feeds before you will be able to activate them.

What to do: To obtain additional licenses, contact your XProtect Corporate vendor, or visit www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) to log into the software registration service center. When you have received an updated license file (.lic) with the new licenses, you can activate your licenses online. See also Getting Additional Licenses (on page 86).

► **Could not acquire a new license. Too many recording server licenses requested.**

Problem: If you have added more recording servers to your XProtect Corporate system than you currently have licenses for, you must purchase additional licenses for these recording servers before you will be able to activate them.

What to do: To obtain additional licenses, contact your XProtect Corporate vendor, or visit www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) to log into the software registration service center. When you have received an updated license file (.lic) with the new licenses, you can activate your licenses online. See also Getting Additional Licenses (on page 86).



Activate licenses offline

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Basics**, right-click **License Information**, and select **Activate License Offline > Export License For Activation** to export a file with your currently added recording servers and cameras.
2. Specify a file name and a location for the license request (.lrq) file.
3. Open an internet browser and go to Milestone's web site at <http://www.milestonesys.com> (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf), then select **Software Registration** from the top menu. Log in with your e-mail and password, if you have used the software registration system before, otherwise, click **New to the System?** to create a new user account.
 - a) Select the SLC under **Current SLCs**.
 - b) In the menu for SLC properties, use the **Upload LRQ** function to upload the generated LRQ file.

How long will this process take? You will immediately after uploading the LRQ file receive an e-mail with the updated license file.

4. When you have received the updated license file (.lic), save it at a location accessible from the Management Client.
5. In the Management Client's Site Navigation pane, expand **Basics**, right-click **License Information**, select **Activate License Offline > Import Activated License**, and select the .lic file to import it.
6. Click **Finish** to end the activation process.

Activating licenses after the grace day period

If the grace day period is exceeded before activation, all cameras which are not activated within the given period will become unavailable, and will not be able to send data to the surveillance system.

If you exceed the grace day period before you activate a license, the license is not lost. You can activate the license as usual.

Configuration, added cameras, defined recording servers, and other settings will not be removed from the Management Client if a license is activated too late.

Manage Licenses

When you purchase XProtect Corporate, you also purchase a certain number of licenses for device channels. Device channels are typically cameras but could also be dedicated input/output boxes.

At first, when you have installed the various XProtect Corporate 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 the so-called grace day period.

When the new surveillance system is working, we recommend that you activate your licenses (see "Activate Licenses" on page 81) before you make the final adjustments. The reason is that you must activate your licenses before the grace day period expires, since all recording servers and cameras for which no licenses have been activated will not be able to send data to the surveillance system if the grace day period is expired.

Which Devices Require a License?

You need licenses for the number of device channels - typically cameras but it could also be dedicated input/output boxes - you want to run on the system. One device channel license enables you to run one camera or one dedicated input/output box. You can use and define an unlimited number of recording servers, microphones, speakers, inputs and outputs.



You can always get more licenses as your surveillance system grows. See *Getting Additional Licenses* (on page 86).

What to Know When Replacing Cameras?

You can replace a camera licensed in the XProtect Corporate system with a new camera, and have the new camera activated and licensed instead.

The total number of purchased device channels corresponds to the total number of cameras that are able to run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

If you replace a camera with a similar camera (manufacturer, brand, and model), and give the new camera the same IP address as the old one, you will maintain full access to all the camera's databases. In this case, you simply 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 replacing a camera with a different model, you must use the Management Client's **Replace Hardware** wizard to map all relevant databases of cameras, microphones, inputs, outputs, etc. When done, remember to activate the license. For details on the **Replace Hardware** wizard, see *Replacing Hardware* (on page 96).

There is no limit to the number of cameras you can replace.

What to Know about Licenses and Milestone Federated Architecture?

Refer to *Milestone Federated Architecture Overview* (on page 293)

Viewing Your License Information

You get an excellent overview of the licenses in your XProtect Corporate system if you expand **Basics** in the Management Client's Site Navigation pane (see "Panels overview" on page 70), and then select **License Information**. This will bring up the **License Information** page, on which you can see:

- Your software license code
- The total number of available device channels (typically cameras but it could also be dedicated input/output boxes) you are licensed to run
- How many licenses you have used, both the number of activated licenses and the number of temporary (not activated) licenses
- Whether you need to get additional licenses in order to have enough licenses for all of your cameras
- Any other installed products used with XProtect Corporate, and—if applicable—their Software License Code

License Information

Type	Total Licenses	Activated Licenses	Temporary Licenses	Expired Licenses	Missing Licenses
Recording Server	Unlimited	1	N/A	N/A	0
Device Channel	255	0	25	0	0
Camera	255	0	25	0	0
Microphone	Unlimited	0	0	0	0
Speaker	Unlimited	0	0	0	0
Input	Unlimited	0	0	0	0
Output	Unlimited	0	0	0	0

The first hardware grace expires 02-09-2008

Example only; numbers and dates may be different on your system



Any expiry dates listed on the page are in the management server's local time. Since you are not necessarily located in the same time zone as the management server, the management server's current local time is displayed in the bottom right corner of the page.

You can activate licenses (on page 81) online or offline, by expanding **Basics** in the Site Navigation pane, and right-clicking **License Information**.

The cameras (or dedicated input/output boxes) for which you do not have a license will not send data to the surveillance system. Cameras added after all available licenses are used are unavailable. Cameras without licenses will be identified by an exclamation mark symbol when listed in the Management Client's overview pane (see "Panels overview" on page 70).

Tip: In the short period until you have obtained additional licenses, you can disable some less important cameras to allow some of the new cameras to run instead.

See Manage Hardware (on page 95) for more information.

Where I Can See How Many Grace Days I Have Left? This information is also available from the **License Information** page where you can see if you need to get more licenses so all added cameras can deliver data to XProtect Corporate. When you add a new camera for which you have a license, you are granted a new full grace day period for the camera in question from the date you added the camera. Therefore the end date of the grace day period displayed on the **License information** page is for the first added but not activated camera. The duration of the full grace day period can be found in a **readme** file which is available from Windows' Start menu, by selecting **All Programs > XProtect Corporate > Read Me**.

Getting Additional Licenses

What if you want to add - or if you already have added - more device channels (cameras or dedicated input/output boxes) than you currently have licenses for? In that case, you must buy additional licenses before the cameras will be able to send data to your XProtect Corporate system.

To get additional licenses for your XProtect Corporate system, contact your XProtect Corporate vendor, or visit www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) to log into the software registration service center.

When you have received an updated license file (.lic) with the new licenses, you can activate your licenses. See Activate Licenses (on page 81) for more information.

Tip: In the short period until you get the additional licenses, you can disable some less important cameras to allow some of the new cameras to run instead.

See Manage Hardware (on page 95) for more information.

Manage Software License Codes (SLC)

When you purchase XProtect Corporate, you receive a Software License Code (SLC), which is used when installing your system.

Registering Your Software License Code (SLC)

The SLC is printed on the product license sheet enclosed with the software DVD as well as on your order confirmation. You should also register your SLC before activating (see "Activate Licenses" on page 81) your XProtect Corporate system's licenses.

The SLC registration process is brief and easy:

1. Go to the Milestone Systems A/S website at www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf), and click the **Software registration** link in the menu.
2. Log in to the Software Registration Service Center with your user name (e-mail address) and password.



Tip: If you have not used the Software Registration Service Center before, click the **New to the system?** link, and follow the instructions for registering yourself as a user; then log in to the Software Registration Service Center using your registered user name and password.

3. In the Software Registration Service Center, click the **Add SLC** link.
4. Type your SLC. When asked whether you want to add the SLC to your account, click **OK**.
5. Once your SLC has been added, click the **main menu** link.
6. Click the **Logout** link to log out of the Software Registration Service Center.

Tip: If you plan to use online activation when activating your licenses, make sure you use the same user name (e-mail address) and password for the activation as you did when registering the SLC.

Changing Your Software License Code (SLC)

Often you run your installation on a trial SLC during the first period. When the trial period is over, and it is time to change the trial SLC to the permanent SLC, you can do this without any un- or reinstall action.

IMPORTANT: This must be done locally on the management server in question; you **cannot** do this from the Management Client.

1. On the management server, go to the notification area of the taskbar (a.k.a. **Systray**).



2. Right-click the XProtect Corporate **Management Server** icon, select **Change License...**
3. The **Change XProtect Corporate License** dialog appears. Click **Import License...**
4. Next, select the SLC license file saved for this purpose. When done, the selected license file location will be added.



5. Click **OK**. You are now ready to perform SLC registration.



Remote Connect Services

About Remote Connect Services

The Remote Connect Services feature contains the Axis One-click Camera Connection technology developed by Axis Communications. It enables XProtect Corporate 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 so-called secure tunnel servers (ST servers).

ST servers use a Virtual Private Network (VPN). Only devices holding a valid key can operate within a VPN. This offers a secure tunnel where data can be exchanged between public networks 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**.

Installing an STS Environment for One-click Camera Connection

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

Working with Axis One-click Camera

Editing the Axis Dispatch Service Properties

1. The Properties pane displays relevant dispatch information on the **Axis Dispatch Service** tab.
2. Edit properties (see "Axis One-Click Camera Connection Properties" on page 90).
3. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Adding or Editing Secure Tunnel Servers

1. Do one of the following:



- a) To add an ST servers, right-click the **Axis Secure Tunnel Servers** topnode, select **Add Axis Secure Tunnel Server...**

or
- 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 (see "Axis One-Click Camera Connection Properties" on page 90).
3. If you chose to use credentials when you installed the **Axis One-Click Connection Component**, make sure to select the **Use credentials** check box and fill in exactly the same user name and password as used for the **Axis One-Click Connection Component**.
4. Click **OK**.

Removing Secure Tunnel Servers

1. To remove an ST server, right-click it, select **Remove Axis Secure Tunnel Server...**
2. Click **Yes**.

Registering a new Axis One-click Camera

1. To register a camera under an ST server, right-click it, select **Register Axis One-click Camera...**
2. In the window that opens, fill in the relevant information (see "Axis One-Click Camera Connection Properties" on page 90).
3. Click **OK**.
4. The camera will now appear under the relevant ST server.

The color coding of the camera is either:

- **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 added, status will always be green. The connection status (see "Read Server Service State Icons" on page 333) is then—as normal—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...**).

Unregistering an Axis One-click Camera

1. To unregister a camera under an ST server, right-click it, select **Unregister Axis One-click Camera**.
2. In the dialog that appears, make sure the check mark is selected and click **Yes**.
3. The camera will disappear from under the relevant ST server.



Axis One-Click Camera Connection Properties

- **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 of the item. Not compulsory.
- **External address:** Enter/Edit the http address of the ST server where the camera(s) connect.
- **Internal address:** Enter/Edit the http address of the ST server where the recording server connects.
Tip: Remember **http://** in front of both the external and internal address.
- **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 Milestone.
- **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:** Same as the MAC address. See **Camera password**.
- **Use credentials:** If it was decided—during installation of the ST server—to use credentials, select the check box.
- **User name** (for Dispatch Server): Enter user name. Must be identical to the one received from Milestone.
- **User name** (for ST server): Enter user name. Must be identical to the one entered when the **Axis One-Click Connection Component** was installed.

Servers

Add Hardware (Cameras, etc.)

The **Add Hardware** wizard helps you detect IP hardware devices, such as cameras and video encoders, on your network and add them to recording servers on your XProtect Corporate system.



To access **Add Hardware**, expand the **Servers** folder in the Management Client's Site Navigation pane (see "Panels overview" on page 70) and select the **Recording Server** node, then in the overview pane (see "Panels overview" on page 70) right-click the required recording server and select **Add Hardware...**



Add Hardware opening page

The wizard offers you four ways of detecting and adding hardware devices: **Express (recommended)**, **Address range scanning**, **Manual** and **Remote connect hardware**. With the **Express** option, XProtect Corporate automatically scans for available hardware on the recording server's local network. With **Address range scanning**, XProtect Corporate scans defined network IP address ranges and detects hardware models. With **Manual**, you manually specify the IP address and port for each device. With **Remote connect hardware**, you can add hardware connected via a remotely connected server. All options offer the possibility of automatically detecting the correct hardware drivers.

Tip: If you are new to XProtect Corporate: use the **Express** hardware detection as it will guide you through each of the steps involved in detecting and adding your IP devices.

It is strongly advised that you **only** add a physical hardware device to **one recording server** at the time.

Express

The **Express (recommended)** option automatically discovers hardware models on the recording server's local network.

1. Select **Express (recommended)** and click **Next**.
2. Specify user names and passwords if your hardware devices are not using the factory default user name and password. You can add as many user names and passwords as required by clicking **Add**. Remember to select the **Include** check box for each required device.

When ready, click **Next**.

3. Wait while the hardware is detected. A status indicator will show the detection process.

Tip: Select the **Show hardware running on other recording servers** check box to see if detected hardware is running on other recording servers.

Once detection is complete, click **Next**.

4. Wait while device-specific information is collected for each hardware device. A status indicator will show the detection process. If collecting hardware information for a device is unsuccessful, click the **Failed** error message to see why. Once collection is complete, click **Next**.

Choose to enable or disable successfully detected hardware and cameras. Detected hardware, such as hardware device, camera, microphone and speaker is listed individually, allowing you to, for example, add a hardware device's camera without enabling its speaker if needed.

You can change the name of the hardware by clicking **Hardware name** and choosing between:



- [Hardware model] [address]
- [Hardware model]

Additionally, you can change name of the device by clicking **Device name** and choosing between:

- [Hardware name] - [Device type] [number]
- [Device type] [number] on [hardware name]
- [Address] - [Device type] [number]

A change of name for hardware and/or device will be applied to all available hardware/devices and will take effect immediately.

Tip: You can disable the hardware, but enable its devices if necessary.

When ready, click **Next**.

5. Select a default group for all device types, or group the devices individually. The devices are listed according to type, for example, camera, microphone, speaker. Click **Finish**.

Address Range Scanning

The **Address Range Scanning** option scans your network for relevant hardware devices based on your specifications regarding required IP ranges, drivers, and device user names and passwords.

1. Select **Address Range Scanning** and click **Next**.
2. Specify user names and passwords if your hardware devices are not using the factory default user name and password. You can add as many user names and passwords as required by clicking **Add**. Remember to select the **Include** check box for each required device. You must add and include at least one user name and password in order for the wizard to proceed.

When ready, click **Next**.

3. Select which drivers to use when scanning. By default, XProtect Corporate will use all known drivers. If your organization only uses certain hardware devices and/or models, you can achieve faster scanning by selecting only the drivers required for those hardware devices. Click **Next**.

Tip: The list of drivers is typically very long, and by default all drivers are selected. With **Select All** and **Clear All**, you can avoid having to select/clear all check boxes manually.

4. Specify the IP address network ranges you want to scan for hardware.
 - **Start address:** First IP address in required range.
 - **End address:** Last IP address in required range. The start and end IP address may be identical, allowing you to only scan for a single hardware device if needed.
 - **Port:** Port number(s) on which to scan. Default is port 80. If your hardware devices are located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP addresses used by the hardware devices.

You can add as many network ranges as needed by clicking **Add** to add another row. You can add any network address between 0.0.0.1 and 255.255.255.255. At least one network range must be selected before you can continue.

Remember to select the **Include** check box for each required range.

You can only specify IPv4 addresses when using **Address Range Scanning**.



Wait while the hardware is detected. A status indicator will show the detection process.

If you successfully detect hardware on a specified network range, a **Success** message will appear in the **Status** column. If you fail to add a network range, you can click the **Failed** error message to see why.

Tip: Select the **Show hardware running on other recording servers** check box to see if detected hardware is running on other recording servers.

Once detection is complete, click **Next**.

5. Wait while device-specific information is collected for each hardware device. A status indicator will show the detection process. If collecting hardware information for a device is unsuccessful, click the **Failed** error message to see why the collection of information has failed. Once collection is complete, click **Next**.
6. Choose to enable or disable successfully detected hardware and cameras. Detected hardware, such as hardware device, camera, microphone and speaker is listed individually, allowing you to, for example, add a hardware device's camera without enabling its speaker if needed.

You can change the name of the hardware by clicking **Hardware name** and choosing between:

- **[Hardware model] [address]**
- **[Hardware model]**

Additionally, you can change name of the device by clicking **Device name** and choosing between:

- **[Hardware name] - [Device type] [number]**
- **[Device type] [number] on [hardware name]**
- **[Address] - [Device type] [number]**

A change of name for hardware and/or device will be applied to all available hardware/devices and will take effect immediately.

Tip: You can disable the hardware, but enable its devices if necessary.

When ready, click **Next**.

7. Select a default group for all device types. The devices are listed according to type, for example, camera, microphone, speaker. Click **Finish**.

Manual

The **Manual** option lets you specify details about each hardware device separately. This can be a good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc.

1. Select **Manual** and click **Next**.
2. Specify user names and passwords if your hardware devices are not using the factory default user name and password. You can add as many user names and passwords as required by clicking **Add**. Remember to select the **Include** check box for each required device. You must choose to add and include at least one user name and password in order for the wizard to proceed.

When ready, click **Next**.

3. Now select which drivers to use when scanning. By default, XProtect Corporate will use all known drivers. If your organization only uses certain hardware devices and/or models, you can achieve faster scanning by selecting only the drivers required for those hardware devices.



Tip: The list of drivers is typically very long, and by default all drivers are selected. With **Select All** and **Clear All**, you can avoid having to select/clear all check boxes manually.

When ready, click **Next**.

4. Specify information for the hardware you want to add. You can also optionally select the type of driver you want to add to speed up hardware detection.
 - **Address:** Specify the IP address of the hardware, you want to add.
 - **Port:** Specify the port number to which the camera is added.
 - **Hardware driver:** Select the driver of the hardware you want to add. Or select **Auto-detect** to let the wizard detect which driver to install.

5. Wait while the hardware is detected. A status indicator will show the detection process. Select or clear the network ranges to use in the detection process.

If you successfully detect hardware, a **Success** message will appear in the **Status** column. If you fail to add a network range, click the **Failed** error message to see why.

Tip: Select the **Show hardware running on other recording servers** check box to see if detected hardware is running on other recording servers.

Once detection is complete, click **Next**.

6. Choose to enable or disable successfully detected hardware and cameras. Detected hardware, such as hardware device, camera, microphone and speaker is listed individually, allowing you to, for example, add a hardware device's camera without enabling its speaker if needed.

You can change the name of the hardware by clicking **Hardware name** and choosing between:

- **[Hardware model] [address]**
- **[Hardware model]**

Additionally, you can change name of the device by clicking **Device name** and choosing between:

- **[Hardware name] - [Device type] [number]**
- **[Device type] [number] on [hardware name]**
- **[Address] - [Device type] [number]**

A change of name for hardware and/or device will be applied to all available hardware/devices and will take effect immediately.

Tip: You can disable the hardware, but enable its devices if necessary.

When ready, click **Next**.

7. Select a default group for all device types or group the devices individually. The devices are listed according to type, for example, camera, microphone, speaker. Click **Finish**.

Remote Connect Hardware

Remote connect hardware automatically scans for hardware connected via a remotely connected server.

1. Select **Remote connect hardware** and click **Next**.
2. Wait while the hardware is detected. A status indicator will show you how far you are in the detection process.



- Once detection has completed, select which hardware you want to add and click **Next**.

Manage Hardware

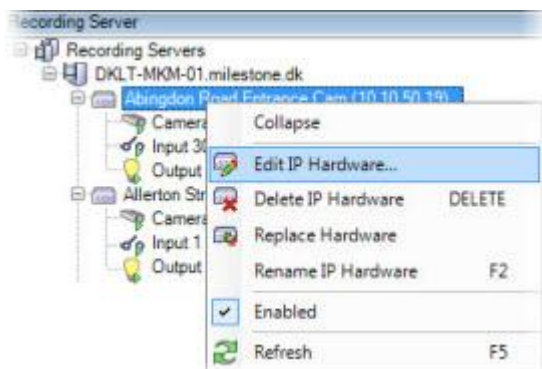
For each recording server on your system, you have several options for managing added IP hardware.

Most configuration and management of individual camera settings (such as a camera's recording settings), input settings, and output settings takes place on a more detailed level; see *Manage Cameras* (on page 125), *Manage Inputs* (see "Manage Input" on page 149), and *Manage Outputs* (see "Manage Output" on page 154).

Editing Basic Hardware Settings (IP, etc.)

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

- In the overview pane (see "Panels overview" on page 70), expand the required recording server, right-click the hardware device you wish to edit.
- From the menu that appears, select **Edit IP Hardware...**:

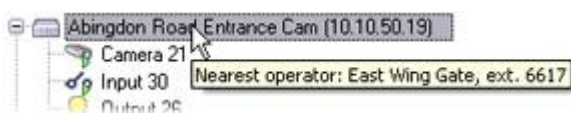


This opens the **Edit Hardware** window, in which you can edit the following:

- Name:** The name of the hardware in the Management Client's lists, etc.

Tip: You can also quickly change the name of a hardware device by selecting **Rename IP Hardware...** from the menu.

- Description:** (Optional) A description or other information about the hardware device. It will, among other places, appear when you pause your mouse pointer over the hardware device in the overview pane.



- Hardware URL:** URL, IP address, or host name of the hardware device.
- User name:** Required to access and use the hardware device.
- Password:** Required to access and use the hardware device.
- Type:** Non-editable field indicating the hardware driver used for the hardware device.

- Click **OK**.



Deleting Individual Hardware

IMPORTANT: When deleting a hardware device, all its recordings are deleted permanently.

1. In the overview pane (see "Panels overview" on page 70), expand the required recording server, right-click the no longer needed hardware device.
2. From the menu that appears, select **Delete IP Hardware**.

Tip: As an alternative, press **DELETE** on your keyboard.

3. Confirm that you want to delete the hardware device.
4. The hardware device is removed from the recording server's listings in the Management Client.

If you ever need to add the hardware device to a recording server again, select the required recording server and use the Add Hardware (see "Add Hardware (Cameras, etc.)" on page 90) wizard.

Replacing Hardware

When you replace a physical camera (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.

Furthermore, when replacing hardware devices, note that your system might be affected by license limitations (see "Manage Licenses" on page 84). Using the **Activate Online** (see "**Activate Licenses**" on page 81) wizard, you must reactivate your licenses **after** replacing hardware devices. Also note, that if the new number of cameras, microphones, inputs, outputs, etc. exceeds the old number of cameras, microphones, inputs, outputs, etc. you might also have to buy new licenses (see "Manage Licenses" on page 84). See your License Information (see "Manage Licenses" on page 84).

1. In the Overview pane (see "Panels overview" on page 70), expand the required recording server, right-click the hardware device you wish to replace.
2. From the menu that appears, 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 relevant hardware device driver from the **Hardware Driver** drop-down list (marked by red arrow in the image). Otherwise select **Auto Detect**. If port, user name or/and password data is different for the new device, also correct this **before starting the auto detect process (if needed)**.

Address	Port	User Name	Password	Hardware Driver
10.100.10.100		root	****	Axis 216MFD Camera

Tip: The wizard is pre-filled with data from the existing hardware device. If you replace it with a similar hardware device, you can reuse some of this data - for example, port and driver information.

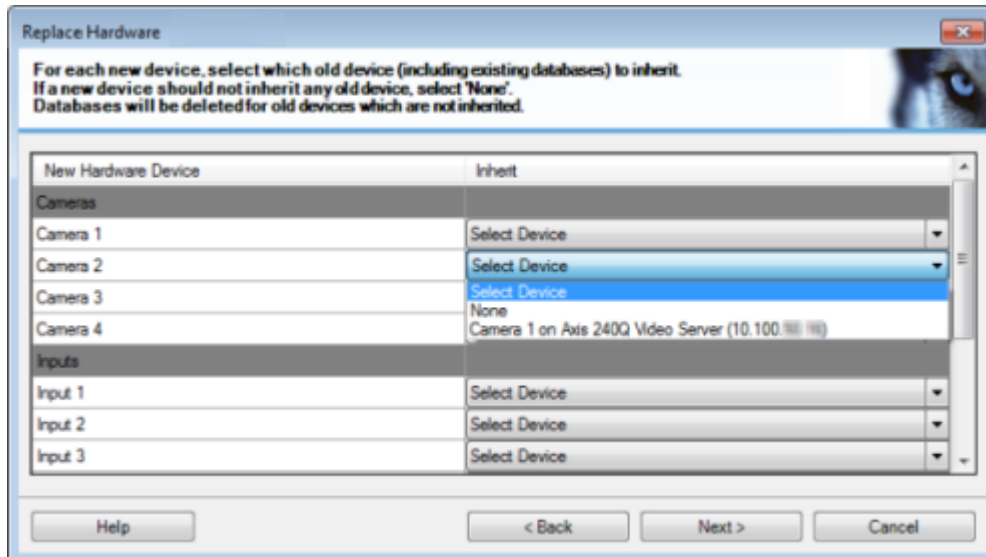
5. Do one of the following:
 - If you selected the required hardware device driver directly from the list, click **Next**.
 - If you selected **Auto Detect** in the list, click **Auto Detect**, wait for this process to be successful (marked by a ✓ to the far left), click **Next**.

This step is designed to help you map devices and their databases, depending on the number of individual cameras, microphones, inputs, outputs, etc., attached to the old hardware device and the new respectively.

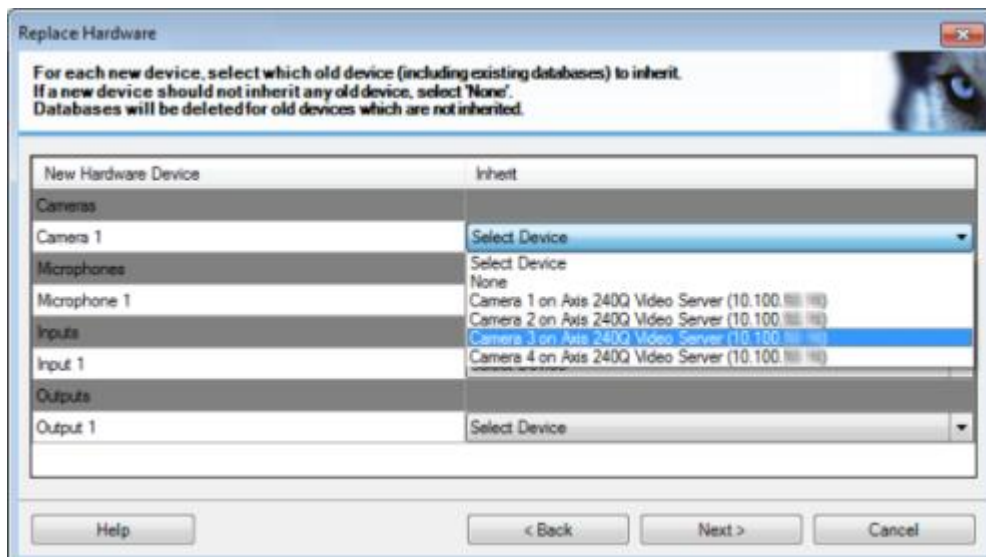
It is important to consider **how** to map databases from the old hardware device to databases of the new hardware device. You do the actual mapping of individual cameras, microphones, inputs, outputs, etc. by selecting a corresponding camera, microphone, input, output or **None** in the right-side column.



IMPORTANT: Make sure to map **all** cameras, microphones, inputs, outputs, etc. Contents stored in databases belonging to cameras, microphones, inputs, outputs, etc. mapped to **None**, will be **lost**.



Example of the old hardware device having more individual cameras, microphones, inputs, outputs, etc., than the new one.



Example of the new hardware device having more individual cameras, microphones, inputs, outputs, etc., 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 an external source (for, for example, reporting purposes) or/and **Close** to end the wizard.



Renaming Hardware

1. In the overview pane (see "Panels overview" on page 70), expand the required recording server, right-click the hardware device you wish to rename.
2. From the menu that appears, select **Rename IP Hardware**.

Tip: As an alternative, press F2 on your keyboard.

3. Overwrite the name of the hardware.

Disabling/Enabling Hardware

Added hardware is by default **enabled**.

In the overview pane (see "Panels overview" on page 70), under the required recording server, enabled/disabled hardware devices are indicated this way:



Enabled

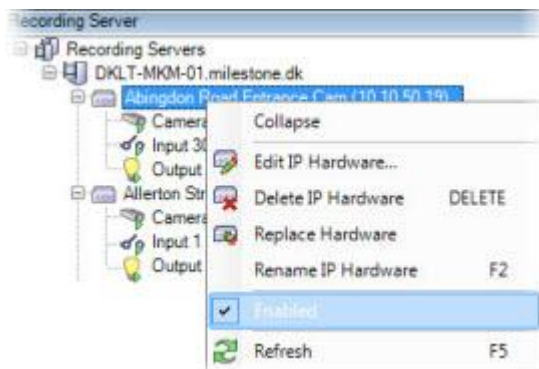


Disabled

Disabling

Disable added hardware, for example, for licensing or performance purposes:

1. In the overview pane (see "Panels overview" on page 70), expand the required recording server, right-click the hardware device you wish to disable.
2. From the menu that appears, select **Enabled** to clear it:



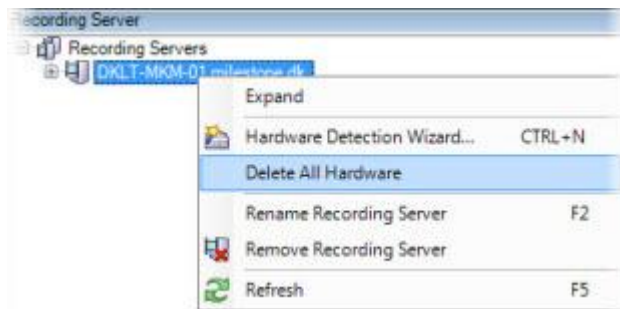
Deleting All Hardware on a Recording Server

IMPORTANT: When deleting hardware devices, all recordings from the hardware devices in question will be deleted permanently.

1. In the overview pane (see "Panels overview" on page 70), right-click the required recording server where you want to delete all hardware.



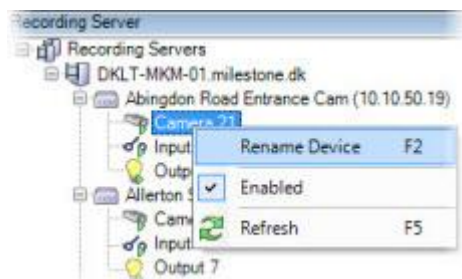
- From the menu that appears, select **Delete All Hardware**:



- Confirm that you want to delete all hardware on the selected recording server.

Renaming Individual Devices

- In the overview pane (see "Panels overview" on page 70), expand the required recording server and the required hardware device. Right-click the camera, input, or output you wish to rename.
- From the menu that appears, select **Rename Device**:



Tip: As an alternative, press F2 on your keyboard.

- Overwrite the name of the selected device.

Enabling/Disabling Individual Devices

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

This means that microphones, speakers, inputs and outputs must be individually enabled before they can be used on the XProtect Corporate system. The reason for this is that surveillance systems inherently rely on cameras, whereas the use of microphones, etc. is highly individual depending on organizations' needs.

In the overview pane (see "Panels overview" on page 70), under the required server, enabled/disabled devices are indicated the following way (examples show indications for an output):



Disabled



Enabled

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

Enabling

- In the overview pane (see "Panels overview" on page 70), expand the required recording server and the required hardware device. Right-click the camera, input, or output you wish to enable.



- From the menu that appears, select **Enabled**:



About Storage and Archiving

When a camera or device records video and/or audio, all specified recordings are per default stored in the storage area defined for the device. More precisely in the storage area's default recording database named **Recording**. A storage area has no default archive(s), but these can easily be created.

Depending on recording settings, the storage areas's recording database will most likely run full at some point and its contents need to be archived in order to be saved. It is therefore possible to create archives within the default storage area and start an archiving process. Furthermore, it is possible to create alternative storage area(s) and configure that selected video/audio recordings must be stored/archived here.

Archiving is the automatic transfer of recordings from a camera's or device's default database to another location. This way, the amount of recordings you are able to store will not be limited by the size of the device's recording database. Archiving also makes it possible to back up your recordings on backup media of your choice.

Storage and archiving is configured on a per-recording server basis.

To ease explanations, the following mostly mentions cameras and video, but all is true about speakers and microphones and audio and sound as well.

IMPORTANT: We recommend that you use a dedicated hard disk drive for the recording server database. Using a dedicated hard disk drive for the database will prevent low disk performance. Furthermore, when formatting 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> (see <http://support.microsoft.com/kb/140365/en-us> - <http://support.microsoft.com/kb/140365/en-us>).

IMPORTANT: The oldest data in a database will always be 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 will be deleted. A database always requires 250MB of free space; if this limit is reached (if data is not deleted fast enough), no more data will be written to the database until enough space has been freed. The actual maximum size of your database will thus be the amount of gigabytes you specify, minus 5GB.

Attaching Devices to a Recording Server

Once you have configured the storage area and archiving settings for a recording server (where to store recordings, archives, how often to transfer recordings to archives, etc.), 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 *Attaching Individual Devices or a Group of Devices to a Storage Area* (on page 103).

Effective Archiving

When archiving is enabled for a camera or a group of cameras, the contents of the camera(s)' database will automatically be moved to an archive at regular intervals.

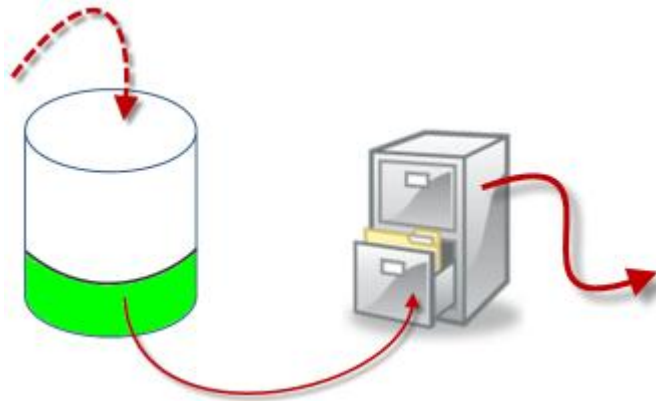


Depending on your requirements, you are able to configure one or more archives for each of your databases. Archives can be located either on the recording server computer itself, or at another location which can be reached by XProtect Corporate, for example on a network drive.

By setting up your archiving in an effective way, you can prune and groom your database storage area usage significantly if needed. Often, it is desired 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 and sound quality a bit. Effective pruning and grooming can help ensure this and can be handled from the **Storage** tab (see "Storage Tab (Recording Server Properties)" on page 113) of a recording server by adjusting several interdependent settings such as:

- 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, recordings are archived when they have "sifted" down into the green area of the database cylinder, or in other words: 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, XProtect Corporate begins to overwrite old recordings in the archive.

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

Encryption and FPS determine the size of the data in the databases.

To have recordings archived, all these parameters must be set 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 due to the fact that the number of retention days stated for an archive includes all retention stated earlier in the process. Furthermore, archiving must always take place more frequently than the retention period is set to, otherwise you risk losing data. If you have a retention time of 24 hours, any data older



than 24 hours will be 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 storage areas (image to the left) has a retention time of 4 days and the following archive (image to the right) a retention time of 10 days. Furthermore, archiving is set to occur every day at 10:30, ensuring a much more frequent archiving than retention time is set to.

You can also control archiving by use of rules and events. See About Rules and Events (on page 162) and Events Overview (on page 216).

Attaching Individual Devices or a Group of Devices to a Storage Area

Once a storage area is configured for a recording server, you can enable it for individual devices (cameras, microphones or speakers) or a group of devices. You can also select which of a recording server's storage areas should be used for the individual device or the group.

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Devices** and select either **Cameras**, **Microphones** or **Speakers** as required.
2. In the Overview pane (see "Panels overview" on page 70), select the required device or a device group.
3. In the Properties pane, select the **Record** tab.
4. In the **Storage** area, select **Select...**
5. In the dialog that appears, select the wanted database, click **OK**.
6. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Viewing Archived Recordings

You view archived recordings in the XProtect Smart Client. As long as the archived recordings are stored locally or on accessible network drives, you can use the XProtect Smart Client's many features (timeline browser, smart search, evidence export, etc.) when browsing archived recordings; just like you would with recordings stored in a cameras' regular databases. The fact that you are viewing archived recordings will be completely transparent.

Remember that individual user rights may prevent particular users from viewing recordings from particular cameras - just as is the case when browsing recordings from cameras' regular databases.

Backing Up Archived Recordings

Many organizations want to back up their recordings, using tape drives or similar. Exactly how you do this is highly individual, depending 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. Creating backups based on the content of individual camera databases may cause sharing violations or other malfunctions.

When scheduling a backup, make sure the backup job does not overlap with your specified archiving times.

Tip: You are able to view each recording server's archiving schedule in each of a recording server's archives, on the **Storage** tab.

Knowing Archive Structure Lets You Target Backups

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

During all regular use of your XProtect Corporate system, the sub-directory structure will be 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 thus primarily interesting if you want to back up your archived recordings (see "Archive Structure" on page 104).

Using the Smart Client – Player to View Archived Video

You can use the Smart Client – Player functionality of your XProtect Smart Client to view archived video. See your XProtect Smart Client documentation for details.

Archive Structure

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

During all regular use of your XProtect Corporate system, the sub-directory structure will be 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 thus primarily interesting if you want to back up your archived recordings.

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

Since you are able to 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 the maximum allowed size of the archive is reached.

The sub-directories are named after the device, followed by an indication of whether recordings come from an edge camera or via SMTP (if relevant), **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\
```

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 such sub-directories will be added if the recordings are technically divided into sequences; something which is often the case if motion detection has been used to trigger recordings.

If you want to back up your archives, knowing the basics of the sub-directory structure enables you to target your backups.

Examples:

If wishing 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\
```

If wishing to only 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\
```

Archiving and Virus Scanning

If you are using virus scanning software on the computer on which the camera databases you want to archive are located, or on a computer to which data is archived, it is likely that the virus scanning will use a considerable amount of system resources on scanning all the data which is being archived.

This may affect system performance negatively. Also, virus scanning software may temporarily lock each file it scans, which may further impact system performance negatively.

If possible, you should therefore disable any virus scanning of camera databases and archiving locations.

Frequently asked questions about archiving

What happens if a storage area becomes unavailable? If a storage area becomes unavailable—for example if the storage area is located on a network drive, and the connection to the drive is lost—it will not be possible to store recordings in the storage area. XProtect Corporate registers the availability of its recording servers' storage areas. This means that when a storage area becomes available again, it will again be possible to save recordings in the storage area. However, any recordings from the period in which the storage area was unavailable will be lost. When creating rules (see "Manage Rules" on page 221), you can use the events **Database Storage Area Unavailable** and **Database Storage Area Available** to trigger actions, such as the automatic sending of e-mail to relevant people in your organization (see **Events Overview** (on page 216) for more information). Furthermore, information about a storage area becoming unavailable/available will be logged (see "Manage Logs" on page 267).

How do I ensure that archiving is set up correctly? Archives are set up by adjusting several interdependent parameters correctly as described previously.

Can I create an archive on a network drive? Archives can be located either on the recording server computer itself, or at another location which can be reached by XProtect Corporate, for example on a network drive.

What happens when the maximum size of an archive is reached? When you create archives from the **Storage** tab (see "Storage Tab (Recording Server Properties)" on page 113), you specify a maximum size limit for the archive, in days and gigabytes. When either of the two maximum limits is reached, recordings in excess of the specified number of days/gigabytes will be removed. However, in order not to remove more recordings than necessary, excess recordings will be removed in chunks of approximately one hour's worth of recordings.

What happens if a scheduled archiving fails? If a scheduled archiving fails, for example because the archive is located on a network drive which is temporarily unavailable, XProtect Corporate will retry archiving after one minute. If that fails, another retry will take place after yet another minute, and so forth.



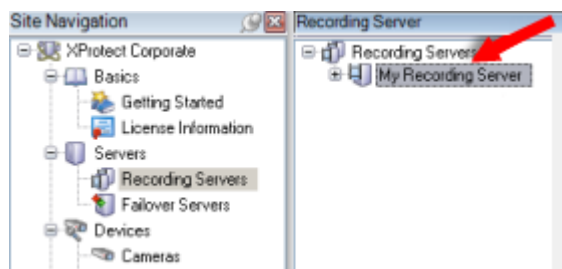
If the time of the next scheduled archiving is reached between two retries, an archiving attempt will be made at the scheduled time; if that attempt fails, XProtect Corporate will retry archiving after an hour, and so forth.

What happens if archiving is not finished before the next scheduled archiving? Your XProtect Corporate system inserts a compulsory period of archiving-free time after each finished archiving job. This ensures that archiving jobs do not overlap in time.

Manage Recording Servers

XProtect Corporate recording servers are used for recording video feeds, and for communicating with cameras and other devices. An XProtect Corporate surveillance system will typically contain several recording servers, although only a single recording server is required for the system to work.

Recording servers on your system— i.e. computers with the XProtect Corporate recording server software installed, and configured to communicate with an XProtect Corporate management server— will be listed in the Management Client's overview pane (see "Panels overview" on page 70) when you expand the **Servers** folder in the Site Navigation pane (see "Panels overview" on page 70) and then select the **Recording Servers** node.



Recording server listed in overview pane

Backward compatibility with recording servers from XProtect Corporate versions older than this current version is limited. You can still access recordings on such older recording servers; but in order for you to be able to change their configuration, they must be of the same XProtect Corporate version as this current one. It is thus highly recommended that all recording servers in your XProtect Corporate system are upgraded (see "Upgrade from previous version" on page 52) to the latest possible version.

IMPORTANT: When the **Recording Server Service** is running, it is **very** important that neither Windows Explorer nor other programs are accessing Media Database files or folders associated with your XProtect Corporate surveillance setup. Otherwise, the recording server might not be able to rename or move relevant media files. Unfortunately, this might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server Service, close the program accessing the media file(s) or folder(s) in question, and simply restart the Recording Server Service.

Authorizing a Recording Server

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

Why must I authorize recording servers? In an XProtect Corporate system, recording servers point to management servers, not the other way round. In theory, recording servers which you do not want to include in your surveillance system could thus be configured to connect to your management servers. By authorizing recording servers before they can be used, surveillance system administrators have full control over which recording servers are able to send information to which management servers.

1. Expand the **Servers** folder in the Management Client's Site Navigation pane and select the **Recording Servers** node.
2. Right-click the required recording server in the overview pane.



3. From the menu that appears, select **Authorize Recording Server**:

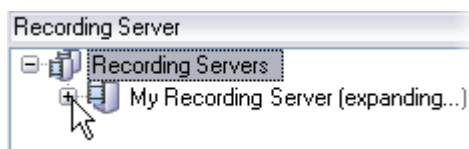


After a short moment, the recording server will be authorized and ready for further configuration.

Viewing/Editing a Recording Server's Properties

When a recording server is authorized, you are able to view/edit the recording server's properties, including its database storage area settings:

When you select the required recording server in the Management Client's overview pane, the recording server's properties are displayed in the properties pane (see "Panels overview" on page 70). Expand the required recording server to see which devices are connected to the recording server. While the Management Client loads information about the recording server, the text (... **expanding**) is displayed next to that recording server:



Adding Hardware (Cameras, etc.) to a Recording Server

You add IP hardware, such as cameras, video encoders, etc., to recording servers on your XProtect Corporate system through the **Add Hardware** wizard. The wizard helps you scan your network for relevant hardware. See the wizard **Add Hardware** (see "Add Hardware (Cameras, etc.)" on page 90) for more information.

Managing Hardware on a Recording Server

You have several options for managing IP hardware, such as cameras, video encoders, etc., on recording servers on your XProtect Corporate system. See Manage IP Hardware (see "Manage Hardware" on page 95).

Renaming a Recording Server

1. Expand the **Servers** folder in the Management Client's Site Navigation pane and select the **Recording Servers** node.
2. Right-click the required recording server listed in the overview pane.
3. From the menu that appears, select **Rename Recording Server**.

Tip: As an alternative to using the menu, press the F2 key on your keyboard.

4. You are now able to overwrite the name of the recording server in the overview pane.



Removing a Recording Server

IMPORTANT: Removing a recording server will remove all configuration specified for the recording server through the **Management Client**, including all of the recording server's associated hardware (cameras, input devices, etc.).

1. Expand the **Servers** folder in the Management Client's Site Navigation pane and select the **Recording Servers** node.
2. Right-click the no longer required recording server in the overview pane.
3. From the menu that appears, select **Remove Recording Server**.
4. You will be asked to confirm that you want to remove the recording server and all of its associated hardware from the XProtect Corporate system. If you are sure, click **Yes**.
5. The recording server and all of its associated hardware will be removed.

Replacing a Recording Server

If a recording server is malfunctioning and you want to replace it with a new server, while letting the new server inherit the settings of the old, malfunctioning recording server, do the following:

1. Retrieve the recording server ID from the old recording server;
 - a) In the Management Client's Site Navigation pane select **Recording Servers**, in the Overview pane select the old, required recording server.
 - b) In the Management Client's Properties pane, 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 found in the lower part of the **Info** tab. Do not copy **ID =** but only the ID itself.



IMPORTANT: Stop the Recording Server service (see "Management Server Service and Recording Server Service" on page 330) on the old recording server, then in Windows' **Services** set the service's **Startup type** to **Disabled**.

2. Replace recording server ID on the new recording server:
 - a) Make sure that the Recording Server service is stopped (see "Management Server Service and Recording Server Service" on page 330) and disabled on the old recording server.

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 Corporate 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>ff0b28852-48-58-8a00-0000-000000000000</id>
```



- e) Paste the copied recording server ID in between the tags `<id>` and `</id>`. Save the **RecorderConfig.xml** file.
- f) Restart the recording server service. When the new Recording Server service starts up, the recording server has inherited all settings on the old recording server.

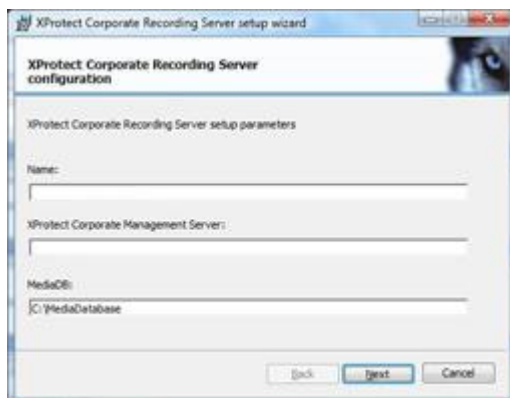
Tip: This procedure also applies if you re-install Windows on the computer running the recording server, even if you do not replace the computer running the recording server.

Troubleshooting: Missing Recording Servers

If you have installed several recording servers on your surveillance system, the recording servers should automatically be listed in the Management Client.

If your Management Client does not list all the recording servers you have installed, the most likely reason is that the missing recording servers have not been correctly configured to connect to a management server (in an XProtect Corporate system, recording servers point to management servers, not the other way round).

The configuration normally takes place during one of the steps in the recording server installation process. Here, you specified recording server setup parameters, among these the IP address or host name of the management server to which the recording server should be connected:



Example from recording server installation: the XProtect Corporate management server field specifies which management server the recording server should connect to.

Fortunately, you do not have to re-install recording servers in order to specify which management servers they should connect to. Once a recording server is installed, you can verify/change its basic configuration the following way:

How to Verify/Change which Management Server a Recording Server Connects to:

In order to verify/change a recording server's basic configuration, the recording server service must be stopped. This means that recording and live viewing will not be possible while you verify/change the recording server's basic configuration.



1. On the computer running the recording server, right-click the recording server icon in the notification area:



Tip: The notification area is occasionally also known as the system tray, it is located at the far right of the recording server computer's Windows taskbar.

2. From the menu that appears, select **Stop Recording Server Service**:



3. Right-click the notification area's **Recording Server** icon again.
4. From the menu that appears, select **Change Settings...**:



The **Recording Server Settings** window appears. Verify/change the following settings:

- **Management server hostname/IP address:** Lets you specify the 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 in order for the recording server to be able to communicate with the management server.
 - **Management server port:** Lets you specify the port number to be used when communicating with the management server. Default is port 9993, although you are able to change this if required.
5. Click **OK**.
 6. To start the Recording Server service again, right-click the notification area's **Recording Server** icon, and select **Start Recording Server Service**:





Read the Recording Server Icons

The following icons are used in the Management Client to indicate the state of individual recording servers:

Recording Server Service Icon	Description
	Recording server is running
	Recording server is communicating
	Recording server requires attention: This icon will typically appear because the recording server service has been stopped. Tip: You can verify whether the recording server is stopped by looking at the recording server icon in the notification area of the computer running the recording server. Right-clicking the recording server icon in the notification area opens a menu with which you can start/stop the recording server service, view recording server status messages, etc. See Recording Server Service Administration (see "Management Server Service and Recording Server Service" on page 330) for more information.
	Recording server must be authorized: Appears when the recording server is loaded for the first time. When first using a recording server, you must authorize it: Right-click the required recording server icon. From the menu that appears, select Authorize Recording Server. After a short moment, the recording server will be authorized and ready for further configuration.
	Ongoing database repair: Appears when databases have become corrupted, and the recording server is repairing them. The repair process may take considerable time if the databases are large. IMPORTANT: During the database repair it is not possible to record video from cameras connected to the recording server in question. Live video viewing will still be possible. How can databases become corrupted? Databases typically become corrupted if the recording server is shut down abruptly, for example due to a power failure or similar. See Protect Databases from Corruption (on page 329) for useful information about how to avoid corrupt databases.

Failover Tab (Recording Server Properties)

A failover server is a spare recording server which can take over if a regular recording server becomes unavailable; see also About Failover Servers (see "Manage Failover Servers" on page 321).

If your organization uses failover servers, use the **Failover** tab to select which groups of failover servers should take over from a regular recording server if the recording server in question becomes unavailable.



To access the **Failover** tab, select the required recording server in the overview pane (see "Panels overview" on page 70), then select the **Failover** tab in the properties pane (see "Panels overview" on page 70).



Selecting Required Failover Groups

- **Benefits of Using Failover Groups**

Grouping has a clear benefit: When you specify which failover servers should be able to take over from a recording server, you do not select a particular failover server; rather you select a failover group. If the selected group contains more than one failover server, this gives you the security of being able to have more than just one failover server ready to take over if the recording server becomes unavailable. For information about configuring failover groups, see Manage Failover Servers (on page 321).

- **Primary and Secondary Failover Group**

For each recording server, you are able to select a primary and an optional secondary failover group. If the recording server becomes unavailable, a failover server from the primary failover group will take over. If you have also selected a secondary failover group, a failover server from the secondary group will take over in case all failover 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 servers in the primary as well as in the secondary failover group are busy.

- **How to Select Required Failover Groups**

1. Select the required failover group from the Primary failover group list.
2. If you also want a secondary failover group for the recording server, repeat the process in the Secondary failover group list.

You cannot select the same failover group for use as both primary and secondary failover group.

Failover Service Communication Port

By default, TCP port 11000 is used for communication between recording servers and failover servers. Such communication is primarily about the configuration of the recording server from which the failover server should take over.

If required, you can change the port number. Note that if you change the port number, you must restart the Recording Server service (see "Management Server Service and Recording Server Service" on page 330) on the recording server in question.



Info Tab (Recording Server Properties)

You are able to verify or edit the name and description of a selected recording server on the **Info** tab. To access the **Info** tab, select the required recording server in the overview pane (see "Panels overview" on page 70), then select the **Info** tab in the properties pane (see "Panels overview" on page 70).



Info tab, displaying information about a recording server.

Info Tab's Fields

- **Name:** Name of the recording server. The name will be used whenever the recording server is listed in XProtect Corporate and clients. A name is not compulsory, but highly recommended. The name does not have to be unique.

To change the name, simply overwrite the existing name and click **Save** in the toolbar (see "Management Client Overview" on page 66).

Tip: If you change the name, it will be updated throughout XProtect Corporate. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- **Description:** Description of the recording server. The description will appear in a number of listings within XProtect Corporate. For example, the description will appear when pausing the mouse pointer over the recording server's name in the overview pane (see "Panels overview" on page 70). A description is not compulsory.

To specify a description, simply type the description and click **Save** in the toolbar (see "Management Client Overview" on page 66).

- **Host name:** Non-editable field, displaying the recording server's host name.
- **Web server URL:** Non-editable field, displaying the URL of the recording server's web server. The web server is used, for example, for handling PTZ camera control commands, and for handling browse and live requests from XProtect Smart Clients. The URL will include the port number used for web server communication (typically port 7563).
- **Time zone:** Non-editable field, displaying the time zone in which the recording server is located.

Storage Tab (Recording Server Properties)

On the **Storage** tab, you are able to setup, manage and view storage areas for selected recording servers. For a more general introduction to storing and archiving, see About Storage and Archiving (on page 101).



What is a storage area? A storage area is a directory in which database content— primarily recordings from the cameras connected to the recording server— is stored in at least a recording database and possibly archived in a number of archiving databases. A default storage area with a default recording database is automatically created for each recording server when the recording server is installed on the system. Unless you specifically define that another storage area should be used for particular cameras, recordings from connected cameras are stored in individual camera databases in the recording server's default storage area. Archives can be added to a storage area at any time convenient.

To access the **Storage** tab, select the required recording server on the Overview pane (see "Panels overview" on page 70), then select the **Storage** tab in the Properties pane (see "Panels overview" on page 70).

It is **not** possible to add databases or edit a storage area if the recording server is offline.

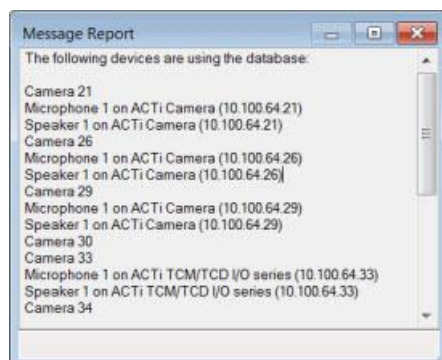


Example of the contents of a **Storage** tab

Storage Tab's Elements

Storage configuration list contents:

- **Name:** Indicates the name of the storage area. Click it to edit it.
- **Device Usage:** Indicates how many devices use the storage. Click the number link to see device details:





- **Default:** Indicates the default storage, i.e. the storage area in which database content is automatically stored unless you specifically define other storage areas for particular cameras. Only one storage at the time can be default.

Recording and archiving configuration list content:



1. Database name
2. Maximum size of the database (and usage; also represented graphically by a proportional filling of the database)
3. Database location
4. Archiving schedule for archiving to the next archive in the list. Note that the number of retention days stated for an archive includes all retention stated earlier in the process.

Tip: Pausing the mouse pointer over a database will show detailed database information.

Creating a New Storage Area

A storage area is always created with at predefined recording database named **Recording**, which cannot be renamed. Besides a recording database, a storage area can contain a number of archives, see [Creating an Archive within an Existing Storage Area](#) (on page 116).

1. To add an extra storage area to a selected recording server, click the  button located below the **Storage configuration** list.
2. This opens the **Storage and Recording Settings** dialog where you must specify the following:
 - **Name:** Rename the storage area if needed; use a descriptive and unique name.
 - **Path:** Type or use the browser link next to the field to specify the path to the directory in which to save the storage area. The storage area does not necessarily have to be located on the recording server computer itself.

Tip: If the directory you plan to use does not already exist, you can create it using the browser dialog. Network drives must be specified using UNC (Universal Naming Convention) format, example: [\\server\volume\directory\](#).

- **Retention time:** Select a number of units and select either **Days** or **Hours** to specify how long recordings should stay in the recording database before being deleted or archived (depending on archive settings). This is useful if you do not want your most recent recordings to be archived (or deleted) straight away even though archiving may be scheduled to take place before the specified number of hours.

Who determines the schedule? You do. You must specify the intervals with which the archiving process will start.

Example: If you specify 24 hours, recordings must be at least a day old before they will be archived. If archiving is scheduled to take place before the 24 hours have passed, only recordings older than 24 hours will be archived. Bear in mind that the archive's scheduling may mean that recordings will be older than the specified number of hours before they are archived. This may especially be the case if you specify an archiving schedule with long time spans between archiving.



Archiving is set up by adjusting several interdependent settings, see About Storage and Archiving (on page 101) for more information.

- **Maximum size:** Select the maximum number of gigabytes of recording data to save in the recording database.

Example: If you want to store up to 100 gigabytes of recording data in the database, select 100. Recording data in excess of the specified number of gigabytes will be auto-moved to the first archive in the list - if any is specified - or deleted.

IMPORTANT: This is one of two maximum size settings for the recording database. The **Retention Time** setting specified earlier may mean that recordings are removed from the recording database before the specified number of gigabytes is reached.

IMPORTANT: The oldest data in a database will always be 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 will be deleted. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data will be written to the database until enough space has been freed. The actual maximum size of your database will thus be the amount of gigabytes you specify, minus 5GB.

- **Signing:** Check this box if you want to write a digital signature to database files containing recorded data. This allows the XProtect Smart Client and the Smart Client – Player to verify that the contents of imported and opened databases have not been tampered with and that no database files have been removed.

Note that signing is turned off per default as it may affect system performance.

- **Encryption:** Select the appropriate level of encryption for the recording database by selecting either **None**, **Light** or **Strong**.

Note that the stronger the encryption, the more CPU usage it will cause.

- **Password:** (mandatory only if you selected **Light** or **Strong** in the **Encryption** field mentioned earlier): Click **Set...** to set a password.

3. Click **OK**.

If needed, you are now ready to create archive(s) within your new storage area, see Creating an Archive within an Existing Storage Area (on page 116).

Creating an archive within an existing storage area

A storage area has no default archive when it is created.

1. To create an archive, select the wanted storage area by clicking it in the **Recording and archiving configuration** list.
2. Next, click the  button located below the **Recording and archiving configuration** list.
3. This opens the **Archive Settings** dialog where you must specify the following:
 - **Name:** Rename if needed; use a descriptive and unique name.
 - **Path:** Type or use the browser link next to the field to specify the path to the directory in which to save the archive. The archive does not necessarily have to be located on the recording server computer itself.

Tip: If the directory you plan to use does not already exist, you can create it using the browser dialog. Network drives must be specified using UNC (Universal Naming Convention) format, example: [\\server\volume\directory\](#).



- **Retention time:** Select a number of units and select either **Days** or **Hours** to specify how long recordings should stay in the archive before being moved to another archive or deleted (depending on archive settings). The retention time must always be longer than the retention time of the last archive or the recording database. This is due to the fact that the number of retention days stated for an archive includes all retention stated earlier in the process.

Who determines the schedule? You do. You must specify the intervals with which the archiving process will start.

Example: If you specify 24 hours, recordings must be at least a day old before they will be archived. If archiving is scheduled to take place before the 24 hours have passed, only recordings older than 24 hours will be archived. Bear in mind that the archive's scheduling may mean that recordings will be older than the specified number of hours before they are archived. This may especially be the case if you specify an archiving schedule with long time spans between archiving.

Archiving is set up by adjusting several interdependent settings, see About Storage and Archiving (on page 101) for more information.

- **Maximum size:** Select the maximum number of gigabytes of recording data to save in the archive.

Example: If you want to store up to 100 gigabytes of recording data in the archive, select 100. Recording data in excess of the specified number of gigabytes will be auto-moved to the next archive in the list - if any is specified - or deleted.

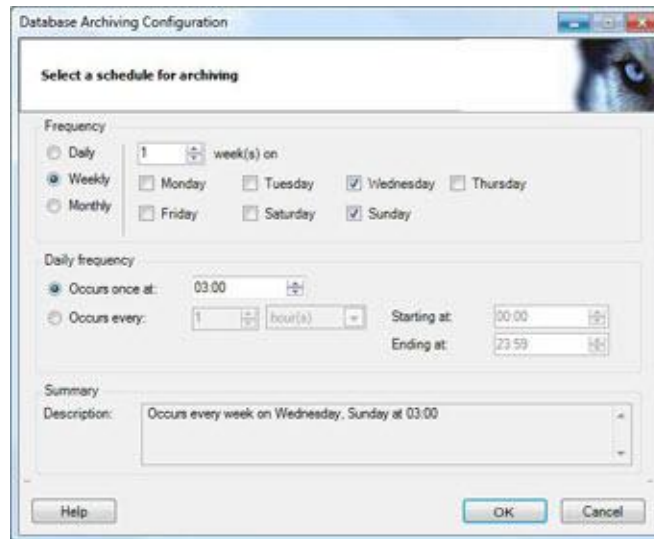
IMPORTANT: This is one of two maximum size settings for the storage area. The **Retention Time** setting specified earlier may mean that recordings are removed from the archive before the specified number of gigabytes is reached.

IMPORTANT: The oldest data in a database will always be 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 will be deleted. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data will be written to the database until enough space has been freed. The actual maximum size of your database will thus be the amount of gigabytes you specify, minus 5GB.

- **Schedule:** Click the **Schedule** icon next to the **Schedule** field to specify an archiving schedule, i.e. the intervals with which the archiving process should start. If required, you are able to make archiving take place very frequently (in principle every hour all year round), or very infrequently (for example, every first Monday of every 36 months).

What is the ideal interval? The ideal interval to use between each archiving process depends entirely upon your organization's needs. Consider your system's recording settings, make an estimate of the amount of data you expect to record within, for example, a day, a week, or a month, then decide on a suitable interval. Bear in mind that your organization's needs may change over time; it is thus a good idea to regularly monitor your archiving settings, and adjust them if required.

In this example, we have selected that archiving should take place twice every week: at three o'clock in the morning on Wednesdays and Sundays. Note that regional settings on your computer may mean that dates and times appear differently in your version of XProtect Corporate.



Tip: The effect of your selections is summed up in the lower part of the dialog. Use the summary to verify that your selections reflect your intentions.

Tip: If required, you can always adjust the archive's settings—including its scheduling—once the archive has been created.

- **Reduce frame rate:** Select the **Reduce frame rate** check box and set a frame per second (FPS) in order to reduce FPS when archiving.

Reducing frame rates by a selected number of FPS's will make your recordings take up less space in the archive. On the other hand, it also reduces quality since a number of frames are erased, leaving only FPS corresponding to the number of FPS selected in the dialog. MPEG/H.264 will be reduced to minimum key-frames.

Tip: It is possible to reduce frame rates to less than 1 FPS, for example as low as 0.1 FPS which means 1 frame every 10 seconds.

4. Click **OK**.

Deleting an Archive from within an Existing Storage

1. To delete an archive, select the wanted archive from the **Recording and archiving configuration** list by clicking it. A selected archive is marked by a dark frame.

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

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

Deleting an Entire Storage Area

Prerequisites

The storage area you want to delete must **not** be set as default storage area. Furthermore, it cannot be used by any devices to hold recordings. This means that you must possibly move devices and their **not yet archived** recordings to another storage area before you are allowed to delete the storage area, see Moving Non-archived



Recordings from One Storage Area to Another (see "Moving Non-archived Recordings from One Storage to Another" on page 119).

To Delete an Entire Storage Area

1. To delete a storage area, select the wanted storage area by clicking it.

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

2. Click the  button located below the **Storage configuration** list.
3. Click **Yes**.

Editing Settings for a Selected Storage Area or Archive

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

Tip: A selected database is marked by a dark frame.

2. Click the  button located below the **Recording and archiving configuration** list.
3. For editing a recording database, see Creating a New Storage Area (on page 115) and for editing an archive, see Creating a New Archive within an Existing Storage Area (see "Creating an archive within an existing storage area" on page 116).

If you change the maximum size of a database, recordings that exceed the new limit are auto-archived to the next archive or deleted - depending on archiving settings.

Moving Non-archived Recordings from One Storage to Another

1. Moving of contents from one recording database to another is done from the **Record** tab of the device in question.
2. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, select the wanted device type. In the Overview pane, select the wanted device.
3. In the Properties pane, click the **Record** tab. In the upper part of the **Storage** area, click **Select...**
4. In the **Select Storage** dialog that follows, select the wanted database.
5. Click **OK**.
6. In the **Recordings Action** dialog that follows, select whether already existing - but **non-archived** - recordings should be moved along to the new storage or deleted.
7. After selecting, click **OK**.

See also Record Tab Overview (on page 170).

About Upgrading

If your system is upgraded to XProtect Corporate 4.0 (or future versions), you might experience that you end up with a lot more storages than before upgrade. This is due to the fact that from XProtect Corporate 4.0 and forwards, database structure is somewhat different than it used to be and during the update process, the system



creates a number of extra databases. However, since your original naming-convention is respected, you are able to reconstruct your former database structure with only little moving about of devices and deletion of obsolete storages or databases.

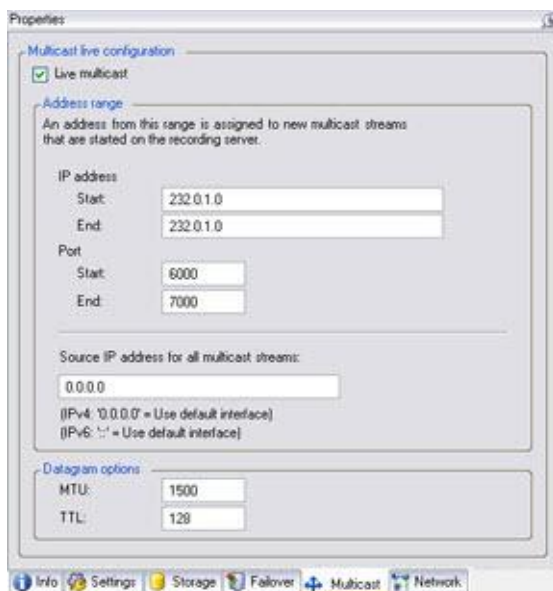
Manage Multicasting

XProtect Corporate supports multicasting of live streams from recording servers. In cases when many XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22) users want to view live video from the same camera, multicasting can help save considerable system resources. Multicasting is thus particularly useful if using XProtect Smart Clients' Matrix functionality, where multiple XProtect Smart Clients often 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 multicast on one of them. Through the Management Client you are able to specify which one to use.

The successful implementation of multicasting also requires that your network equipment (switches, etc.) has been set up 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.



What Is Multicasting?

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

- When using **unicasting**, the source must transmit one data stream for each recipient.
- When using **multicasting**, only a single data stream is required on each network segment.

Multicasting is therefore an interesting option for streaming live video from recording servers to XProtect Smart Client s since video streams will not be duplicated on each network segment.

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

With multicasting, you work with a clearly 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), etc. Thus,



multicasting should not be confused with the much more primitive method **broadcasting**, which would send data to everyone connected to the network, even if the data is perhaps not relevant for everyone:

- **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 thus significantly slow down network communication.

What Are the Requirements?

In order to use multicasting, your network infrastructure must support IGMP (Internet Group Management Protocol, an IP multicasting standard).

Furthermore, multicasting must be configured through the Management Client.

Enabling Multicasting

On the **Multicast** tab, select the **Live multicast** check box.

If the entire IP address range for multicast is already in use on one or more other recording servers, you cannot enable multicasting on further recording servers without freeing up some multicasting IP addresses first.

Assigning IP Address Range

In this section you specify the range from which you want to assign addresses for multicast streams from the selected recording server. Clients will connect to these addresses when viewing multicast video from the recording server in question.

- **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. For more info, see the following.
- **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:** If a recording server has more than one network interface card, it is only possible to multicast on one of them. This field is therefore relevant if your recording server has more than one network interface card—or if it has a network interface card with more than one IP address.

To use the recording server's default interface, leave the value 0.0.0.0 (IPv4) or :: (IPv6) in the field. If you want to use another network interface card, or a different IP address on the same network interface card, specify the IP address of the required interface.

Specifying Datagram Options

In this section you specify settings for data packets (datagrams) transmitted through multicasting.

- **MTU:** Maximum Transmission Unit, the largest allowed physical data packet size (measured in bytes). Messages larger than the specified MTU will be split into smaller packets before being sent. 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.



Enabling Multicasting for Individual Cameras

Even when you have specified multicasting settings for the selected recording server, multicasting will not work until you enable it for required cameras:

Select the required recording server in the Management Client's Site Navigation pane (see "Panels overview" on page 70), select the required camera in the overview pane (see "Panels overview" on page 70), then select **Live multicast** on the Client tab (see "Client Tab (Camera Properties)" on page 127) in the properties pane (see "Panels overview" on page 70). Repeat for all required cameras under the recording server in question.

Specify IP Address Range

To specify the range from which you want to assign addresses for multicast streams from the selected recording server do the following:

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

Example: If you want multicast for 1000 cameras, you would need either:

- 1 IP address and a range of 1000 different ports, OR
- a range of two IP addresses and a range of 500 different ports (or any matching combination), OR
- a range of 1000 IP addresses and a single port

When specifying the 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.

Tip: If required, a range may include only one IP address (IPv4 example: 232.0.1.0-232.0.1.0)

IP addresses for multicasting must be within a special range set aside for dynamic host allocation by IANA (the authority overseeing global IP address allocation). If using IPv4, there is a certain range which goes from 232.0.1.0 to 232.255.255.255. If using IPv6 (on page 338), the range is different.

Manage Public Addresses

You define a recording server's public IP address on the **Network** tab. To access the **Network** tab, select the required recording server in the overview pane (see "Panels overview" on page 70), then select the **Network** tab in the properties pane (see "Panels overview" on page 70).

This description is also valid for failover servers (see "Manage Failover Servers" on page 321).

Why Use a Public Address?

When an access client, such as an 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 completely 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. See also Manage Local IP Address Ranges (on page 292).
- When clients connect from the internet, the surveillance system should reply with the recording server's public address, i.e. 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).



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

Enabling Public Access

To enable public access, select the **Network** tab's **Enable public** access box.

Defining Public Address and Port

When public access is enabled, you are able to define the recording server's public address and public port number in the **Public address** and **Public port** fields respectively.

As public address, use the address of the firewall or NAT router which clients accessing the surveillance system from the internet must go through in order to reach recording servers.

Specifying a public port number is compulsory; it is always a good idea that port numbers used on the firewall or NAT router are different from the ones used locally.

When using public access, the firewall or NAT router used must be configured so requests sent to the public address and port are forwarded to the local address and port of relevant recording servers.

Local IP Ranges

There are cases when the recording server's public address should not be used: When clients connect from the local network, the surveillance system should reply with local addresses and port numbers. 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 are able to define a list of IP ranges which the surveillance system should recognize as coming from a local network. You do this by clicking **Configure...** on the **Network** tab. See Manage Local IP Address Ranges (on page 292) for more information.

Servers and Clients Require Time-Synchronization

Part of the security surrounding the use of remote clients with XProtect Corporate is based on so-called time-based tokens.

Why Servers Require Time-Synchronization

When a client logs in to the surveillance system, the client receives a token from the management server. The token contains important security-related time information.

The management server also sends a similar token to the required recording server(s). This is partly due to the fact that recording servers may be located all around the world; each recording server thus uses the token to validate the client's token against the local time in the recording server's own time zone.

The validity of a token expires after a while. It is therefore important that time on your management server and all of your organization's recording servers is synchronized (minute and second-wise; hours may of course be different in different locations around the world). If time on the servers is not synchronized, you may experience that a recording server is ahead of the management server's time.

When a recording server is ahead of the management server's time, it may result in a client's token expiring on the recording server earlier than intended by the management server. Under unfortunate circumstances you might even experience that a recording server claims that a client's token has already expired when it receives it; effectively preventing the client from viewing recordings from the recording server.



How to synchronize time on your organization's servers depends on your network configuration, internet access, use of domain controllers, etc. Often, servers on a domain are already time-synchronized against the domain controller. If so, you should be fine as long as all required servers belong to the domain in question.

If your servers are not already time-synchronized, it will be necessary to synchronize the servers' time against a time server, preferably the same time server.

The following articles from Microsoft describe what to do in different situations:

- How to configure an authoritative time server in Windows Server 2003 (see <http://support.microsoft.com/kb/816042/en-us> - <http://support.microsoft.com/kb/816042/en-us>)
- Registry entries for the W32Time service (see <http://support.microsoft.com/kb/223184/en-us> - <http://support.microsoft.com/kb/223184/en-us>)

If these links do not work for you, try searching www.microsoft.com (see <http://www.microsoft.com/> - <http://www.microsoft.com/>) for time server, time service, synchronize servers or similar.

It is also very important that XProtect Smart Client s are time-synchronized with the management server.

Why Clients Require Time-synchronization

Because configuration communication is facilitated by the service channel (see "About the Service Channel" on page 330), it is advantageous that XProtect Smart Client s are also time-synchronized with the management server and the computer running the Service Channel service. A time difference of five minutes between XProtect Smart Client and servers is tolerated.

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 in Setup mode. This means that users risk overwriting each other's configuration changes.



Devices

About Devices

To add cameras, go to Add Hardware (see "Add Hardware (Cameras, etc.)" on page 90). To replace cameras, go to Manage Hardware (on page 95).

In the Management Client's Site Navigation pane (see "Panels overview" on page 70), you are able to work with the following under **Devices**:

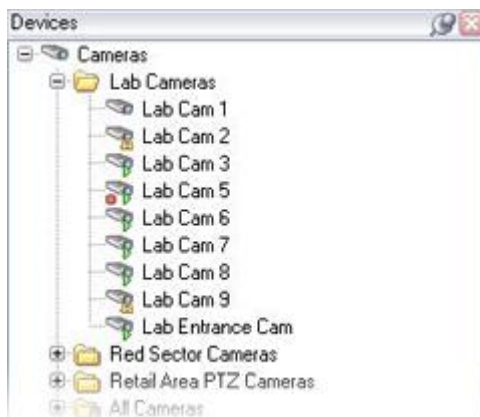
- **Cameras:** (see "Manage Cameras" on page 125) Lets you handle the majority of camera configuration and management. **Microphones:** (see "**Manage Microphones**" on page 144) On many devices you are able to attach external microphones; some devices even have built-in microphones.
- **Speakers:** (see "**Manage Speakers**" on page 147) On many devices you are able to attach external loudspeakers; some devices even have built-in speakers.
- **Inputs:** (see "**Manage Input**" on page 149) On many devices you are able to attach external units, typically external sensors, to input ports on the device. Input from such external input units can be used for many purposes in XProtect Corporate.
- **Outputs:** (see "**Manage Output**" on page 154) On many devices you are able to attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through XProtect Corporate.

Manage Cameras

To add cameras, go to Add Hardware (see "Add Hardware (Cameras, etc.)" on page 90). To replace cameras, go to Manage Hardware (on page 95).

Enabling/disabling as well as renaming of individual cameras takes place on the recording server hardware management level; see Managing Hardware (see "Manage Hardware" on page 95).

For all other configuration and management of cameras, expand **Devices** in the Management Client's Site Navigation pane (see "Panels overview" on page 70), then select **Cameras**. In the overview pane (see "Panels overview" on page 70), you group your cameras for an easy overview of your cameras. Grouping also lets you specify common properties for all cameras within a group in one go. See Using Device Groups (see "About Device Groups" on page 159) for information about creating groups as well as adding cameras to your groups.



Device groups are used for grouping cameras

Once you have placed your cameras in groups, configuration can begin.



Configuring Individual Cameras

You configure individual cameras by selecting the required camera in the list, then specifying the camera's required settings on the tabs in the **Properties** pane:

- The Info tab (see "Info Tab Overview" on page 166) for managing the selected camera's name, etc.
- The Settings tab (see "Settings Tab Overview" on page 174) for managing the selected camera's general settings.
- The Streams tab (see "About Multi-streaming" on page 163) for managing the selected camera's video streams.
- The Record tab (see "Record Tab Overview" on page 170) for managing the selected camera's recording, database and archiving storage settings.
- The Presets tab (see "PTZ Tab (Hardware Properties)" on page 168) for managing the selected camera's preset positions (only available if the selected camera is a PTZ camera).
- The Patrolling tab (see "PTZ Patrolling Tab (Camera Properties)" on page 136) for managing the selected camera's patrolling profiles (only available if the selected camera is a PTZ camera).
- The Events tab (see "Events Tab Overview" on page 164) for managing hardware configurable events.
- The Client tab (see "Client Tab (Camera Properties)" on page 127) lets you specify information which will affect client's use of the selected camera.
- The Privacy Mask tab (see "Privacy Mask Tab (Camera Properties)" on page 133) lets you enable and configure privacy masking for the selected camera.
- The Motion tab (see "Motion Tab (Camera Properties)" on page 129) for managing the selected camera's motion detection settings.

Read the Camera List's Status Icons

The following icons are used to indicate status of cameras (see "Manage Cameras" on page 125), microphones (see "Manage Microphones" on page 144), speakers (see "Manage Speakers" on page 147), input (see "Manage Input" on page 149) and output (see "Manage Output" on page 154) events in item lists:

Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item enabled: Can communicate with the recording server, and can if required be started/stopped automatically through a rule.
					Item recording. Speaker being recorded: Note that what is being said through the speaker can be recorded, but cannot subsequently be played back or exported (for example to prove that a warning was given).

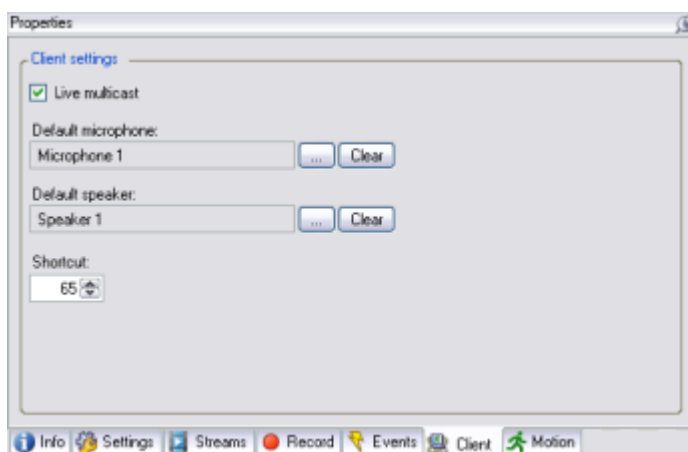


Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item temporarily stopped or has no feed: Often shown when an item is communicating with XProtect Corporate while it is being disabled or enabled. Also shown if the Default Start Audio Feed Rule is not active; see Managing Rules. When stopped, no information is transferred to XProtect Corporate. In which case—if it is a camera—neither live viewing nor recording will be possible. However, a stopped item will still be able to communicate with the recording server, as opposed to when an item is disabled.
					Item disabled: Cannot be started automatically through a rule and will not be able to communicate with the recording server. In the case of a camera, when a camera is disabled, neither live viewing nor recording will be possible.
					Item database being repaired.
					Item requires attention.
					Status unknown.
					Note that some icons may be combined, as in this example where Item is enabled is combined with Item is recording (since a recording item is also an enabled item).

Client Tab (Camera Properties)

The **Client** tab lets you specify information which will affect clients' use of the selected camera. To access the **Client** tab, select the required camera in the overview pane (see "Panels overview" on page 70), then select the **Client** tab in the properties pane (see "Panels overview" on page 70).

Due to the limited feature set of the Remote Client (on page 24), settings on the **Client** tab will only affect XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22)s' use.



Client settings

- **Live multicast:** XProtect Corporate supports multicasting (see "Manage Multicasting" on page 120) (sending of single data packets to multiple recipients within a group, thereby saving bandwidth and system resources) of live streams from recording servers to XProtect Smart Clients (see "Installing the



XProtect Smart Client" on page 22). To enable multicasting of live streams from the selected camera, select the check box.

Remember that for the feature to work, multicasting must also be configured for the recording server; see Manage Multicasting (on page 120). If multicasting is not possible, for example due to restrictions on the network or on individual clients, XProtect Corporate will revert to unicasting (sending of separate data packets to separate recipients).

- **Default microphone:** By defining a default microphone, you can determine from which microphone XProtect Smart Client users should by default hear recordings when they select the camera in question in their XProtect Smart Clients. The users can subsequently select another microphone if they require so.

Bear in mind that although you have defined a default microphone for a camera, it cannot be guaranteed that all XProtect Smart Client users will hear audio from the microphone in question: Some users may not have speakers attached, some users may not have the rights required to listen to audio, etc.

- **Default Speaker:** By defining a default speaker, you can determine through which microphone XProtect Smart Client users should by default be able to speak when they select the camera in question in their XProtect Smart Clients. The users can subsequently select another speaker if they require so.

Bear in mind that although you have defined a default speaker for a camera, it cannot be guaranteed that all XProtect Smart Client users will be able to talk through the speaker in question: Some users may not have a microphone attached, some users may not have the rights required to talk through speakers, etc.

- **Shortcut:** Users of the XProtect Smart Client can take advantage of a range of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers, which are used to identify each camera. In the Management Client, each camera's shortcut number is specified in the **Shortcut** field.

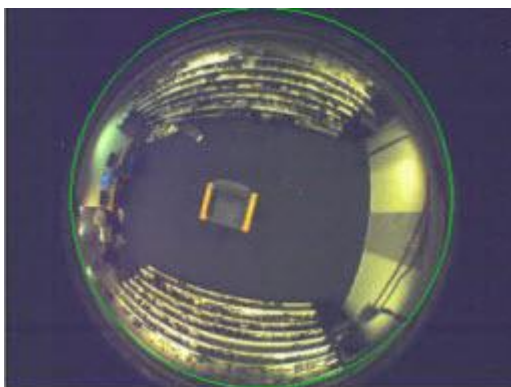
A camera shortcut number must not contain any letters or special characters, and cannot be longer than four digits. Examples of correct camera shortcut numbers: **3**, **1234**. Examples of incorrect camera shortcut numbers: **A*3**, **12345**. Always use a unique camera shortcut number for each camera.

Tip: Find more information about audio and keyboard shortcuts from an XProtect Smart Client user's perspective in the separate XProtect Smart Client documentation available on the XProtect Corporate software DVD as well as from www.milestonesys.com.

Fisheye Tab (Camera Properties)

Use of the fisheye technology requires a dedicated fisheye camera.

The **Fisheye** tab lets you configure the fisheye functionality of a camera. Fisheye is a technology that allows viewing of 360° panoramic images through an advanced lens.



Configuration



If the camera is mounted on a ceiling, you can adjust the behavior of the navigation buttons to reflect this by selecting the **Ceiling mount** check box.

The camera's fisheye functionality is configured by adjusting its fisheye view field, indicated by a green ellipse in the preview image, so it encloses the actual image area of the fisheye lens. Click **Auto Calculate** to do this automatically.

It is also possible to adjust the fisheye view manually. You do this by specifying a number of values which will be used by the fisheye technology for converting the elliptic image into an ordinary rectangular image.

You can set the ellipse's X-radius, Y-radius, X-center, and Y-center by using the arrow buttons to adjust the ellipse.

Preview

In the preview section of the **Fisheye** tab you can set a particular position in the fisheye-rendered view as the camera's home position: Navigate to the required position, using the navigation buttons, then click **Set as Home Position**.

The navigation buttons let you move the camera as follows:

Icon	What it does...	
	Moves the view	up and to the left
		up
		up and to the right
		to the left
		to its default position
		to the right
		down and to the left
		down
		down and to the right
	Zooms in (one zoom level per click)	
	Zooms out (one zoom level per click)	

Motion Tab (Camera Properties)

The **Motion** tab lets you enable and configure motion detection for the selected camera. Motion detection configuration is a key element in your XProtect Corporate surveillance solution: Your motion detection configuration may determine when video is recorded, when events are generated, when external output (such as lights or sirens) is triggered, etc.



Time spent on finding the best possible motion detection configuration for each camera may therefore help you later avoid unnecessary alarms, etc. Depending on the physical location of the camera, it may be a very good idea to test motion detection settings under different physical conditions (day/night, windy/calm weather, etc.).

Before you configure motion detection for a camera, it is highly recommended that you have configured the camera's image quality settings, such as resolution, compression, etc., on the **Settings** tab (see "Settings Tab Overview" on page 174). 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 motion detection for all cameras in a device group (see "Manage Cameras" on page 125) in one go. Note, however, that some motion detection settings must be configured individually for each camera. This is the case with exclude regions (areas in which not to use motion detection), as these are very likely to vary from camera to camera.

Enabling and Disabling Motion Detection

Motion detection is enabled by default. To enable/disable motion detection for a camera, select/clear the **Motion** tab's **Motion detection** check box.

When motion detection is disabled for a camera, any motion detection-related rules (see "Manage Rules" on page 221) for the camera will not work.

Motion Detection Settings

You are able to specify settings relating to the amount of change required in a camera's video in order for the change to be regarded as motion. You are also able to specify intervals between motion detection analyses, any areas of an image in which motion should be ignored, etc.

Sensitivity slider:

Determines **how much each pixel** in the camera's images must change before it is regarded as motion.

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 will be allowed in each pixel before it is regarded as motion.



The **lower** the sensitivity level, the more change in each pixel will be allowed before it is regarded as motion. This way you are able to allow insignificant changes, which should not be regarded as motion.

Pixels in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted.



Highlighted motion in the preview image

Tip: Your exact sensitivity slider setting is indicated by a number from 0-300 in the right side of the slider. This way you are able to compare the exact sensitivity slider setting between cameras.

Tip: If you find the concept of motion detection sensitivity difficult to grasp, try dragging the slider to the left towards the highest possible sensitivity (0) position: The more you drag the slider towards the highest possible sensitivity position, the more of the preview image becomes highlighted in green. This is because with a very high sensitivity level even the slightest change in each pixel will be regarded as motion.

Motion slider:

Determines **how many pixels** in the camera's images image must change before it is regarded as motion.

The selected motion level is indicated by the black vertical line in the motion indication bar above the sliders.

The black vertical line in the motion indication serves as a threshold: When detected motion is above the selected sensitivity level, the bar changes color from green to red, indicating a positive detection.



Motion indication bar deflection changes color from green to red when above the threshold, indicating a positive motion detection

Tip: Your exact motion slider setting is indicated by a number from 0-10.000 in the right side of the slider. This way you are able to compare the exact motion slider setting between cameras.

Keyframe settings:

Determines if motion detection should be done on keyframes only or on the entire video stream.

Select **Keyframes only** to do motion detection on keyframes only.

Image processing interval:

Lets you select how often motion detection analysis should be carried out on video from the camera.

From the **Process image every (msec):** list, select the required interval: every 100 milliseconds (i.e. once every tenth of a second), every 250 milliseconds, every 500 milliseconds, every 750 milliseconds, or every 1000 milliseconds (i.e. once every second). Default is every 500 milliseconds.

The interval is applied regardless of the camera's frame rate settings.

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 will reduce the amount of processing power used to carry out the analysis, but will also mean a less accurate motion detection.



In the **Detection method** drop down-box, select the wanted detection method.

Exclude regions:

Lets you disable motion detection in specific areas of a camera's images. Parts of images in which motion should be ignored this way are called **exclude regions**.

Disabling motion detection in specific areas may help 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.

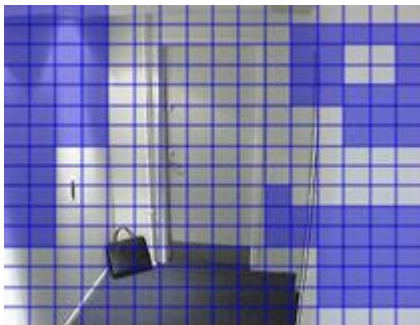
When exclude regions are used with PTZ cameras and you pan/tilt/zoom the camera, the excluded area will not move accordingly. This might mean that objects originally excluded will be included. This is due to the fact that the exclude region is locked according to the camera's view, not the excluded region. Consequently, it is not recommended to use exclude regions with PTZ cameras.

To use exclude regions, select the **Use exclude regions** check box.

When done, the preview image will be divided into selectable sections by a grid.

To define exclude regions, drag the mouse pointer over the required areas in the preview image. Pressing down the left mouse button selects a grid section; right mouse button clears a grid section.

You are able to define as many exclude regions as you require. Excluded regions are shown in blue.



Three exclude regions defined in the preview window. In this case, the grid is visible.

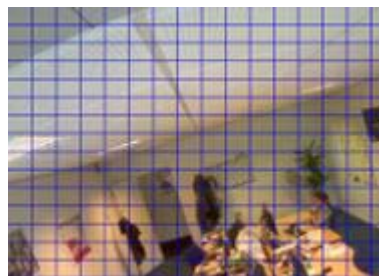
The blue exclude area indications will only appear in the preview image on the **Motion** tab, not in any other preview images in the Management Client or access clients.

- **Grid Size**
The value selected in the **Grid size** list determines the density of the grid, regardless whether the grid is shown or not.

Select between the values 8×8 (i.e. a grid dividing the image into eight sections along the X-axis and eight sections along the Y-axis), 16×16, 32×32 or 64×64.

With a grid of 8×8, the image will be divided into relatively few sections for you to select for exclude regions. Each section will be relatively large; you will not be able to define very detailed exclude regions. With a grid size of 64×64, the image will be divided into relatively many sections for you to select for exclude regions. Each section will be relatively small, enabling you to define more detailed exclude regions.

Examples of 8×8, 16×16, 32×32 and 64×64 grids respectively:





The four different grid sizes.

- **Show Grid**

The grid may be visible or hidden, depending on whether the **Show grid** check box is selected or not.

When the **Show grid** check box is selected (default), the preview image will feature a grid indicating the division of the preview image into selectable sections. The grid may help you when selecting exclude regions in the preview image.

The density of the grid is determined by the value selected in the **Grid size** list.

Showing the grid is not a requirement for selecting exclude regions; even without the grid you are able to select exclude regions as described earlier. Hiding the grid may provide a less obscured view of the preview image.

- **Show Regions**

When the **Show regions** check box is selected (default), exclude regions will be highlighted in blue in the preview image.

Hiding exclude regions may provide a less obscured view of the preview image. However, under normal circumstances it is highly recommended that you keep the **Show regions** box selected; otherwise exclude regions may exist without you or your colleagues being aware of it.

The blue exclude area indications will only appear in the preview image on the **Motion** tab, not in any other preview images in the Management Client or access clients.

- **Pen size**

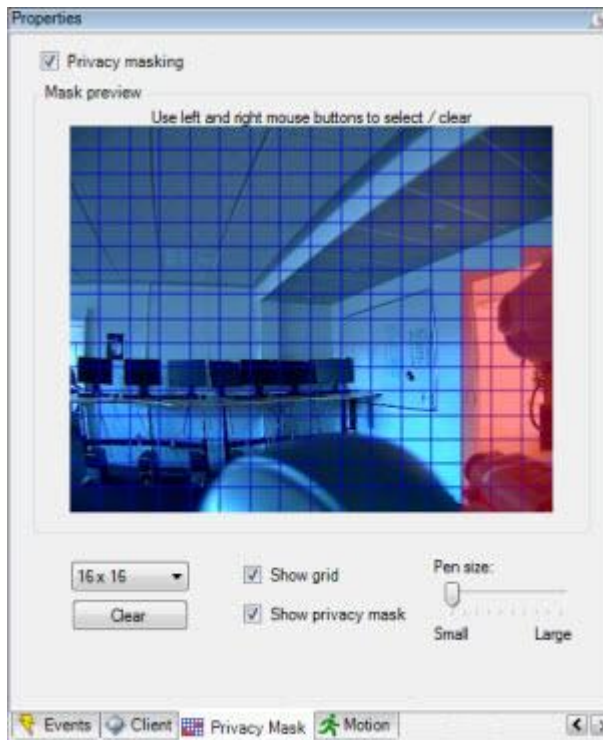
Use the **Pen size** slider to indicate the size of the selections you wish to make when clicking and dragging the grid to select regions for privacy masking. Default is set to small, which is equivalent to one square in the grid.

Privacy Mask Tab (Camera Properties)

The **Privacy Mask** tab lets you enable and configure privacy masking for the selected camera. Among other things, you can define if and how selected areas of a camera's view should be masked before distribution. For example, if a surveillance camera films a street, in order to protect residents privacy, you can mask certain areas of a building (could be windows and doors) with privacy masking. This is even needed in some countries to comply with national legislation.



As Administrator you are also able to see through privacy masked areas, and can turn showing of privacy masked areas on and off. When viewed via XProtect Smart Client, Remote Client, or any other media, privacy masked areas will be represented as black areas and it is impossible to see behind the privacy masking or in any way remove it.



Red areas indicate the areas masked for privacy.

When privacy masks are used with PTZ cameras and you pan/tilt/zoom the camera, the selected area masked for privacy will **not** move accordingly. This might mean that objects masked for privacy become visible. This is due to the fact that the masked area is locked according to the camera's view, not the masked object. Consequently, it is not recommended to use privacy masking with PTZ cameras.

Enabling and Disabling Privacy Masking

The privacy masking feature is enabled by default. To enable/disable the privacy masking feature for a camera, select/clear the **Privacy Mask** tab's **Privacy masking** check box.

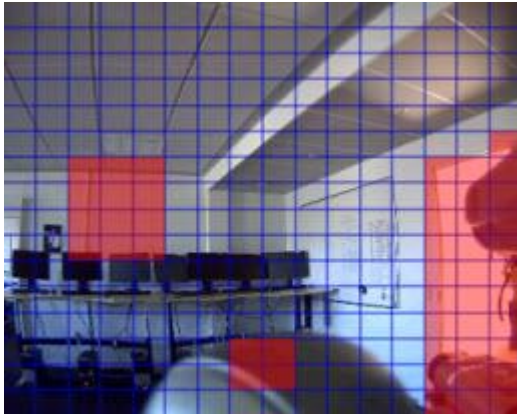
Privacy Masking Settings

When you enable privacy masking, the preview image is divided into selectable sections by a grid.

To define privacy mask regions, drag the mouse pointer over the required areas in the preview image. Pressing down left mouse button selects a grid section; right mouse button clears a grid section.



You are able to define as many privacy mask regions as you require. 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 will also appear in the preview image on the **Motion** tab.

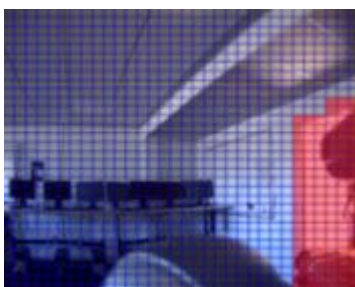
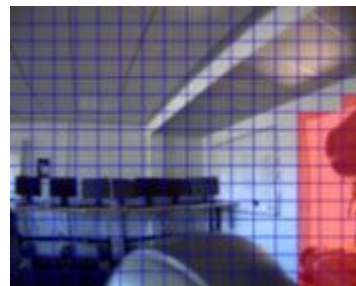
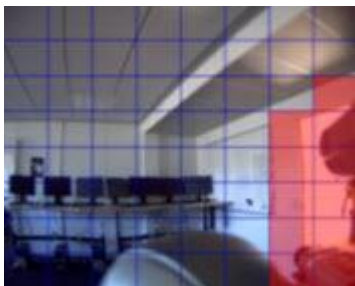
- **Grid Size**

The value selected in the **Grid size** list determines the density of the grid, regardless whether the grid is shown or not.

Select between the values 8×8 (i.e. a grid dividing the image into eight sections along the X-axis and eight sections along the Y-axis), 16×16, 32×32 or 64×64.

With a grid of 8×8, the image will be divided into relatively few sections for you to select for privacy mask regions. Each section will be relatively large; you will not be able to define very detailed privacy mask regions. With a grid size of 64×64, the image will be divided into relatively many sections for you to select for privacy mask regions. Each section will be relatively small, enabling you to define more detailed privacy mask regions.

Examples of 8×8, 16×16, 32×32 and 64×64 grids respectively:



The four different grid sizes.



- **Show Grid**

The grid may be visible or hidden, depending on whether the **Show grid** check box is selected or not.

When the **Show grid** check box is selected (default), the preview image will feature a grid indicating the division of the preview image into selectable sections. The grid may help you when selecting privacy mask regions in the preview image.

Showing the grid is not a requirement for selecting privacy mask regions; even without the grid you are able to select privacy mask regions as described above. Hiding the grid may provide a less obscured view of the preview image.

- **Show Privacy Masks**

When the **Show privacy masks** check box is selected (default), privacy mask regions will be highlighted in red in the preview image.

Hiding privacy mask regions may provide a less obscured view of the preview image.

However, under normal circumstances it is highly recommended that you keep the **Show privacy masks** box selected; otherwise exclude privacy mask regions may exist without you or your colleagues being aware of it.

- **Pen size**

Use the **Pen size** slider to indicate the size of the selections you wish to make when clicking and dragging the grid to select regions for privacy masking. Default is set to small, which is equivalent to one square in the grid.

PTZ Patrolling Tab (Camera Properties)

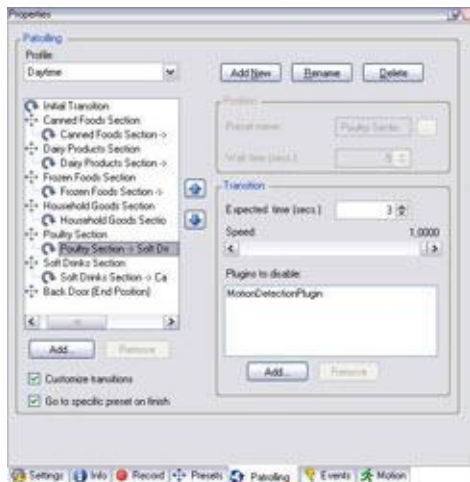
The **Patrolling** tab lets you create patrolling profiles, the automatic movement of a PTZ (Pan/Tilt/Zoom) camera between a number of preset positions (see "PTZ Presets tab (camera properties)" on page 140). Before you are able to work with patrolling, you must have specified at least two preset positions for the camera.

You manage patrolling on the **Patrolling** tab, which is available only when the selected camera is a PTZ camera.

Patrolling profiles are the definitions of how patrolling should take place. This includes the order in which the camera should move between preset positions, how long it should remain at each position for, etc. You are able to create an unlimited number of such patrolling profiles and use them in your rules (see "Manage Rules" on page 221). For example, you may create a rule specifying that one patrolling profile should be used during daytime opening hours, and another during nights.



In order to use PTZ cameras' features, including the ability to pan, tilt, and zoom, operators must have a role which gives them the necessary rights. See About Roles (on page 249) for more information, including step-by-step descriptions of how to assign users to roles and how to specify the rights of roles.



Patrolling tab, displaying a patrolling profile with customized transitions

Adding a New Patrolling Profile

1. Click **New**. This will open the **Add Profile** dialog.
2. In the **Add Profile** dialog, specify a name for the patrolling profile:

Tip: Use a descriptive name; the name may later be used in situations where you will not have access to details about the item, e.g. when using it in a rule.

3. Click **OK**. The new patrolling profile will be added to the **Patrolling** tab's **Profile** list. You are now able to specify required preset positions and other settings for the patrolling profile.

Specifying Preset Positions for Use in a Patrolling Profile

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



2. Click **Add**. This will open the **Select Preset** dialog.
3. In the **Select Preset** dialog, select the preset positions required for your patrolling profile:





- Click **OK**. The selected preset positions are added to the list of preset positions for the patrolling profile:



- The preset position at the top of the list will be used as the first stop when the camera patrols according to the patrolling profile, the preset position in second position from the top will be the second stop, and so forth.

If required, change the sequence by selecting the required preset position and using the up/down buttons:

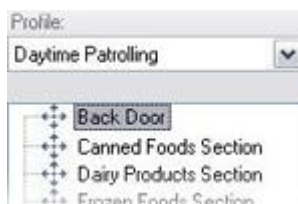


Tip: If required, you can easily add more preset positions to the list by clicking **Add**, or remove unwanted preset positions from the list by selecting the unwanted preset position, then clicking **Remove**.

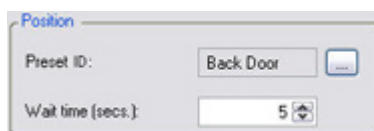
Specifying How Long to Stay at Each Preset Position for

When patrolling, the PTZ camera will by default remain for 5 seconds at each preset position specified in the patrolling profile before it moves on to the next preset position. To change the number of seconds for which the PTZ camera will remain at a specific preset position, do the following:

- Select the required patrolling profile in the **Profile** list.
- In the list of preset positions for the selected patrolling profile, select the preset position for which you want to change the time:



- Specify the required time (in number of seconds) in the **Wait time (secs.)** field:



- If required, repeat for other preset positions.

Customizing Transitions

By default, the time required for moving the camera from one preset position to another, known as **transition**, is estimated to be 3 seconds. During this time, motion detection is by default disabled on the camera, as irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions. Transitions are also known as PTZ scanning.

Customizing speed for transitions is only supported if your camera supports PTZ scanning and is of the type where preset positions are configured and stored on the XProtect Corporate server (type 1 PTZ camera). Otherwise the **Speed** slider is grayed out.



You can customize the transitions between each of the preset positions in a patrolling profile. You are able to customize the following:

- The estimated transition time
- The speed with which the camera will move during a transition
- Which plug-ins to disable during transition.

To customize transitions between preset positions in a patrolling profile, do the following:

1. Select the required patrolling profile in the **Profile** list.
2. Select the **Customize transitions** check box:



This will add transition indications to the list of preset positions for the selected patrolling profile.

3. In the list, select the required transition:



4. Specify the estimated transition time (in number of seconds) in the **Expected time (secs.)** field:



5. Use the **Speed** slider to specify the required transition speed. When the slider is in its rightmost position, the camera will move with its default speed. The more you move the slider to the left, the slower the camera will move during the selected transition.

Tip: A number indicating the exact speed is displayed near the top right corner of the slider. When required, the number (from 0.0001 (very slow) to 1.0000 (default speed)) allows you to define exactly the same custom speed across transitions.

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.

To add a plug-in to the list, click **Add...**, and select the required plug-in. This requires that one or more other plug-ins are available, and that they can be disabled.

To remove a plug-in from the list, for example if you do not want motion detection to be disabled during the transition, select the plug-in and click **remove**.

7. Repeat as required for other transitions.

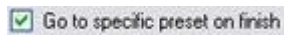
Specifying an End Position

You are able to specify that the camera should move to a specific preset position when patrolling according to the selected patrolling profile ends.

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



2. Select the **Go to specific preset on finish** check box:



This will open the **Select Preset** dialog.

3. In the **Select Preset** dialog, select the required end position, and click **OK**.

Tip: 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 list of preset positions for the selected patrolling profile. When patrolling according to the selected patrolling profile ends, the camera will go to the specified end position.

Renaming an Existing Patrolling Profile

1. Select the required patrolling profile in the **Profile** list.
2. Click **Rename**. This will open the **Rename Profile** dialog.
3. In the **Rename Profile** dialog, type a new name for the patrolling profile.

Tip: Use a descriptive name; the name may later be used in situations where you will not have access to details about the item, e.g. when using it in a rule.

4. Click **OK**.

Specifying Manual PTZ Session Timeout

Patrolling of PTZ cameras may be interrupted manually by XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22) users with the necessary user rights.

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

1. In the Management Client's menu bar, select **Tools > Options**. This will open the **Options** window.
2. On the **Options** window's **General** tab, select the required amount of time in the **PTZ manual session timeout** list (default is 15 seconds).

The setting will apply for all PTZ cameras on your XProtect Corporate system.

PTZ Presets tab (camera properties)

The **Presets** tab lets you create preset positions to be used, for example, in rules (see "Manage Rules" on page 221) for making a PTZ (Pan/Tilt/Zoom) camera move to a specific preset position when an event occurs, as well as in patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 136), the automatic movement of a PTZ camera between a number of preset positions.

You manage preset positions on the **Presets** tab, which is available only when the selected camera is a PTZ (Pan/Tilt/Zoom) camera. The **Presets** tab will not be available if the selected PTZ camera does not support preset positions.



In order to use PTZ cameras' features, including the ability to pan, tilt, and zoom, operators must have a role which gives them the necessary rights. See About Roles (on page 249) for more information, including step-by-step descriptions of how to assign users to roles and how to specify the rights of roles.



Presets tab, with eight preset positions defined

Adding a preset position (type 1)

As an alternative to defining preset positions in XProtect Corporate, preset positions may for some PTZ cameras also be defined on the camera device itself (typically by accessing a device-specific configuration web page) and imported into XProtect Corporate by selecting **Use presets from device** (see "Using preset positions from device (type 2)" on page 143).

To add a preset position for the camera in XProtect Corporate, do the following:

1. Click **Add....** This will open the **Add Preset** window:



2. The **Add Preset** window displays a preview image from the camera; use the navigation buttons and/or sliders to move the camera to the required preset position. While you do this, you are able to verify the position of the camera through the preview image.
3. Specify a name or number for the preset position in the **Name** field.

Tip: Use a descriptive name; the name may later be used in situations where you will not have access to details about the item, e.g. when using it in a rule.



4. Optionally, type a description of the preset position in the **Description** field.
5. Click **OK**. This will close the **Add Preset** window, and add the preset position to the **Presets** tab's list of available preset positions for the camera.

How to Use the Navigation Buttons

The navigation buttons let you move the camera as follows:

Icon	What it does...	
	Moves the view	up and to the left
		up
		up and to the right
		to the left
		to its default position
		to the right
		down and to the left
		down
		down and to the right
	Zooms in (one zoom level per click)	
	Zooms out (one zoom level per click)	

How to Use the Axes Navigation Sliders

The navigation sliders let you to move the camera along each of its axes. Click inside the sliders to move the sliders' red handles to the required positions.

The slider for the **X-axis** (allowing you to pan left/right) is located immediately below the preview image.

The slider for the **Y-axis** (allowing you to tilt the camera up/down) is located immediately to the left of the preview image.

The slider for the **Z-axis** (allowing you to zoom in and out) is located immediately above the preview image. The camera will zoom in when you move the slider towards **Tele**, and zoom out when you move the slider towards **Wide**.



Example: **Add Preset** window's X-axis slider

How to Use the Iris Slider

Iris settings are only available for some cameras.

Iris settings control the amount of light in images. The higher the iris setting, the lighter images will appear.

Click inside the slider to move the slider's red handle to the required position.



How to Use the Focus Slider

Focus settings are only available for some cameras.

Click inside the slider to move the slider's red handle to the required position.

Using preset positions from device (type 2)

As an alternative to specifying preset positions in XProtect Corporate, preset positions may for some PTZ cameras also be defined on the camera device itself (typically by accessing a device-specific configuration web page).

Such device-defined presets can subsequently be imported into XProtect Corporate by selecting **Use presets from device**.

If importing presets from the camera device, any presets you have previously defined for the camera in XProtect Corporate will be removed; this will affect any patrolling profiles in which these presets are used, as well as any rules in which the affected patrolling profiles are used.

If you later wish to edit such device-defined presets, editing should take place on the camera device.

Assigning a default preset position

If required, you are able to assign one of a PTZ camera's preset positions at the camera's default preset position.

Having a default preset position can be useful because it allows you to define rules (see "Manage Rules" on page 221) specifying that the PTZ camera should go to the default preset position under particular circumstances, for example after the PTZ camera has been operated manually.

To assign a preset position as the default, select the required preset in your list of defined preset positions, then select the **default preset** box below the list.

Only one preset position can be the default preset position.

Editing a Preset Position

To edit an existing preset position defined in XProtect Corporate (presets imported from a device should be edited on the device itself), do the following:

1. Select the required preset position in the **Presets** tab's list of available preset positions for the camera.
2. Click **Edit...** This will open the **Edit Preset** window:



Example only; features are camera-dependent



3. The **Edit Preset** window displays a preview image from the preset position in question; 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.

Tip: Use a descriptive name; the name may later be used in situations where you will not have access to details about the item, e.g. when using it in a rule.

5. Click **OK**.

Testing a Preset Position

1. Select the required preset position in the **Presets** tab's list of available preset positions for the camera.
2. Click **Test**.
3. The **Presets** tab's preview image will move to the selected preset position.

Tip: If the preview image does not appear to move to the selected preset position when you click **Test**, verify that preview image does not already show the selected preset position. In that case, try testing another preset position first.

360° Lens tab (camera properties)

Use of 360° technology requires a dedicated ImmerVision 360° lens mounted.

In this way, 360° technology enables a.o.t. panomorph technology through an advanced lens.

The **360° Lens** tab lets you enable and configure panomorph support for the selected camera.



Enabling and Disabling Panomorph Support

The panomorph feature is disabled by default.

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

Panomorph Settings

When enabling the panomorph support functionality, you must also select a Registered Panomorph Lens (RPL) number from the **ImmerVision Enables® panomorph RPL number** list. This is to ensure identification and correct configuration of the lens used with the camera in question. The RPL number is usually found 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>).

You must also indicate the physical position/orientation of the camera in question. This is done by selecting its position from the **Camera position/orientation** list.

Manage Microphones

On many devices you are able to attach external microphones; some devices even have built-in microphones.



Devices' microphones are automatically detected when you add the devices to your XProtect Corporate system through the Management Client's **Add Hardware** (see "**Add Hardware (Cameras, etc.)**" on page 90) wizard, regardless of which of the wizard's detection options you use.

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.

Who is able to listen to audio recorded by microphones? Users of the XProtect Smart Client can—provided microphones are available, and the users have the rights to use them—listen to audio from microphones. Roles determine users' right to listen to microphones. You cannot listen to microphones from the Management Client.

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

You have two entry points for managing microphones:

- In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, select **Microphones**, expand the required device group, and select the required microphone. If no device groups are available, you must first group your microphones: See Using Device Groups (see "About Device Groups" on page 159) for information about creating groups as well as adding microphones to your groups.
- In the Management Client's Site Navigation pane, expand **Servers** and select **Recording Servers**, then in the overview pane (see "Panels overview" on page 70) expand the required recording server, expand the required device and select the required microphone.

Check the XProtect Corporate release notes to verify that microphones are supported for the devices and firmware used.

Enabling Microphones

When microphones are detected with the wizard **Add Hardware** (see "**Add Hardware (Cameras, etc.)**" on page 90) they are by default disabled. You can enable microphones when needed. If a device has several microphones you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Servers** and select **Recording Servers**.
2. In the Overview pane (see "Panels overview" on page 70), expand the relevant recording server, and find the device on which the microphone is placed.
3. Right-click the required microphone, and select **Enabled**.

On some devices, a microphone can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If a microphone does not work after enabling it in the Management Client, you should thus verify whether the problem may be due to the microphone being disabled on the device itself.

Configuring Individual Microphones

You configure individual microphones by selecting the required microphone in the list, then specifying the microphone's required settings on the tabs in the Properties pane (see "Panels overview" on page 70):

- The **Info** tab (see "Info Tab Overview" on page 166) for managing the selected microphone's name, etc.
- The **Settings** tab (see "Settings Tab Overview" on page 174) for managing the selected microphone's general settings.
- The **Record** tab (see "Record Tab Overview" on page 170) for managing the selected microphone's recording, database and archiving storage settings.
- The **Events** tab (see "Events Tab Overview" on page 164) for managing hardware configurable events.



Viewing Current State of a Microphone

When you have selected a microphone in the Management Client, information about the current status of the selected microphone is presented in the preview pane (see "Panels overview" on page 70).

When the microphone is not active, it is shown as:



When the microphone is active, it is shown as:



Read the Microphone List's Status Icons

The following icons are used to indicate status of cameras (see "Manage Cameras" on page 125), microphones (see "Manage Microphones" on page 144), speakers (see "Manage Speakers" on page 147), input (see "Manage Input" on page 149) and output (see "Manage Output" on page 154) events in item lists:

Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item enabled: Can communicate with the recording server, and can if required be started/stopped automatically through a rule.
					Item recording. Speaker being recorded: Note that what is being said through the speaker can be recorded, but cannot subsequently be played back or exported (for example to prove that a warning was given).
					Item temporarily stopped or has no feed: Often shown when an item is communicating with XProtect Corporate while it is being disabled or enabled. Also shown if the Default Start Audio Feed Rule is not active; see Managing Rules. When stopped, no information is transferred to XProtect Corporate. In which case—if it is a camera—neither live viewing nor recording will be possible. However, a stopped item will still be able to communicate with the recording server, as opposed to when an item is disabled.
					Item disabled: Cannot be started automatically through a rule and will not be able to communicate with the recording server. In the case of a camera, when a camera is disabled, neither live viewing nor recording will be possible.
					Item database being repaired.
					Item requires attention.
					Status unknown.



Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Note that some icons may be combined, as in this example where Item is enabled is combined with Item is recording (since a recording item is also an enabled item).

Manage Speakers

On many devices you are able to attach external loudspeakers; some devices even have built-in speakers.

Devices' speakers are automatically detected when you add the devices to your XProtect Corporate system through the Management Client's **Add Hardware** (see "**Add Hardware (Cameras, etc.)**" on page 90) wizard, regardless of which of the wizard's detection options you use. 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.

Who is able to talk through speakers? Users of the XProtect Smart Client can—provided speakers are available, and the users have the rights to use them—click a button to talk through speakers. Roles determine users' right to talk through speakers. You cannot talk through speakers from the Management Client.

What happens if two users want to speak at the same time? Roles determine users' right to talk through speakers. As part of the roles definition, you are able to 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 will win 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.

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

You have two entry points for managing speakers:

- In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, select **Speakers**, expand the required device group, and select the required speaker. If no device groups are available, you must first group your speakers: See About Device Groups (on page 159) for information about creating groups as well as adding speakers to your groups.
- In the Management Client's Site Navigation pane, expand **Servers** and select **Recording Servers**. In the overview pane (see "Panels overview" on page 70), expand the required recording server and select the required speaker.

Check the XProtect Corporate release notes to verify that speakers are supported for the devices and firmware used.

Enabling Speakers

When speakers are detected with the wizard **Add Hardware**, they are by default disabled. You can enable speakers when needed. If a device has several speakers you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Servers** and select **Recording Servers**.
2. In the Overview pane (see "Panels overview" on page 70), expand the relevant recording server, and find the device on which the speaker is placed.
3. Right-click the required speaker, and select **Enabled**.



On some devices, a speaker can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If a speaker does not work after enabling it in the Management Client, you should thus verify whether the problem may be due to the speaker being disabled on the device itself.

Configuring a Speaker

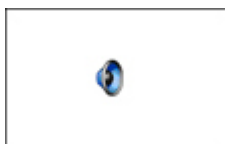
You configure individual speakers by selecting the required speaker in the list, then specifying the speaker's required settings on the tabs in the Properties pane:

1. The **Info** tab (see "Info Tab Overview" on page 166) for managing the selected speaker's name, etc.
2. The **Settings** tab (see "Settings Tab Overview" on page 174) for managing the selected speaker's general settings.
3. The **Record** tab (see "Record Tab Overview" on page 170) for managing the selected speaker's recording, database and archiving storage settings.

Viewing Current State of a Speaker

When you have selected a speaker in the Management Client, information about the current status of the selected speaker is presented in the preview pane.

When a speaker is not active, it is shown as:



When a speaker is active, it is shown as:



Read the Speaker List's Status Icons

The following icons are used to indicate status of cameras (see "Manage Cameras" on page 125), microphones (see "Manage Microphones" on page 144), speakers (see "Manage Speakers" on page 147), input (see "Manage Input" on page 149) and output (see "Manage Output" on page 154) events in item lists:

Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item enabled: Can communicate with the recording server, and can if required be started/stopped automatically through a rule.
					Item recording. Speaker being recorded: Note that what is being said through the speaker can be recorded, but cannot subsequently be played back or exported (for example to prove that a warning was given).



Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item temporarily stopped or has no feed: Often shown when an item is communicating with XProtect Corporate while it is being disabled or enabled. Also shown if the Default Start Audio Feed Rule is not active; see Managing Rules. When stopped, no information is transferred to XProtect Corporate. In which case—if it is a camera—neither live viewing nor recording will be possible. However, a stopped item will still be able to communicate with the recording server, as opposed to when an item is disabled.
					Item disabled: Cannot be started automatically through a rule and will not be able to communicate with the recording server. In the case of a camera, when a camera is disabled, neither live viewing nor recording will be possible.
					Item database being repaired.
					Item requires attention.
					Status unknown.
					Note that some icons may be combined, as in this example where Item is enabled is combined with Item is recording (since a recording item is also an enabled item).

Manage Input

On many devices you are able to attach external units to input ports on the device. Input units are typically external sensors. Such external sensors may, for example, be used for detecting if doors, windows, or gates are opened. Input from such external input units is treated as events by XProtect Corporate.

Such events can be used in rules (see "Manage Rules" on page 221). 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.

Devices' input ports are automatically detected when you add the devices to your XProtect Corporate system through the Management Client's Add Hardware (see "Add Hardware (Cameras, etc.)" on page 90) wizard, regardless of which of the wizard's detection options you use.

You have two entry points for managing input:

- In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, select **Inputs**, expand the required device group, and select the required input. If no device groups are available, you must first group your input: See About Device Groups (on page 159) for information about creating groups as well as adding input to your groups.
- In the Management Client's Site Navigation pane, expand **Servers** and select the **Recording Server** node, then expand the required recording server in the overview pane (see "Panels overview" on page 70) and select the required input.

Before you specify use of external input and output units on a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Corporate release notes to verify that input- and output-controlled operations are supported for the devices and firmware used.

Enabling Input



When inputs are detected with the **Add Hardware** (see "**Add Hardware (Cameras, etc.)**" on page 90) process, they are by default disabled. You can activate inputs when needed. If a device has several inputs you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Servers** and select **Recording Servers**.
2. In the Overview pane (see "Panels overview" on page 70) expand the relevant recording server, and find the device on which the input is placed.
3. Right-click the required input, and select **Enabled**.

Specifying Input Properties

Each input typically has several properties. You can access these properties in two ways:

- In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, and select **Inputs**. In the Overview pane expand the required inputs folder and select the required input.
- or -
- In the Overview pane (see "Panels overview" on page 70), select a device group to define settings for all inputs in the group, or expand a device group, and select the required input.

The properties of the selected input, or the common properties for all inputs in a selected device group, will be displayed on the following tabs: **Settings**, **Info**, and **Events**.

To learn more about the properties of the selected input, or the common properties for all inputs in a selected device group, see:

Viewing the Current State of an Input

The change of an input's state is regarded as an event by XProtect Corporate. Events can be used in rules and hereby trigger actions when the state of an input is changed.

See Define Input- and Output-Related Rules (on page 157) for more information about how to include an input event in a rule.

To view the current state of an input in the Management Client, do the following:

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, and select **Inputs**.
2. In the Overview pane (see "Panels overview" on page 70), expand the required inputs folder and select the required input.

Tip: You may select a group of inputs to view the current status of all inputs in the group.

3. Information about the current status of the selected input is presented in the preview pane.

When an input is deactivated, it is shown by a gray indicator:





When the input is activated, the indicator lights up green:



Fill in Properties on the Info Tab

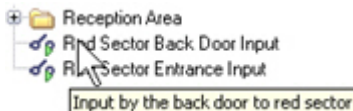
Lets you view and edit basic information about an input. Contains the following fields:

- **Name:** Name of the input. Not compulsory, but highly recommended. Used whenever the input is listed in XProtect Corporate and clients. Does not have to be unique.

To change the name, overwrite the existing name and click **Save** in the toolbar (see "Management Client Overview" on page 66).

Tip: If you change the name, it will be updated throughout XProtect Corporate. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- **Description:** Description of the input. Not compulsory. Will appear in a number of listings within XProtect Corporate. For example, the description will appear when pausing the mouse pointer over the item's name in the Overview pane (see "Panels overview" on page 70):



To specify a description, type the description and click **Save** in the toolbar (see "Management Client Overview" on page 66).

- **Hardware name:** Name of the hardware with which the input unit is connected. The field is non-editable from here, but can be changed by clicking **Go To** next to it. This takes you to hardware information, where the name is editable.
- **Unit number:** Non-editable field, displaying the unit on which the input can be found on the hardware. For hardware capable of having more than one input unit attached, the unit number will typically indicate the number of the input port to which the input is attached. For hardware with, for example, four input ports, the numbers will typically range from **0** to **3**.

Fill in Properties on the Settings Tab

Lets you verify or edit key input settings, for a selected input, or for all inputs within a selected device group. If the selected device group contains 400 or more inputs, the **Settings** tab will be unavailable for viewing and editing because changing settings for so many devices in one go takes too long time.

The content of the **Settings** tab is determined entirely by the devices in question, and is thus likely to vary depending on the input selected.

Content may vary, but you will typically see the following property:

- **Input rises on:** Lets you define whether the input signal should be considered rising on **Circuit closed** or **Circuit open**. The value of this setting is used on the input's **Events** tab, where you define properties for input events: **Input Rising** event, **Input Falling** event, and **Input Changed** event. See also the description of the properties of the **Events** tab (see "Fill in Properties on the Events Tab" on page 152).



The content of the **Settings** tab is displayed in a table, in which the first column lists the available settings, and the second column lists the value of each setting.

You are typically able to change the values:

1. Select the row with the property you want to change
2. Click the  button to the right of the properties column.
3. Change the value of the property.
4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

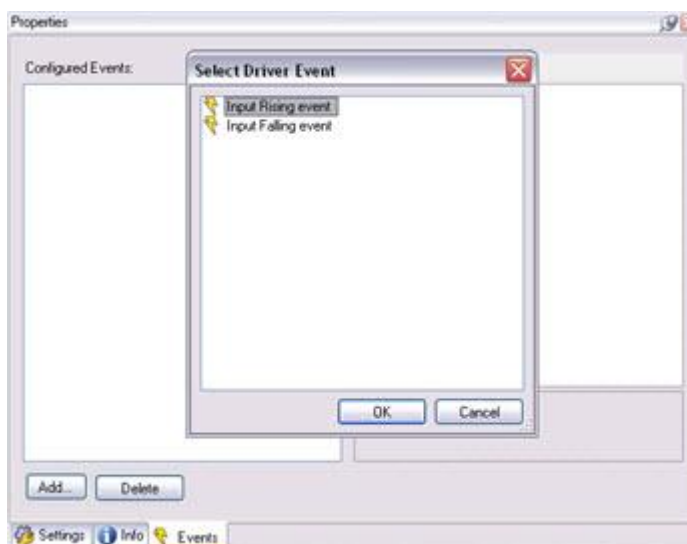
When you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the gray information box below the settings table.

Fill in Properties on the Events Tab

Lets you define events based on changes of the input's state, from circuit opened to circuit closed or the reverse order. The events you define can subsequently be used in rules.

You can define events for a selected input, but not for all inputs in a device group.

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, and select **Inputs**.
2. In the Overview pane (see "Panels overview" on page 70), select the required input.
3. Select the **Events** tab, and click **Add...**



4. In the **Select Driver Event** dialog, select the appropriate option (**Input Rising event**, **Input Falling event**, or **Input Changed event**).
5. Click **OK**. Your selected type of input event will now appear in the **Events** tab's **Configured events** list.

To the right of the list, settings for the selected input event are displayed in a table. The table's first column lists available settings, the second column lists the value of each setting.

The settings on the **Events** tab is determined entirely by the devices in question, and is thus likely to vary depending on the input selected.

Content may vary, but you will typically see the following property:



- **Enabled:** Select between **True** (enabled), or **False** (disabled).

You are typically able to change the values:

1. Select the row with the property you want to change.
2. Click the  button to the right of the properties column.
3. Change the value of the property.
4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

When you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the grey information box below the settings table.

Read the Input List's Status Icons

The following icons are used to indicate status of cameras (see "Manage Cameras" on page 125), microphones (see "Manage Microphones" on page 144), speakers (see "Manage Speakers" on page 147), input (see "Manage Input" on page 149) and output (see "Manage Output" on page 154) events in item lists:

Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item enabled: Can communicate with the recording server, and can if required be started/stopped automatically through a rule.
					Item recording. Speaker being recorded: Note that what is being said through the speaker can be recorded, but cannot subsequently be played back or exported (for example to prove that a warning was given).
					Item temporarily stopped or has no feed: Often shown when an item is communicating with XProtect Corporate while it is being disabled or enabled. Also shown if the Default Start Audio Feed Rule is not active; see Managing Rules. When stopped, no information is transferred to XProtect Corporate. In which case—if it is a camera—neither live viewing nor recording will be possible. However, a stopped item will still be able to communicate with the recording server, as opposed to when an item is disabled.
					Item disabled: Cannot be started automatically through a rule and will not be able to communicate with the recording server. In the case of a camera, when a camera is disabled, neither live viewing nor recording will be possible.
					Item database being repaired.
					Item requires attention.
					Status unknown.
					Note that some icons may be combined, as in this example where Item is enabled is combined with Item is recording (since a recording item is also an enabled item).



Manage Output

On many devices you are able to attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through XProtect Corporate.

Output may be used when creating rules (see "Manage Rules" on page 221). 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 also be triggered manually from the Management Client and the **XProtect Smart Client**.

Devices' output ports are automatically detected when you add the devices to XProtect Corporate through the Management Client's **Add Hardware** (see "**Add Hardware (Cameras, etc.)**" on page 90) wizard, regardless of which of the wizard's detection options you use. By default, output are disabled. You can enable output when needed.

You have two entry points for managing outputs:

- In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Devices**, select **Outputs**, expand the required device group, and select the required output. If no device groups are available, you must first group your output: See About Device Groups (on page 159) for information about creating groups as well as adding output to your groups.
- In the Management Client's Site Navigation pane, expand **Servers** and select **Recording Servers**, then in the overview pane (see "Panels overview" on page 70) expand the required recording server and select the required output.

Before you specify use of external input and output units on a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Corporate release notes to verify that input- and output-controlled operations are supported for the devices and firmware used.

Enabling Output

When outputs are detected with the **Add Hardware** (see "**Add Hardware (Cameras, etc.)**" on page 90) process, they are by default disabled. You can activate outputs when needed.

If a device has several outputs you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Servers** and select **Recording Servers**.
2. In the Overview pane (see "Panels overview" on page 70) select the relevant recording server, and find the device on which the output is placed.
3. Right-click the required output, and select **Enabled**.

Specifying Output Properties

Each output has several properties which can be found on the output's **Settings** and **Info** tabs. You can access these tabs in two ways:

- In the Site Navigation pane (see "Panels overview" on page 70), expand **Devices** and select **Outputs**, then in the Overview pane expand the required outputs folder and select the required output.

- or -

- In the Overview pane (see "Panels overview" on page 70), select a device group to change the settings for all outputs in this group, or expand a device group and select the required output.

The properties of the selected output, or the common properties for all outputs in a selected device group, will be displayed on the following tabs: **Settings** and **Info**.



To learn more about the properties of the selected output, or the common properties for all outputs in a selected device group, see:

Automatic and Manual Activation of Output

Output can be activated automatically or manually:

- **Automatic Activation of Output**
With the Management Client's rules (see "Manage Rules" on page 221) feature, you are able to create rules that automatically activate or deactivate output, and rules that trigger actions when the state of an output is changed.
- For example, you may create a rule specifying that a siren should sound if motion is detected on a particular camera, or you may create a rule specifying that a camera should start recording if a siren sounds. See Define Input- and Output-Related Rules (on page 157) for more information.
- **Manual Activation of Output**
Output may be activated manually from the Management Client and the **XProtect Smart Client**:
 1. In the Site Navigation pane (see "Panels overview" on page 70), expand **Devices** and select **Outputs**.
 2. In the Overview pane (see "Panels overview" on page 70), expand the required outputs folder and select the required output.

Tip: You may select a group of outputs, for example **All Outputs**, to manually activate all outputs in the group.

The availability of features for manually activating an output depends entirely on the device in question, and may thus vary.

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:



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.

Fill in Properties on the Info Tab

Lets you view and edit basic information about an output:

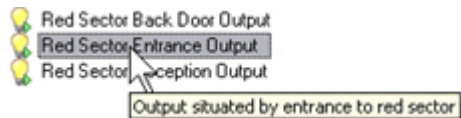
- **Name:** Name of the output. Not compulsory, but highly recommended. Used whenever the output is listed in XProtect Corporate and clients. Does not have to be unique.



- To change the name, overwrite the existing name and click **Save** in the toolbar (see "Management Client Overview" on page 66).

Tip: If you change the name, it will be updated throughout XProtect Corporate. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- Description:** Description of the output. Not compulsory. Will appear in a number of listings within XProtect Corporate. For example, the description will appear when pausing the mouse pointer over the item's name in the Overview pane (see "Panels overview" on page 70):



To specify a description, type the description and click **Save** in the toolbar (see "Management Client Overview" on page 66).

- Hardware name:** Name of the hardware with which the output unit is connected. The field is non-editable from here, but can be changed by clicking **Go To** next to it. This takes you to hardware information, where the name is editable.
- Unit number:** Non-editable field, displaying the unit on which the output can be found on the hardware. For hardware capable of having more than one output unit attached, the unit number will typically indicate the number of the output port to which the output is attached. For hardware with, for example, four output ports, the numbers will typically range from **0** to **3**.

Fill in Properties on the Settings Tab

Lets you verify or edit key output settings, such as active output state, output trigger time, etc., for a selected output, or for all outputs within a selected device group. However, if the device group contains 400 cameras or more the **Settings** tab will not be available for viewing and editing because changing settings for so many devices in one go takes too long time.

The content of the **Settings** tab is determined entirely by the drivers for the cameras in question, and is thus likely to vary depending on the output selected.

Some devices are only able to apply outputs for a relatively short time, for example max. 5 seconds. Refer to the documentation for the device in question for exact information.

Content is displayed in a table, in which the first column lists the available settings, and the second column lists the value of each setting.

You are typically able to change the values:

- Select the row with the property you want to change
- Click the  button to the right of the properties column.
- Change the value of the property.
- In the toolbar (see "Management Client Overview" on page 66), click **Save**.

When you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the grey information box below the settings table.

Read the Output List's Status Icons



The following icons are used to indicate status of cameras (see "Manage Cameras" on page 125), microphones (see "Manage Microphones" on page 144), speakers (see "Manage Speakers" on page 147), input (see "Manage Input" on page 149) and output (see "Manage Output" on page 154) events in item lists:

Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item enabled: Can communicate with the recording server, and can if required be started/stopped automatically through a rule.
					Item recording. Speaker being recorded: Note that what is being said through the speaker can be recorded, but cannot subsequently be played back or exported (for example to prove that a warning was given).
					Item temporarily stopped or has no feed: Often shown when an item is communicating with XProtect Corporate while it is being disabled or enabled. Also shown if the Default Start Audio Feed Rule is not active; see Managing Rules. When stopped, no information is transferred to XProtect Corporate. In which case—if it is a camera—neither live viewing nor recording will be possible. However, a stopped item will still be able to communicate with the recording server, as opposed to when an item is disabled.
					Item disabled: Cannot be started automatically through a rule and will not be able to communicate with the recording server. In the case of a camera, when a camera is disabled, neither live viewing nor recording will be possible.
					Item database being repaired.
					Item requires attention.
					Status unknown.
					Note that some icons may be combined, as in this example where Item is enabled is combined with Item is recording (since a recording item is also an enabled item).

Define Input- and Output-Related Rules

To be able to automatically

- activate an output or trigger an event activated by an output, you must, after you have enabled an output,
- trigger an action activated by an input, you must, after you have enabled the input and created an event based on the input,

include it in a rule.

See Manage Output (on page 154) or Manage Input (on page 149) for more information.

For example, you may create a rule specifying that:

- a siren should sound if motion is detected on a particular camera, or you may create a rule specifying that a camera should start recording if a siren sounds (output).



- a camera should record if a particular input is activated (input).

For the following examples to be useful you should have general knowledge about managing rules (see "Manage Rules" on page 221). See also Create Typical Rules (on page 194) for other step-by-step descriptions of how to create rules.

Tip: When you create a rule based on an in- or output event, the actions you specify in the rule do not have to relate to the device on which the external in- or output was activated; you can easily specify that the actions should take place on one or more different devices— even across recording servers.

Defining a Rule that Activates/Deactivates an Output

1. Start the **Manage Rule** and in step 1 select a rule type and, if necessary, a condition in step 2.
2. In **Manage Rule's** step 3 (**Step 3: Actions**) select the **Set device output to <state>** action.
3. If you like the output to be activated/deactivated immediately, skip this step. If you do not want to activate or deactivate the output immediately after the event, click the **immediately** link in the initial rule description, and select an interval between the event and the activation/deactivation of the output. Click **OK** to confirm your selection.
4. Click the **state** link in the initial rule description, and select whether you want to activate or deactivate the output. Click **OK** to confirm your selection.
5. Click the **devices** link in the initial rule description, and select which output you want to activate or deactivate. Click **OK** to confirm your selection.
6. If wanted you can select more actions in the **Manage Rule's** step 3 (**Step 3: Actions**). Do so or simply click **Next** to continue to the next step.
7. In **Manage Rule's** step 4 (**Step 4: Stop criteria**) select one of the stop actions, for instance to deactivate the output after a certain time or event.
8. Click **Finish** to save the rule.

Defining a Rule where an Output Triggers an Action

In the **Rules** feature, all registered external output (activation, deactivation or change) is treated as an event. Based on an event, you are able to specify a wide variety of actions to take.

To define a rule where an output activates an action, do the following:

1. Start the **Manage Rule**.
2. In **Manage Rule's** step 1 (**Step 1: Type of rule**) select the **Perform an action on <event>** option.
3. Click the **event** link in the initial rule description.
4. In the **Select an Event** dialog's **Built-in** group, select the appropriate option for your rule: **Output Activated**, **Output Changed** or **Output Deactivated**. Click **OK** to confirm your selection.
5. Click the **devices/recorders/servers** link in the initial rule description.
6. In the **Select Devices and Groups** dialog select the required output. Click **OK** to confirm your selection.
7. Click **Next** to continue to the **Manage Rule's** step 2 (**Step 2: Conditions**) and select, if necessary, a condition.
8. Continue to step 3 (**Step 3: Actions**) and select one or more actions.



9. If you do not want to define a stop action, skip this step. If you want to define a stop action— for instance to deactivate the output again— click **Next** to continue to step 4 (**Step 4: Stop criteria**), and select a stop action.
10. Click **Finish** to save the rule.

Defining a Rule where an Input Triggers an Action

In the **Rules** feature, all registered external input (activation, deactivation, or change) is treated as an event. Based on an event, you are able to specify a wide variety of actions to take.

To define a rule specifying that an input should result in one or more actions (for example the starting of recording on a certain camera), do the following:

1. Start **Managing Rules**.
2. In **Managing Rules**'s step 1 (**Step 1: Type of rule**) select the **Perform an action on <event >** option.
3. Click the **event** link in the initial rule description.
4. In the **Select an Event** dialog's **Hardware Configurable** group, select the appropriate option for your rule: **Input Activated**, **Input Changed**, or **Input Deactivated**. Click **OK** to confirm your selection.
5. Click the **devices/recording servers/management servers** link in the initial rule description.
6. In the **Select Devices and Groups** dialog select the required input. Click **OK** to confirm your selection.
7. Click **Next** to continue to **Managing Rules**'s step 2 (**Step 2: Conditions**) and select, if necessary, a condition.
8. Continue to step 3 (**Step 3: Actions**) and select one or more actions.
9. Click **Next** to continue to step 4 (**Step 4: Stop criteria**), and select a stop criteria. **Click Next to continue to step 5 (Step 5: Stop actions), and select a stop action.**
10. Click **Finish** to save the rule.

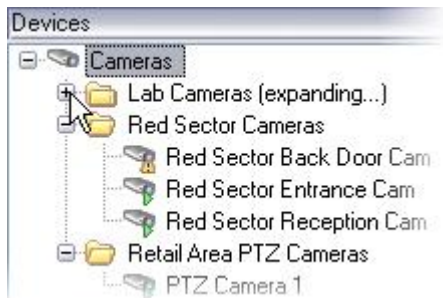
About Device Groups

You are able to group different types of devices (cameras, microphones, speakers, inputs, outputs) on your XProtect Corporate system by using device groups. The use of device groups has several benefits:

- Device groups help you maintain an intuitive overview of devices on your system
- You are able to specify common properties for all devices within a device group in one go
- When dealing with roles (see "About Roles" on page 249), you are able to specify common security settings for all devices within a device group in one go
- When dealing with rules (see "Manage Rules" on page 221), you are able to apply a rule for all devices within a device group in one go



You can add as many device groups as required; you are completely free to decide which devices to include. The only restriction is that you cannot mix different types of devices (for example cameras and speakers) in a device group.



Example: cameras grouped into device groups

If a device group contains 400 devices or more, the **Settings** tab is unavailable for viewing and editing. For camera groups, the **Streams** tab is also unavailable for editing and viewing if the group contains 400 cameras or more. When you click the plus sign next to the device folder, your XProtect Corporate system will load the contents of the device folder, which may take a few seconds. While expanding, the text (**expanding...**) is displayed next to the folder name.

The following examples are based on grouping cameras into device groups, but the principle applies for microphones, speakers, inputs and outputs as well.

Adding a Device Group

1. In the overview pane (see "Panels overview" on page 70), right-click the item under which you wish to create the new device group.
2. Select **Add Device Group**:



Tip: You may also simply press CTRL+N on your keyboard.

The **Add Device Group** dialog will appear.

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



The description will later appear when pausing the mouse pointer over the device group in the device list.



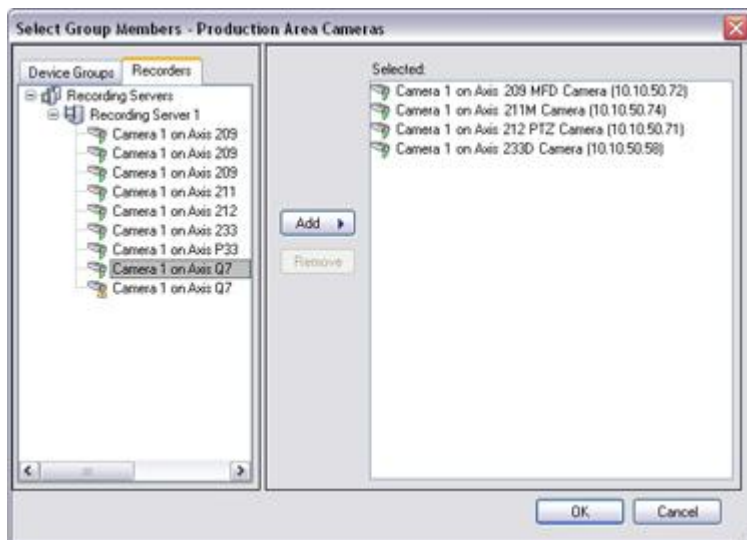
- Click **OK**. A folder representing the new device group is added to the list. You are now able to specify which devices should belong in the device group.

Tip: If required, you are able to add device groups as subgroups under other device groups, as illustrated here:



Specifying Which Devices to Include in a Device Group

- In the Overview pane (see "Panels overview" on page 70)'s device list, right-click the required device group folder.
- Select **Edit Device Group Members**. The **Select Group Members** window will appear.
- In the **Select Group Members** window, select either:
 - The **Device Groups** tab, which lists devices based on existing device groups.
 - The **Recording Servers** tab, which lists devices based on which recording servers the devices belong on.
- Select the devices you wish to include, and click **Add**. This will copy the selected devices to the **Selected** box:



Tip: You may also double-click a device to copy it from one box to the other, or you may simply drag devices between the two boxes.

Tip: To select several devices in one go, press the CTRL key on your keyboard while selecting.

- Click **OK**. The selected devices will be added to your device group on the device list.

Specifying Common Settings for All Devices in a Device Group



When using device groups, you are able to quickly specify common properties for all devices within a given device group:

1. In the overview pane (see "Panels overview" on page 70)'s device list, click the required device group.

In the properties pane (see "Panels overview" on page 70), all properties **which are available on all of the device group's devices** will be listed, grouped on tabs.

2. Specify the required common properties.

Properties not available on **all** of the devices in the device group will not be listed; such properties must still be configured individually for each device.

If the device group contains 400 or more devices the **Settings** tab (see "Enabling and Disabling Edge Recording—Camera Only" on page 173) is unavailable for viewing and editing. For camera groups the **Streams** tab is also unavailable for viewing and editing if the group contains 400 cameras or more.

Tip: The Settings tab has convenient functionality for quickly switching between settings for the device group and settings for individual devices.

Deleting a Device Group

1. In the overview pane (see "Panels overview" on page 70)'s device list, right-click the unwanted device group folder.
2. Select **Delete Group**.

Tip: You may also simply press **DELETE** on your keyboard.

3. You will be asked to confirm that you want to delete the device group. Verify that you are deleting the correct device group, then click **Yes**.

Remember that you have only deleted the device group itself. If you wish to delete IP hardware - such as a camera - from your XProtect Corporate system, do so on a recording server level (see Managing Hardware (see "Manage Hardware" on page 95)).

About Rules and Events

Events are a central element in XProtect Corporate, primarily used for triggering actions. Actions are configurable through rules (see "Manage Rules" on page 221).

Example: You 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.

In the Management Client's Site Navigation pane (see "Panels overview" on page 70), you are able to work with the following under **Rules and Events**:

- **Rules (see "Manage Rules" on page 221):** Rules are a central element in XProtect Corporate. The behavior of your surveillance system is to a very large extent determined by rules.
- **Time profiles (see "Manage Time Profiles" on page 229):** Time profiles are periods of time defined in the Management Client. They can be used when creating 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 (see "Manage Notification Profiles" on page 233):** With notification profiles you can set up ready-made e-mail notifications, which can automatically be triggered by a rule, for example when a particular event occurs.
- **User-defined Events (see "Manage User-defined Events" on page 238):** User-defined events are custom made events making it possible for users to manually trigger events in the system or react to inputs from the system.



- **Generic Events (see "Manage Generic Events" on page 242):** Generic events allow you to trigger actions in the XProtect event server by sending simple strings via the IP network to XProtect Corporate.
- **Hardware Configurable Events: (see "Hardware Configurable Events" on page 188)** Some hardware is capable of creating events themselves. For example, some cameras are themselves able to detect motion or static/moving objects, and their detections can be used as events in XProtect Corporate. Such events must obviously be configured on the hardware before they can be used in XProtect Corporate, therefore they are called hardware configurable events. Read more about hardware configurable events for cameras (see "Manage Cameras" on page 125), inputs (see "Manage Input" on page 149) and microphones (see "Manage Microphones" on page 144) respectively.

See Events Overview (on page 216) for a list of events.

About Multi-streaming

Viewing of live video and playing back of recorded video does not necessarily require the same settings to achieve the best result. To handle this, XProtect Corporate and some cameras support multi-streaming, with which you can establish two independent streams to the recording server. **Either** one stream for live viewing and another stream for playback purposes **or** two 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 will help preserve disk space.

Example 2, two 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 considerably between different cameras. Refer to camera's documentation for exact information. To see if a camera offers different types of streams, see the **Settings** tab (see "Settings Tab Overview" on page 174).

You manage multi-streaming on the **Streams** tab. The tab is only available when the selected camera or device group supports multi-streaming.

If you select a device group with 400 or more cameras, the **Streams** tab will not be available for viewing and editing because changing settings for so many devices in one go takes too long time.

To access the **Streams** tab, expand **Devices** in the Management Client's Site navigation pane (see "Panels overview" on page 70), expand the relevant camera folder in the Overview pane (see "Panels overview" on page 70), select the required camera and then select the **Streams** tab in the Properties pane (see "Panels overview" on page 70).

The tab will by default list a single stream—the selected camera's default stream, used for live video as well as for video which is being recorded for playback purposes.

Note that while it is possible to set up and use two live streams, only one of the enabled live streams is able to record video at a time. To change which stream to use for recording, use the **Record** box.

Adding a New Stream

1. On the **Streams** tab, click **Add**. This will add a second stream to the list (you cannot have more than two streams).

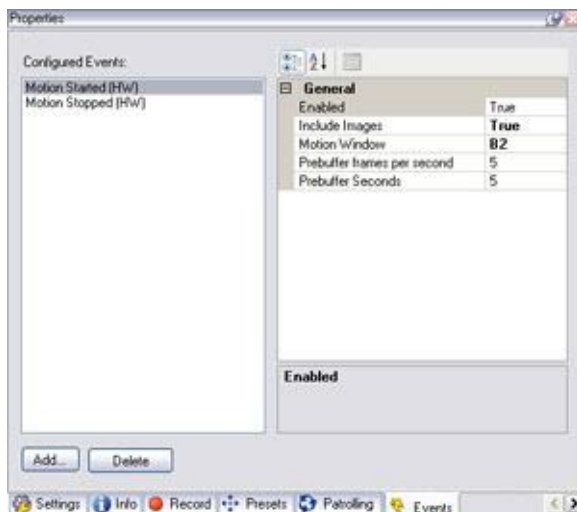


2. Optional: In the **Name** column, edit the name of the stream.
3. In the **Live Mode** column, select when live streaming is needed.
4. In the **Default** column, select which stream is the default one.
5. In the **Record** column, select the check box if you want to use the stream for recorded video or leave it cleared if you only want to use it for live video.
6. In the **Edge Recording** column it is indicated whether the selected stream supports edge recording (see "Record Tab Overview" on page 170) or not.
7. Click **Save**.

Events Tab Overview

For items (cameras or microphones) supporting events, you are able to manage the hardware configurable events on the **Events** tab. To access the **Events** tab, select the required item in the overview pane (see "Panels overview" on page 70), then select the **Events** tab in the properties pane (see "Panels overview" on page 70).

The **Events** tab will only be available if the selected item supports hardware configurable events.



Event tab, example from camera

Even when an item supports hardware configurable events, it is always your decision whether you want to use such events on your XProtect Corporate system. Therefore, you simply add each hardware configurable event you want to be able to use on each item.

About the Event Tab for Camera

In addition to XProtect Corporate's motion detection, some cameras can themselves be configured to detect motion. If a camera is capable of such detection, the camera's detections can be used as events. Such events can in turn be used when creating event-based rules (see "Events Overview" on page 216). Events from cameras are called hardware configurable events as they technically occur on the actual camera hardware rather than on the surveillance system.

Even though events based on signals from input and/or output units connected to camera devices are technically also hardware configurable events, they are managed elsewhere. See Manage Inputs (see "Manage Input" on page 149) and Manage Outputs (see "Manage Output" on page 154).

About the Event Tab for Microphone



Some devices are capable of creating events themselves. Such events can be used when creating event-based rules (see "Events Overview" on page 216) in XProtect Corporate. Events from such devices are called hardware configurable events, as they technically occur on the actual camera hardware rather than on the surveillance system.

Adding a Hardware Configurable Event

1. On the **Events** Tab, click **Add....** This opens the **Select Driver Event** window.
2. Select the required hardware configurable event:



You can only select one hardware configurable event at a time.

3. Click **OK**. The selected event will be added to the **Events** tab's list of configured events.
4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

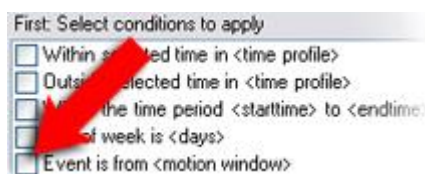
Using Several Instances of a Hardware Configurable Event

To be able to specify different properties for different instances of an event, you are able to add a hardware configurable event more than once (see also Specifying Hardware Configurable Event Properties (see "Specify Hardware Configurable Event Properties" on page 166)).

The following example is specific to **cameras**.

Example: The camera in question has been configured 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 use of motion window A1; in the properties of the other instance, you have specified use of motion window A2.

When you use the hardware configurable event in a rule, you are able to specify that the event should be based on motion detected in a specific motion window in order for the rule to be triggered:



Example: Specifying specific motion window as part of a rule's conditions

Deleting a Hardware Configurable Event

Bear in mind that deleting a hardware configurable event will affect any rules in which the event is used.

1. In the **Events** tab's **Configured Events** list, select the no longer required event.



Tip: If there are several instances of the same event, use the properties list in the right side of the tab to verify that you have selected the correct event.

2. Click **Delete**.

The selected event will be deleted without further warning.

3. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Specify Hardware Configurable Event Properties

For each hardware configurable event you have added, you are able to specify properties. The number of properties depends on the item in question. In order to work as intended, some or all of the properties must be specified identically on the item as well as on XProtect Corporate.

Even though the following list is not exhaustive, you may often be able to specify the following properties:

- **Enabled:** Determines whether use of the hardware configurable event is enabled. Select **True** to enable; select **False** to disable.

Enabled is the only property you will always see for microphones.

- **Include Images:** Determines whether video should be sent from the camera to XProtect Corporate when the event occurs. Select **True** if video is required; select **False** if video is not required.
- **Motion Window:** Many cameras capable of detecting motion can be configured with different motion detection settings for different parts the camera's images. For example, if a camera covers a 2-lane road, different motion detection settings may have been defined for the right lane and left lane area of the camera's images. Such areas are generally known as motion windows.

Provided one or more motion windows have been defined on the camera device, the **Motion Window** setting lets you specify which motion window to use for the event. When the camera detects motion within the specified motion window, the event will occur.

When specifying use of a motion window, make sure you type the name of the motion window, exactly as it has been specified on the camera.

You can only specify one motion window in the field. However, you are able to add more than one instance of an event (see "Using Several Instances of a Hardware Configurable Event" on page 165).

- **Prebuffer frames per second :** Determines the frame rate to be used for prebuffered video. See also the next description of **Prebuffered Seconds** setting.
- **Prebuffer Seconds :** Determines the number of seconds for which video from the camera should be stored for possible later use.

What does "prebuffer" mean? Prebuffering is essentially the ability to store video from before the initial boundaries of a recording. It allows you to view video from **before** an event occurred.

If, for example, you are going to use the hardware configurable event in a rule specifying that recording should start when the event occurs, being able to see what happened immediately prior to the door being opened may also be important.

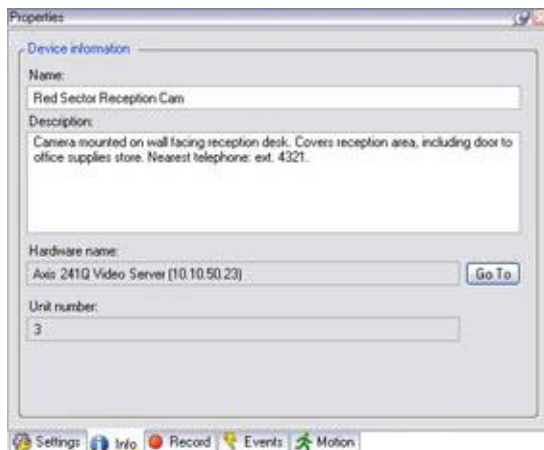
Example: If using five seconds of prebuffering, video from the camera will always be stored provisionally for five seconds. If the event occurs, five seconds' worth of video will be available for attaching to any recording triggered by the event, as specified in a rule.

Info Tab Overview

The **Info** tab lets you view and edit basic information about a selected item in a number of fields. The following items under **Devices** have an **Info** tab:



- Cameras (see "Manage Cameras" on page 125)
- Hardware (see "Manage Hardware" on page 95)
- Microphones (see "Manage Microphones" on page 144)
- Speakers (see "Manage Speakers" on page 147)



Example of Info tab from a camera...

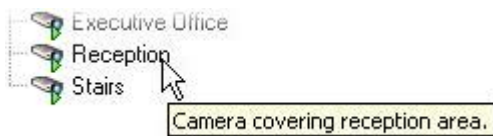
Description of Info Tab's Fields

- **Name:** Name of the item. Not compulsory, but highly recommended. Used whenever the item is listed in XProtect Corporate and clients. Does not have to be unique.

To change the name, overwrite the existing name and click **Save** in the toolbar (see "Management Client Overview" on page 66).

Tip: If you change the name, it will be updated throughout XProtect Corporate. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- **Description:** Description of the item. Not compulsory. Will appear in a number of listings within XProtect Corporate. For example, the description will appear when pausing the mouse pointer over the item's name in the overview pane:



Example from a camera...

To specify a description, type the description and click **Save** in the toolbar (see "Management Client Overview" on page 66).

- **Hardware name:** (only relevant for Camera, Microphone and Speaker) Name of the hardware, with which the item is connected. The field is non-editable from here, but can be changed by clicking **Go To** next to it. This will take you to hardware information, where the name is editable.
- **Unit number:** (only relevant for Camera, Microphone and Speaker) Non-editable field displaying the unit on which the item is attached on the hardware.



For single-device hardware, the unit number will typically be **1**. For multi-device hardware, such as video servers with several channels, the unit number will typically indicate the channel on which the item is attached, e.g. **3**.

- **Shortcut:** (only relevant for Camera) Users of the XProtect Smart Client can take advantage of a range of keyboard shortcuts, some of which let the user toggle between viewing different cameras. Such shortcuts include numbers used to identify each camera. In the Management Client, each camera's shortcut number is specified in the **Shortcut** field.

A camera shortcut number cannot contain letters or special characters, and must be no longer than four digits:

- Examples of correct camera shortcut numbers: **3**, **1234**.
- Examples of incorrect camera shortcut numbers: **A*3**, **12345**.

It is highly recommended that you use a unique camera shortcut number for each camera.

Tip: Find more information about keyboard shortcuts from an XProtect Smart Client user's perspective in the separate XProtect Smart Client documentation available on the XProtect Corporate software DVD as well as from www.milestonesys.com.

- **Serial Number:** (only relevant for Hardware) Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
- **Firmware version:** (only relevant for Hardware) Firmware version as specified by the manufacturer.
- **MAC address:** (only relevant for Hardware) Hardware MAC address. A MAC (Media Access Control) address is a 12-character hexadecimal number uniquely identifying each device on a network.
- **Product ID:** (only relevant for Hardware) Product identifier.
- **Hardware host name:** (only relevant for Hardware) Host name or IP address of the hardware.

Tip: By clicking the  button next to the field, you are able to connect to the hardware's own configuration page. The page opens in a separate window.

PTZ Tab (Hardware Properties)

The **PTZ** tab lets you enable PTZ (Pan/Tilt/Zoom) for video encoders. It is only available if the selected hardware is a video encoder.

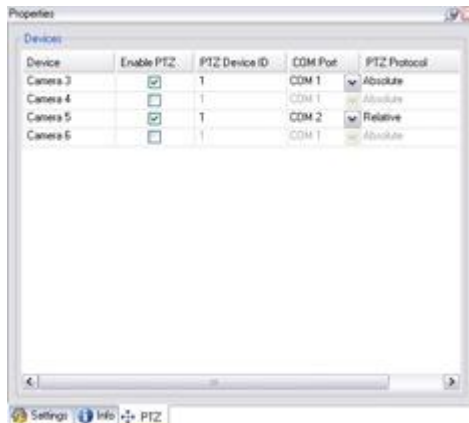
What is a video encoder? A video encoder, also known as video server, is a piece of hardware which is able to stream video from a number of connected cameras. Video encoders contain image digitizers, making it possible to connect analog cameras to a network.

For video encoders, the use of PTZ must be enabled on the hardware level before you can use the PTZ features of PTZ cameras attached to the video encoder. The **Settings** tab lets you enable the use of PTZ separately for each of the video encoder's channels.

To access the **PTZ** tab, select the required hardware in the overview pane (see "Panels overview" on page 70), then select the **PTZ** tab in the properties pane (see "Panels overview" on page 70).



Not all video encoders support the use of PTZ cameras. Even video encoders which support the use of PTZ cameras may require configuration, such as installation of additional drivers (typically through accessing a browser-based configuration interface on the device's IP address) before PTZ cameras can be used.



PTZ tab, with PTZ enabled for two of a video encoder's channels

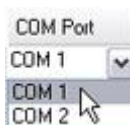
Enabling PTZ on a Video Encoder

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

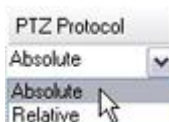
1. In the list of devices connected to the video encoder, select the **Enable PTZ** box for the camera(s) on which you want to use PTZ:



2. In the **PTZ Device ID** column, verify the ID of the PTZ camera(s) in question.
3. In the **COM Port** column, select which of the video encoder's COM (serial communications) ports should be used for controlling PTZ functionality on each required PTZ camera:



4. In the **PTZ Protocol** column, select which positioning scheme to use for each required PTZ camera:



- **Absolute:** When operators use Pan/Tilt/Zoom 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 Pan/Tilt/Zoom controls for the camera, the camera is adjusted relative to its current position

Refer to the camera's documentation if in doubt.

5. In the toolbar (see "Management Client Overview" on page 66), click **Save**.



You are now able to configure preset positions (see "PTZ Presets tab (camera properties)" on page 140) and patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 136) for the PTZ camera(s) in question.

Record Tab Overview

Recordings from an item (camera, microphone or speaker) will only be saved in the items's database when recording is enabled and recording-related rule (see "Manage Rules" on page 221) criteria are met.



Record tab, example from camera

Camera

Lets you specify recording and storage settings for the selected camera.

What does recording mean? In IP video surveillance systems, the term **recording** means **saving video from a camera in the camera's database on the surveillance system**. In many IP video surveillance systems, all of the video received from cameras is not necessarily saved. Instead, saving of video in a camera's database, i.e. recording, is started only when there is a reason to do so: For example when motion is detected, when an event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, when motion is no longer detected, when an event occurs, when a time period ends, or similar. The term **recording** originates from the analog video era, when video was taped only when the record button was pressed.

Microphone

Lets you specify recording and storage settings for the selected microphone. Microphones' recording and storage settings are completely independent of cameras and speakers.

Speaker

Lets you specify recording and storage settings for the selected speaker.

Enabling and Disabling Recording

Recording is by default enabled.

To enable/disable recording for the selected item, select/clear the **Record** tab's **Recording** check box.

Recording must be enabled for the item before you are able to record (i.e. save) video or audio from the camera. A rule (see "Manage Rules" on page 221) specifying that an item should record under particular circumstances will not work if recording is disabled for the item in question.

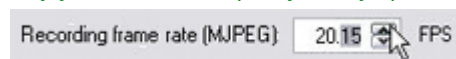


Setting Recording Frame Rate—Camera Only

Specifying recording frame rate is only possible for MJPEG, a video codec (technology for compressing and decompressing data) with which each frame is separately compressed into a JPEG image.

1. Select or type the required recording frame rate (in FPS, Frames Per Second) in the **Recording frame rate** box.
2. Clicking the **Recording frame rate** box' up/down arrows will increase/reduce the value in increments of 1 FPS.

Tip: If you click inside the **Recording frame rate** box, two decimals will be added to the value. By selecting the number before or after the separator, you are able to increase/reduce the numbers in increments of 1 unit. This way you are able to specify a very specific recording frame rate average over time, for example of 20.15 FPS:



Specifying a specific recording frame rate

Working with Prebuffering

Prebuffering is essentially the ability to save video and audio in the camera's or microphone's database before the initial boundaries of a recording.

Use of prebuffering can be highly advantageous: It allows you to save video and audio from **before** the events or times used to start recordings.

How Prebuffering Works for Cameras and Microphones...

If, for example, you have created a rule specifying that recording should start when a door is opened, being able to see what happened immediately prior to the door being opened may be useful. Such prebuffering is possible since XProtect Corporate continuously receives streams of video and audio from connected cameras and microphones (unless the transfer of video or audio from cameras or microphones has in some way been disabled). Storing video and audio from before the initial boundaries of a recording is therefore not a problem: video and audio passes through XProtect Corporate anyway.

When prebuffering is enabled for a camera or a microphone, XProtect Corporate continuously records video or audio from the camera's or microphones stream and provisionally stores it in the database for a specified number of seconds before automatically deleting it— unless the provisionally stored video or audio turns out to be required for a recording, in which case it is automatically added to the recording.

How Prebuffering Works for Speakers...

Unlike video and incoming audio, which XProtect Corporate continuously receives from connected cameras and microphones, outgoing audio is only transmitted when XProtect Smart Client users press a button to talk through speakers. This can, depending on which events or times are used to start recordings, mean that there will be very little or no outgoing audio available for prebuffering.



The following example illustrates how prebuffered video or audio is added to a recording:

This is the stream received by XProtect Corporate:



These are the initial boundaries of a recording, as defined, for example, by start and stop events:



However, a rule specifies that recording should start 5 seconds prior to the start event, so 5 seconds of prebuffered video or audio is added:



This is what is actually recorded:



Enabling and Disabling Prebuffering

Prebuffering is by default enabled; with a prebuffer size of 3 seconds. To enable/disable prebuffering, select/clear the **Enable prebuffering** check box. When enabling, remember to specify a prebuffer size.

Specifying Prebuffer

Select or type the required prebuffer size (in seconds) in the **Prebuffer size** box. Clicking the **Prebuffer size** box' up/down arrows will increase/reduce the value in increments of one second.

The number of seconds you specify in the **Prebuffer size** box must be sufficiently large to accommodate your requirements.

Example: If, like in this rule example, you plan to be able to save video from five seconds prior to detected motion, the prebuffer size must be at least five seconds.

Using Prebuffering in Rules

The use of prebuffering enables you to create rules (see "Manage Rules" on page 221) specifying that recording should begin prior to the event or time triggering the rule.

Example: Your ability to use this example rule— specifying that recording should start on a camera 5 seconds before motion is detected on the camera— depends on prebuffering being enabled for the camera in question.

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 prebuffering

Working with Storage Area

In the **Storage** area you can monitor and edit database settings for the selected item.



At the top of the **Storage** area, the selected database for the item in question and its status is stated. In this example, the selected database is **Local Default** and its status is **Active**.



Possible Statuses for Selected Database:

- **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 moving data from one or more selected devices from one location to another.
- **Data for the device is currently moving to another location** - database is active and running and moving data from the selected device is currently moving from one location to another.
- **Information unavailable in failover mode** - status information about the database cannot be collected when database is in failover mode. See Manage Failover Servers (on page 321).

Further down in the **Storage** area it is also possible to see which archive(s) are associated with the selected database, their individual status (**OK** or **Old Storage**), location and how much space they each use.

In the **Total used space** field, the total spaced used for the entire storage is indicated.

Selecting a Different Storage:

1. In the upper part of the **Storage** area, click **Select...** to change database for the item in question.
2. In the **Select Storage** dialog that follows, select the wanted database.
3. Click **OK**.
4. Next, in the **Recordings Action** dialog, select whether already existing—**non-archived**—recordings should be moved along to the new storage or deleted.
5. After selecting, click **OK**.

Deleting All Recordings:

1. To delete all recordings for the selected item, click **Delete All Recordings** at the bottom of the **Storage** area.
2. Click **Yes**.

Enabling and Disabling Edge Recording—Camera Only

The **Edge recording** area will only be enabled if the selected camera supports edge recording.

If disabled, select the **Use edge recording if device is unavailable** check box to enable edge recording.

Note that the **Retrieve edge storage recordings from <devices>** rule (see "Actions and Stop Actions Overview" on page 188) can be used independently of this setting.

IMPORTANT: Edge recording cannot coexist with pre-alarm image functionality (see "Actions and Stop Actions Overview" on page 188), action **Send notification to <profile>**). So if a camera is setup to do edge recording, it is not possible to export pre-alarm images from that camera, and vice versa.

What is edge recording? Some cameras are capable of edge recording. This means, that to minimize loss in case connection between the camera and the recording server is lost or broken unexpectedly, they are able to use their own local storage to store recorded video and audio. In that case, cameras with edge recording capabilities can record on their own storage and when communication is re-established, recordings are transferred from the camera to the surveillance system.

Your organization may not want to retrieve recordings from a camera at all times, but rather retrieve it from the camera's edge storage at a specific time of day to save bandwidth, for example, if your organization has cameras in several locations and a Recording Server situated at a central location away from the cameras. To avoid constantly having traffic on the network connection between the cameras and the recording server, your

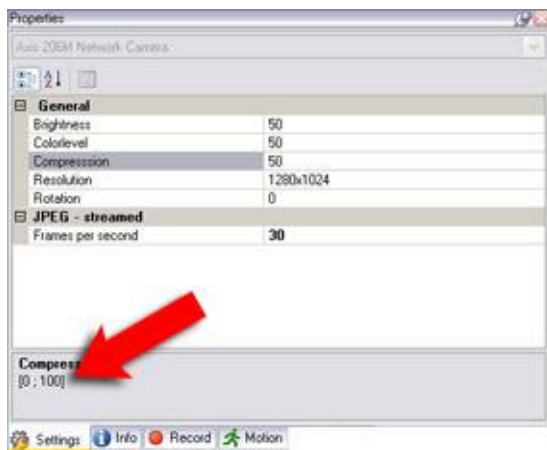


organization can then set up a rule (see "Manage Rules" on page 221) which on a specific time, or within a Time Profile (see "Manage Time Profiles" on page 229), retrieves recordings within a specified time interval, for example eight hours of recordings during business hours which are transferring from the cameras' edge storages to the Recording Server during your organization's closing hours.

Settings Tab Overview

If you select a device group with 400 or more items the **Settings** tab will not be available for editing because changing settings for so many devices in one go takes too long time.

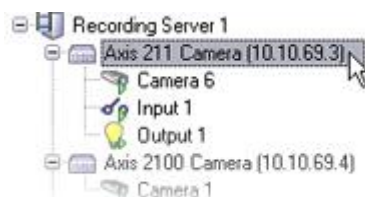
The content of the **Settings** tab is displayed in a table, in which the first column lists the available settings, and the second column lists the value of each setting. You are typically able to change values; when you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the information box below the settings table:



Settings tab, example from camera. Red arrow indicates allowed range; in this example the value used to specify compression must be a number between 0 and 100. Content of **Settings** tab varies depending on selected device type and selected device.

Tip: Some organizations may be required to establish a secure HTTPS connection using SSL (Secure Sockets Layer) between a hardware device and the Matrix and/or XProtect Smart Client. To establish such a connection, you must upload a certificate to the hardware device to enable HTTPS support on the hardware device. Certificates are generated differently by camera vendors. Consult your camera vendor to find out how to get a certificate for your hardware device.

1. In the Management Client's overview pane (see "Panels overview" on page 70), right-click the required recording server to see its device groups. Select the relevant hardware under the wanted device group. On the **Settings** tab, all settings which are common to all of the device group's hardware will be listed.



Selecting hardware under a recording server

2. Select if you want to enable HTTPS on the hardware device. This is not enabled by default.
3. Enter the port to which the HTTPS connection is connected. The port number can be any numeric value between 1 and 65535.



4. Make changes as needed
5. Click **Save**.

HTTPS is enabled for the entire hardware device, that is, for example, a hardware device's camera, microphone and speaker.

Camera

Lets you verify or edit settings, such as default frame rate, resolution, compression, the maximum number of frames between keyframes, on-screen date/time/text display, etc., for a selected camera, or for all cameras within a selected device group.

The content of the **Settings** tab is determined entirely by the drivers for the cameras in question, and is thus likely to vary depending on the types of cameras selected.

Some cameras may support more than one type of stream, for example MPEG4 and MJPEG. In that case, you can use multi-streaming (see "About Multi-streaming" on page 163). If you change a camera's settings, you can quickly verify the effect of your change if you have the preview pane (see "Panels overview" on page 70) enabled. Note, however, that you cannot use the preview pane to judge the effect of frame rate changes, as a special frame rate for the preview pane's thumbnail images is used (defined in the Options dialog (see "Options" on page 285)).

Changing the settings for **Max. frames between keyframes** and **Max. frames between keyframes mode** may lower performance of a number of functionality in the XProtect Smart Client.

Microphone and Speaker

Lets you verify or edit settings for selected microphones and speakers, or for all microphones or speakers within a selected device group.

Content of the **Settings** tab may vary depending on the types of microphones or speakers selected.

Hardware

Lets you verify or edit settings for the hardware selected under a recording server.

The content of the **Settings** tab is determined entirely by the hardware in question, and may thus vary depending on the type of hardware selected. For some types of hardware, the **Settings** tab may display no content at all.

Specify Common Settings for All Items in a Device Group—Cameras, Microphones and Speakers

If using Device Groups (see "About Device Groups" on page 159), you are able to quickly specify common settings for all devices within a given device group:

1. In the list of device in the Management Client's Overview pane (see "Panels overview" on page 70), right-click the required device group. On the **Settings** tab, all settings which are common to all of the device group's items (i.e. cameras, microphones or speakers) will be listed.



2. You are now able to verify or change both common settings and settings for individual item types within the device group.



Example are from camera.

From the menu above the settings list, select the required type of item:



Example are from camera.



3. Make changes as needed.

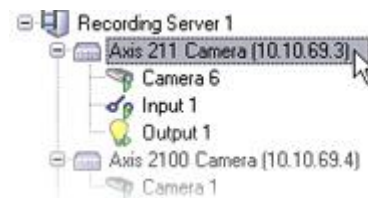


Example are from camera.

4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Specify Common Settings for All Items in a Device Group—Hardware

1. In the Management Client's Overview pane (see "Panels overview" on page 70), right-click the required recording server to see its device groups. Select the relevant hardware under the wanted device group. On the **Settings** tab, all settings which are common to all of the device group's hardware will be listed.



Selecting hardware under a recording server

2. You are now able to verify or change both common settings and settings for the individual hardware types within the device group.

From the menu above the settings list, select the required type of hardware.

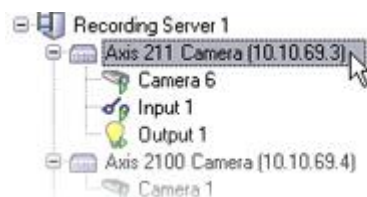
3. Make changes as needed
4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Set up a secure connection on all items in a Device Group

Tip: Some organizations may be required to establish a secure HTTPS connection using SSL (Secure Sockets Layer) between a hardware device and the Matrix and/or XProtect Smart Client. To establish such a connection, you must upload a certificate to the hardware device to enable HTTPS support on the hardware device. Certificates are generated differently by camera vendors. Consult your camera vendor to find out how to get a certificate for your hardware device.



1. In the Management Client's overview pane (see "Panels overview" on page 70), right-click the required recording server to see its device groups. Select the relevant hardware under the wanted device group. On the **Settings** tab, all settings which are common to all of the device group's hardware will be listed.



Selecting hardware under a recording server

2. Select if you want to enable HTTPS on the hardware device. This is not enabled by default.
3. Enter the port to which the HTTPS connection is connected. The port number can be any numeric value between 1 and 65535.
4. Make changes as needed
5. Click **Save**.

HTTPS is enabled for the entire hardware device, that is, for example, a hardware device's camera, microphone and speaker.

Status Icons Overview

The following icons are used to indicate status of cameras (see "Manage Cameras" on page 125), microphones (see "Manage Microphones" on page 144), speakers (see "Manage Speakers" on page 147), input (see "Manage Input" on page 149) and output (see "Manage Output" on page 154) events in item lists:

Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item enabled: Can communicate with the recording server, and can if required be started/stopped automatically through a rule.
					Item recording. Speaker being recorded: Note that what is being said through the speaker can be recorded, but cannot subsequently be played back or exported (for example to prove that a warning was given).
					Item temporarily stopped or has no feed: Often shown when an item is communicating with XProtect Corporate while it is being disabled or enabled. Also shown if the Default Start Audio Feed Rule is not active; see Managing Rules. When stopped, no information is transferred to XProtect Corporate. In which case—if it is a camera—neither live viewing nor recording will be possible. However, a stopped item will still be able to communicate with the recording server, as opposed to when an item is disabled.
					Item disabled: Cannot be started automatically through a rule and will not be able to communicate with the recording server. In the case of a camera, when a camera is disabled, neither live viewing nor recording will be possible.



Cam- era	Micro phone	Spea- ker	In- put	Out- put	Description
					Item database being repaired.
					Item requires attention.
					Status unknown.
					Note that some icons may be combined, as in this example where Item is enabled is combined with Item is recording (since a recording item is also an enabled item).

Client

About clients

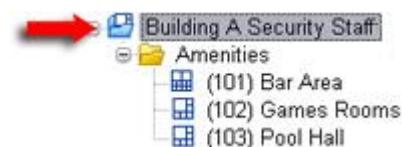
In the Management Client's Site Navigation pane (see "Panels overview" on page 70), you are able to work with the following under **Clients**:

- **Manage View Groups (on page 179):** Here you manage your View Groups, which are basically containers for one or more logical groups of views.
- **Manage XProtect Smart Client Profiles (see "Manage Smart Client Profiles" on page 182):** Here you manage your XProtect Smart Client Profiles. These impact what users of the XProtect Smart Client can and cannot do within the XProtect Smart Client.
- **Manage Matrix Recipients (see "Manage XProtect Matrix Recipients" on page 185):** Here you manage your Matrix Recipients. However, this is only relevant if you use XProtect Matrix.

Manage View Groups

The way in which video from one or more cameras is presented in clients (XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22) and Remote Client (on page 24)) is called a view. A view group is basically a container for one or more logical groups of such views.

In the clients a view group is presented as an expandable folder from which users can select the group, and subsequently the view they want to see:



Example from XProtect Smart Client: Arrow indicates a view group, which contains a logical group (called **Amenities**), which in turn contains three views.



More about View Groups

By default, each role you define in the Management Client is also created as a view group: when you add a role in the XProtect Corporate Management Client, the role will by default appear as a view group for use in clients.

Examples:

XProtect Smart Client displaying a view with video from six different cameras (the view is highlighted in red frame):



A role added in the XProtect Corporate Management Client:



The role appearing as a view group in the XProtect Smart Client:



- A view group based on a role will by default only be available to users/groups who have been assigned to the role in question. You are able to change this; see **View Group Rights** in Specify Rights of a Role (on page 256).
- A view group based on a role will by default carry the role's name.

Example: If you create a role with the name **Building A Security Staff**, it will by default appear in the XProtect Smart Client as a view group called **Building A Security Staff**. You are able to change the name; see the following for more information.



- In addition to the view groups you get when you add roles, you are able to create as many other view groups as you require. You can also delete view groups which you do not want to use, including those automatically created when adding roles. See the following for more information.
- Even though a view group is by default created each time you add a role (see "Manage Roles" on page 251), view groups do not have to correspond to roles. You are therefore able to add any number of view groups—if required—and rename or remove each of your view groups if required. This is no matter whether the view groups were created automatically when adding a role or whether you added them manually.

View groups from a client user's perspective

For more information about views from a client user's perspective, see the separate XProtect Smart Client and Remote Client documentation available on the XProtect Corporate software DVD as well as from www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf).

Adding a View Group

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand the **Clients** node, right-click **View Groups**, and select **Add View Group**. This opens the **Add View Group** dialog.
2. Type the name of the new view group, then click **OK**.
3. Optionally; in the Management Client's Overview pane, select the added view group, then in the Properties pane add a description of the view group.

No roles will have the right to use the newly added view group until you have specified such rights; see **View Group Rights** in Specify Rights of a Role (on page 256) for more information.

Also, even when you have specified which roles should be able to use the newly added view group, already connected client users with the relevant roles must log out and log in again before they will be able to see the view group.

Renaming a View Group

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Clients** and select **View Groups**.
2. In the Management Client's Overview pane, right-click the required view group and select **Rename View Group**.
3. Change the view group's name as required, then press the return key on your keyboard.

Client users already connected must log out and log in again before the name change will be visible.

Removing a View Group

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Clients** and select **View Groups**.
2. In the Management Client's Overview pane, right-click the required view group and select **Delete View Group**.
3. Click **Yes**.



Manage Smart Client Profiles

With Smart Client profiles, XProtect Corporate administrators can control exactly how the XProtect Smart Client should look and behave and exactly what features/panes XProtect Smart Client users are able to work with, and which not. Controllable user right settings are, for example, 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 much, much more.

To manage Smart Client profiles in XProtect Corporate, expand **Client** in the Management Client's Site Navigation pane (see "Panels overview" on page 70), 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 "Working with Smart Client Profiles, Roles and Time Profiles" on page 183).

Add and Configure a Smart Client Profile

You must complete the creation of a Smart Client profile before you can configure it. In other words, the configuration process is done **after** the creation of the profile.

1. In the Management Client's Site Navigation pane, expand **Client**, right-click **Smart Client Profiles**.
2. Select **Add Smart Client Profile...**. This will open the **Add Smart Client Profile** dialog.
Tip: As an alternative to using the menu, press the **CTRL+N** keys on your keyboard.
3. In the **Add Smart Client Profile** dialog, type a name and description of the new profile.
4. Click **OK**.
5. In the Overview pane (see "Panels overview" on page 70), click the profile you just created to configure it. This is done by adjusting settings (see "Adjust settings on a Smart Client Profile" on page 184) on one, more or all of the available tabs.
6. Click **OK**.

Copying a Smart Client Profile

If you have a Smart Client profile with complicated settings and/or rights and need a similar—or almost 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. In the Management Client's Site Navigation pane, expand **Client**, click **Smart Client Profiles**, right-click the required profile in the Overview pane, select **Copy Smart Client Profile...**
2. In the dialog that opens, give the copied profile a new unique name and description.
3. Click **OK**.
4. In the Overview pane, click the profile you just created to configure it. This is done by adjusting settings (see "Adjust settings on a Smart Client Profile" on page 184) on one, more or all of the available tabs.
5. Click **OK**.

Deleting a Smart Client Profile

1. In the Management Client's Site Navigation pane, expand **Client** and right-click **Smart Client Profiles**.
2. Right-click the unwanted profile in the Overview pane, and select **Delete Smart Client Profile**.



Tip: Alternatively, press **DELETE** on your keyboard.

3. Click **Yes**.

Renaming a Smart Client Profile

1. In the Management Client's Site Navigation pane, expand **Client**, and right-click **Smart Client Profiles**.
2. Right-click required profile in the overview pane, and select **Rename Smart Client Profiles...**

Tip: Alternatively, press **F2** on your keyboard.

3. In the dialog that opens, change the name of the profile.

Tip: You are also able to edit the name and description of the profile by simply typing in the **Name** and **Description** fields on the **Info** tab.

4. Click **OK**.

Working with Smart Client Profiles, Roles and Time Profiles

When working with Smart Client profiles, it is important to understand the interaction between Smart Client profiles, roles (see "Manage Roles" on page 251) and time profiles (see "Manage Time Profiles" on page 229).

- Smart Client profiles deal with user right settings in Smart Client
- Roles deal with security settings in Smart Client
- Time profiles deal with time aspects of the two profiles-types

Together these three features provide unique control and customizing possibilities with regards to Smart Client user rights.

Note, that the time profiles mentioned here are general time profiles (see "Manage Time Profiles" on page 229). To learn about the time profiles used in Alarms, see Manage Alarms (on page 273).

Example: Let's say 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 (or use an existing if you have a suitable one). Let's call it **Live only**.
2. Specify the needed live/playback settings on **Live only**.
3. Create a time profile (or use an existing if you have a suitable one). Lets call it **Daytime only**. See Manage Time Profiles (on page 229).
4. Specify the needed time period on **Daytime only**.
5. Create a new role (or use an existing if you have a suitable one), see Manage Roles (on page 251), **Adding a Role and Manage its Smart Client and Time Profiles**. Let's call it **Guard (Selected cameras)**.
6. Specify which cameras **Guard (Selected cameras)** is allowed to work with. See Specify the Rights of a Role (see "Specify Rights of a Role" on page 256).
7. Finally, 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.

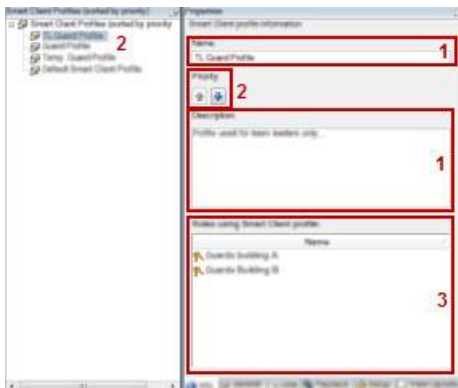


Note also that it is possible to do the setup in a different order, for example, creating the role first and then the Smart Client and the time profile, or any other order preferred.

Adjust settings on a Smart Client Profile

For the needed Smart Client profile, select...

- **Info** to work with; name and description, edit priority of existing profiles and get an overview of which roles use the profile.



Info tab of Smart Client profiles:

1. Name and description of profile (editable)
2. Sorted profile overview and arrow-buttons to move profile priority up and down
3. List of roles using the profile

How does Smart Client profiles work? If a user is a member of more than one role—each with their individual Smart Client profile—the user will get the Smart Client profile with the highest priority.

- **General** to work with; settings such as show/hide and mini- and maximize menu settings, login/-out, startup, timeout, info and messaging options, Sequence Explorer settings and much more.
- **Advanced** to work with; advanced settings such as maximum decoding threads, deinterlacing and time zone settings.

What is maximum decoding threads and deinterlacing? **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.

With **deinterlacing**, you convert video into a non-interlaced format. Interlacing determines how an image is refreshed on a screen. The image is refreshed by first scanning the odd lines in the image, then scanning the even lines. This allows a faster refresh rate because less information is processed during each scan. However, interlacing may cause flickering, or the changes in half of the image's lines may be noticeable.

- **Live** to work with; which live tabs/panes should be available, should camera playback and overlay buttons be available, bookmark and live-related MIP plug-in availability.
- **Playback** to work with; which playback tabs/panes should be available, layout of print reports, should independent playback be available and bookmark and playback-related MIP plug-in availability.



- **Setup** to work with; which general setup/panes/buttons should be available, setup-related MIP plug-in availability, if it the rights to edit a map should be available and if it should be possible to edit live video buffering.
- **Exports** to work with; 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.
- **Timeline** to work with; whether to include audio or not, visibility of indication of time and motion, and finally how to handle playback gaps.
- **View Layouts** to work with; 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.

Note that, on some tabs, in the **Settings** column, most settings are selectable as drop downs. However, a few must be filled in as text-fields. In the **Locked** column, many selections can be locked so that choices made here cannot be changed by users in the Smart Client.

Manage XProtect Matrix Recipients

With XProtect Matrix—XProtect Corporate's integrated solution for distributed viewing of video—you can send video from any camera on a network operating XProtect Corporate to Matrix recipients.

A Matrix recipient is basically a computer capable of displaying Matrix-triggered video. There are two kinds of Matrix recipients: computers running a dedicated Matrix Monitor application and computers running the XProtect Smart Client. (see "Installing the XProtect Smart Client" on page 22)

To see a list of Matrix recipients configured in the Management Client, expand the **Client** node in the Management Client's Site Navigation pane (see "Panels overview" on page 70), 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.

Adding Matrix recipients

To add an existing Matrix recipient— i.e. an existing Matrix Monitor or XProtect Smart Client installation— through the Management Client, do the following:

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand the **Clients** node, then select **Matrix**.
2. In the Management Client's Overview pane (see "Panels overview" on page 70), right-click Matrix **Configurations** and select **Add Matrix...** This opens the **Add Matrix** dialog.

3. In the **Name** field, enter a descriptive name for the Matrix recipient.



4. In the **Description** field, enter a description of the Matrix recipient.
5. In the **Address** field enter the IP address or the host name of the required Matrix recipient
6. In the **Port** field enter the port number used by the Matrix recipient installation.
7. In the **Password** field enter the Matrix recipient's password. Remember that passwords are case sensitive, i.e. there is a difference between typing **amanda** and **Amanda**.

Tip: If in doubt, you can find the port number (default 12345) and password this way: For a Matrix Monitor application, go to the Matrix Monitor's **Configuration** dialog. For an XProtect Smart Client, see the separate Matrix Monitor or XProtect Smart Client documentation.

8. In the **Type** field select the type of Matrix recipient you are adding—a Matrix Monitor or an XProtect Smart Client.

XProtect Corporate 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. Therefore, make sure that you enter the information correctly.

9. Click **OK** to save the settings.

You are now able to use the Matrix recipient in rules.

Defining rules sending video to Matrix recipients

To be able to send video to Matrix recipients you must— after you have configured a Matrix recipient— include the Matrix recipient in a rule that triggers the video transmission to the requested Matrix recipient.

1. Start the **Manage Rule** and in step 1 select a rule type and, if necessary, a condition in step 2. See Manage Rules (on page 221) for more information.
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 MatrixConfiguration** dialog, select the required 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 will stop working.

Advanced tips for Smart Client Matrix recipients

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

1. In the Smart Client, create the required views, and Matrix positions that share the same port number and password.
2. In the Management Client, add the Smart Client in question as a Matrix recipient.
3. You may include the Matrix recipient in a rule (see "Defining rules sending video to Matrix recipients" on page 186).



Rules and Events

About Rules and Events

Events are a central element in XProtect Corporate, primarily used for triggering actions. Actions are configurable through rules (see "Manage Rules" on page 221).

Example: You 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.

In the Management Client's Site Navigation pane (see "Panels overview" on page 70), you are able to work with the following under **Rules and Events**:

- **Rules (see "Manage Rules" on page 221):** Rules are a central element in XProtect Corporate. The behavior of your surveillance system is to a very large extent determined by rules.
- **Time profiles (see "Manage Time Profiles" on page 229):** Time profiles are periods of time defined in the Management Client. They can be used when creating 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 (see "Manage Notification Profiles" on page 233):** With notification profiles you can set up ready-made e-mail notifications, which can automatically be triggered by a rule, for example when a particular event occurs.
- **User-defined Events (see "Manage User-defined Events" on page 238):** User-defined events are custom made events making it possible for users to manually trigger events in the system or react to inputs from the system.
- **Generic Events (see "Manage Generic Events" on page 242):** Generic events allow you to trigger actions in the XProtect event server by sending simple strings via the IP network to XProtect Corporate.
- **Hardware Configurable Events: (see "Hardware Configurable Events" on page 188)** Some hardware is capable of creating events themselves. For example, some cameras are themselves able to detect motion or static/moving objects, and their detections can be used as events in XProtect Corporate. Such events must obviously be configured on the hardware before they can be used in XProtect Corporate, therefore they are called hardware configurable events. Read more about hardware configurable events for cameras (see "Manage Cameras" on page 125), inputs (see "Manage Input" on page 149) and microphones (see "Manage Microphones" on page 144) respectively.

See Events Overview (on page 216) for a list of events.

User-defined Events

If the event you require is not on the **Events Overview** list, you can create your own user-defined events (see "Manage User-defined Events" on page 238). Such user-defined events can be useful if you want to integrate other systems with your surveillance system.

Example: With user-defined events, you can use data received from a third-party access control system as events in XProtect Corporate; the events can subsequently trigger actions. This way, you can, for example, begin recording video from relevant cameras when somebody enters a building.

User-defined events can also be used for manually triggering events while viewing live video in the XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22).



Hardware Configurable Events

Some hardware is capable of creating events themselves. For example, some cameras are themselves able to detect motion or static/moving objects, and their detections can be used as events in XProtect Corporate. Such events must obviously be configured on the hardware before they can be used in XProtect Corporate, therefore they are called hardware configurable events. Read more about hardware configurable events for cameras (see "Manage Cameras" on page 125), inputs (see "Manage Input" on page 149) and microphones (see "Manage Microphones" on page 144) respectively.

Actions and Stop Actions Overview

When creating rules in the **Manage Rule** wizard (see Manage Rules (on page 221)), you are able to select between a number of different actions:



Example: Selecting actions

Some of these actions will require a subsequent stop action.

Example: If you select the action **Start recording**, recording will start and potentially continue indefinitely. Therefore, the action **Start recording** has a compulsory stop action called **Stop recording**.

Manage Rule makes sure you specify such stop actions when necessary; stop actions are typically specified on one of the last steps of the wizard:



Selecting stop actions. In the example, note the compulsory stop action (selected, dimmed), the non-relevant stop actions (dimmed) and the optional stop actions (selectable).

Each type of action is described (additional actions may, however, be available if your XProtect Corporate installation uses add-on products, special plug-ins, etc.). For each type of action, stop action information is listed as well:

Action	Description
Start recording	Begin recording, i.e. begin saving video in the database of the selected camera. When selecting this type of action, Manage Rule will prompt you to specify when recording should start (either immediately or a number of seconds before the triggering event/beginning of the triggering time interval) as well as on which devices the action should take place. This type of action requires that recording has been enabled on the cameras to which the action will be linked. Being able to save video from before an event or time interval is only possible if prebuffering is enabled for the cameras in question. You enable recording and specify prebuffering settings for a camera on the Record tab (see



Action	Description
	"Record Tab Overview" on page 170). Stop action required: This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Stop recording. Without this stop action, recording would potentially continue indefinitely. You will also have the option of specifying further stop actions.
Start feed on <devices>	Begin video feed from camera devices to XProtect Corporate. When the feed from a device is started, video will be transferred from the device to XProtect Corporate, in which case live viewing and recording of video will be possible. IMPORTANT: While this type of action enables access to selected cameras' video feeds, it does not guarantee that video will be recorded, as cameras' recording settings must be specified separately. When selecting this type of action, Manage Rule (see "Manage Rules" on page 221) will prompt you to specify on which devices feeds should be started. Tip: XProtect Corporate has a default rule ensuring that feeds are always started on all cameras. Note however, that the default rule may have been manually deactivated or modified. Stop action required: This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Stop feed. You will also have the option of specifying further stop actions. Note that using the compulsory stop action Stop feed to stop the feed from a device means that video will no longer be transferred from the device to XProtect Corporate, in which case live viewing and recording of video will no longer be possible. However, a device on which the feed has been stopped will still be able to communicate with the recording server, and the feed can be started again automatically through a rule, as opposed to when the device has been manually disabled in the Management Client.
Set live frame rate on <devices>	Sets a particular frame rate to be used when displaying live video from the selected cameras, instead of the cameras' default frame rate (specified on the Settings tab (see "Settings Tab Overview" on page 174)). When selecting this type of action, Manage Rule will prompt you to specify which frame rate to set, and on which devices. Always verify that the frame rate (number of frames per second) you specify is available on the cameras in question. Stop action required: This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Restore default live frame rate. Without this stop action, the default frame rate would potentially never be restored. You will also have the option of specifying further stop actions.
Set recording frame rate on <devices>	Sets a particular frame rate to be used when saving recorded video from the selected cameras in the database, instead of the cameras' default recording frame rate. When selecting this type of action, Manage Rule will prompt you to specify which recording frame rate to set, and on which cameras. Specifying recording frame rate is only possible for MJPEG, a video codec (technology



Action	Description
	for compressing and decompressing data) with which each frame is separately compressed into a JPEG image. This type of action also requires that recording has been enabled on the cameras to which the action will be linked. You enable recording for a camera on the Record tab (see "Record Tab Overview" on page 170). The maximum frame rate you will be able to specify will depend on the camera types in question, and on their selected image resolution. Stop action required: This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Restore default recording frame rate. Without this stop action, the default recording frame rate would potentially never be restored. You will also have the option of specifying further stop actions.
Start patrolling on <device> using <profile> with PTZ priority <priority>	Begins PTZ patrolling (the continuous moving of a camera between a number of preset positions) according to a particular patrolling profile (the exact definition of how patrolling should be carried out, including the sequence of preset positions, timing settings, etc.) for a particular PTZ camera with a particular priority. What is Priority? When several users on a surveillance system wish to control the same PTZ camera at the same time, conflicts may occur. PTZ priority lets you alleviate the problem 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. Default PTZ priority is 3000. If your system is upgraded from an older version of XProtect Corporate, the old values (Very Low, Low, Medium, High and Very High) have been translated as follows: ▶ Very Low = 1000 ▶ Low = 2000 ▶ Medium = 3000 ▶ High = 4000 ▶ Very High = 5000 If your system is upgraded to XProtect Corporate 4.0 (or future versions), rule priority settings is a new feature. Existing rules (created without priority) automatically get priority 1. It is strongly recommended to reconsider this lowest possible priority for all affected rules. When selecting this type of action, Manage Rule will prompt you to select a patrolling profile. Only one patrolling profile on one device can be selected; it is not possible to select several patrolling profiles. This type of action requires that the device to which the action will be linked is a PTZ (Pan/Tilt/Zoom) device, and that at least one patrolling profile has been defined for the device. You define patrolling profiles for a PTZ camera on the Patrolling tab (see "PTZ Patrolling Tab (Camera Properties)" on page 136). Stop action required: This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Stop patrolling. Without this stop action, patrolling would potentially never stop. You will also have the option of specifying further stop actions.



Action	Description
Pause patrolling on <devices>	Pauses PTZ patrolling (the continuous moving of a camera between a number of preset positions). When selecting this type of action, Manage Rule will prompt you to specify the devices on which patrolling should be paused. This type of action requires that the devices to which the action will be linked are PTZ (Pan/Tilt/Zoom) devices, and that at least one patrolling profile has been defined for those devices. You define patrolling profiles for a PTZ camera on the Patrolling tab (see "PTZ Patrolling Tab (Camera Properties)" on page 136). Stop action required: This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Resume patrolling. Without this stop action, patrolling would potentially pause indefinitely. You will also have the option of specifying further stop actions.
Move <device> to <preset> position with PTZ priority <priority>	Moves a particular camera to a particular preset position - however always according to priority. When selecting this type of action, Manage Rule will prompt you to select a preset position. Only one preset position on one camera can be selected; it is not possible to select several preset positions. If your system is upgraded to XProtect Corporate 4.0 (or future versions), rule priority settings is a new feature. Existing rules (created without priority) automatically get priority 1. It is strongly recommended to reconsider this lowest possible priority for all affected rules. This type of action requires that the devices to which the action will be linked are PTZ (Pan/Tilt/Zoom) devices, and that at least one preset position has been defined for those devices. You define preset positions for a PTZ camera on the Presets tab (see "PTZ Presets tab (camera properties)" on page 140). No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Move to default preset on <devices> with PTZ priority <priority>	Moves one or more particular cameras to their respective default preset positions - however always according to priority. When selecting this type of action, Manage Rule will prompt you to select which devices the action should apply for. If your system is upgraded to XProtect Corporate 4.0 (or future versions), rule priority settings is a new feature. Existing rules (created without priority) automatically get priority 1. It is strongly recommended to reconsider this lowest possible priority for all affected rules. This type of action requires that the devices to which the action will be linked are PTZ (Pan/Tilt/Zoom) devices, and that default preset positions have been defined for those devices. You define default preset positions for a PTZ camera on the Presets tab (see "PTZ Presets tab (camera properties)" on page 140). No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Set device output to <state>	Sets an output on a device to a particular state (activated or deactivated). When selecting this type of action, Manage Rule will prompt you to specify which state to set, and on which devices. This type of action requires that the devices to which the action will be linked each have at least one external output unit connected to an output port. No compulsory stop action: This type of action does not require a stop action;



Action	Description
	although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Create bookmark on <device>	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 (on page 285) dialog. When selecting this type of action, Manage Rule will prompt you to specify bookmark details and select device. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Send notification to <profile>	Sends a notification, using a particular notification profile. When selecting this type of action, Manage Rule will prompt you to select a notification profile, and which devices to include pre-alarm images from. Only one notification profile can be selected; it is not possible to select several notification profiles. Tip: Even though you are only able to select a single notification profile, bear in mind that a single notification profile may contain several recipients. This type of action requires that at least one notification profile (see "Manage Notification Profiles" on page 233) has been set up. Pre-alarm images will only be included if e-mail notification is used and the Include images option has been enabled for the notification profile in question. IMPORTANT: Pre-alarm images functionality cannot coexist with edge recording (see "Record Tab Overview" on page 170). So if a camera is setup to export pre-alarm images it is not possible to enable edge recording on that camera, and vice versa. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Make new <log entry>	Generates an entry in the rule log (see "Manage Logs" on page 267). When selecting this type of action, Manage Rule will prompt you to specify a text for the log entry. Tip: When specifying the log text, you will be able to quickly insert variables, such as \$DeviceName\$, \$EventName\$, etc. into the log message wording. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Start plug-in on <devices>	Starts one or more plug-ins. When selecting this type of action, Manage Rule will prompt you to select required plug-ins, and on which devices to start the plug-ins. This type of action requires that at one or more plug-ins are available on your system. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Stop plug-in on <devices>	Stops one or more plug-ins. When selecting this type of action, Manage Rule will prompt you to select required plug-ins, and on which devices to stop the plug-ins. This type of action requires that at one or more plug-ins are available on your system. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Apply new settings on <devices>	Changes device settings. When you select this type of action, Manage Rule will prompt you to select required devices, and you will be able to define required settings



Action	Description
	on the devices you have specified. If defining settings for more than one device, you will only be able to change settings that are available for all of the specified devices. Example: You specify that the action should be linked to Device 1 and Device 2. Device 1 has the settings A, B and C, and Device 2 has the settings B, C and D. In this case, you will only be able to change the settings that are available for both devices, namely settings B and C. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Set Matrix to view <devices>	Makes video from the selected cameras appear on a computer capable of displaying Matrix (see "Manage XProtect Matrix Recipients" on page 185) -triggered video, i.e. a computer on which either an XProtect Smart Client or a Matrix Monitor application is installed. When you select this type of action, Manage Rule will prompt you to select a Matrix recipient (see "Manage XProtect Matrix Recipients" on page 185), and one or more devices from which to display video on the selected Matrix recipient. This type of action lets you 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. Tip: By right-clicking a rule in the Rules list you are able to copy and re-use the content of rules. This way you can avoid having to create near-identical rules from scratch. As part of the configuration on the Matrix recipients themselves, users must specify the port number and password required for the Matrix communication. Make sure that the users have access to this information. The users must typically also define the IP addresses of allowed hosts, i.e. hosts from which commands regarding display of Matrix-triggered video will be accepted. In that case the users must also know the IP address of the XProtect Corporate management server (or any router or firewall used).
Send SNMP trap	Generates a small message which logs events on selected devices. The text of SNMP traps are auto-generated and cannot be customized. It will typically contain the source type and name of the device on which the event occurred. To configure who receives SNMP trap messages, see SNMP Support (on page 335). No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Retrieve edge storage recordings from <devices>	Retrieves and stores edge recordings from selected devices (that support edge recording (see "Enabling and Disabling Edge Recording—Camera Only" on page 173)). Can be set to execute immediately or at a certain point in time. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time. Note that this rule is independent of the Use edge recording if device is unavailable setting (see "Enabling and Disabling Edge Recording—Camera Only" on page 173).
Save attached image	Ensures that when an image is received from the Images Received event (see "Events Overview" on page 216) (sent via SMTP e-mail from a camera) it is saved for future usage. In future, other events might also be able to trigger this action. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.



Action	Description
Activate archiving on <archives>	Starts archiving on one or more archives. When you select this type of action, Manage Rule will prompt you to select required archives. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
On <site> trigger <user-defined event>	Relevant mostly within Milestone Federated Architecture (see "Milestone Federated Architecture Overview" on page 293), but can also be used in a single server setup. Used for triggering a user defined event on a site - normally a remote site within a federated hierarchy. No compulsory stop action: This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.

Create Typical Rules

The following is a introduction to examples of typical rules, what you can do with them and how they can be constructed. The descriptions are examples only. If wishing to base real-life rules on the examples, be prepared to substitute the examples' device names and parameters with device names and parameters relevant to your system. Numerous other rule configurations are possible. If the rule you require is not listed among the examples, it by no means indicates that the rule you require cannot be created in XProtect Corporate.

Basic Rules

- **Use Higher Live Frame Rate on Motion:** Ensures that when motion is detected on a specific camera, XProtect Corporate will use a higher than default live frame rate for the camera, and return to using the camera's default live frame rate when motion is no longer detected. The effect is higher quality live video whenever there is motion. When the specified part of the day ends, the PTZ camera will stop patrolling.

PTZ-Related Rules

- **Use Specific PTZ Patrolling Profile During Specific Part of Day:** Ensures that during a specific part of the day, a PTZ (Pan/Tilt/Zoom) camera will patrol according to a specific patrolling profile (i.e. the exact definition of how patrolling should be carried out, including the sequence for moving between preset positions, timing settings, etc.). When the specified part of the day ends, the PTZ camera will stop patrolling.
- **Use Different PTZ Patrolling Profiles for Day/Night:** Ensures that during daytime, a PTZ camera will patrol according to a specific patrolling profile. And during nights, according to another patrolling profile.
- **Pause PTZ Patrolling and Go to PTZ Preset on Input:** Ensures that a specific external input is activated, a PTZ camera will pause its patrolling, move to a specific preset position, and remain at the preset position for a specific period of time, after which it will resume patrolling.

Click to get more detailed step-by-step descriptions of how to create the above mentioned example rules:

Use Higher Live Frame Rate on Motion

In this example, the camera has a default live frame rate of 10 frames per second (FPS), and the rule will increase the live frame rate to 25 FPS when applied. The effect will be a higher quality live video for as long as motion is detected on the camera.

Note that recording frame rate (the frame rate with which video sequences will be saved) is specified separately, and will not be affected by this rule.



If you want to permanently change the default frame rate for a camera, do not use a rule. Change the camera's default frame rate on the **Settings** tab (see "Settings Tab Overview" on page 174) instead.

Motion is normally detected by XProtect Corporate when video received from cameras is analyzed. This is the type of motion detection dealt with in this example. However, some cameras are— depending on configuration of the camera hardware— themselves able to detect motion. Such hardware-configurable motion detection can also be used in XProtect Corporate rules, although that is beyond the scope of this example.

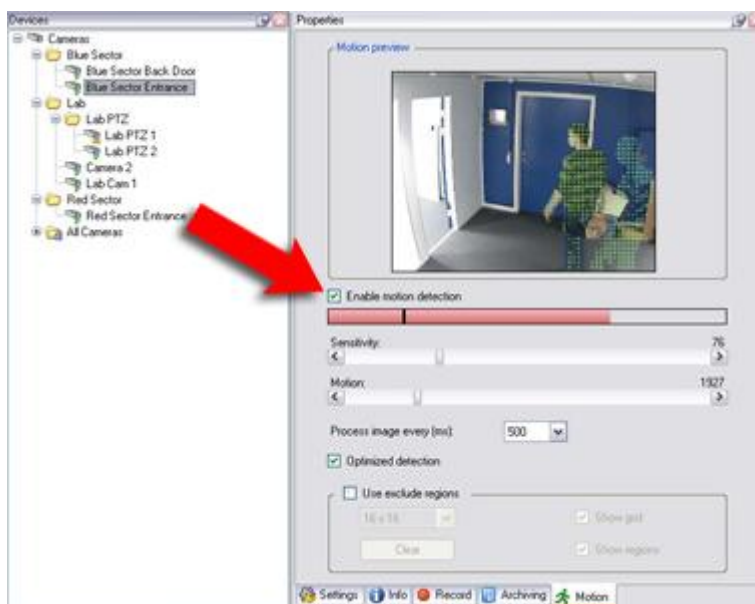
Prerequisites

This rule is based on motion detection on a specific camera. Therefore, motion detection must be enabled on the camera in order for the rule to work as intended. Before creating a rule like this, always verify the following:

- Motion detection is enabled for the camera in question

Show me how to verify this...

To verify that motion detection has been enabled for a camera, expand Devices in the Management Client's Site Navigation pane, and select Cameras. This will display a list of cameras in the overview pane. Select the required camera from the list, and select the Motion tab in the Properties pane. On the Motion tab, verify that the Enable motion detection check box is selected.



Arrow indicates position of **Enable motion detection** check box

Note that other settings on the **Motion** tab, such as **Sensitivity**, will determine what will be interpreted as motion. Merely enabling motion detection may thus not be sufficient to meet your requirements. Time spent on finding the best possible balance of motion detection settings under different conditions (day/night, calm/windy weather, etc.) will help you later avoid unnecessary recordings, etc.



Creating the Rule

1. In the Management Client's Site Navigation pane, expand **Rules and Events**, then right-click Rules and select **Add New Rule...**:



Tip: Instead of right-clicking to select **Add New Rule**, you can press CTRL+N on your keyboard.

2. The **Manage Rule** wizard opens. Type a name for the new rule in the **Rule name** field.



In this example... the rule will cover a specific camera, Camera 1. We therefore overwrite the default rule name (e.g. New Rule 001) with a descriptive name:



Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of **Manage Rule**, select the required rule type.



In this example... we want to base the rule on an event, namely detected motion. Therefore, we select **Perform an action on <event>**. Our selection is immediately reflected in the initial rule description in the lower half of the wizard window:

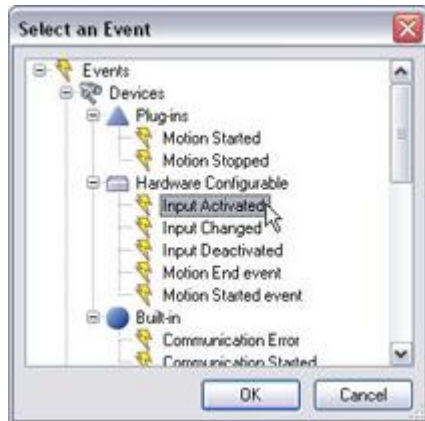


4. Click the underlined items in the rule description in order to specify its exact content:

Event link: Clicking the **event** link lets you select the event which must occur in order for the rule to apply. In order for you to get a good overview, selectable events are listed in groups according to whether they are related to plug-ins, dependent on hardware configuration, built into XProtect Corporate itself, etc.



➔ **In this example** ... we want the event to be detected motion. Motion detection events are technically related to XProtect Corporate's motion detection plug-in, so we go to the **Plug-ins** group, select the event **Motion Start**, and click **OK**:



Devices/recording server/management server link: When you have selected the required event, clicking the **devices/recording server/management server** link opens the **Select Group Members** window, which lets you specify the devices on which device the event should occur in order for the rule to apply.

➔ **In this example** ... the event should occur on Camera 1 in order for the rule to apply. In the **Select Group Members** window we therefore drag Camera 1 to the **Selected** list and click **OK**. By doing this we have specified the exact content of the first part of the wizard's rule description, which now looks like this:

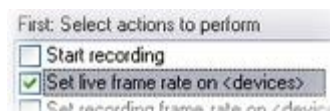


- Click **Next** to move to step 2 of the wizard. On step 2 of the wizard, specify which time conditions should be met in order for the rule to apply.

➔ **In this example** ... we simply want the rule to apply whenever motion is detected on Camera 1, regardless of time. When creating event-based rules it is possible to bypass the time conditions; we therefore want to skip step 2 entirely.

- Click **Next** to move to step 3 of the wizard. On step 3 of the wizard, first specify which actions to perform.

➔ **In this example** ... we want to set a specific live frame rate. We therefore select the action **Set live frame rate on <devices>**:



Based on the selection of actions, the wizard automatically extends the rule description in the lower part of the wizard window.



In this example ... Based on our selection **Set live frame rate on <devices>**, the wizard automatically suggests a rule description in which the frame rate should be set on **the device on which event occurred**. The wizard furthermore prompts us to specify the required number of frames per second:



To specify the required number of frames per second, we click the **frames per second** link, specify a frame rate of 25, and click **OK**:

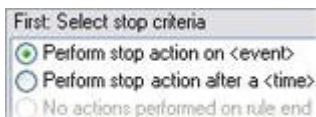


The rule description now indicates that the frame rate will be set to 25 frames per second.

7. Click **Next** to move to step 4 of the wizard. On step 4 of the wizard, select stop criteria. Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.



In this example ... Without a stop criterion, the rule in this example would set the frame rate for the camera to 25 FPS indefinitely upon motion detection. Based on the elements in our rule description, the wizard therefore automatically suggests the stop criterion **Perform stop action on <event>**:



Note that the stop criterion **No actions performed on rule end** is not available: a stop criterion must be defined for this type of rule. In the rule description, the wizard furthermore automatically suggests that the stop action is performed when motion is no longer detected on Camera 1:



This is just what we want; we do not need to change any of the wizard's suggestions. However, we still need to define exactly which kind of stop action should take place when motion ends on Camera 1.

8. Click **Next** to move to the next step of the wizard. In this step, the wizard suggests one or more stop actions based on the previously selected start actions.



In this example ... Based on the start action **set frame rate** in our rule description, the wizard automatically suggests the stop action **restore default frame rate**. It furthermore suggests that the default frame rate should be restored immediately after the last detected motion:



This is also just what we want; we do not need to change it, although by clicking the **immediately** link we could have specified a delay of e.g. 3 seconds.

Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met. If you do not want the rule to be active straight away, clear the **Active** check box in the top part of the **Manage Rule** window:



Tip: You can always activate/deactivate the rule later.

9. Click **Finish**. This will add your new rule to the list of rules.

Use Specific PTZ Patrolling Profile During Specific Part of Day

Tip: When patrolling stops, you can—if needed—get the PTZ camera to start patrolling immediately after according to another patrolling profile.

Prerequisites

When a PTZ camera patrols according to a patrolling profile, it continuously moves between different preset positions. Therefore, the required preset positions and at least one patrolling scheme must be defined for the PTZ camera in question. Before creating a rule like this, always verify the following:

- The camera in question is a PTZ camera
- At least two preset positions are defined for the camera

How to define preset positions...

To define preset positions for a PTZ camera, expand Devices in the Management Client's Site Navigation pane (see "Panels overview" on page 70) and select Cameras. In the overview pane (see "Panels overview" on page 70), select the required PTZ camera from the list, then select the Presets tab in the properties pane (see "Panels overview" on page 70). For descriptions of the exact functionality of the Presets tab, see Preset Positions (see "PTZ Presets tab (camera properties)" on page 140).

- At least one patrolling profile is defined for the camera

How to define a patrolling profile...

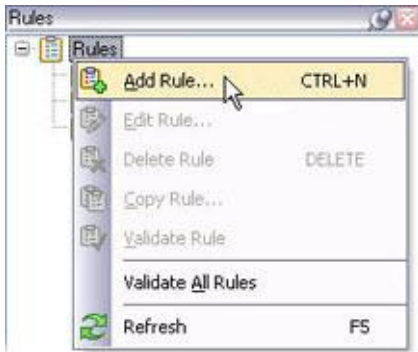
To define patrolling profiles for a PTZ camera, expand Devices in the Management Client's Site Navigation pane (see "Panels overview" on page 70) and select Cameras. In the overview pane (see "Panels overview" on page 70), select the required PTZ camera from the list, then select the Patrolling tab



in the properties pane (see "Panels overview" on page 70). For descriptions of the exact functionality of the **Patrolling** tab, see Patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 136).

Creating the Rule

1. In the Management Client's Site Navigation pane, expand **Rules and Events**, then right-click Rules and select **Add New Rule...**:

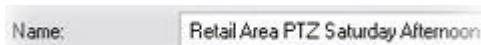


Tip: Instead of right-clicking to select **Add New Rule**, you can press CTRL+N on your keyboard.

2. The **Manage Rule** wizard opens. Type a name for the new rule in the **Rule name** field.



In this example... the rule will only cover a specific camera (simply called **PTZ Camera**) and how it should patrol on Saturday afternoons. We therefore overwrite the default rule name (e.g. **New Rule 001**) with a descriptive name:

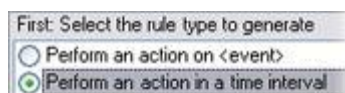


Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of **Manage Rule**, select the required rule type.



In this example... we want to base the rule on a time period. Therefore, we select **Perform an action in a time interval**:

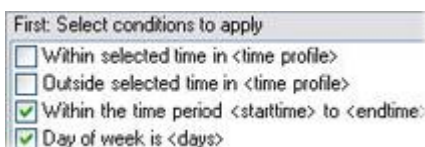


Click **Next** to move to the next step of the wizard.

4. On the wizard's next step, specify which time conditions should be met in order for the rule to apply.



In this example... we want the rule to apply between 1:00 and 8:00 on Saturdays, so two time conditions are required: one which specifies use of a start time and end time, and one which specifies use on a particular day of the week. We therefore select **Within the time period <start time> to <end time>** and **Day of week is <day>**:





Our selection is immediately reflected in the initial rule description in the lower half of the wizard window:



Tip: If we had previously created a suitable time profile covering the required period of time, we could have just selected the time condition Within selected time in <time profile>, then pointed to the time profile in question.

Read more about time profiles under Managing Time Profiles (see "Manage Time Profiles" on page 229).

5. Click the underlined items in the rule description in order to specify its exact content:

start time: Clicking the start time link lets you specify required start time.



In this example ... we want the start time to be one o'clock in the afternoon, so we specify 1:00, and click OK:

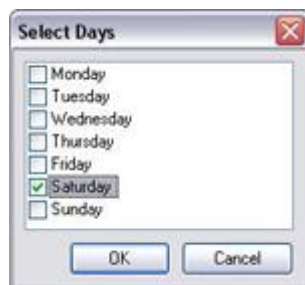


end time: The **end time** link works just like the **start time** link. We specify 8:00.

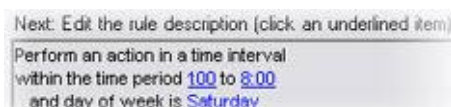
days: Clicking the **days** link lets you specify required days of the week.



In this example ... our rule should only apply on Saturdays, so we select **Saturday**, and click **OK**:



By doing this, we have specified the exact content of the first part of the wizard's rule description, which now looks like this:



Click **Next** to move to step 3 of the wizard.

6. On step 3 of the wizard, first specify which actions to perform.

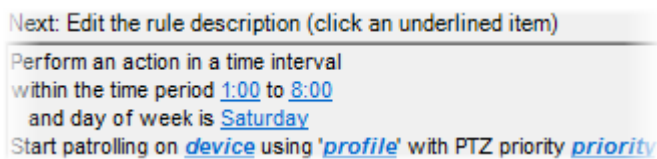


➔ In this example ... we want to start patrolling according to a specific patrolling profile. We therefore select the action **Start patrolling on <device> using <profile> with PTZ priority <priority>**:



Based on the selection of actions, the wizard automatically extends the rule description in the lower part of the wizard window.

➔ In this example... Based on our selection **Start patrolling on <device> using <profile> with PTZ priority <priority>**, the wizard automatically prompts us to specify the required camera, patrolling profile and its priority (see "Actions and Stop Actions Overview" on page 188):



We click the **device** link, expand the relevant camera folder, select the required camera, and click **OK**:



Next we click the **profile** link, select the required patrolling profile from our list of previously defined patrolling profiles, and click **OK**:



Finally, we click the **priority** link to set the priority (see "Actions and Stop Actions Overview" on page 188) of the patrolling profile.



By doing this, we have further specified the content of the wizard's rule description, which now looks like this:

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

Perform an action in a time interval
within the time period 1:00 to 8:00
and day of week is Saturday
Start patrolling on Retail Area PTZ using 'Retail Area Saturday Afternoon' with PTZ priority 5000

Click **Next** to move to step 4 of the wizard.

- On step 4 of the wizard, select stop criteria. Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.



In this example... Without a stop criterion, the rule in this example would start patrolling within the specified time period, but never stop it. Based on the elements in our rule description, the wizard therefore automatically suggests the stop criterion **Perform stop action when time interval ends**:

First: Select stop criteria

☒ Perform stop action when time interval ends
☐ No actions performed on rule end

Note that the stop criterion **No actions performed on rule end** is not available: a stop criterion must be defined for this type of rule. We still need to define exactly which kind of stop action should take place when the time period ends.

Click **Next** to move to the next step of the wizard.

- In this step, the wizard suggests one or more stop actions based on the previously selected start actions.



In this example ... Based on the start action start patrolling in our rule description, the wizard automatically suggests the stop action **Stop patrolling**. It furthermore suggests that patrolling is stopped immediately when the time period ends:

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

Perform an action in a time interval
within the time period 1:00 to 8:00
and day of week is Saturday
Start patrolling on Retail Area PTZ using 'Retail Area Saturday Afternoon' with PTZ priority 5000

Perform an action when time interval ends
Stop patrolling immediately

This is just what we want; we do not need to change it, although by clicking the **immediately** link we could have specified a delay of e.g. 60 seconds.

Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met. If you do not want the rule to be active straight away, clear the **Active** check box in the top part of the **Manage Rule** window:



Tip: You can always activate/deactivate the rule later.



9. Click **Finish**. This will add your new rule to the list of rules:



Use Different PTZ Patrolling Profiles for Day/Night

In this example, **daytime** is defined by a time profile covering the period between 08.00 and 20.00 on all days of the week and **nights** are defined as periods not covered by the **daytime** time profile. This requires two near-identical rules; one for each patrolling profile. When you have created the first rule, you can make a copy of it, and quickly create the second rule based on the copy. Both rules are covered in this example.

Prerequisites

This rule is based on a PTZ camera being able to patrol according to two different patrolling profiles, and a time profile being used to determine which patrolling profile should be used. Before creating a rule like this, always verify the following:

- You have specified a time profile covering at least one of the time periods you want to differentiate between. You could specify time profiles covering both time periods, but it will not be necessary since rules can be set up to apply **within** as well as outside a time profile.

How to specify a time profile...

To specify a time profile, expand **Rules and Events** in the Management Client's Site Navigation pane (see "Panels overview" on page 70), then select Time Profiles. The **Time Profiles** list will appear. In the **Time Profiles** list, right-click Time Profiles, and select Add Time Profile... For detailed information about specifying time profiles, see Managing Time Profiles (see "Manage Time Profiles" on page 229).

- The camera in question is a PTZ camera.
- Preset positions and at least two patrolling profiles are defined for the camera.

How to define preset positions and patrolling profiles...

When a PTZ camera patrols according to a patrolling profile, it moves between a number of preset positions. Thus, before you are able to define patrolling profiles for a PTZ camera, the preset positions required for the patrolling profiles must be defined.

To define preset positions for a PTZ camera, expand **Devices** in the Management Client's Site Navigation pane (see "Panels overview" on page 70) and select **Cameras**. This will display a list of cameras in the overview pane (see "Panels overview" on page 70). Select the required PTZ camera from the list, and select the Presets tab in the properties pane (see "Panels overview" on page 70). For details of how to define preset positions on the **Presets** tab, see Preset Positions (see "PTZ Presets tab (camera properties)" on page 140).

Once you have defined the required preset positions, patrolling profiles for the PTZ camera are defined on the neighboring **Patrolling** tab. For details of how to define patrolling profiles on the **Patrolling** tab, see Patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 136).



Creating the First Rule; Patrolling During Daytime

1. In the Management Client's Site Navigation pane, expand **Rules and Events**, then right-click Rules and select **Add New Rule...**:

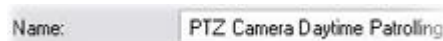


Tip: Instead of right-clicking to select **Add New Rule**, you can press CTRL+N on your keyboard.

2. The **Manage Rule** wizard opens. Type a name for the new rule in the **Rule name** field.



In this example...the rule will cover a specific camera and how it should patrol during daytime. We therefore overwrite the default rule name (e.g. **New Rule 001**) with a descriptive name:

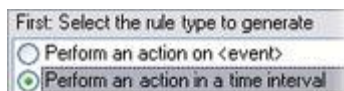


Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of **Manage Rule**, select the required rule type.



In this example...we want to base the rule on a time period. Therefore, we select **Perform an action in a time interval**:

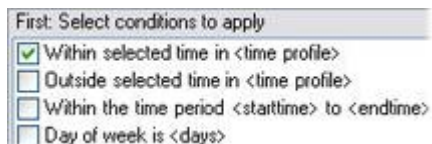


Click **Next** to go to step 2 of the wizard.

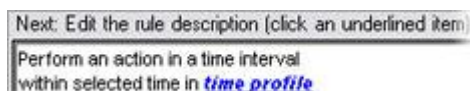
4. On step 2 of the wizard, specify which time conditions should be met in order for the rule to apply.



In this example... we want the rule to apply within a specific time profile, so we select the time condition **Within selected time in <time profile>**:



Based on our selection, the wizard prompts us to specify the required time profile in the rule description:



Click the underlined item to specify the exact content of the rule description.



➔ In this example... we click the time **profile** link, select the time profile **Daytime**, and click **OK**:



The rule description now reflects our selection:

Next: Edit the rule description (click an underlined item)
Perform an action in a time interval
within selected time in Daytime

Click **Next** to move to step 3 of the wizard.

- On step 3 of the wizard, first specify which actions to perform.

➔ In this example...we want patrolling according to a specific patrolling profile. We therefore select the action **Start patrolling on <device> using <profile> with PTZ priority <priority>**:

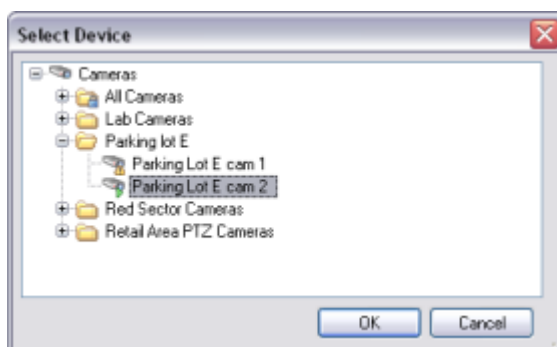


Based on the selection of actions, the wizard extends the rule description, and prompts us to specify the required device, patrolling profile and its priority (see "Actions and Stop Actions Overview" on page 188):

Next: Edit the rule description (click an underlined item)
Perform an action in a time interval
within selected time in Daytime
Start patrolling on device using 'profile' with PTZ priority priority

Click the underlined items in the extension of the rule description in order to specify their exact contents:

➔ In this example... we first click the **device** link and in the **Select device** dialog opening we select a device and click **OK**:



Then we click the **profile** link and select a patrolling profile in the dialog opening and then click OK.



Finally, click the **priority** link to set the priority (see "Actions and Stop Actions Overview" on page 188) of the patrolling profile.

The rule description now reflects our selection:

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

Perform an action in a time interval
within selected time in [Daytime](#)
Start patrolling on [Parking Lot E cam 2](#) using 'My Patrolling Profile' with PTZ priority [5000](#)

Click **Next** to move to step 4 of the wizard.

- On step 4 of the wizard, select stop criteria.

Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.



In this example...Without a stop criterion, the rule in this example would make the PTZ camera start patrolling according to the selected patrolling profile, but it would never stop. Based on the elements in our rule description, we therefore must select a stop criterion. Since our rule is triggered when a time period starts, the wizard automatically suggests that stop action is performed when the time period ends:

First: Select stop criteria

☒ Perform stop action when time interval ends
☐ No actions performed on rule end

The suggestion is also reflected in the rule description. However, we still need to specify exactly which stop action we want performed.

Click **Next** to move to the next step of the wizard.

- In this step, the wizard suggests one or more stop actions based on the previously selected start actions.



In this example...Based on the start action **start patrolling** in our rule description, the wizard automatically suggests the stop action **stop patrolling**. It furthermore suggests that patrolling is stopped immediately when the time period ends:

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

Perform an action in a time interval
within selected time in [Daytime](#)
Start patrolling on [Parking Lot E cam 2](#) using 'My Patrolling Profile' with PTZ priority [5000](#)

Perform an action when time interval ends
Stop patrolling [immediately](#)

This is exactly what we want; we do not need to change it.

Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met.

If you do not want the rule to be active straight away, clear the **Active** check box in the top part of the **Manage Rule** window:

Name: PTZ Camera
Description:
Active: ☒

Tip: You can always activate/deactivate the rule later.



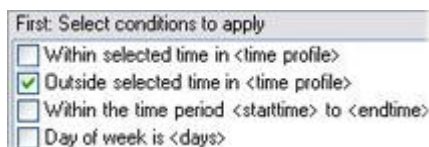
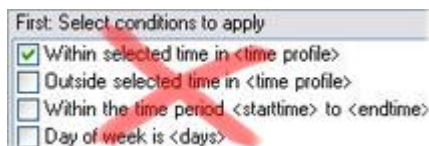
8. Click **Finish**. This will add your new rule to the list of rules:



Creating the Second Rule; Patrolling During Nighttime

Tip: You do not have to create the second rule from scratch; you can make a copy of the first rule, then change it. To copy a rule, select the rule in the **Rules** list, right-click, and select **Copy Rule...** This will open **Manage Rule**, which will display an editable copy of the rule.

1. Copy the first rule, then make the following changes to the rule:
 - Change the rule name so it better describes the new rule, for example to **PTZ Camera Nighttime Patrolling**.
 - On the time conditions selection step, select that the rule should apply not within but **outside** the time profile:



- In the rule description, click the link in the sentence **Start patrolling on ...**, and select a patrolling profile matching your nighttime requirements rather than your daytime requirements:



2. Click **Finish**.

Pause PTZ Patrolling and Go to PTZ Preset on Input

In this example, we assume that patrolling has already been set up for the PTZ camera, and that the external input unit is a door sensor connected to an input port on a device on the XProtect Corporate system: When the door sensor is activated, the PTZ camera will pause patrolling, move to a preset position covering the door area, remain at the preset position for 15 seconds, then resume patrolling.

Prerequisites

This rule is based on an input being activated, and on a patrolling PTZ camera moving to a specific preset position. Therefore, an external input unit must be available, i.e. connected to the input port of a device on the



XProtect Corporate system. Furthermore, the preset position to which the PTZ camera should move when the rule is applied must have been defined. Before creating a rule like this, always verify the following:

- An external input unit is successfully connected to an input port on a device, and the states of the input unit (activated/deactivated) work as required.
- The camera in question is a PTZ camera with the required preset positions and patrolling defined.

How to define preset positions and patrolling profiles...

When a PTZ camera patrols according to a patrolling profile, it moves between a number of preset positions. Thus, before you are able to define patrolling profiles for a PTZ camera, the preset positions required for the patrolling profiles must be defined.

To define preset positions for a PTZ camera, expand **Devices** in the Management Client's Site Navigation pane (see "Panels overview" on page 70) and select **Cameras**. This will display a list of cameras in the overview pane (see "Panels overview" on page 70). Select the required PTZ camera from the list, and select the Presets tab in the properties pane (see "Panels overview" on page 70). For details of how to define preset positions on the **Presets** tab, see Preset Positions (see "PTZ Presets tab (camera properties)" on page 140).

Once you have defined the required preset positions, patrolling profiles for the PTZ camera are defined on the neighboring **Patrolling** tab. For details of how to define patrolling profiles on the **Patrolling** tab, see Patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 136).

Creating the Rule

1. In the Management Client's Site Navigation pane, expand **Rules and Events**, then right-click Rules and select **Add New Rule...**:

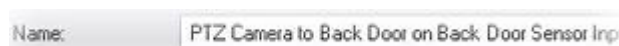


Tip: Instead of right-clicking to select **Add New Rule**, you can press CTRL+N on your keyboard.

2. The **Manage Rule** wizard opens. Type a name for the new rule in the **Rule name** field.



In this example... the rule will cover a specific camera (simply called **PTZ Camera**) and how it should behave upon an activated input. We therefore overwrite the default rule name (e.g. **New Rule 001**) with a descriptive name:



Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of **Manage Rule**, select the required rule type.



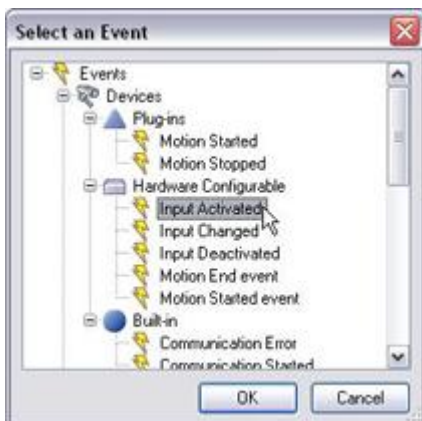
➔ **In this example...** we want to base the rule on an event. Therefore, we select **Perform an action on** on **<event>**. Our selection is immediately reflected in the initial rule description in the lower half of the wizard window:



Click the underlined items in the rule description in order to specify its exact content:

Event link: Clicking the **event** link lets you select the event which must occur in order for the rule to apply. In order for you to get a good overview, selectable events are listed in groups according to whether they are related to plug-ins, dependent on hardware configuration, built into XProtect Corporate itself, etc.

➔ **In this example...** we want the event to be activated input. Input comes from— and is configured on— separate hardware rather than on XProtect Corporate itself, so we go to the **Hardware Configurable** group, select the event **Input Activated**, and click **OK**:



Devices/recording server/management server link: When you have selected the required event, clicking the **devices/recording server/management server** link opens the **Select Devices and Groups** window, which lets you specify the devices on which the event should occur in order for the rule to apply.

➔ **In this example...** the event should occur on an input called **Back Door Sensor** in order for the rule to apply. In the **Select Devices and Groups** window we therefore drag the input **Back Door Sensor** to the **Selected** list and click **OK**. By doing this we have specified the exact content of the first part of the wizard's rule description, which now looks like this:



Click **Next** to move to step 2 of the wizard.

4. On step 2 of the wizard, specify which time conditions should be met in order for the rule to apply.

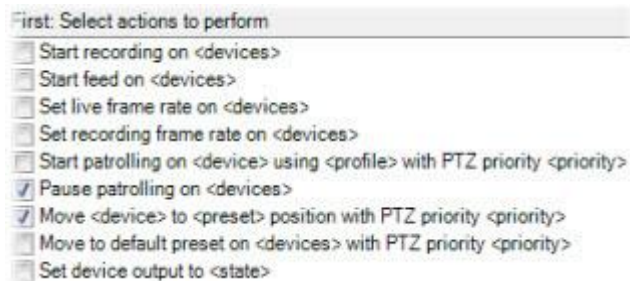
➔ **In this example...** we simply want the rule to apply whenever input is activated on the back door sensor, regardless of time. When creating event-based rules it is possible to bypass the time conditions; we therefore want to skip the wizard's step 2 entirely.

Click **Next** to move to step 3 of the wizard.

5. On step 3 of the wizard, first specify which actions to perform.

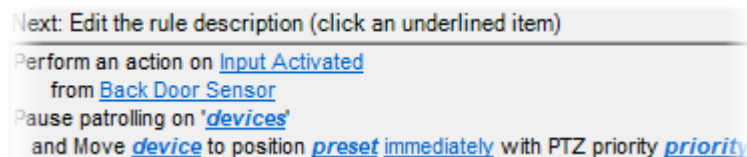


➔ **In this example...**we want two things to happen: patrolling should pause, and the PTZ camera should move to a specific preset position with a specific priority (see "Actions and Stop Actions Overview" on page 188). We therefore select the actions **Pause patrolling on <devices>** and **Move <device> to <preset> position with PTZ priority <priority>**.



Based on the selection of actions, the wizard automatically extends the rule description in the lower part of the wizard window.

➔ **In this example...**Based on our selections **Pause patrolling on <devices>** and **Move <device> to <preset> position with PTZ priority <priority>** the wizard automatically suggests an extension to the existing rule description:



- Click the underlined items in the extension of the rule description in order to specify its exact content:

devices: Clicking the **devices** link lets you select the devices on which patrolling should be paused. Only PTZ cameras will be selectable.

➔ **In this example...**patrolling should be paused on our PTZ camera. In the **Select Group Members** window we therefore drag **PTZ Camera to the Selected** list and click **OK**.

device: Clicking the **device** link lets you select to move another device than the device(s) on which patrolling was paused. You are also able to select to move the device on which patrolling was paused.

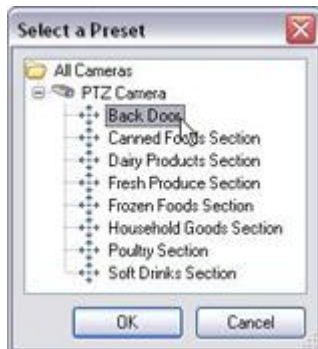
➔ **In this example...**we select to move the same PTZ camera on which patrolling was paused, and click **OK**:



preset: Clicking the **preset** link lets you select which preset position the PTZ camera should move to. You will be able to select from a list of preset positions defined for the PTZ camera you selected before.



➔ In this example...we select a preset position called **Back Door**, and click **OK**:



immediately: The wizard automatically suggests that the camera moves to the preset position **immediately** after it has paused patrolling. Clicking the immediately link lets you specify a delay, if required.

priority: Clicking the **priority** link lets you specify the priority (see "Actions and Stop Actions Overview" on page 188) of the camera position.

➔ In this example...the wizard's suggestion **immediately** suits us fine, so we simply leave it as it is.

The rule description now indicates which camera will pause patrolling, which preset position it will move to, and how soon:

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

Perform an action on Input Activated
 from Back Door Sensor
 Pause patrolling on 'PTZ Camera'
 and Move PTZ Camera to position PTZ Camera: Back Door immediately with PTZ priority 5000

Click **Next** to move to step 4 of the wizard.

7. On step 4 of the wizard, select stop criteria.

Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.

➔ In this example...Without a stop criterion, the rule in this example would make the camera pause patrolling, then move to the preset position and remain there indefinitely. Based on the elements in our rule description, we therefore **must** select a stop criterion.

Since our rule is triggered by an event, the wizard automatically suggests that we base our stop action on an event as well. In the rule description, the wizard even suggests that the stop action is performed when input is deactivated on the back door sensor. However, we want something different, so we select **Perform stop action after <time>**:





In the rule description, the wizard now prompts us to specify the required time:

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

Perform an action on Input Activated
from Back Door Sensor

Pause patrolling on 'PTZ Camera'
and Move PTZ Camera to position PTZ Camera: Back Door immediately with PTZ priority 5000

Perform action time

We click the **time** link, specify 15 seconds, and click **OK**:

Relative Time

Select time [secs.]:

15

OK Cancel

The rule description now indicates the 15 seconds selected.

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

Perform an action on Input Activated
from Back Door Sensor

Pause patrolling on 'PTZ Camera'
and Move PTZ Camera to position PTZ Camera: Back Door immediately with PTZ priority 5000

Perform action 15 seconds after

Based on the start action **pause patrolling** in our rule description, the wizard automatically suggests the stop action **resume patrolling**. It furthermore suggests that patrolling is resumed immediately after the 15 second pause:

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

Perform an action on Input Activated
from Back Door Sensor

Pause patrolling on 'PTZ Camera'
and Move PTZ Camera to position PTZ Camera: Back Door immediately with PTZ priority 5000

Perform action 15 seconds after
Resume patrolling immediately

This is exactly what we want; we do not need to change it, although by clicking the **immediately** link we could have specified a delay of e.g. 3 seconds.

Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met. If you do not want the rule to be active straight away, clear the **Active** check box in the top part of the **Manage Rule** window:

Name: PTZ Camera

Description:

Active: ☒

Tip: You can always activate/deactivate the rule later.



8. Click **Finish**. This will add your new rule to the list of rules:



Default Rules

XProtect Corporate comes with a number of default rules, ensuring that basic features work without any user intervention being required.

IMPORTANT: Like other rules, default rules can be deactivated and/or modified as required. The fact that default rules are present does therefore not in itself guarantee that your XProtect Corporate system will work. Nor does it guarantee that video feeds or audio feeds will automatically be fed to the XProtect Corporate system, as the default rules may subsequently have been deactivated or modified.

Default Goto Preset when PTZ Is Done rule

Ensures that PTZ (Pan/Tilt/zoom) cameras will go to their respective default preset positions after they have been operated manually.

IMPORTANT: This rule is by default not enabled. Even when the rule is enabled, you must have defined default preset positions for the required PTZ cameras in order for the rule to work; you do this on the **Presets** tab (see "PTZ Presets tab (camera properties)" on page 140).

In case you accidentally delete the default goto preset when PTZ is done rule, you can recreate it with the following content:

```
Perform an action on PTZ Manual Session Stopped from All Cameras
Move immediately to default preset on the device on which event occurred
```

Default Record on Bookmark rule

Ensures that video will be recorded automatically when a bookmark is set by an operator in the XProtect Smart Client. This is provided recording is enabled (see "Record Tab Overview" on page 170) for the cameras in question (recording is by default enabled).

IMPORTANT: The default recording time for this rule is three seconds before the bookmark is set and 30 seconds after the bookmark is set. However, these default recording times can be edited in the rule.

In case you accidentally delete the default record on bookmark rule, you can recreate it with the following content:

```
Perform an action on Bookmark Reference Requested from All Cameras, All
Microphones, All Speakers start recording 3 seconds before on the device on
which event occurred
Perform action 30 seconds after stop recording immediately
```

Default Record on Motion rule

Ensures that as long as motion is detected in video from cameras, the video will be recorded, provided recording is enabled (see "Record Tab Overview" on page 170) for the cameras in question (recording is by default enabled).



IMPORTANT: While the default rule specifies recording based on detected motion, it does not guarantee that video will be recorded, as individual cameras' recording may have been disabled for one or more cameras. Even when recording is enabled, bear in mind that the quality of recordings may be affected by individual camera's recording settings.

In case you accidentally delete the default record on motion rule, you can recreate it with the following content:

```
Perform an action on Motion Started from All Cameras start recording 3
seconds before on the device on which event occurred

Perform stop action on Motion Stopped from All Cameras stop recording 3
seconds after
```

Default Record on Request rule

Ensures that video will be recorded automatically when an **external** request occurs, provided recording is enabled (see "Record Tab Overview" on page 170) for the cameras in question (recording is by default enabled).

IMPORTANT: The request is always triggered by a system integrating externally with XProtect Corporate, and the rule is primarily used by integrators of external systems or plug-ins.

In case you accidentally delete the default record on bookmark rule, you can recreate it with the following content:

```
Perform an action on Request Start Recording from External start recording
immediately on the devices from metadata

Perform stop action on Request Stop Recording from External stop recording
immediately
```

Default Start Audio Feed rule

Ensures that audio feeds from all connected microphones and speakers are automatically fed to the XProtect Corporate system.

IMPORTANT: While the default rule enables access to connected microphones' and speakers' audio feeds immediately upon installing the system, it does not guarantee that audio will be recorded (see "Record Tab Overview" on page 170), as recording settings must be specified separately.

In case you accidentally delete the default start audio feed rule, you can recreate it with the following content:

```
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
```

Default Start Feed rule

Ensures that video feeds from all connected cameras are automatically fed to the XProtect Corporate system.

IMPORTANT: While the default rule enables access to connected cameras' video feeds immediately upon installing the system, it does not guarantee that video will be recorded, as cameras' recording settings must be specified separately.

In case you accidentally delete the default start feed rule, you can recreate it with the following content:

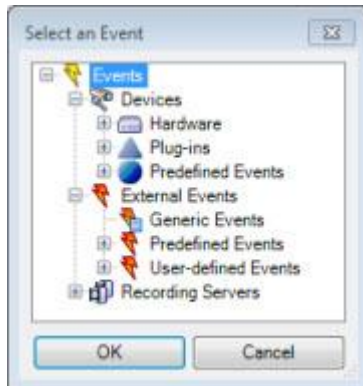
```
Perform an action in a time interval always start feed on All Cameras

Perform an action when time interval ends stop feed immediately
```



Events Overview

When creating an event-based rule in the **Manage Rule** wizard (see Manage Rules (on page 221)), you are able to select between a number of different events.



Select an Event dialog from the wizard **Manage rule**.

In order for you to get a good overview, selectable events are listed in groups according to whether they are:

Devices

Dependent on hardware configuration

Event	Description
 Events Dependent on Hardware Configuration The configuration on which these events depend may only be possible on some hardware. For example, only selected cameras may be able to detect tampering or temperature changes.	
Audio Falling	Occurs when the audio signal on an audio-enabled device is falling. For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the device in question. This type of event requires that at least one device on your system has an audio unit connected. The event will not work until configured on the hardware itself.
Audio Passing	Occurs when the state of an audio-enabled device is changed, regardless of which state the device is changed to. This type of event requires that at least one device on your system has an audio unit connected. The event will not work until configured on the hardware itself.
Audio Rising	Occurs when the audio signal on an audio-enabled device is rising. For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the device in question. This type of event requires that at least one device on your system has an audio unit connected. The event will not work until configured on the hardware itself.
Images Received	Occurs when pre-alarm images are received from a camera (using the Include Images option in Send notification to <profile> action (see "Actions and Stop Actions Overview" on page 188)). Pre-alarm images are available for selected cameras only; such cameras are capable of sending of one or more single still images from immediately before an event took place to the surveillance system via SMTP e-mail. This type of event requires that at least one camera on your system supports pre-alarm



Event	Description
	images. The event will not work until configured on the hardware itself. IMPORTANT: Pre-alarm images functionality cannot coexist with edge recording (see "Record Tab Overview" on page 170). So if a camera is setup to export pre-alarm images it is not possible to enable edge recording on that camera, and vice versa. Tip: Consider using prebuffering, defined on the Record tab, as an alternative to pre-alarm images.
Input Activated	Occurs when an external input unit connected to an input port on a device is activated. This type of event requires that at least one device on your system has an external input unit connected to an input port. The event will not work until configured on the hardware itself.
Input Changed	Occurs when the state of an external input unit connected to an input port on a device is changed, regardless of which state the external input unit is changed to. This type of event requires that at least one device on your system has an external input unit connected to an input port. The event will not work until configured on the hardware itself.
Input Deactivated	Occurs when an external input unit connected to an input port on a device is deactivated. This type of event requires that at least one device on your system has an external input unit connected to an input port. The event will not work until configured on the hardware itself.
Motion Started (HW)	Occurs when a camera detects motion in its video stream. In addition to XProtect Corporate's motion detection, some cameras are— depending on configuration of the camera hardware— themselves able to detect motion. Such camera-detected motion detection can also be used in XProtect Corporate rules. The event will not work until configured on the camera hardware itself. Exact use of camera-based motion detection depends on the configuration of the cameras in question.
Motion Stopped (HW)	Occurs when a camera no longer detects motion in its video stream. See also the description of the Motion Started event earlier. The event will not work until configured on the camera hardware itself. Exact use of camera-based motion detection depends on the configuration of the cameras in question.
Tampering	Occurs when a device detects that it is being tampered with. The event will not work until configured on the hardware itself. Exact use of tampering detection depends on the configuration of the devices in question.
Temperature	Occurs when a device detects a temperature change, that a certain temperature is exceeded, or similar. The event will not work until configured on the hardware itself. Exact use of temperature detection depends on the configuration of the devices in question.
Video Lost	Occurs when a device detects that a video signal is lost. The event will not work until configured on the hardware itself. Exact use of this type of detection depends on the configuration of the devices in question.

Related to plug-ins

Event	Description
-------	-------------



Event	Description
Events Related to Plug-ins	
Motion Started	Occurs when XProtect Corporate detects motion in video received from cameras. This type of event requires that XProtect Corporate's motion detection is enabled for the cameras to which the event will be linked. Exactly what constitutes motion depends on the motion detection settings specified for individual cameras in XProtect Corporate. In addition to XProtect Corporate's motion detection, some cameras are— depending on configuration of the camera hardware— themselves able to detect motion. Such camera-detected motion detection can also be used in XProtect Corporate rules. Such events are called Hardware Configurable, as they do not work until configured on the camera hardware itself. See Events dependent on hardware configuration (see man_rul_Events_Overview.htm#EventsDependentonHardwareConfiguration - man_rul_Events_Overview.htm#EventsDependentonHardwareConfiguration).
Motion Stopped	Occurs when motion is no longer detected in received video. See also the description of the Motion Started event.

Predefined events (related to devices)

Event	Description
Predefined Events	
Communication Error	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	Occurs when communication with a device is successfully established.
Communication Stopped	Occurs when communication with a device is successfully stopped.
Bookmark Reference Requested	Occurs when a bookmark is made in live mode in the XProtect Smart Client. Furthermore, a requirement for using the Default Record on Bookmark rule (on page 214).
Feed Overflow Started	Feed overflow (a.k.a. Media overflow) occurs when a recording server is unable to process received video as quickly as specified in the configuration and therefore is forced to discard some images. If the server is healthy, feed overflow usually happens because of slow disk writes. It can be resolved 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. This will in general 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. Tip: This rare event can be used for triggering actions that will help you avoid the problem, e.g. for lowering the recording frame rate.
Feed Overflow Stopped	Occurs when feed overflow (see description of the Feed Overflow Started event) ends.
Live Client Feed Requested	Occurs when a user of the XProtect Smart Client or Remote Client requests a live stream from a device. The event occurs upon the request— even if the client user's request subsequently 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.
Output Activated	Occurs when an external output unit connected to an output port on a device is activated. This type of event requires that at least one device on your system has an external input



Event	Description
	unit connected to an output port.
Output Changed	Occurs when the state of an external output unit connected to an output port on a device is changed, regardless of which state the external input unit is changed to. This type of event requires that at least one device on your system has an external input unit connected to an output port.
Output Deactivated	Occurs when an external output unit connected to an output port on a device is deactivated. This type of event requires that at least one device on your system has an external input unit connected to an output port.
Live Client Feed Terminated	Occurs when a user of the XProtect Smart Client or Remote Client no longer requests a live stream from a device.
Manual PTZ 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 will be linked are PTZ (Pan/Tilt/Zoom) cameras.
Manual PTZ 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 will be linked are PTZ (Pan/Tilt/Zoom) cameras.
Recording Started	Occurs when recording is started.
Recording Stopped	Occurs when recording is 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

Generic

Event	Description
 Generic Events	
Generic events allow you to trigger actions in the XProtect event server by sending simple strings via the IP network to XProtect Corporate.	
The aim of generic events (see "Manage Generic Events" on page 242) is to allow as many external sources as possible to interact with XProtect Corporate.	

Predefined events (related to external events)

Event	Description
 Predefined Events	
Request Start Recording and Request Stop Recording . Activated when start or stop recordings are requested via the MIP SDK.	



Event	Description
Through the Milestone Integration Software Development Kit (MIP SDK) a third party vendor can develop custom plug-ins (for example, integration to external Access Control Systems or similar) to XProtect Corporate.	

User-defined events

Event	Description
 User-defined Events	
A number of events custom made to suit your system may also be selectable. Such user-defined events can be used for:	
• Making it possible for end users to manually trigger events while viewing live video in the XProtect Smart Client. • Countless other purposes. For example, you may create user-defined events which will occur if a particular type of data is received from a device.	
For information about how to define user-defined events in the Management Client, see Managing User-defined Events (see "Manage User-defined Events" on page 238).	

Related to recording servers

Event	Description
 Events Related to Recording Servers	
Archive Available	Occurs when an archive (see "About Storage and Archiving" on page 101) for a recording server becomes available after having been unavailable (see Archive Unavailable next).
Archive Unavailable	Occurs when an archive (see "About Storage and Archiving" on page 101) for a recording server becomes unavailable, for example if the connection to an archive located on a network drive is lost. When this is the case, it will not be possible to archive recordings. You can use the event to, for example, trigger a notification profile so an e-mail notification is automatically sent to relevant people in your organization.
Archive Not Finished	Occurs when an archive (see "About Storage and Archiving" on page 101) for a recording server is not finished with the last archiving round when the next is scheduled to start.
Database Disk Full	Occurs when a database disk is full. A database disk is considered to be full when there is less than 500 MB of space is left on the disk: In order to prevent operating system failures due to insufficient disk space, the oldest records in the database will automatically be deleted for all cameras recording on the disk in question when less than 500 MB of space is left on the disk containing the database, regardless of any time or size limits specified for the database. This will help ensure that at least 500 MB of disk space will be available for operating system use.
Database Full - Auto Archive	Occurs when an archive (see "About Storage and Archiving" on page 101) for a recording server is full and needs to auto-archive to an archive in the hierarchy.
Database Repair	Occurs if a database becomes corrupted, in which case XProtect Corporate will automatically attempt two different database repair methods: a fast repair and a thorough repair.
Database Storage Area Available	Occurs when a storage area (see "About Storage and Archiving" on page 101) for a recording server becomes available after having been unavailable (see Database Storage Area Unavailable next). You can, for example, use the event to start recording if it has been stopped by a Database



Event	Description
	Storage Area Unavailable event (see next).
Database Storage Area Unavailable	Occurs when a storage area (see "About Storage and Archiving" on page 101) for a recording server becomes unavailable, for example if the connection to a storage area located on a network drive is lost. When this is the case, it will not be possible to store recordings. You can use the event to, for example, stop recording and trigger a notification profile (see "Manage Notification Profiles" on page 233) so an e-mail notification is automatically sent to relevant people in your organization.
Failover Started	Occurs when a failover server (see "Manage Failover Servers" on page 321) takes over from a recording server. A failover server is a spare recording server which can take over if a regular recording server becomes unavailable.
Failover Stopped	Occurs when a recording server becomes available again, and is able to take over from a failover server (see "Manage Failover Servers" on page 321).

Manage Rules

Rules are a central element in XProtect Corporate. The behavior of an XProtect Corporate surveillance system is to a very large extent determined by rules. Rules determine highly important settings, such as when cameras should record, when PTZ (Pan/Tilt/Zoom) 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

You create and manage rules in the Management Client.

1. In the Management Client's **Navigation** pane, expand the **Rules and Events** folder, then select **Rules**. In the overview pane (see "Panels overview" on page 70), a **Rules** list, providing an overview of all existing rules in your system, will appear.
2. In needed, create, edit, copy and/or validate rules from the list, see below. See also Create Typical Rules (on page 194) for a complete step-by-step guide to creating often required rules or see Default Rules (on page 214) to learn about the rules already default in XProtect Corporate.

What You Can Do with Rules

In short, rules specify actions which should be carried 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 (see "Manage XProtect Matrix Recipients" on page 185) (Matrix is an integrated system for viewing of video from any camera on any monitor on a network operating with XProtect Corporate)
- Start and stop plug-ins
- Start and stop feeds from devices

How is stopping the feed from a device different from manually disabling the device? Stopping a device means that video will no longer be transferred from the device to XProtect Corporate, in which case neither live viewing nor recording will be possible. However, a device on which the feed has been stopped will still be able to communicate with the recording server, and the feed from device can be started 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 devices in question. For example, a rule specifying that a camera should record will not work as intended if recording is not enabled for the camera in question. Before creating a rule it is therefore highly recommended that you verify that the devices involved will be able to perform as intended. For a number of typically required rules, such prerequisites are described in Create Typical Rules (on page 194).

How a Rule Is Triggered

Rules can be triggered by two types of conditions:

- **Events:** When events occur on the surveillance system (for example when motion is detected, when the system receives input from external sensors, etc.)
- **Time:** When specific periods of time are entered (for example **Thursday 16th August 2007 from 07.00 to 07.59**, or **every Saturday and Sunday**)

What You Can Cover in a Rule

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, however, provide a high degree of flexibility: You are able to combine event and time conditions, you are able to specify several actions in a single rule, and very often you are able to 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  **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.**

And you can create very simple event-based rules, involving events on one device only:



Example ➔ **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.**

However, even though 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.

Example ➔ **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).**

You can of course also combine events and scheduled times in a rule:

Example ➔ **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).**

The required complexity of rules will vary from organization to organization: Some may require only a number of simple rules; some may require a mix of simple and complex rules.

Create Many Simple or a Few Complex Rules?

Depending on your organization's requirements, it is often a good idea to create many simple rules rather than a few complex rules.

Even though this will lead to you having more rules, it will generally make it much easier for you to maintain an overview of what your rules do.

Keeping your rules simple also means that you will have much more flexibility when it comes to deactivating/activating individual rule elements— with simple rules, you can deactivate/activate entire rules when required.

Default Rules

XProtect Corporate comes with a number of default rules, ensuring that basic features work without any user intervention being required. See Default Rules (on page 214).

Creating a New Rule

When you create rules, you will be guided by the wizard **Manage Rule** which provides a highly intuitive approach. It helps you stay focused by listing only relevant options. It ensures that a rule will not contain missing elements. And finally, based on your rule's content, it automatically suggests suitable stop actions (i.e. what should take place when the rule no longer applies), ensuring that you will not unintentionally create a never-ending rule.

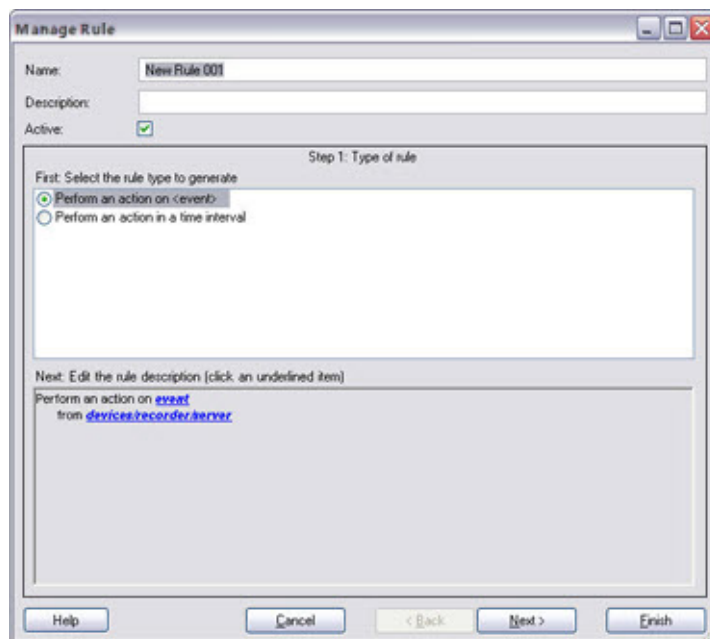


1. In the Overview pane (see "Panels overview" on page 70), right-click the **Rules** item, and select **Add Rule...**:



Tip: Instead of right-clicking to select **Add Rule**, you can press CTRL+N on your keyboard.

This will open the wizard **Manage Rule**:



The wizard will guide you through the process of specifying the content of your rule. The wizard makes the process interactive, yet intuitive: based on your main selections, it will ask you to specify your exact requirements for the rule.

2. Begin by specifying a name (compulsory) and a description (optional) of the new rule in the **Name** and **Description** fields respectively.

Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. Then select the required 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 a specific period of time is entered:

Perform an action on <event>

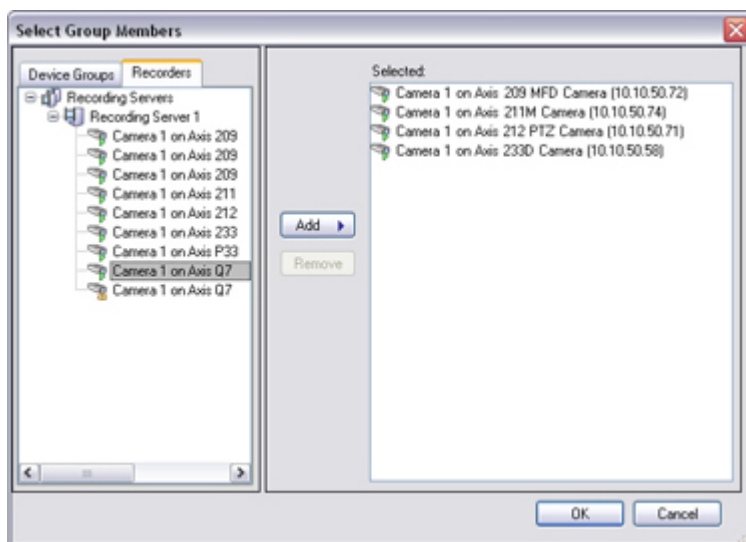


If you select an event-based rule, the lower part of the wizard window will display an initial rule description:



Click the underlined items in the rule description in order to specify its exact content:

- **Event:** Clicking the **event** link lets you select the event which must occur in order for the rule to apply (for example **Motion Started**).
- **Devices/recording server/management server:** When you have selected the required event, clicking the **devices/recording server/management server** link lets you specify the devices on which the event should occur in order for the rule to apply. Depending on your event specification, you may be able to select from a list of cameras, inputs, outputs, etc. In this example illustration, the selectable devices are all cameras:



You specify the required devices by moving them from the **Available devices** list to the **Selected devices** list.

To move a device from the **Available devices** list to the **Selected devices** list, either select the device and click the **Add** button, double-click the device, or simply drag the device from one list to the other.

Tip: When devices are grouped into so-called device groups, you can quickly move all devices in a group simply by moving the group folder.

When the required devices are listed in the **Selected devices** list, click **OK**.

You have now specified the exact content of the first part of the rule description:



Example only; your selections may be different

Perform an action in a time interval

If you select a time-based rule, no more information is required on the wizard's first step.



- Click **Next** to go to the wizard's second step. On the wizard's second step you are able to define further conditions for the rule.
- 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, the lower part of the wizard window lets you edit the rule description:

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 would let you select one or more days of the week on which the rule should apply.

- Having specified your exact conditions, click **Next** to move to the next step of the wizard and select which actions should be covered by the rule.

Depending on the content and complexity of your rule, further wizard steps may let you define further information, 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.

- Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met.

If you do not want the rule to be active straight away, clear the **Active** check box:

Name: My Third Rule

Description: Make ... rights are

Active: ☒

Tip: You can always activate/deactivate the rule later.

- Click **Finish**.

To view step-by-step descriptions of how to create typically required rules, see Create Typical Rules (on page 194).

Editing, Copying and Renaming a Rule

- In the Overview pane (see "Panels overview" on page 70), right-click the required rule.
- Select either:

Edit Rule...

or

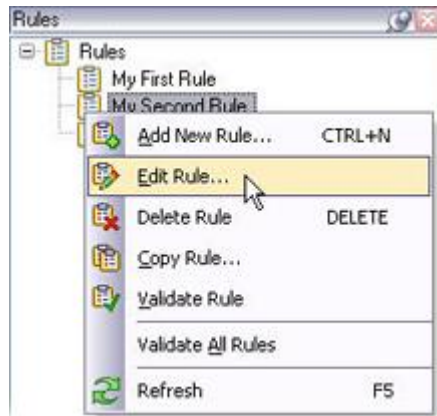
Copy Rule...



or

Rename Rule...

depending on your needs.



Example when selecting **Edit Rule...**

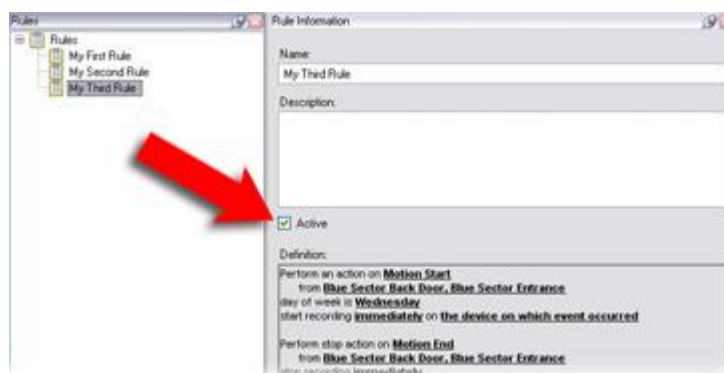
The wizard **Manage Rule** opens.

3. In the wizard, rename and/or change the rule as required. If you selected **Copy Rule...**, the wizard opens, displaying a copy of the selected rule.
4. Click **Finish**.

Deleting a Rule

Tip: You do not necessarily have to delete an unwanted rule; you may also just temporarily deactivate the rule by clearing the **Active** check box in the **Rule Information** pane for the rule in question, then saving the setting by selecting the Management Client's **File** menu.

Show me where to find the **Active** check box



If you wish to delete an existing rule, do the following:

1. In the Overview pane (see "Panels overview" on page 70), right-click the rule you wish to delete, and select **Delete Rule...**

Tip: Instead of right-clicking to select **Delete Rule**, you may simply press the DELETE key on your keyboard.



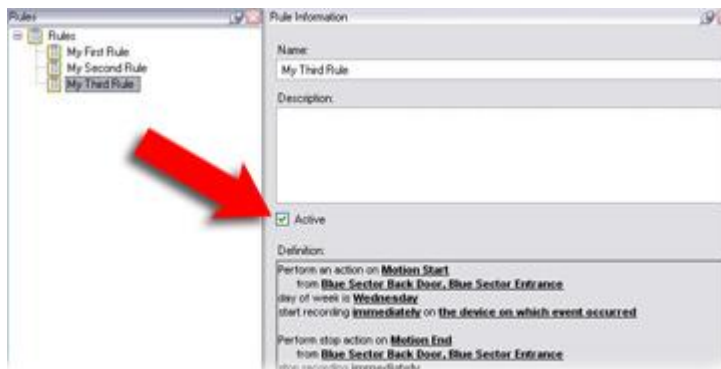
2. You will be asked to confirm that you wish to delete the rule. If you are sure that you wish to delete the rule, click **Yes**.
3. The rule will be removed from the Overview pane's **Rules** list.

Deactivating and Activating a Rule

A rule is by default active, meaning that XProtect Corporate will apply the rule as soon as the rule's conditions apply. If you do not want a rule to be active, you can deactivate the rule. When the rule is deactivated, XProtect Corporate will not apply the rule, even if the rule's conditions apply. A deactivated rule can easily be activated later.

Deactivating a Rule:

1. In the Overview pane (see "Panels overview" on page 70), select the required rule.
2. Clear the **Active** check box in the Properties pane (see "Panels overview" on page 70):



3. Save the setting by clicking **Save** in the Management Client's toolbar (see "Management Client Overview" on page 66).
4. The deactivated rule will be indicated by a different icon in the **Rules** list:



Example: Different icon indicates that third rule is deactivated

Activating a Rule

When you want to activate the rule again, simply select the required rule, select the **Activate** check box, and save the setting.

Validating Rule(s)

You are able to validate the content of an individual rule or all rules in one go.

Why would I need to validate the content of rules? When you create a rule, the **Manage Rule** ensures that all of the rule's elements make sense. However, 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 will not work if the time profile in question has subsequently been



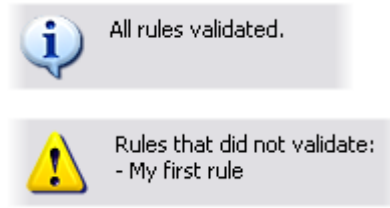
deleted. Such unintended effects of configuration may be hard to keep an overview of; rule validation helps you keep track of which rules have been affected.

IMPORTANT: Validation takes place on a per-rule basis; each rule is validated in isolation. It is currently not possible to validate rules against each other (for example in order to see whether one rule conflicts with another rule), not even if using the **Validate All Rules** feature.

Furthermore, it is not possible to 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 will validate OK if the elements in the rule itself are correct, even though motion detection (which is enabled on a camera level, not through rules) has not been enabled for the camera in question.

To validate an individual rule or all rules in one go, do the following in the Management Client:

1. In the Overview pane, right-click the rule you wish to validate, and select **Validate Rule** or **Validate All Rules** (depending on your needs):
2. A simple dialog will inform 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 will list the names of the affected rules:



Manage Time Profiles

Time profiles are periods of time defined by the administrator. Time profiles can be used when creating rules (see "Manage Rules" on page 221), for example, a rule specifying that a certain action should take place within a certain time period. An alternative to Time profiles are Day Length Time profiles (see "Manage Day Length Time Profiles" on page 232).

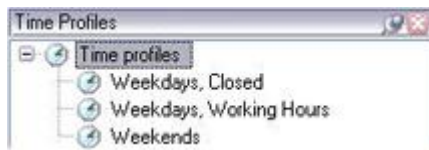
Time profiles are also assigned to roles (see "Manage Roles" on page 251), along with Smart Client profiles (see "Manage Smart Client Profiles" on page 182). Per default, all roles are assigned the default time profile **Always**. This means that members of roles with this default time profile attached has no time-based limits to their user rights in the XProtect Corporate system. An alternative time profile can easily be assigned to a role, see Adding a Role and Manage its Smart Client and Time Profiles. (see "More About Administrators role" on page 251) See also Working with Smart Client Profiles, Roles and Time Profiles section (see "Working with Smart Client Profiles, Roles and Time Profiles" on page 183), to learn more about their relationship.

Time profiles are highly flexible: they can be based 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 will 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 (e.g. recording on cameras) associated with time profiles will be carried out in each recording server's local time. Example: If you have a time profile covering the period 08.30 to 09.30, any associated actions on a recording server placed in New York will be 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 will be carried out some hours later, when the local time is 08.30 to 09.30 in Los Angeles.



You create and manage time profiles in the Management Client by expanding the Site Navigation pane (see "Panels overview" on page 70)'s **Rules and Events** folder, then selecting **Time Profiles**. A **Time Profiles** list will appear in the overview pane:



Example only

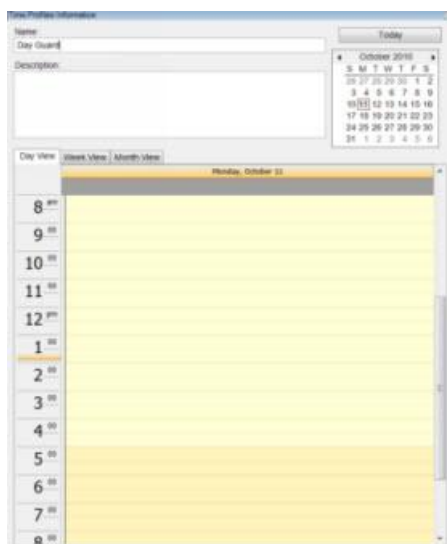
Specifying a Time Profile

1. In the **Time Profiles** list, right-click **Time Profiles**, and select **Add Time Profile...**:



Tip: Instead of right-clicking to select **Add Time Profile...**, you can press CTRL+N on your keyboard.

This will open the **Time Profile** window:



Time and date format may be different on your system

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...**

Tip: If you select a time period by dragging in the calendar before right-clicking, the selected period will automatically be used in the dialog that appears when you select **Add Single Time...** or **Add Recurring Time...**



Specifying a Single Time

When you select **Add Single Time...**, the **Select Time** window appears:

The **Select Time** dialog box contains the following fields and controls:

- Start time:** A date and time selector showing **Mon 9/5/2010** and **1:30 PM**.
- End time:** A date and time selector showing **Mon 9/5/2010** and **3:00 PM**.
- All day event:** An unchecked checkbox.
- Buttons:** **OK** and **Cancel** buttons at the bottom.

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**.

Tip: A time profile is able to contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.

Specifying a Recurring Time

When you select **Add Recurring Time...**, the **Select Recurring Time** window appears:

The **Select Recurring Time** dialog box contains the following fields and controls:

- Time range:** Start: **1:30 PM**, End: **3:00 PM**, Duration: **1.5 hours**.
- Recurrence pattern:** Radio buttons for **Daily**, **Weekly** (selected), **Monthly**, and **Yearly**. Below, "Recur every **1** week(s) on:" with checkboxes for **Sunday**, **Monday** (checked), **Tuesday**, **Wednesday**, **Thursday**, **Friday**, and **Saturday**.
- Range of recurrence:** Start: **Mon 9/5/2005**. Radio buttons for **No end date** (selected), **End after:** **10** occurrences, and **End by:** **Mon 11/7/2005**.
- Buttons:** **OK** and **Cancel** buttons at the bottom.

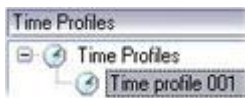
Time and date format may be different on your system

1. In the **Select Time** window, specify time range, recurrence pattern and range of recurrence.
2. Click **OK**.

Tip: A time profile is able to contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.



1. When you have specified the required time periods for your time profile, click **OK** in the **Time Profile** window. Your new time profile is added to the **Time Profiles** list in the Overview pane (see "Panels overview" on page 70):

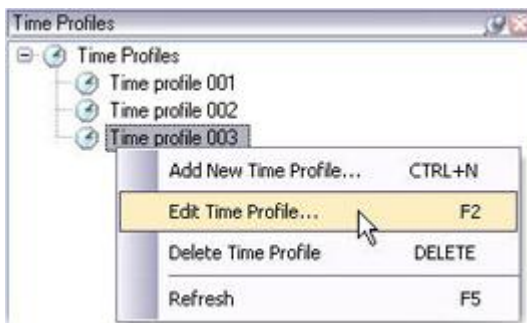


New time profile appearing in **Time Profiles** list

If at a later stage you wish to edit or delete the time profile, you can do that from the **Time Profiles** list.

Editing a Time Profile

1. In the Overview pane (see "Panels overview" on page 70)'s **Time Profiles** list, right-click the required time profile, and select **Edit Time Profile...**:



Tip: Instead of right-clicking to select **Edit Time Profile**, you can select the required time profile and press F2 on your keyboard.

This will open the **Time Profile** window.

2. In the **Time Profile** window, edit the time profile as required.

When you have made the required changes to the time profile, click **OK** in the **Time Profile** window. You will be returned to the Overview pane's **Time Profiles** list.



You browse months by clicking the small back/forward buttons.

Tip: In the **Time Profile Information** window, edit the time profile as required. Remember that a time profile may contain more than one time period, and that time periods may be recurring.

Tip: The small month overview in the top right corner of the **Time Profile Information** window 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 time periods have been specified on several days, and that a recurring time may have been specified on Mondays.

Manage Day Length Time Profiles

When cameras are placed outside, it is often required to lower the cameras resolution, enable black/white, or change other settings when it gets dark or vice versa 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 (see "Manage Time Profiles" on page 229) to adjust camera settings according to light conditions.

To overcome this, Day Length Time profiles can be created and defined in XProtect Corporate according to the sunrise and sunset in a specified geographical area. Via GPS coordinates, the system, on a daily basis, calculates the sunrise and sunset time, even incorporating daylight saving time. As a result, it 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.

In addition, it is possible to 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.

Day Length Time profiles can be used when creating both rules (see "Manage Rules" on page 221) and roles (see "About Roles" on page 249).

Creating a Day Length Time Profile

1. In the Management Client, expanding the Site Navigation pane (see "Panels overview" on page 70)'s **Rules and Events** folder, select **Time Profiles**.
2. In the overview pane, 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. In order to deal with transition periods between lightness and darkness, it is possible to offset activation and deactivation of the profile.

Furthermore, time and month names are shown in the language dictated by your computer's language/regional settings.

4. To see the location of the entered GPS coordinates in a map, click **Show Position in Browser...** (will open a browser).
5. Click **OK**.

Day Length Time Profile Properties

- **Name:** Name of the profile.
- **Description** (optional): Description of the profile.
- **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).

Manage Notification Profiles

With notification profiles you can set up ready-made e-mail notifications, which can automatically be triggered by a rule (see "Manage Rules" on page 221), for example when a particular event occurs. You are even able to include still images and AVI video clips in the e-mail notifications.

Note that when using the SMTP Service with .NET 4.0, it is not possible to send attachments over 3 MB. However two hotfixes (must be installed on the management server in the listed order) from Microsoft can be found at: <http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226> (see



<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226> -
<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226>)
<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723> (see
<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723> -
<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723>)

TLS (Transport Layer Security) and its predecessor SSL (Secure Socket Layer) is not supported; if the sender belongs on a server that requires TLS or SSL, e-mail notifications will not work properly. Also, you may be required to disable any e-mail scanners that could prevent the application sending the e-mail notifications.

Prerequisites

Before you can create notification profiles, you must specify settings for the outgoing SMTP mail server you are going to use for the e-mail notifications.

Optionally, if you want the notification profile's e-mail notifications to be able to contain AVI video clips, the compression settings for use when generating the AVI files must also be specified.

1. Go to the Management Client's menu bar, and select **Tools > Options...** This will open the **Options** window.
 - For **outgoing SMTP Mail Server**: Specify settings for the outgoing SMTP mail server on the **Mail Server** tab. For more information, see Outgoing SMTP Mail Server Settings (on page 291).
 - For **AVI Compression**: Specify compression settings the **AVI Generation** tab. For more information, see AVI Compression Settings (on page 290).

Adding New Notification Profiles

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, right-click **Notification Profiles**, and select **Add Notification Profile...** This will open the **Add Notification Profile** wizard.
2. On the wizard's first step, specify name and description.
Click **Next**.
3. On the wizard's second step, verify that **Email** is selected, click **Next**.



- On the wizard's third step, specify recipient, subject, message text and time between e-mails:

- If you want send a test e-mail notification to the specified recipients, click **Test E-mail**.
- If you want to include pre-alarm still images in e-mail notifications under the notification profile, select **Include images**, and specify number of images, time between images and whether images should be embedded in e-mail or not.
- If you want to include AVI video clips in e-mail notifications under the notification profile, select **Include images**, and specify time before and after event and frame rate.
- Click **Finish**.

IMPORTANT: Pre-alarm images functionality cannot coexist with edge recording, see Enabling and Disabling Edge Recording—Camera Only (on page 173). So if a camera is setup to export pre-alarm images it is not possible to enable edge recording on that camera, and vice versa.

Using Rules to Trigger E-mail Notifications

You use the **Manage Rule** for creating rules. The wizard takes you through all required steps. You specify the use of a notification profile during the step on which you specify the rule's actions:



When selecting the action **Send notification to <profile>**, you get the option of selecting the required notification profile. You also get the option of selecting which cameras any recordings to be included in the notification profile's e-mail 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

Bear in mind that recordings cannot be included in the notification profile's e-mail notifications unless something is actually being recorded.

If still images or AVI video clips are required in the notification profile's e-mail notifications, you should therefore verify that the rule you are creating— or another existing 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)

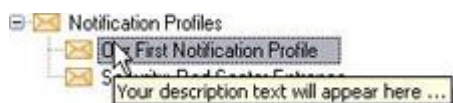
Perform an action on Input Activated
from Red Sector Door Sensor
start recording 5 seconds before on Red Sector Entrance Cam
and Send notification to 'Security: Red Sector Entrance'
images from Red Sector Entrance Cam

Perform action 10 seconds after
stop recording immediately

For more information about rules in general, see **Manage Rules** (on page 221).

Fill in Notification Profile Details

- **Name:** (Compulsory) Type a descriptive name for the notification profile. The name will later appear whenever you select the notification profile during the process of creating a rule.
- **Description:** (Optional) Type a description of the notification profile. The description will, among other places, appear 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.

If typing 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 notifications.

Tip: 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 will automatically contain this information:
 - What triggered the e-mail notification.
 - The source of any attached still images or AVI video clips
- **Time btw. e-mail:** Specify required minimum time (in seconds) to pass between the sending of each e-mail notification. Examples:

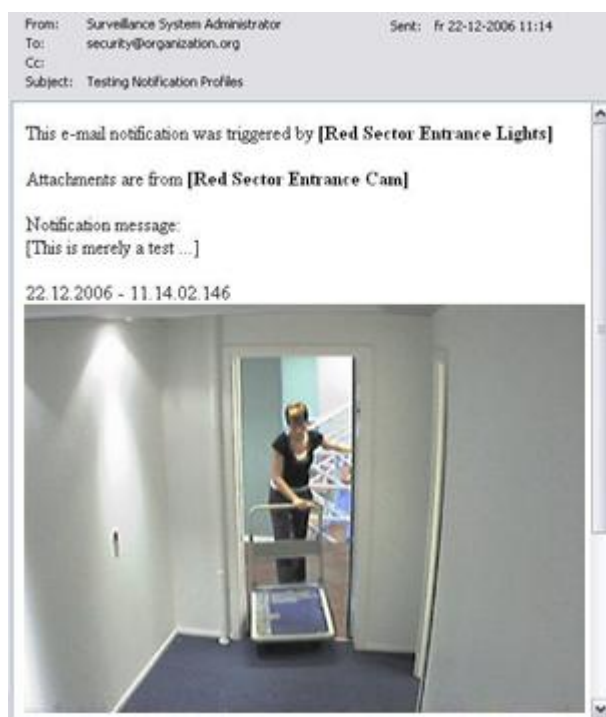


- If specifying a value of **120**, a minimum of 2 minutes will pass between the sending of each e-mail notification, even if the notification profile is triggered again by a rule before the 2 minutes have passed.

If specifying a value of **0**, e-mail notifications will be 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 btw. 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 will show recordings with half a second between them.
- **Embed images in e-mail:** If selected (default), images will be inserted in the body of e-mail notifications. If not, images will be included in e-mail notifications as attached files. **Example**

Example of e-mail notification with embedded images. Note that the size of the embedded images will depend on individual camera settings.



- **Time before event (secs.):** This setting is used to specify the start of the AVI file. By default the AVI file will contain recordings from 2 seconds before the notification profile is triggered; you are able to change this to the number of seconds you require.
- **Time after event (secs.):** This setting is used to specify the end of the AVI file. By default the AVI file will end 4 seconds after the notification profile is triggered; you are able to 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.



Manage User-defined Events

User-defined events are events which are custom made to suit your system. Like other events, user-defined events can be used in rules (see "Manage Rules" on page 221) in order to trigger actions. Thus, when a user-defined event occurs, a rule can trigger that one or more actions should take place on the XProtect Corporate system.

Example: When user-defined event 37 occurs, PTZ camera 224 should stop patrolling and go to preset position 18.

Through roles (see "Manage Roles" on page 251), you define which of your users should be able to trigger the user-defined events; see Specify Rights of a Role (on page 256) for more information.

User-defined events can be used in two ways, simultaneously if required:

- **For Providing the Ability to Manually Trigger Events in the XProtect Smart Client**

In this case, user-defined events make it possible for end users to manually trigger events while viewing live video in the XProtect Smart Client. Thus, when a user-defined event occurs because it is manually triggered by an XProtect Smart Client user, a rule can trigger that one or more actions should take place on the XProtect Corporate system.

- **For Providing the Ability to Trigger Events through API**

In this case, user-defined events can be triggered from 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 though the user-defined events can be triggered from outside the surveillance system, only authorized users will be able to do it.

Also, user-defined events can via API be associated with meta-data, defining certain devices or device groups. This is highly usable when using user-defined events to trigger rules: you avoid having a rule for each device, basically doing the same thing. Example: A company uses access control, having 35 entrances, each with an access control device. When an access control device is activated, a user-defined event is triggered in XProtect Corporate. This user-defined event is used in a rule to start recording on a camera associated with the activated access control device. It is defined in the meta-data which camera is associated with what rule. This way the company does not need to have 35 user-defined events and 35 rules triggered by the user-defined events; a single user-defined event and a single rule are enough.

When user-defined events are used this way, you may not always want them to be available for manual triggering in the XProtect Smart Client. You can use roles to define which user-defined events should be visible in the XProtect Smart Client; see Specify the Rights of a Role (see "Specify Rights of a Role" on page 256).

Whichever way you choose to use user-defined events, each user-defined event must first be added through the Management Client:

Adding a New User-defined Event

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, and select **User-defined Events**.
2. In the Overview pane (see "Panels overview" on page 70), right click **Events** and select **Add User-defined Event...**
3. Type a name for the new user-defined event, and click **OK**. The newly added user-defined event will now appear in the list in the Overview pane.



User rights permitting (see roles (see "About Roles" on page 249)), the user-defined event can now be manually triggered from XProtect Smart Clients. Already connected XProtect Smart Client users must log out and log in again before the user-defined event will be visible.

Remember to create one or more rules (see "Manage Rules" on page 221) specifying what should take place when the custom event occurs.

Editing the Name of an Existing User-defined Event

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, and select **User-defined Events**.
2. In the Overview pane (see "Panels overview" on page 70), select the required user-defined event.
3. In the Properties pane (see "Panels overview" on page 70), overwrite the existing name.
4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Already connected XProtect Smart Client users must log out and log in again before the name change will be visible.

Deleting an Existing User-defined Event

Bear in mind that deleting a user-defined event will affect any rules in which the user-defined event is used.

A deleted user-defined event will not disappear from XProtect Smart Clients immediately; only after XProtect Smart Client users log out.

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, and select **User-defined Events**.
2. In the Overview pane (see "Panels overview" on page 70), right click the unwanted user-defined event, and select **Delete New User-defined Event...**
3. You will be asked to confirm that you want to delete the user-defined event; if you are sure, click **Yes**.

Managing 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:

1. Part one, enabling the analytics events feature and setting up its security. A list of allowed addresses can be used to control who can send event data to the system and which port the server listens on.
2. Part two, creating the analytics event, possibly with a description of the event, and test it.
3. Part three, using the analytics event as the source of an alarm definition.

Furthermore, to use VCA-based events, a third-party VCA tool is required for supplying data to XProtect Corporate. Which VCA tool to use is entirely up to you, as long as the data supplied by the tool adheres to the applied formatting rules set out in the **Milestone Analytics Events; Developers Manual**. Contact Milestone 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 XProtect Corporate.



Creating a New Analytics Event

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), 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. **Optionally**, type a description text in the **Description** field.

Tip: Description texts can, for example, be used to give more background info on the event and how it is used. The description is not visible to users of the XProtect Smart Client.

4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Optionally, you can test the validity of the event by clicking **Test Event** (see "Testing an Analytics Event" on page 240).

Tip: You can continually correct errors indicated in the test and run the test as many times as you wish and from anywhere in the process.

Editing an Existing Analytics Event

1. To edit an existing analytics event, click it. This opens the **Analytics Event Information** window where you can edit relevant fields.
2. **Optionally**, you can test the validity of the event by clicking **Test Event**. (see "Testing an Analytics Event" on page 240)

Tip: You can continually correct errors indicated in the test and run the test as many times as you wish and from anywhere in the process.

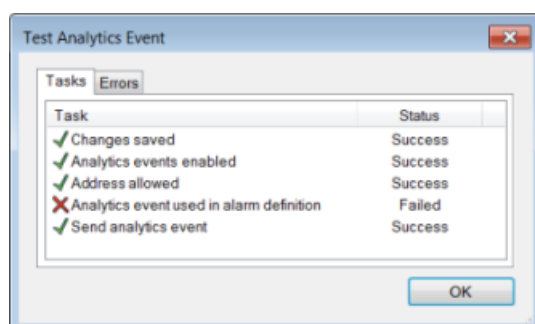
Testing an Analytics Event

Optionally, you can test the validity of an event by clicking **Test Event**.

Tip: You can carry out this test at any step of the analytics event creation/editing process and as many times as you wish.

To test an analytics event you must first create one, see Creating a New Analytics Event (on page 240).

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:





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

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

Step 1:

Changes saved: If the event is new, is it saved? Or if there are changes to the event name, are these changes saved?

Step 2:

Analytics Events enabled: Is the Analytics Event feature enabled?

Step 3:

Address allowed: Is the IP address/hostname of the machine sending the event(s) allowed (listed on the address list)?

Step 4:

Analytics event used in alarm definition: Is the analytics event used actively in any alarm definitions?

Step 5:

Send analytics event: Did sending a test event to the event server succeed?

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

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

Error corresponding to step 1:

Save changes before testing analytics event. Solution/Explanation: Save changes.

Error corresponding to step 2

Analytics events have not been enabled. Solution/Explanation: Enable the Analytics Event feature (see "Analytics Events" on page 287).

Errors corresponding to step 3:

The local host name must be added as allowed address for the Analytics Event service.

Solution/Explanation: Add your machine to the list of allowed IP addresses/hostnames.

Error resolving the local host name. Solution/Explanation: The IP address/hostname of the machine cannot be found or is invalid.

Error corresponding to step 4:

Analytics event is not used in any alarm definition. Solution/Explanation: Use the analytics event in an alarm definition.

Errors corresponding to step 5:

Event server not found. Solution/Explanation: Unable to find event server on the list of registered services.

Error connecting to Event server. Solution/Explanation: Unable to connect to event server on the stated port (most likely due to network problems, event server being stopped or similar).

Error sending analytics event. Solution/Explanation: 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. Solution/Explanation: Event sent to event server but no reply received (most likely due to network problems or port being busy (see the event server log, typically located at **ProgramData\Milestone\XProtect Event Server\logs**—can be opened in Microsoft Notepad or similar tool)).



Analytics event unknown by event server. Solution/Explanation: 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. Solution/Explanation: Event format is somehow incorrect.

Sender unauthorized by event server. Solution/Explanation: Most likely because your machine is not on the list of allowed IP addresses/hostnames.

Internal error in event server. Solution/Explanation: Event server error, see the event server log, typically located at ProgramData\Milestone\XProtect Event Server\logs—can be opened in Microsoft Notepad or similar tool).

Invalid response received from Event server. Solution/Explanation: Response is invalid (possibly due to port being busy or network problems (see the event server log, typically located at ProgramData\Milestone\XProtect Event Server\logs—can be opened in Microsoft Notepad or similar tool)).

Unknown response from event server. Solution/Explanation: Response is valid but not understood (possibly due to port being busy or network problems (see the event server log, typically located at ProgramData\Milestone\XProtect Event Server\logs—can be opened in Microsoft Notepad or similar tool)).

Unexpected error. Solution/Explanation: Not likely to occur. If the accompanying text in the error does not provide enough information and problem continues, contact Milestone Support (support@milestonesys.com (mailto:support@milestonesys.com)) for help.

- Remember to save any changes made during the test. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

When done, check the presence of your test event in the XProtect Smart Client's Alarm list. Sort by type: **Test Alarm**. See XProtect Smart Client documentation for more details.

Editing Analytics Events Settings

In the Management Client toolbar, go to **Tools > Options** (on page 285) > **Analytics Events Settings** (see "Analytics Events" on page 287) to edit relevant settings.

Manage Generic Events

IMPORTANT: This feature will 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 XProtect Corporate.

Any hard- or software, which can send strings via TCP or UDP, can be used to trigger generic events. XProtect Corporate is able to analyze received TCP or UDP data packages, and automatically trigger generic events when specific criteria are met. This way you may integrate your XProtect Corporate system with external sources, for example access control systems, alarm systems, etc. The aim is to allow as many external sources as possible to interact with XProtect Corporate.

With the concept of data sources you avoid having to adapt third party tools to meet XProtect Corporate standards. Data sources lets you to communication with a particular piece of hard- or software on a specific IP port and to 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. If you are writing your own third party program, do not worry about data sources, just write your code to fit one of the two default data sources available, see **Specify Generic Event Data Source Settings**, further down. Their IP configuration can be found from the **Generic Events** tab of the **Options** menu (see "Options" on page 285).



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, XProtect Corporate provides the tools, but not the solution.

Unlike user-defined events (see "Manage User-defined Events" on page 238), 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 however allow other client IP addresses from the **Generic Events** tab of the **Options** menu (see "Options" on page 285).

- **String to send as generic event:** An event string to be tested—from within XProtect Corporate—by the event server as a generic event.
- **Data source to send event string to:** See **Data source** (see "Generic Events" on page 288) described here.
- **Echo from event server and local error message:** A window displaying the echo of the string from the event server in the following default 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.

If no generic events are defined or if no data sources are enabled, an information message will be displayed instead. Other echo formats can be selected (see "Generic Events" on page 288).

Creating a Generic Event

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, right-click Generic Events, and select Add New....
2. Fill in the needed information and properties.
3. **Optional:** In the **Check if expression matches event string:** field, enter the expression you would like to validate.
4. **Optional:** Below the **Check if expression matches event string:** field you will 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**.

Testing a Generic Event

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, select **Generic Events**.
2. In the Overview pane, 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 might get a response (an echo from the XProtect event server) in the **Echo from event server and local error message** field. This can be either successful or failed. See **Specify Generic Event Properties** further down.



Example: How to Create and Test a Simple Generic Event

To trigger recording on **Camera1**, you must send the string **RecordCamera1** to a TCP port on the XProtect Corporate event server. But the XProtect Corporate event server will not understand **RecordCamera1** as such, you will have to teach it:

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), 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.

Next, add a rule (see "Manage Rules" on page 221) defining that when the generic event **RecCam1** is triggered, recording should start on Camera1.

When done, test the scenario from the Management Client:

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Rules and Events**, select **Generic Events**.
2. In the Overview pane, select the top-node Generic Event.
3. In the Properties pane do the following:
 - 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 (see Generic Event Data Source Settings (see "Generic Events" on page 288)), you should get the following response in **Echo from event server and local error message:** **1,39,1,RecCam1**. This means that request number **1** had **39** characters and that there was **1** match with a generic event named **RecCam1**.

To try out the event from a non-XProtect Corporate 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.

What is Telnet? Telnet is a terminal emulation program used on TCP/IP networks. With Telnet, you can connect to a server from a computer on the network, and execute commands through Telnet as if you were entering them directly on the server. Windows includes a client for use with Telnet, however you might have to enable Telnet on your machine before using it.

Generic Event Properties

- **Name:** Unique name for the generic event.
 Name must be unique among all types of events. such as user defined events, analytics events, etc.
- **Enabled:** Generic events are by default enabled. Clear the check box to disable the event.
- **Expression:** Expression that XProtect Corporate should look out for when analyzing data packages. The following operators may be used:
 - **()**: Used to ensure that related terms are processed together as a logical unit; in other words, they can be used to force a certain processing order in the analysis.



Example: If using (**User001 OR Door053**) AND **Sunday**, the two terms inside the parenthesis will be processed first, then the result will be combined with the last part of the string. In other words, XProtect Corporate will first look for any packages containing either of the terms **User001** or **Door053**, then it will take the results and run through them in order to see which packages also contain the term **Sunday**.

- **AND:** With an AND operator, you specify that the terms on both sides of the AND operator must be present.

Example: If using **User001 AND Door053 AND Sunday**, the term **User001** as well as the term **Door053** as well as the term **Sunday** must be present in order for the criterion to be met. It is not enough for only one or two of the terms to be present. As a rule of thumb, the more terms you combine with AND, the fewer results you will retrieve: Combinations with AND yields few results.

- **OR:** With an OR operator, you specify that either one or another term must be present.

Example: If using **User001 OR Door053 OR Sunday**, the term **User001** or the term **Door053** or the term **Sunday** must be present in order for the criterion to be met. The criterion is satisfied even if only one of the terms is present. As a rule of thumb, the more terms you combine with OR, the more results you will retrieve: Combinations with OR yields many results

- **Expression type.** Indicates how particular XProtect Corporate should be when analyzing received data packages. The options are the following:

- **Search:** In order for the event to occur, the received data package must contain the text specified in the **Expression:** field, but may also have more content.

Example: If you have specified that the received package should contain the terms **User001** and **Door053**, the event will be triggered if the received package contains the terms **User001** and **Door053** and **Sunday** since your two required terms are contained in the received package.

- **Match:** In order for the event to occur, the received data package must contain exactly the text specified in the **Expression:** field, and nothing else.
- **Regular expression:** In order for the event to occur, the text specified in the **Expression:** field must identify specific patterns in the received data packages.

If you switch from **Search:** or **Match:** to **Regular expression:**, the text in the **Expression:** field is automatically translated to a regular expression.

- **Data source:** Selectable data sources. You can choose between two default data sources and any number of data sources created by you. What to select depends on what kind of third party program you work with and/or what kind of hard- or software you want to interface from:

- **Compatible:** Factory properties are enabled, echoes all bytes, TCP and UDP, Ipv4 only, port 1234, no separator, local host only, current code page encoding (ANSI), compatible with XProtect Enterprise version 6 and newer.
- **International:** Factory properties are enabled, echoes statistics only, TCP only, Ipv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10).
- [Data source A]
- [Data source B]
- Etc.

- **Priority:** The priority must be specified as a number between 0 (lowest priority) and 999999 (highest priority).

The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events. When XProtect Corporate receives a TCP and/or UDP package, analysis of the packet



will start 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 will be 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 the priority in question will be triggered.

- **Check if expression matches event string:** An event string to be tested against the expression entered in the **Expression:** field.



Generic Event Test Properties

- **String to send as generic event:** An event string to be tested—from within XProtect Corporate—by the event server as a generic event.
- **Data source to send event string to:** See **Data source (see "Generic Events" on page 288) described here.**
- **Echo from event server and local error message:** A window displaying the echo of the string from the event server in the following default 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.

If no generic events are defined or if no data sources are enabled, an information message will be displayed instead. Other echo formats can be selected (see "Generic Events" on page 288).

Generic Event Data Source Properties

- **Data source:** Selectable data sources. You can choose between two default data sources and any number of data sources created by you. What to select depends on what kind of third party program you work with and/or what kind of hard- or software you want to interface from:
 - **Compatible:** Factory properties are enabled, echoes all bytes, TCP and UDP, Ipv4 only, port 1234, no separator, local host only, current code page encoding (ANSI), compatible with XProtect Enterprise version 6 and newer.
 - **International:** Factory properties are enabled, echoes statistics only, TCP only, Ipv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10).
 - [Data source A]
 - [Data source B]
 - Etc.
- **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, except the name entered in the **Name:** field.
- **Port:** Indicates the port number used.
- **Protocol type selector:** Selectable protocols which XProtect Corporate should listen for, and analyze, in order to detect the generic event:
 - **Any:** TCP as well as UDP.
 - **TCP:** TCP only.



- **UDP:** UDP only.

Tip: It is OK for TCP and UDP packages used for generic events to contain special characters, such as @, #, +, å, ~, etc.

- **IPv type selector:** Selectable IPv address types: IPv4, IPV6 or both.
- **Separator bytes:** Indicates the separator bytes used to separate individual generic event records. Default for data source type **International** (see **Data sources:** earlier) is **13,10**. (13,10 = <cr><if>).
- **Echo type selector:** Selectable echo return formats:
 - **Echo statistics:** Echoes the following format:
`[X],[Y],[Z],[Name of generic event]`
`[X]` = request number.
`[Y]` = number of characters.
`[Z]` = number of matches with a generic event.
`[Name of generic event]` = name entered in the **Name:** field.
 - **Echo all bytes:** Echoes all bytes.
 - **No echo:** Suppresses all echoing.
- **Encoding type selector:** Selectable encodings. By default, the list only shows the most relevant options. Select **Show all** (see next bullet) to display all available encodings.

 Encoding is used for interpreting incoming bytes and turning these into strings of characters which can be matched against the strings entered as expressions for generic events.
- **Show all:** See previous bullet.
- **Allowed external IPv4 addresses:** Allowed IPv4 addresses.
- **Allowed external IPv6 addresses:** Allowed IPv6 addresses.

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

About Security

In the Management Client's Site Navigation pane (see "Panels overview" on page 70), you are able to work with the following under **Security**:

- **Roles:** (see "**About Roles**" on page 249) Roles determine which of your XProtect Corporate solution's features users and groups (see "Manage Users and Groups" on page 249) are able to use. In other words, roles determine rights. You create roles first, then you add users and groups and associate an XProtect Smart Client profile (see "Manage Smart Client Profiles" on page 182) and a time profile (see "Manage Time Profiles" on page 229) to the roles.



About Roles

Roles determine which of your XProtect Corporate solution's features users and groups (see "Manage Users and Groups" on page 249) are able to use. In other words, roles determine rights and handles security within the application.

You define roles first, then you add users/groups and an XProtect Smart Client profile (see "Manage Smart Client Profiles" on page 182) and a time profile (see "Manage Time Profiles" on page 229) to each role.

One role is predefined in XProtect Corporate, and cannot be deleted: the **Administrators** role. In addition to the **Administrators** role, you are able to add as many roles as required in your organization.

To manage roles in XProtect Corporate, expand the **Security** folder in the Management Client's Site Navigation pane (see "Panels overview" on page 70), and select **Roles**.

For more information see:

- Manage Users and Groups (on page 249)
- Assign and Remove Users and Groups to/from Roles (on page 254)
- Manage Roles (on page 251)
- Specify Rights of a Role (on page 256).

Note that roles may also determine access to views in clients; see Manage View Groups (on page 179).

Manage Users and Groups

In XProtect Corporate, you define roles (see "About Roles" on page 249) first, then you add users/groups to the roles.

Roles determine which of XProtect Corporate's features users and groups are able to use. In other words, roles determine rights.

Once you have defined roles, you can add users and groups; see Assign and Remove Users & Groups to/from a Role (see "Assign and Remove Users and Groups to/from Roles" on page 254).

Prerequisites

In order to be able to add users and groups through the Active Directory service, a server with Active Directory installed, and acting as domain controller, must be available on your network. Consult your network administrator if in doubt.

Adding Users and Groups through Active Directory (Normal Way)

Users and groups are normally added from Active Directory, although users can also be added without Active Directory.

What is 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. Users as well as groups are specified centrally in Active Directory.

Using Active Directory for adding existing user and group information to XProtect Corporate has several benefits: The fact that users as well as groups are specified centrally in Active Directory means that you will not have to create any user accounts from scratch in XProtect Corporate. It also means that you will not have to configure any authentication of users on XProtect Corporate; authentication is handled by Active Directory.

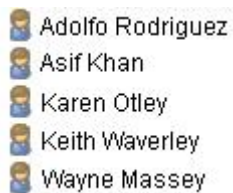
Active Directory User and Group Concepts

Active Directory uses the concepts of users and groups.



Users

Users are Active Directory objects representing individuals with a user account. Example:



Groups

Groups are Active Directory objects capable of containing several users. In this example, the Management Group has three members (i.e. it contains three users):



Groups can contain any number of users. By adding a group to XProtect Corporate, you add all of its members in one go. Once the group has been added to XProtect Corporate, any changes subsequently made to the group in Active Directory (such as new members added or old members removed) will immediately be reflected in XProtect Corporate.

Note that a user can be a member of more than one group at a time.

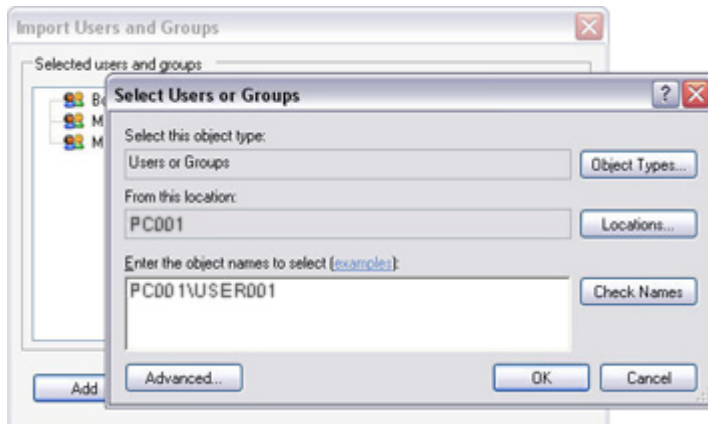
Adding Users Not Using Active Directory

While you primarily add XProtect Corporate users and groups to roles (see "About Roles" on page 249) through Active Directory, it is also possible to add individual users—but not groups—without Active Directory. If not using Active Directory, note the following:

- When installing the management server, the user under which the management server service runs must be a local PC user on the server. See also Management Server Installation (see "Install management server" on page 28).
- On the computer running the management server, simple file sharing must be disabled the following way:
 1. On the computer running management server, right-click **Start**, and select **Explore**.
 2. In the window that opens, select the **Tools** menu, then select **Folder Options...**
 3. Select the **View** tab.
 4. Scroll to the bottom of the **Advanced settings** list, and make sure that the **Use simple file sharing (Recommended)** check box is cleared.
 5. Click OK, and close the window.



- You add users to roles through the Management Client almost as when adding users from Active Directory (see Assign and Remove Users & Groups to/from a Role (see "Assign and Remove Users and Groups to/from Roles" on page 254). However, when adding users, you must refer to particular users on particular computers, as in this example where the user USER001 on the computer PC001 is added:



When users added this way log in to XProtect Corporate, the user must **not** specify any server name, PC name, or IP address as part of their user names. Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The users should of course still specify their passwords, etc.

Manage Roles

Roles determine which of your XProtect Corporate solution's features users and groups (see "Manage Users and Groups" on page 249) are able to use. In other words, roles determine rights and handles security within the application.

You define roles first, then you add users/groups and an XProtect Smart Client profile and a time profile to each role. Added roles automatically also become view groups (see "Manage View Groups" on page 179).

One role is predefined in XProtect Corporate, and cannot be deleted: the **Administrators** Role.

In addition to the **Administrators** role, you are able to add as many roles as required in your organization.

To manage roles in XProtect Corporate, expand the **Security** folder in the Management Client's Site Navigation pane (see "Panels overview" on page 70), and select **Roles**.

For more information see also Assign and Remove Users and Groups to/from Roles (**on page 254**) and Specify Rights of a Role (**on page 256**).

Note that roles may also determine access to views in clients; see Manage View Groups (on page 179).

More About Administrators role

The **Administrators** role is predefined, and cannot be deleted. Users and groups with the **Administrators** role have complete and unrestricted access to the entire XProtect Corporate system. For this reason it is not necessary to specify role settings for the **Administrators** role. Because the **Administrators** role has complete and unrestricted access, it is associated with the **Default Smart Client Profile** profile and does not have a time profile (see "Manage Time Profiles" on page 229).

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 (on page 254).



Role settings tabs are not available for **Administrators** role as users and groups with this role have unrestricted access to the system



IMPORTANT: Users with **local machine administrator** rights on the computer running the management server will automatically have administrator rights on the management server. It is therefore important that you verify which users have **local machine administrator** rights on the computer running the management server: Only users whom you trust as administrators of your XProtect Corporate system should have **local machine administrator** rights on the computer running the management server.

Add a role and manage its Smart Client and Time Profiles

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security**, and right-click **Roles**.
2. Select **Add Role**. This will open the **Add Role** dialog.
3. In the **Add Role** dialog, type a name and description of the new role:



4. Then click **OK**.
5. The new role is added to the **Roles** list in the Overview pane (see "Panels overview" on page 70). By default, a new role does not have any users/groups associated with it, but it does have the default profile **Default Smart Client Profile** and the default time profile **Always** associated.
6. To change the default Smart Client or time profiles, in the Properties pane (see "Panels overview" on page 70), click the wanted drop down dialog.



7. You are now able to assign users/groups to the role, and to specify which of XProtect Corporate's features they should be able to access. See Assign and Remove Users & Groups to/from a Role (see "Assign and Remove Users and Groups to/from Roles" on page 254) and Specify Rights of a Role (on page 256).

Copying 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. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security**, click **Roles**, right-click the required role in the Overview pane (see "Panels overview" on page 70), select **Copy Role...**
2. In the dialog that opens, give the copied role a new unique name and description.
3. Click **OK**.

Deleting a Role

Before deleting a role (see "About Roles" on page 249), bear in mind that you are able to delete a role even when users and/or groups have been assigned to the role. It is therefore often a good idea to verify if any users/groups are assigned to the role before deleting it.

Verifying if Any Users/Groups Are Assigned to a Role

- In the Management Client's Site Navigation pane, expand **Security**, and right-click **Roles**.
- Select the required role in the Overview pane (see "Panels overview" on page 70), then select the **Users and Groups** tab in the Properties pane. Any users and/or groups assigned to the role will be listed on the **Users and Groups** tab.

How to Delete a Role

Deleting a role will not delete a view group based upon the role. For information about deleting view groups, see Manage View Groups (on page 179).

1. In the Management Client's Site Navigation pane, expand **Security**, and right-click **Roles**.
2. Right-click the unwanted role in the Overview pane, and select **Delete Role**.
Tip: Alternatively, press **DELETE** on your keyboard.
3. Click **Yes**.

Renaming a Role

Renaming a role will not change the name of a view group based upon the role. For information about renaming view groups, see Manage View Groups (on page 179).

1. In the Management Client's Site Navigation pane, expand **Security**, and right-click **Roles**.
2. Right-click required role in the Overview pane (see "Panels overview" on page 70), and select **Rename Role...**
Tip: Alternatively, press **F2** on your keyboard.
3. In the dialog that opens, change the name of the role.
Tip: You are also able to change the description of the role.
4. Click **OK**.

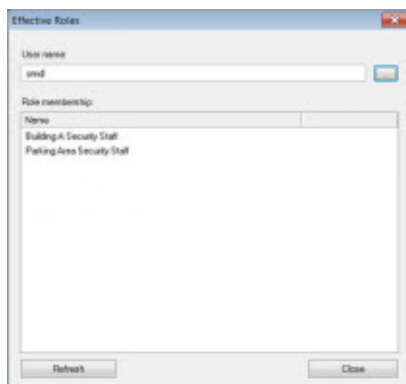


Viewing Effective Roles

With the Effective Roles feature, you are able to view all roles (see "About Roles" on page 249) of a selected user or group (see "Manage Users and Groups" on page 249). This ability is especially convenient if you are using groups; in fact it is the only way of viewing the roles of individual group members.

1. Open the **Effective Roles** window. There are three ways in which you can open the **Effective Roles** window:
 - From the Management Client's menu bar, by selecting **Tools > Effective Roles...**
 - From the Overview pane (see "Panels overview" on page 70) (when working with roles), by right-clicking anywhere inside the pane, then selecting **Effective Roles...**
 - From the Site Navigation pane, by expanding **Security**, then right-clicking **Roles**, then selecting **Effective Roles...**
2. In the **Effective Roles** window's **User name** field, type the user name of the required user.

Tip: By clicking the browse button to the right of the field, you are able to browse for the user in question, using Active Directory.



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 will be displayed automatically.

Assign and Remove Users and Groups to/from Roles

To assign or remove users or groups to/from a role, do the following:

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security**, and select **Roles**. Then select the required role in the overview pane (see "Panels overview" on page 70):



2. In the properties pane (see "Panels overview" on page 70), select the **Users & Groups** tab:





Assigning Users and Groups to a Role

- a** On the **Users & Groups** tab, click **Add....** This will open the **Select Users, Computers and Groups** dialog:

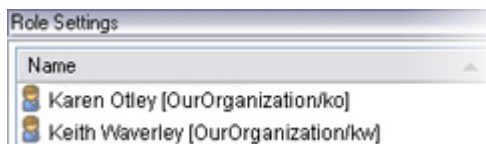


- b** Verify that the required object type is specified. If, for example, you need to add a computer, click **Object Types** and mark **Computer**. Furthermore, verify that the required domain is specified in the **From this location** field. If not, click **Locations...** to browse for the required domain.

- c** In the **Enter the object names to select** box, type the required user names, initials, or other types of identifier which Active Directory will be able to recognize.

Tip: Typing part of a name is often enough. Use the **Check Names** feature to verify that the names, initials, etc. you have typed are recognized by Active Directory.

- d** Click **OK**. The selected users/groups are now added to the **Users & Groups** tab's list of users who have been assigned the selected role:



Removing Users and Groups from a Role

Bear in mind that a user may also have roles through group memberships. When that is the case, you cannot remove the individual user from the role. Furthermore group members may also hold roles as individuals. To find out which roles user, groups, or individual group members have, use the Effective Roles (see "Manage Roles" on page 251) feature.

- a** On the **Users & Groups** tab, select the user or group you want to remove, then click **Remove** in the lower part of the tab.

Tip: You can select more than one user or group, or a combination of groups and individual users, if required.

- b** Confirm that you want to remove the selected user(s) or and group(s). Click **Yes**.



Specify Rights of a Role

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security**, and select **Roles**. Then select the required role in the overview pane (see "Panels overview" on page 70):



2. In the properties pane (see "Panels overview" on page 70), specify required rights for the role on the relevant tabs:

Device Rights

The **Device** tab lets you specify which features users/groups with the selected role should be able to use for each device (e.g. a camera) or device group.

The tab is divided into two halves: In the upper half you select the device or device group for which you want to specify role rights. In the lower half you then specify which of the selected device's or device group's features users/groups with the selected role should have the right to access.

Remember to repeat for each required device/device group.



Device tab, with role rights for a selected device, in this case a camera. Note that you can also select a device group, and specify role rights for the entire device group in one go.

Camera-Related Rights

Setting determines whether...

- o **AUX Commands:** ...it will be possible to use auxiliary commands from the XProtect Smart Client.

What are AUX Commands? AUX is short for Auxiliary. Such commands offer the user control of, for example, wipers on a camera connected via a video server. Camera-associated devices connected via auxiliary connections are controlled from the XProtect Smart Client.



- **Add:** ...it will be possible to add bookmarks in recorded video from the XProtect Smart Client.
- **Delete:** ...it will be possible to delete bookmarks in recorded video from the XProtect Smart Client.
- **Edit:** ...it will be possible to edit bookmarks in recorded video from the XProtect Smart Client.
- **View:** ...it will be possible to view bookmarks in recorded video from the XProtect Smart Client.
- **View live within time profile:** ...live viewing of video from the selected camera(s) will be possible in access clients.
- **Export video:** ...the database export feature can be used when browsing recorded video from selected camera(s) in the XProtect Smart Client. Furthermore, the AVI, JPEG and export features can be used in similar way in all access clients.
- **Get sequences:** ...the **Sequences** feature can be used when browsing recorded video from the selected camera(s) in access clients.
- **Playback Video:** ...playing back of recorded video from the selected camera(s) will be possible in access clients.
- **Smart Search:** ...the **Smart Search** feature can be used when browsing recorded video from the selected camera(s) in the XProtect Smart Client.
- **Visible:** ...the selected camera(s) will be visible in access clients.

The **View live** right also requires that the role has been granted the right to view the access clients' **Live** tab. This right is granted as part of the application rights.

The **Export Video** and **Playback Video** rights also require that the role has been granted the right to view the access clients' **Browse** tab. This right is granted as part of the application rights.

Microphone-Related Rights

Setting determines whether...

- **Visible:** ...the selected microphone(s) will be visible in the XProtect Smart Client.
- **Listen to live audio:** ...listening to live audio from the selected microphone(s) will be possible in the XProtect Smart Client.
- **Browse audio:** ...browsing of recorded audio from the selected microphone(s) will be possible in the XProtect Smart Client.
- **Export audio:** ...the export feature can be used when browsing recorded audio from the selected microphone(s) in the XProtect Smart Client.
- **Get sequences:** **This feature is currently not supported** ...the **Sequences** feature can be used when browsing recorded audio from the selected microphone(s) in the XProtect Smart Client.

Speaker-Related Rights

Setting determines whether...

- **Visible:** ...the selected speaker(s) will be visible in the XProtect Smart Client.
- **Listen to live audio:** ...listening to live audio from the selected speaker(s) will be possible in the XProtect Smart Client.
- **Browse audio:** ...browsing of recorded audio from the selected speaker(s) will be possible in the XProtect Smart Client.
- **Export audio:** ...the export feature can be used when browsing recorded audio from the selected speaker(s) in the XProtect Smart Client.



- **Get sequences:** This feature is currently not supported ...the **Sequences** feature can be used when browsing recorded audio from the selected speaker(s) in the XProtect Smart Client.

IMPORTANT: Although what is being said through a speaker can be recorded and archived (see "About Storage and Archiving" on page 101), there is currently no way of playing back or exporting such recorded outgoing audio. Therefore, some of the speaker-related rights currently have no effect. Features for playing back and exporting recorded outgoing audio, etc. will be available in subsequent releases as soon as possible.

Input-Related Rights

- **Visible:** Determines whether information about the selected input(s) will be visible to users of the XProtect Smart Client as well as users of XProtect Central, an add-on product for providing complete overview of surveillance system status and alarms.

Output-Related Rights

Setting determines whether...

- **Visible:** ...the selected output(s) will be visible in the XProtect Smart Client. If visible, the output will be selectable on a list in the XProtect Smart Client.
- **Activate output:** ...the selected output(s) can be activated from the XProtect Smart Client.

Outputs are selected and activated on the XProtect Smart Client's **Live** tab. Both rights thus require that the role has been granted the right to view the XProtect Smart Client's **Live** tab; this right is granted as part of the application security rights.

Why are some check boxes filled with squares? Square-filled check boxes can only appear if you are specifying role rights for a device group, in which case they indicate that the right in question currently applies for some, but not all, devices within the device group.



Square-filled check boxes indicate that settings currently apply for some, but not all, devices within a device group

You can still select or clear such square-filled check boxes, but note that your choice will in that case apply for **all** devices within the device group. Alternatively, select the individual devices in the device group to verify exactly which devices the right in question applies for.

PTZ Rights

Relevant only if PTZ (Pan/Tilt/Zoom) cameras are available on your XProtect Corporate system, the **PTZ** tab lets you specify which features users/groups with the selected role should be able to use.

The **PTZ** tab is divided into two halves: In the upper half you select the PTZ camera or device group for which you want to specify settings— note that only PTZ cameras and device groups containing PTZ cameras are available for selection. In the lower half you then specify what users/groups with the selected role should be able to do when operating the selected PTZ cameras in the XProtect Smart Client.

Setting determines whether users/groups...

- **Allow PTZ Control:** ...with the selected role are able to use the pan, tilt and zoom features of the selected PTZ camera(s).
 - False: Users/groups with the selected role will not be able to use the pan, tilt and zoom features of the selected PTZ camera(s)



- True: Users/groups with the selected role will be able to use the pan, tilt and zoom features of the selected PTZ camera(s)
- **PTZ Priority:** ...have priority for PTZ cameras and how. When several users on a surveillance system wish to control the same PTZ camera at the same time, conflicts may occur. This setting lets you alleviate the problem 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.

Default PTZ priority is 3000.

Example: You specify that the role **Security Manager** should have very high priority when using a PTZ camera, whereas the role **Security Assistant** should have low priority when using the PTZ camera. Now, if a user with the role **Security Manager** and a user with the role **Security Assistant** want to control the PTZ camera at the same time, the user with the role **Security Manager** will win the ability to control the camera.

If your system is upgraded from an older version of XProtect Corporate, the old values (**Very Low**, **Low**, **Medium**, **High** and **Very High**) have been translated as follows:

- **Very Low = 1000**
- **Low = 2000**
- **Medium = 3000**
- **High = 4000**
- **Very High = 5000**

Users of the XProtect Smart Client are able to stop/resume a patrolling PTZ camera's patrolling through a context menu in the XProtect Smart Client view. This PTZ feature is not regulated by PTZ priority.

- **Allow activation of PTZ presets:** ...with the selected role are able to move the selected PTZ camera(s) to preset positions.
 - False: Users/groups with the selected role will not be able to move the selected PTZ camera(s) to preset positions
 - True: Users/groups with the selected role will be able to move the selected PTZ camera(s) to preset positions

For the rights to work, the role must also be granted the right to view the XProtect Smart Client's **Live** tab. This right is granted as part of the application rights. Furthermore, the PTZ camera(s) must be **visible** in XProtect Smart Clients; you determine as part of the device rights.

Speech rights

Relevant only if loudspeakers are available on your XProtect Corporate system.

The **Speech** tab is divided into two halves: In the upper half you select the speaker or device group for which you want to specify settings. In the lower half you then specify what users/groups with the selected role should be able to do when operating the selected speaker(s) in the XProtect Smart Client.

The following rights are available:

- **Speak live:** Determines whether users with the selected role will be able talk through the selected speaker(s).
- **Speak priority:** When several XProtect Smart Client users want to talk through the same speaker at the same time, conflicts may occur. This setting lets you alleviate 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**.



Example: You specify that the role **Security Manager** should have very high priority when talking through a speaker, whereas the role **Security Assistant** should have low priority when talking through the speaker. Now, if a user with the role **Security Manager** and a user with the role **Security Assistant** want to talk through the speaker at the same time, the user with the role **Security Manager** will win the ability to talk.

If two users with the same role want to speak at the same time, the first-come first-served principle applies.

For the right to work, the role must also be granted the right to view the XProtect Smart Client's **Live** tab. This right is granted as part of the application rights. Furthermore, the speaker(s) must be **visible** in XProtect Smart Clients; you determine as part of the device rights.

Application Rights

The **Application** tab lets you specify which applications in your XProtect Corporate system users/groups with the selected role should be able to use. Users must be a member of the **Administrator** role to have access to the Management Client. Simply select the required applications:

Setting determines whether users/groups with the selected role are able to use the...

- **Browse:** ...**Browse** tab in the XProtect Smart Client and Remote Client.
- **Live:** ...**Live** tab in the XProtect Smart Client and Remote Client.
- **Setup:** ...**Setup** button in the XProtect Smart Client and Remote Client.
- **Status API:** ...**Status API** (Application Program Interface). The **Status API** is used in connection with XProtect Central, an add-on product that provides complete overview of surveillance system status and alarms.
- **Service Registration API:** ...**Service Registration API**. The **Service Registration API** is used in connection with the service channel, a service that enables automatic and transparent configuration communication between servers and clients in your XProtect Corporate.

External Event Rights

The **External Events** tab is divided into two halves. In the upper half, select the external event for which you want to specify settings. In the lower half, specify what users/groups with the selected role should be able to do with the selected external event in the XProtect Smart Client.

- **Trigger external event with time profile:** On the XProtect Smart Client's **Live** tab it is possible to manually trigger your surveillance system's external events. This right determines whether users with the selected role should be able to trigger the selected external event in their XProtect Smart Clients.

For the right to work, the role must also be granted the right to view the XProtect Smart Client's **Live** tab. This right is granted as part of the application rights.

View Group Rights

The **View Group** tab lets you specify which view groups (i.e. groups of views in clients; see Manage View Groups (on page 179) for more information) users/groups with the selected role should be able to use.

The tab is divided into two halves: In the upper half you select the view group for which you want to specify role rights. In the lower half you then specify how users/groups with the selected role should be able to access the selected view group.

Setting determines whether users/groups with the selected role are able to...

- **Visible:** ...see the selected view group (and any views contained in the view group) in clients.



- **Modify:** ...make changes to the selected view group (and any views contained in the view group) in clients.
- **Delete:** ...to delete the selected view group (and any views contained in the view group) in clients.
- **Create subgroups and views:** ...create subgroups and views in the selected view group.

Enterprise Server rights

Specifying role rights on the Enterprise **Servers** tab is only relevant if you have integrated XProtect Enterprise servers into your XProtect Corporate solution; see Manage XProtect Enterprise Servers (on page 279) for more information.

The tab is divided into two halves: In the upper half you select the XProtect Enterprise server for which you want to specify role rights. In the lower half you then specify which authentication settings should apply for users/groups with the selected role. The process is described in detail in Defining Access Roles for XProtect Enterprise Servers (see "Manage XProtect Enterprise Servers" on page 279).

Matrix rights

Specifying role rights on the **Matrix** tab is only relevant if you have configured Matrix recipients (see "Manage XProtect Matrix Recipients" on page 185) on your XProtect Corporate system.

From the XProtect Smart Client it is possible to send video to selected Matrix recipients. The **Matrix** tab lets you specify which Matrix recipients should be selectable for this purpose in the XProtect Smart Client.

The tab is divided into two halves: In the upper half you select the Matrix recipient for which you want to specify role rights. In the lower half you then specify if users/groups with the selected role should be able to select the Matrix recipient in the XProtect Smart Client.

- **Visible:** Determines whether users/groups with the selected role will be able to select and send video to the Matrix recipient from the XProtect Smart Client.

Alarms Rights

Specifying role rights on the **Alarms** tab is only relevant if you use alarms in your system setup to provide central overview and control of your federated XProtect Enterprise and XProtect Corporate installation. See About Alarms (see "Alarms" on page 273).

The **Alarms** tab lets you specify which alarm rights (i.e. how alarms can be handled in the XProtect Smart Client, see Alarms (on page 273)) users/groups with the selected role should have.

The tab is divided into two halves. In the upper half, select the alarm role for which you want to specify alarm role rights. In the lower half, specify how users/groups with the selected role should be able to handle the selected alarms.

Determines whether users/groups with the selected role will be able to do the following in the XProtect Smart Client:

- **Manage:**
 - Manage alarms (for example change priorities of alarms and re-delegate alarms to other users)
 - Acknowledge alarms
 - Change state (for example from **New** to **Assigned**) of several alarms simultaneously (otherwise state must be changed on a per-alarm basis)
- **View:**
 - View alarms



- Print alarms reports.

MIP Rights

Through the Milestone Integration Platform Software Development Kit (MIP SDK) a third party vendor can develop custom plug-ins (for example, integration to external Access Control Systems or similar) to XProtect Corporate.

Custom settings for these plug-ins—if any—can be found on the **MIP** tab.

Manage View Groups

The way in which video from one or more cameras is presented in clients (Smart Client (see "Installing the XProtect Smart Client" on page 22) and Remote Client (on page 24)) is called a view. A view group is basically 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 subsequently 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.

More about View Groups

By default, each role you define in the Management Client is also created as a view group: when you add a role in the XProtect Corporate Management Client, the role will by default appear as a view group for use in clients.

Examples:

XProtect Smart Client displaying a view with video from six different cameras (the view is highlighted in red frame):





A role added in the XProtect Corporate Management Client:



The role appearing as a view group in the XProtect Smart Client:



- A view group based on a role will by default only be available to users/groups who have been assigned to the role in question. You are able to change this; see **View Group Rights** in Specify Rights of a Role (on page 256).
- A view group based on a role will by default carry the role's name.

Example: If you create a role with the name **Building A Security Staff**, it will by default appear in the XProtect Smart Client as a view group called **Building A Security Staff**. You are able to change the name; see the following for more information.

- In addition to the view groups you get when you add roles, you are able to create as many other view groups as you require. You can also delete view groups which you do not want to use, including those automatically created when adding roles. See the following for more information.
- Even though a view group is by default created each time you add a role (see "Manage Roles" on page 251), view groups do not have to correspond to roles. You are therefore able to add any number of view groups—if required—and rename or remove each of your view groups if required. This is no matter whether the view groups were created automatically when adding a role or whether you added them manually.

View Groups from a Client User's Perspective

For more information about views from a client user's perspective, see the separate Smart Client and Remote Client documentation available on the XProtect Corporate software CD as well as from [www.milestonesys.com](http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf).

Adding a View Group

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand the Clients node, right-click View Groups, and select **Add View Group**. This opens the **Add View Group** dialog.
2. Type the name of the new view group, then click **OK**.



3. Optionally; in the Management Client's overview pane, select the added view group, then in the properties pane add a description of the view group.

No roles will have the right to use the newly added view group until you have specified such rights; see **View Group Rights** in Specifying the Rights of a Role (see "Specify Rights of a Role" on page 256) for more information.

Also, even when you have specified which roles should be able to use the newly added view group, already connected client users with the relevant roles must log out and log in again before they will be able to see the view group.

Renaming a View Group

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand Clients, and select **View Groups**.
2. In the Management Client's overview pane, right-click the required view group and select **Rename View Group**.
3. Change the view group's name as required, then press the return key on your keyboard.

Client users already connected must log out and log in again before the name change will be visible.

Removing a View Group

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand Clients and select **View Groups**.
2. In the Management Client's overview pane, right-click the required view group and select **Delete View Group**.
3. Click **Yes**.

System Dashboard

About System Dashboard

In the Management Client's Site Navigation pane (see "Panels overview" on page 70), you are able to work with the following under **System Dashboard**:

- **System Monitor:** (see "**About System Monitor**" on page 264) Here you can view and print detailed system reports on servers, devices and cameras.
- **Current Task:** (see "**About Current Task**" on page 266) Here you can get an overview of tasks under a selected recording server.
- **Configuration Report:** (see "**About configuration report**" on page 266) From here you can decide what to include in, and print, XProtect Corporate system configuration reports.

About System Monitor

From the Site Navigation pane (see "Panels overview" on page 70), expand **System Dashboard**, and click **System Monitor**. This brings up the System Monitor using embedded browser technology.



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

A Data Collector Server service is dedicated to collect performance counter values on servers and cameras to be used in the System Monitor functionality.

About Data Collector Server service

The Data Collector Server service is automatically installed on the same machines as the management, recording, log and event server(s).

Normally, the Data Collector Server service requires no maintenance. However, if the service **does** stops, it will result in missing live feed to the System Monitor (clearly indicated in the system monitor by error texts). On the machine where the Data Collector Server service is installed, do the following to restart it:

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 Corporate Data Collector Server**. Right-click it. From the menu that appears, select **Start** to restart the **Milestone XProtect Corporate Data Collector Server** service.

Working with System Monitor

Use the <, > and home icons to navigate the System Monitor.

From here you can view system information and create reports on:

- **Management server:** shows data on **your management server**
- **Recording servers:** shows data on **any number of recording servers** in your surveillance setup, which can be viewed per:
 - **Disks**
 - **Storage**
 - **Network**
 - **Cameras**
- **Failover servers:** shows data on **any number of failover servers** in your surveillance setup
- **Additional servers:** shows data on **log servers, event servers etc.** in your surveillance setup
- **Cameras:** shows data **on any camera in any camera group** in your surveillance setup.

Each of these corresponds to a clickable, expandable area, most of which contains sub-areas. Each sub-area represents a server. When clicked, they provide relevant dynamic data on this server.

The **Cameras** bar however, contains a list of camera-groups to select from. Once a group is selected, you can select a specific camera and see dynamic data for it.

All servers display **CPU usage** and **available memory** information. Furthermore, recording servers also display **connection status** information.



Within each view, you can 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.

If you want to save and/or print reports, click the **Send to PDF** icon.

About Current Task

To get an overview of tasks under a selected recording server, their begin time, estimated end time and progress, do the following:

From the Site Navigation pane (see "Panels overview" on page 70), expand **System Dashboard**, and click **Current Task**.

In general, all information showed in **Current Tasks** are snapshots and are refreshed by clicking on the refresh button in the lower right corner of the **Properties** pane.

About configuration report

When creating XProtect Corporate pdf configuration reports, you can include any possible elements of your XProtect Corporate system which you want to see in the report. Examples of what can be included ranges from licenses over device to alarm configuration, and much more.

Furthermore, you can customize your font and page setup and include a customized front page as listed:

Creating a Configuration Report

1. From the Site Navigation pane, 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.

Remember to select **Front page** as an element to include in your report, otherwise the front page you customize will not be 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 your report.

Tip: Remember, not all fonts support all special characters. If you have trouble viewing your special characters, try selecting a different font.

Configuration Report Details

The following buttons are available when setting up reports:

- **Select All:** Selects all elements in the list
- **Clear All:** Clears all elements in the list
- **Front Page...:** Opens a dialog allowing you to customize the front page
- **Formatting...:** Opens a dialog allowing you to format the report
- **Export...:** Opens a dialog allowing you to select the save location for the report and create the pdf.



Server Logs

Manage Logs

In the Management Client, you are able to view and copy contents from different logs related to the management server. The different logs have different purposes:

- Audit Log records user activity.
- Event Log records event-related information (see "Events Overview" on page 216).
- Rule Log records rules (see "Manage Rules" on page 221) in which the **Make new <log entry>** action (see "Actions and Stop Actions Overview" on page 188) has been specified.
- System Log records system-related information.

XProtect Corporate has a number of default settings related to the different logs, see Handling Log Settings (on page 271). Furthermore, you are able to view logs in a number of different languages, export them, and save the exported logs as tab delimited text (.txt) files at a location of your choice; see Exporting Log (on page 270).

Viewing Log

To view a log, expand the **Management Server Logs** item in the Management Client's Site Navigation pane (see "Panels overview" on page 70), then select appropriate the log.

Reading and Copying Log Content

Each row in a log represents a log entry. A log entry contains a number of information fields which are listed and briefly explained. Note, it is also possible to double-click any row and have all its details presented in a Log Details window. From the Log Details window, it is also possible to copy/paste any log contents:

- **Level**
 - **All logs:** Display an icon indicating the level of the log entry:
 -  indicates info
 -  indicates error
 -  indicates warning.
- **UTC Time**
 - **All logs:** Timestamp in coordinated universal time (UTC), an international high-precision time standard.
- **Local Time**
 - **All logs:** Timestamp in the local time of the XProtect Corporate server.
- **Description**
 - **All logs:** Description of the logged incident.
- **Source Type**



- **Rule Log only:** Type of equipment on which the logged incident occurred. Since log entries are administrator-defined and relate to incidents on the XProtect Corporate system, source type will normally be **System**.
- **Event and System Logs only:** Type of equipment on which the logged incident occurred, for example **Management Server** or **Device**.
- **Audit Log only:** Type of equipment on which the logged incident occurred. Since remote user access is handled by the XProtect Corporate management server, source type will typically be **Server**.
- **ID**
 - **All logs:** Identification number of the logged incident.
- **Event Type**
 - **All logs, except Audit Log:** Type of event represented by the logged incident.
For more information about event types, see also the events overview (on page 216).
- **Source Name**
 - **All logs:** Name of the management server, device, etc. on which the logged incident occurred.
- **Service Name**
 - **Event and Rule Logs only:** Name of service on which the logged incident occurred.
- **Audit Type**
 - **Audit Log only:** Type of logged incident.
- **Granted**
 - **Audit Log only:** Information about whether the remote user action was allowed (granted) or not.
- **User**
 - **Audit Log only:** User name of the remote user causing the logged incident.
- **Location**
 - **Audit Log only:** IP address or host name of the computer from which the remote user caused the logged incident.
- **Rule Name**
 - **Rule Log only:** Name of the rule triggering the log entry.
- **Generator Type**
 - **Rule Log only:** Type of equipment on which the logged incident was generated. Since the log entries are administrator-defined and relate to incidents on the XProtect Corporate system, generator type will normally be **System**.
- **Generator Name**
 - **Rule Log only:** Name (if any) of the equipment on which the logged incident was generated.



Navigating Log

If a log contains more than one page of information, you are able to navigate between the log's pages by clicking the buttons in the bottom right corner of the log pane:



lets you move one step towards the log page containing the most recent log entries.

indicates which page you are currently viewing (e.g. page 1 of 171). By clicking the button, you are able to specify a page number and go straight to that page.

lets you move one step towards the log page containing the oldest log entries.

Furthermore, in the lower left corner lets you jump to a specific date and time in the log.

Changing Log Language

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

Show log in: English (United States) ▼

You can choose from the following log languages:

- Danish
- English
- French
- German
- Italian
- Japanese
- Portuguese
- Russian
- Simplified Chinese
- Spanish
- Traditional Chinese.

2. The log is displayed in the selected language.

Next time you open the log, it is reset to the default language.

Searching Log

To search a log, use the **Search criteria** box in the top part of the log pane:



1. Specify your search criteria by selecting the required user name, location, etc. from the lists.

Tip: You can combine selections, or make no selection in certain lists, as required. The more search criteria you combine, the less search results you will typically get.

2. Click **Refresh** to make the log page reflect your search criteria.

Tip: To clear your search criteria, and return to viewing all of the log's content, click **Clear**.

Exporting Log

You are able to export logs, and save the exported logs as tab delimited text (.txt) files at a location of your choice.

Example of an exported log .txt file

Example of an exported log .txt file viewed in Notepad.

Timestamp	Level	EventType	Source	Description
1/4/2007 1:47:26 PM	Error	Communication Error	Camera 14	Device Communication Error
1/4/2007 1:47:33 PM	Error	Communication Error	Camera 10	Device Communication Error
1/4/2007 1:47:37 PM	Error	Communication Error	Camera 12	Device Communication Error
1/4/2007 1:47:39 PM	Error	Communication Error	Camera 11	Device Communication Error
1/4/2007 1:48:24 PM	Error	Communication Error	Camera 18	Device Communication Error
1/4/2007 1:48:40 PM	Error	Communication Error	Camera 18	Device Communication Error
1/4/2007 1:49:13 PM	Error	Communication Error	Camera 18	Device Communication Error
1/4/2007 1:49:41 PM	Error	Communication Error	Camera 18	Device Communication Error
1/4/2007 1:49:52 PM	Error	Communication Error	Camera 18	Device Communication Error

You are able to target the exported log content by specifying which log, which log elements, and which time range to include in the export. For example, you are able to specify that only the System Log's error-related log messages from between January 2nd 2007 08:00:00 and January 4th 2007 07:59:59 should be included in your export.

To export a log, do the following:

1. Expand the **Management Server Logs** item in the Management Client's Site Navigation pane (see "Panels overview" on page 70), and select the required log.
2. If you want to target the exported log's content, select the required criteria in the **Search criteria** section above the log. For example, you may select that your export should only contain log messages at a particular level, such as errors or warnings.

Remember to click **Refresh** to make the log page reflect your selected criteria.

3. In the Management Client's menu bar, select **Action > Export Log...** This will open the **Export Log** window:

4. In the **Export Log** window's **Filename** field, specify a name for the exported log file.



By default, exported log files will be saved in your **My Documents** folder. However, you are able to specify a different location by clicking the browse button  next to the field.

5. Any criteria you have selected in order to target the content of the exported log will be listed in the **Filters** field. The field is non-editable; if you find that you need to change your criteria, close the window, and repeat steps 2-4.
6. Specify the time period you want the export to cover. You do this by specifying the required boundaries in the **Start date and time** and **End date and time** fields respectively. By clicking the arrow, you are able to select the required date from a calendar:



To specify an exact time, overwrite the required time elements (hours:minutes:seconds) with the required values. In this example, the hours element is being overwritten:



Tip: When you have selected time elements in order to overwrite them, you are also able to use your keyboard's UP ARROW and DOWN ARROW keys to increase/reduce the numbers in increments of one unit.

7. Click **Export** to export the required log content to the required location.

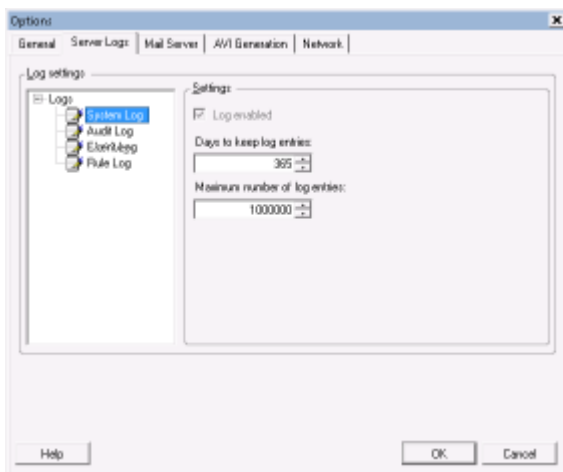
Handling Log Settings

XProtect Corporate has a number of default settings related to its logs. To verify or change these settings, do the following:

1. Go to the Management Client's menu bar, and select **Tools > Options...**
2. In the **Options** window, select the **General** tab. One of the tab's settings applies for all types of logs:
 - o **Number of log rows to retrieve per page:** Lets you specify the number of log rows you want to view on a single log page. If a log contains more than the specified number of rows, you will be able view the remaining rows on subsequent log pages.



3. Go to the **Options** window's **Management Server Logs** tab:



In the tab's left box, select the required log. The selected log's settings are displayed in the tab's right box:

- **Log enabled:** Lets you enable/disable the selected log. By default, all logs—**except the Event Log**—are enabled.
 The **System Log** and **Audit Log** cannot be disabled by clearing the box.
- **Days to keep log entries:** Lets you specify how many days the log's information should be kept for. Default is 30 days.
 Excess log content will be deleted if the log reaches its maximum allowed size (see **Maximum number of entries**) before the specified number of days is reached.
- **Maximum number of entries:** Lets you specify the maximum size of the log. Default is 50.000 entries.
 Excess log content will be deleted if it reaches its maximum allowed age (see **Days to keep log entries**) before the specified number of entries is reached.

For the **Audit Log**, you will furthermore see:

- **Enable user access logging:** Lets you include detailed information about specific user actions in the audit log, e.g. about users' viewing of live video (and associated audio), PTZ actions, activation of output and events, export, playback of video and audio, use of playback features, any denied access to features, etc.
- **Playback sequence logging length:** Lets you specify how long a playback sequence may last and still be considered and logged as **one** sequence.
Example: If you select 60 seconds, you may view 60 consecutive seconds of playback video but still only leave one log entry in the Audit Log. Specifying a high number of seconds may help limit the number of viewed sequences logged, and thus reduce the size of the audit log.
- **Records seen before logging:** Lets you specify the number of records to be viewed before logging the sequence.

4. Click **OK**.



Alarms

Manage Alarms

IMPORTANT: This feature will not work if you do not have the XProtect event server installed.

Based on functionality handled in the XProtect event server, the Alarms feature provides central overview, control and scalability of alarms in any number of federated (see "Milestone Federated Architecture Overview" on page 293) XProtect Enterprise and XProtect Corporate installations throughout your organization. It can be configured to generate alarms based on either:

- **Internal system related events;**

For example, motion, server responding/not responding, archiving problems, lack of disk space, etc.

- **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.

- **Milestone Integration Platform plug-in events;**

Through the Milestone Integration Platform Software Development Kit (MIP SDK) a third party vendor can develop custom plug-ins (for example, integration to external Access Control Systems or similar) to XProtect Corporate.

To ease overview, delegation and handling of alarms, these will appear in the alarm list of the XProtect Smart Client and can, if relevant, be integrated with map functionality. Alarms is thus a powerful monitoring tool, providing instant overview of alarms and possible technical problems.

More About Alarms

Alarm configuration includes among other things:

- 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.

What is a VCA-based system? VCA-based systems provide third-party video content analysis, spanning from face recognition, over advanced motion detection, to complex behavioral analysis, where various types of abnormal behavior, both of humans and vehicles, can be detected. VCA systems and their output can seamlessly be integrated with—and hook into—XProtect Corporate and be used for, for example, triggering alarms. Within XProtect Corporate, the events resulting from VCA systems are called analytics events.

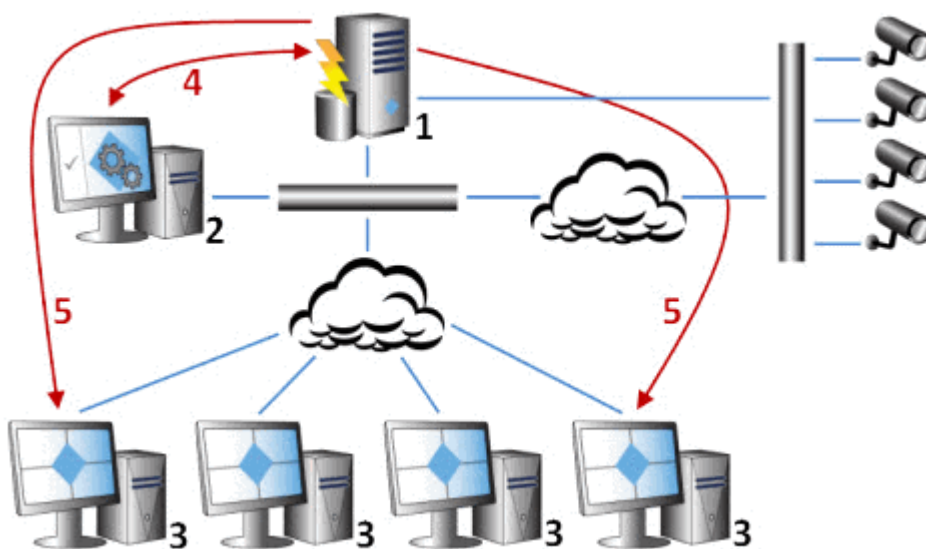
In general, alarms are controlled by the visibility of the object causing the alarm. This means that four possible aspects can play a role with regards to alarms and who can control/manage them and to what degree.

- **Source/device visibility.** If the device causing the alarm is not set to be visible to the user's role, the user will not be able to see the alarm in the alarm list in the XProtect Smart Client. See Device Rights (on page 256).



- **Right to trigger user-defined events** might be an issue. This right determines if the user's role can trigger selected user-defined events in the XProtect Smart Client. See **External Event Rights** (on page 260).
- **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—like much else—on the user's role and on settings configured for that particular role. See **Alarms Rights** (on page 261).

Illustration: How do the Alarms Feature and the Event Server work?



Legend:

1. Surveillance System
2. XProtect Corporate Management Client
3. XProtect Smart Client
4. Alarm Configuration
5. Alarm Data Flow

FAQs: XProtect Central and Alarms - Same Thing?

Does Alarms cover the same functionality as XProtect Central? Yes, to a large extent, since configuration of former XProtect Central functionality is now located in Alarms. XProtect Central was an independent product consisting of two parts; a dedicated server and a number of dedicated clients. Alarms, on the other hand, is an integrated part of XProtect Corporate. Thus, Alarms configuration uses the Management Client's users, groups and roles functionality. This means that much configuration needed in XProtect Central is redundant with Alarms. Client-wise Alarms uses the XProtect Smart Client—among other things its view and map feature.

However, **Alarm Definitions**, **Time Profiles** and **Log Options** must still be configured in the Management Client (under **Tools, Options**) and are more or less unchanged from XProtect Central. Finally, under **Roles**, alarm **Security settings** must be set.

Can I reuse old alarm and map definitions from XProtect Central? No, you will have to redefine your alarms and maps in Alarms.



Can I reuse old map definitions from XProtect map server? Yes, your old map definitions will be available in Alarms.

Does Alarms cover the same functionality as XProtect Analytics Generic VA? Yes, to a large extent, since what was before a plugin to XProtect Analytics is now an integrated part of the event server and covers the same functionality. See also **Does Alarms cover the same functionality as XProtect Central?** FAQ earlier.

Defining Alarms

IMPORTANT: Alarms can register and handle events from both XProtect Corporate and XProtect Enterprise system servers, but they must all be run as federated sites (see "Milestone Federated Architecture Overview" on page 293) for Alarms to work.

When a particular event (for example **Motion Detected**) is registered on your surveillance system, Alarms can be configured to cause this alarm to appear in the XProtect Smart Client. You must define alarms before you can use them and they are defined based on events registered on your XProtect Corporate (and possibly XProtect Enterprise) system(s) servers.

Tip: You can even use user-defined events for triggering alarms and if required, the same event can be used to trigger several different alarms.

Creating a New Alarm

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Alarms**, right-click **Alarm Definitions**. Select **Add New....** A window appears.
2. Fill in these properties:

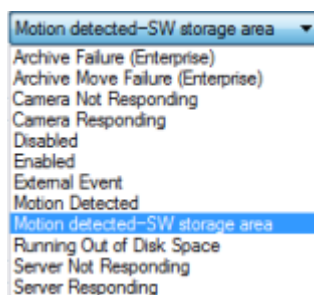
- **Enable:** Lets you enable the Alarms feature.
- **Name:** Lets you type a name for the alarm. The alarm's name will appear whenever the alarm is listed.

Tip: Alarm names do not have to be unique, but using unique and descriptive alarm names are advantageous in many situations.

- **Description:** Lets you type a description text (optional).
- **Triggering event:** Lets you select the (event) messages to be used when the alarm is triggered. It is divided into two drop-downs.

The first drop-down, lets you select the **type** of event to use. It is possible to choose between analytics events, system events and relevant plug-in related events.

Based on your selection above, the last drop-down lets you select the specific **event message** to be used:



List of selectable triggering events; the highlighted one is created and customized using analytics events.



- **Sources:** Lets you select which cameras and/or other devices, including plug-in defined sources (VCA, MIP, etc), the event should originate from in order to trigger the alarm. Your options depend upon which type of event you have selected.
3. Next, for alarm activation, choose between **Time profile** and **Event based**.
- **Time profile:** If you select **Time profile**, you must select when the alarm should be enabled for triggering. If you have not defined time profiles (see "Manage Time Profiles" on page 229), you will only be able to select **Always**. If you have defined one or more time profiles, they will be selectable from this list.
 - **Event based:** If you select **Event based**, you must select which events should start and stop the alarm. Events available for selection are hardware events defined on cameras, video servers and input (see "Events Overview" on page 216). Also global/manual event definitions (see "Manage User-defined Events" on page 238) can be used.
- Note that when selecting **Event based** it is not possible to define alarms based on outputs—only on inputs.
4. Choose the time limit for when operator action is required, and what event to trigger when the time limit is reached.
- **Time limit:** Select a time limit for when operator action is required. Default is 1 minute. The time limit is not active before an event is attached.
 - **Events triggered:** Lets you select which event to trigger when the time limit has been reached.
5. Choose additional settings.
- **Related cameras:** Lets you select (a maximum of 15) cameras for inclusion in the alarm definition even though 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 could attach the cameras' recordings of the incident to the alarm.
 - **Related map:** Lets you assign a map to the alarm when it is listed in the XProtect Smart Client's *Alarm Manager*.
 - **Initial alarm owner:** Lets you select a default user responsible for the alarm.
 - **Initial alarm priority:** Lets you select a priority (**High**, **Medium** or **Low**) for the alarm. Priorities can be used for sorting purposes and workflow control in the XProtect Smart Client.
 - **Initial Alarm Category:** Lets you select an alarm category for the alarm. This could be for example *False alarm* OR *Needs investigation*.
 - **Event triggered by alarm:** Lets you define an event to be triggered by the alarm in the XProtect Smart Client (if needed).
 - **Auto-close alarm:** Lets you select if the alarm should automatically be closed upon a particular event. This is possible for alarms triggered by some (but not all) events.
- Tip:** If you want to disable the new alarm from the beginning, clear the **Enable** check box in the upper right corner before saving.
6. In the toolbar (see "Management Client Overview" on page 66), click **Save**.

Editing Existing Alarms

Click an existing alarm to edit it.



Setting Alarm Data

When you configure alarm data settings (see "Defining Alarms" on page 275), specify the following:

Alarm Data Levels tab:

Priorities table:

- **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 (see "Defining Alarms" on page 275).
- **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** (see "**Setting Alarm Sounds**" on page 277).

States table:

- **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 *Alarm List*.
- **Name:** Type a name for the entity. You can create as many as you like.

Categories table:

- **Level:** Add new categories with level numbers of your choosing. These category levels are used to configure the **Initial alarm category** setting (see "Defining Alarms" on page 275).
- **Name:** Type a name for the entity. You can create as many as you like.

Alarm List Configuration tab:

- In **Available columns**, use > to select which columns should be available in the XProtect Smart Client's *Alarm List*. 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 *Solved-Trespasser* or *False Alarm*. You can create as many as you like.

Setting Alarm Sounds

When you configure **Sound Settings**, specify the following:

- **Sounds:** Select the sound to be associated with the alarm. The list of sounds contain a number of default Windows sounds. These cannot be edited. However, you can add new sounds of the file type .wav, but only if these are encoded in Pulse Code Modulation (PCM).

Although 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 will therefore be unable to play them. To ensure an identical sound all over, you should import and use your own .wav files encoded in PCM.

- **Add:** Lets you 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:** Lets you test the sound. In the list, select the sound. The sound will be played once.

Set Up Alarms Using Enterprise Slaves

User name and password

If your surveillance setup includes one or more XProtect Enterprise slaves and you wish to include one or more of these in your Alarms, setup, it is important that the login name and password specified when adding the slave, is the same as used in the XProtect Central add-on in the XProtect Enterprise Server.

Otherwise, the XProtect event server is unable to login to the XProtect Central add-on in XProtect Enterprise and collect status information.

Port number

Furthermore, if at some point 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 in the same way.

This is done directly in the affected configuration file.

How to update port number information...

1. On the server running the XProtect event server, click **Start > Control Panel > Administrative Tools > Services**.
2. Right-click the Milestone XProtect event server, click **Stop**.
3. Open **C:\Program Files\Milestone \XProtect event server \config\XPconfig.xml** in Microsoft® Notepad or another editing tool of your choice.
4. In the XML file, edit the port number information so it matches the port number(s) specified in XProtect Central add-on in the XProtect Enterprise Server.

```
<host>
guid>cb4735ae-fb4a-48e2-b8b5-a9f72309d5ad</guid>
guidParent>00000000-0000-0000-0000-000000000000</guidParent>
id>10.100.0.183</id>
user>SysTest</user>
pass>06/ZTZ7hLA8=</pass>
port>1237</port>
IMuser>SysTest</IMuser>
IMpass>06/ZTZ7hLA8=</IMpass>
IMport>8080</IMport>
event>True</event>
serverType>1</serverType>
engineName>XPE Systest4-v2</engineName>
<path />
```



5. Save the changes you have made to the XML file.
6. Restart the XProtect event server by repeating steps 1 & 2. Instead of **Stop**, click **Restart**.



Enterprise

Manage XProtect Enterprise Servers

If your organization has XProtect Enterprise installations, you can integrate XProtect Enterprise servers into your XProtect Corporate solution. You do this by adding the XProtect Enterprise servers through the XProtect Corporate Management Client.

Integration only works with XProtect Enterprise servers running XProtect Enterprise version 6.0 or later. Integration is not possible if your XProtect Corporate system uses IPv6 (see "IPv6 (vs. IPv4)" on page 338).

When added, XProtect Enterprise servers can send data and video to the XProtect Corporate surveillance system. You can compare added XProtect Enterprise servers with recording servers and these will likewise be available for viewing in clients.

Note that roles defined in XProtect Corporate's Management Client can be given access to data from XProtect Enterprise servers. This is done by coupling XProtect Corporate roles with XProtect Enterprise user rights.

Furthermore, XProtect Enterprise servers added in the XProtect Corporate Management Client will be listed in the **Add/Remove XProtect Enterprise Servers** dialog which you can open by selecting **XProtect Enterprise Servers...** from the **Tools** menu.

XProtect Enterprise's Recording Server service must be running for XProtect Corporate to receive data from the XProtect Enterprise installation. See the XProtect Enterprise documentation for more information.

Limitations when Adding XProtect Enterprise Servers

There are a few limitations to how XProtect Enterprise servers will work when added as slaves to the XProtect Corporate surveillance system. They will provide operational status and status details on cameras and XProtect Enterprise servers but not on any other device types.

Also, you cannot define cameras, user rights, scheduling, or other settings for the XProtect Enterprise installation, or see previews of the cameras in XProtect Corporate. All necessary XProtect Enterprise settings must be made in XProtect Enterprise's **Administrator** application or other relevant XProtect Enterprise applications. See the XProtect Enterprise documentation for more information.

For client users, it will be completely transparent whether feeds come from an XProtect Enterprise server or from an XProtect Corporate recording server. The users have access to cameras depending on their roles defined in the XProtect Corporate Management Client. If a role has borrowed user rights from an added XProtect Enterprise server, users with that role have access to data from the XProtect Enterprise server according to the borrowed user rights. See About Roles (on page 249) and Defining Access Roles for XProtect Enterprise Servers (on page 280).

Prerequisites for Access Roles for XProtect Enterprise Servers

On the XProtect Enterprise server, open the **Image Server Administrator** window to see if one of the XProtect Enterprise users has user rights that can be used in connection with an XProtect Corporate role.

Write the XProtect Enterprise user's user name and password or Windows account down. You will need this information when you use XProtect Corporate's Management Client to define roles with access to XProtect Enterprise servers. Note that user names and passwords are case sensitive.

You can also create a new user in XProtect Enterprise, and assign the required user rights in XProtect Enterprise, so they match the XProtect Corporate role. See the XProtect Enterprise documentation for more information about creating new users in XProtect Enterprise.

Before you are able to give roles access to XProtect Enterprise servers, the servers must be added through XProtect Corporate's Management Client. See Manage XProtect Enterprise Servers (on page 279).



Defining Access Roles for XProtect Enterprise Servers

To give access to data from XProtect Enterprise servers, do the following in the XProtect Corporate Management Client:

1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security**, and select **Roles**.
2. Select the required role from the list. If you want to define a new role, see About Roles (on page 249) for more information.
3. At the bottom of the **Role Settings** pane select the **Enterprise Servers** tab.
4. Select the XProtect Enterprise server to which you want to assign the role.



5. Select a user with the XProtect Enterprise user rights that represent the correct user rights for the XProtect Corporate role you are assigning it to. You can do this in two ways:
 - In the **Basic Authentication** section, enter the user name and password for a user which is defined as basic authenticated user in XProtect Enterprise.
 - or -
 - In the **Windows Authentication** section, enter the Windows account name for a user which is defined as a Windows authenticated user in XProtect Enterprise.

Tip: If in doubt whether a user is defined as a Basic or Windows authenticated user in XProtect Enterprise, open the **Image Server Administrator** window on the XProtect Enterprise server, and click **User Setup....** See the XProtect Enterprise documentation for more information

The selected XProtect Enterprise user has not automatically been assigned to the role in question through XProtect Corporate's Management Client. The user's XProtect Enterprise user rights have just been borrowed by the role, but the actual user has not been assigned to the role.

XProtect Corporate does not verify that the specified user name or password is correct or that the specified user name, password or Windows account name correspond to a defined user in XProtect Enterprise. Therefore, make sure that you enter the information correctly. Note also that user names and passwords are case sensitive.

6. In the toolbar (see "Management Client Overview" on page 66), click **Save**.



Adding XProtect Enterprise Servers

To add an existing XProtect Enterprise installation to your XProtect Corporate system, do the following:

1. From the XProtect Corporate Management Client's **Tools** menu select XProtect Enterprise **Servers...**
2. In the **Add/Remove XProtect Enterprise Servers** dialog click **Add....**
3. Enter the IP address or the host name of the required XProtect Enterprise server in the **XProtect Enterprise server IP / Host name** field.



4. Enter the port number used by the XProtect Enterprise server's Image Server in the **Port number** field.

Tip: The default port number is 80; if in doubt, you can find the port number in the **Image Server Administrator** window on the XProtect Enterprise server.

5. Now enter information about the administrator of the XProtect Enterprise server. You can do this in two ways:
 - o Select **Windows** and click the browse button to the right of the **User name** field to use the Windows authentication method which authenticates the administrator through the administrator's Windows login.
 - or -
 - o Select **Basic** and enter the XProtect Enterprise administrator's user name and password in the **User name** and **Password** fields.

The reason why it is important that you enter the XProtect Enterprise administrator information, is that you as administrator then will have unlimited rights to data from both XProtect Corporate and the XProtect Enterprise installation.

The connection to the XProtect Enterprise server is now established, but no roles in the XProtect Corporate Management Client—except the Administrator role—have been given access to data from the XProtect Enterprise server. See Defining Roles with Access to XProtect Enterprise Servers (see "Defining Access Roles for XProtect Enterprise Servers" on page 280) for more information about giving users access to data from added XProtect Enterprise servers.

Remember to define the network configuration settings, so the XProtect Corporate management server will be able to handle the token authentication of clients for added XProtect Enterprise servers.

In the XProtect Corporate Management Client, you must add all XProtect Enterprise servers you would like to receive data from. The XProtect Enterprise system's internal master/slave setup cannot be reused by XProtect Corporate.



XProtect Enterprise Server network configuration

With the network configuration settings you specify the XProtect Corporate management server's server address so that the XProtect Corporate management server can handle the token authentication of clients for added XProtect Enterprise servers.

From the XProtect Corporate Management Client's **Tools** menu select XProtect Enterprise **Servers...**

1. In the **Add/Remove Registered Services** window, click **Network...**
2. Specify the LAN and/or WAN IP address of the XProtect Corporate management server.

If all involved servers (both the XProtect Corporate management server and the trusted servers or the required XProtect Enterprise) 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**.

Editing XProtect Enterprise Servers

1. From the XProtect Corporate Management Client's **Tools** menu select XProtect Enterprise **Servers...**
2. Select an XProtect Enterprise server from the list, and click **Edit...** in the **Add/Remove XProtect Enterprise Servers** dialog.
3. Edit the relevant settings and click **OK**.

Registered Services

Manage Network Configuration

1. In the **Add/Remove Registered Services** window, click **Network...**
2. Specify the LAN and/or WAN IP address of the XProtect Corporate management server.



If all involved servers (both the XProtect Corporate management server and the trusted servers or the required XProtect Enterprise) 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**.

For more details, see *Manage Registered Services* (on page 283) and *Manage XProtect Enterprise Servers* (on page 279).

Manage Registered Services

Occasionally, you have servers and/or services which should be able to communicate with XProtect Corporate even though they are not directly part of the XProtect Corporate surveillance system. A typical example is an XProtect Transact server with which you want to use video from the XProtect Corporate system (XProtect Transact is a transaction management system, typically used for loss prevention through video evidence combined with time-linked POS or ATM transaction data).

Some services, but not all, can register themselves automatically in XProtect Corporate. Services that can automatically be registered are:

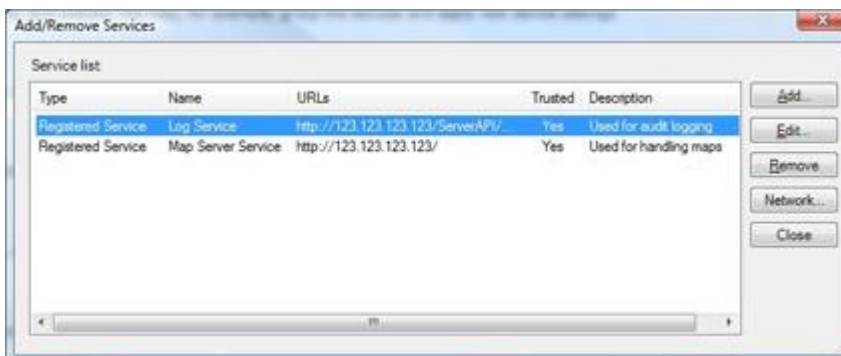
- Event Server service (see "The Management Server" on page 14)
- Log service (see "The Management Server" on page 14)
- Service Channel service (see "About the Service Channel" on page 330)

Automatically registered services are displayed in the list of registered services.

You can manually specify servers/services as registered services in the Management Client:

Accessing Registered Services Configuration

1. In the Management Client's menu bar, select **Tools > Registered Services...**
2. The **Add/Remove Registered Services** window opens. From this window you can manage registered services.





Adding and Editing 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 the following:
 - **Service type:** Pre-filled field.
 - **Name:** Name of the registered service; the name is only used for display purposes in the Management Client.
 - **Description:** Description of the registered service; the description is only used for display purposes in the Management Client.
 - **URLs:** Click **Add** to add the IP address or hostname of the registered service in question. If specifying a hostname as part of a URL, the host in question must exist and be available on the network. URLs must begin with **http://** or **https://** and must not contain any of the following characters: < > & ' " * ? | [] ".

Example of a typical URL format: <http://ipaddress:port/directory> (where port and directory are optional).

Note that you can add more than one URL if required.

- **External:** Select if the registered service connects to the management server with a public IP address.
- **Trusted:** Select if the registered service should be trusted immediately (this is often the case, but the option gives you the flexibility to add the registered service and then mark it as trusted by editing the registered service later).

Note that changing the trusted state will also change the state of other registered services sharing one or more of the URLs defined for the registered service in question.

3. Click **OK**.

Network Configuration

With the network configuration settings you specify the XProtect Corporate management server's server LAN and WAN addresses in order for the XProtect Corporate management server and the trusted servers to be able to communicate.

1. In the **Add/Remove Registered Services** window, click **Network...**
2. Specify the LAN and/or WAN IP address of the XProtect Corporate management server.

If all involved servers (both the XProtect Corporate management server and the trusted servers or the required XProtect Enterprise) 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**.

Options

Options

The Management Client's **Options** dialog lets you specify a number of settings related to the appearance of the application, to logging, to mail server configuration, etc.

You access the **Options** dialog from the Management Client's menu bar (see "Management Client Overview" on page 66), by selecting **Tools > Options**.

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

General

The **Options**' (see "Options" on page 285) **General** tab lets you specify the following:

- **Number of log rows to retrieve per page:** Lets you select the number of log rows you want to view on a single log page. Default is 50 rows. If a log contains more than the specified number of rows, you will be able view the remaining rows on subsequent log pages.
- **Default preview frame rate:** Lets you select which frame rate to use for the thumbnail camera images displayed in the preview pane (see "Panels overview" on page 70). Default is 1 frame per second.

Refreshing the Management Client' layout (by pressing F5 on your keyboard or selecting **Action > Refresh** from the menu bar) is required for a change to take effect.

Note that a high frame rate (i.e. a high image quality) in combination with a large number of thumbnail images in the preview pane may slow the system down. You are able to limit the number of thumbnail images with the **Max. number of previews** setting.

- **Max. number of previews:** Lets you select the maximum number of thumbnail images displayed in the preview pane. Default is 64 thumbnail images.

Refreshing the Management Client' layout (by pressing F5 on your keyboard or selecting **Action > Refresh** from the menu bar) is required for a change to take effect.

Note that a large number of thumbnail images in combination with a high frame rate (i.e. a high image quality) may slow the system down. You are able to limit the frame rate used for the thumbnail images with the **Default preview frame rate** setting.

- **Motion detection 'on' when adding camera devices:** Lets you select whether motion detection should be enabled while cameras are being added to a recording server through the **Add Hardware** (see "Add Hardware (Cameras, etc.)" on page 90) wizard.

Select check box to enable motion detection while using the wizard (default).

Note that this setting only applies while **Add Hardware** is in use. When the wizard is not in use, motion detection will be active for all cameras for which it has been enabled, regardless of this setting.

Why would I want to disable motion detection while using Add Hardware? Motion detection is a key element in the surveillance system, and is thus by default enabled for all cameras on the system. However, motion detection uses a relatively large amount of computing resources. If your system features a very large number of cameras, and motion detection is enabled on all cameras, the system may thus be slowed down slightly, and adding of new cameras may take longer than usual. In order to be



able to add new cameras as quickly as possible, you therefore have the option of disabling motion detection while the wizard **Add Hardware** is used.

- **Enable multicast live when adding camera devices:** Lets you select whether multicast (see "Manage Multicasting" on page 120) should be enabled while cameras are being added to a recording server through the wizard **Add Hardware**.

Select check box to enable multicast while using the wizard (default).

Note that this setting only applies while **Add Hardware** is in use. When the wizard is not in use, multicast will be active for all cameras for which it has been enabled, regardless of this setting.

- **Language:** Lets you select which language your Management Client system should run. You can choose from the following languages:

Danish

English

French

German

Italian

Japanese

Portuguese

Russian

Simplified Chinese

Spanish

Traditional Chinese.

IMPORTANT: A restart of the Management Client is required for language changes to take effect.

- **Timeout for PTZ sessions:** Handling of PTZ cameras may be interrupted manually by XProtect Smart Client users with the necessary user rights. This setting lets you select how much time should pass before regular patrolling is resumed after a manual interruption. The setting will apply for all PTZ cameras on your XProtect Corporate system.
- **Ignore device communication errors if communication reestablished before:** Lets you select how long a communication error may last without being logged by the system log—or in other words, when it is brief enough to be ignored.

Server Logs

The **Options** (see "Options" on page 285) **Server Log** tab lets you specify settings for XProtect Corporate's five different management server logs.

See Manage Logs (on page 267) for more information.

Mail Server

The **Options** (see "Options" on page 285) **Mail Server** tab lets you specify settings for the outgoing SMTP mail server you are going to use with your XProtect Corporate system.

See Outgoing SMTP Mail Server Settings (on page 291) for more information.



AVI Generation

The **Options'** (see "Options" on page 285) **AVI Generation** tab lets you specify compression settings for the generation of AVI video clip files. Specifying these settings is a prerequisite if you want to include AVI files in e-mail notifications sent out by rule-triggered notification profiles (see "Manage Notification Profiles" on page 233). See AVI Compression Settings (on page 290) for more information.

Network

The **Options'** (see "Options" on page 285) **Network** tab lets you specify local IP address ranges. See Manage Local IP Address Ranges (on page 292) for more information.

Bookmarks

The **Options'** (see "Options" on page 285) **Bookmarks** tab lets you specify settings for how bookmarks should be ID'ed and function in the XProtect Smart Client.

See Specify Rights of a Role (on page 256), Device Rights (on page 256) and XProtect Smart Client documentation.

User Settings

The **Options'** (see "Options" on page 285) **User Settings** tab lets you specify settings for user preference, such as whether a message should be shown when edge recording is enabled.

See **Record** tab Overview (on page 170) for more information.

Analytics Events Settings

The **Options'** (see "Options" on page 285) **Analytics Events Settings** tab lets you specify settings for analytics events:

- **Enable:** Lets you specify whether this feature should be enabled or not. As default, the service is disabled.
- **Port:** Lets you specify the port used by this service. Default port is 9090.

Make sure that relevant VCA tool providers also use this port number. If you change the port number, remember to make sure that these providers also change their port number.

- **All network addresses or Specified network addresses:** Lets you specify whether—in principle—events from all IP addresses/hostnames are accepted, or only events from IP addresses/hostnames specified in a list (see the following) are allowed.
- **Address list:** Lets you specify a list of trusted IP addresses/hostnames that you want this service to recognize. The list is used to filter and allow incoming data so that only events from certain IP addresses/hostnames are allowed. Both Domain Name System (DNS), IPv4 and IPv6 (see "IPv6 (vs. IPv4)" on page 338) address formats can be used in the list.

You have two ways of adding addresses to your list: Either by manually entering each IP address or hostname, or by importing an external list of addresses.

- **Manual entering:** Type the required IP address/hostname in the address list. Repeat for each required address.
- **Import:** Click **Import...** to browse for the required external list of addresses. To be able to import an external list, the external list must have been saved in a .txt file format and each IP address or hostname must appear on a separate line in the .txt file. Windows' simple text editor Microsoft® Notepad is an excellent tool for creating such .txt files.



Event Server Settings

The **Options'** (see "Options" on page 285) **Event Server Settings** tab lets you specify settings for alarms, events and logs:

- **Keep closed alarms for:** Lets you select the number of days to keep closed alarms, i.e. alarms in the states **Closed**, **Ignore**, and **Reject**.
- **Keep all other alarms for:** Lets you select the number of days for which to keep all other alarms, i.e. alarms not in the states **Closed**, **Ignore**, and **Reject**.

IMPORTANT: Alarms always have associated timestamps. Furthermore, if the alarm is camera-based, the timestamp has an image from the relevant video recording attached. While the alarm information itself is stored on the XProtect event server, the video recordings corresponding to the attached image are fetched from the relevant surveillance system server when users wish to view them. Therefore, if it is vital to have access to video recordings from all your alarms, make sure that video recordings from relevant cameras are stored on relevant surveillance system servers for at least as long as you intend to keep alarms on the event server.

- **Keep events for:** Lets you specify the number of days for which to keep events.
- **Keep logs for:** Lets you specify the number of days for which to keep the Alarms log.

On all the above, default setting is 30 days, but you can define any number up to 99.999 days, server space permitting. The value 0 can be used to indicate keep closed alarms indefinitely, server space permitting

- **Log server communication:** Select 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

The **Options'** (see "Options" on page 285) **Generic Events** tab lets you specify generic events and data source related settings:

- **Data source:** Selectable data sources. You can choose between two default data sources and any number of data sources created by you. What to select depends on what kind of third party program you work with and/or what kind of hard- or software you want to interface from:
 - **Compatible:** Factory properties are enabled, echoes all bytes, TCP and UDP, Ipv4 only, port 1234, no separator, local host only, current code page encoding (ANSI), compatible with XProtect Enterprise version 6 and newer.
 - **International:** Factory properties are enabled, echoes statistics only, TCP only, Ipv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10).
 - [Data source A]
 - [Data source B]
 - Etc.
- **New:** Click to create a new data source.
- **Name:** Name of the data source.
- **Port:** Indicates the port number used.



- **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, except the name entered in the **Name:** field.
- **Protocol type selector:** Selectable protocols which XProtect Corporate should listen for, and analyze, in order to detect the generic event:
 - **Any:** TCP as well as UDP.
 - **TCP:** TCP only.
 - **UDP:** UDP only.

Tip: It is OK for TCP and UDP packages used for generic events to contain special characters, such as @, #, +, å, ~, etc.

- **IPv type selector:** Selectable IPv address types: IPv4, IPv6 or both.
- **Separator bytes:** Indicates 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>).
- **Echo type selector:** Selectable echo return formats:
 - **Echo statistics:** Echoes the following format:
[X],[Y],[Z],[Name of generic event]
[X] = request number.
[Y] = number of characters.
[Z] = number of matches with a generic event.
[Name of generic event] = name entered in the **Name:** field.
 - **Echo all bytes:** Echoes all bytes.
 - **No echo:** Suppresses all echoing.
- **Encoding type selector:** Selectable encodings. By default, the list only shows the most relevant options. Select **Show all** (see next bullet) to display all available encodings.

Encoding is used for interpreting incoming bytes and turning these into strings of characters which can be matched against the strings entered as expressions for generic events.
- **Show all:** See previous bullet.
- **Allowed external IPv4 addresses:** Select between allowed addresses. Depending on you selection in the IPv type selector (see earlier), this property might be disabled.
- **Allowed external IPv6 addresses:** Select between allowed addresses. Depending on you selection in the IPv type selector (see earlier), this property might be disabled.

It is recommended to enter at least some allowed IP addresses, otherwise it will only be possible to communicate with events internally on the management server.

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**.



AVI Compression Settings

You are able to specify compression settings for the generation of AVI video clip files. Specifying these settings is a prerequisite if you want to include AVI files in e-mail notifications sent out by rule-triggered notification profiles (see "Manage Notification Profiles" on page 233).

To specify compression settings for AVI file generation, do the following:

1. Go to Management Client's menu bar, and select **Tools > Options...**
2. In the **Options** window, select the **AVI Generation** tab:



3. Specify the following:

- **Compressor:** Select the required codec (compression/decompression technology).

Tip: If in doubt about which codec to select, try using Indeo® 5.10 (if available). This codec generally provides a good compromise between quality and file size.

Tip: For some but not all codecs you are able to configure them by clicking **Configure....** Configuration options are entirely codec-specific. And also view detailed information about version number etc. by clicking **About....**

- **Compression quality:** (Not available for all codecs). Use the slider to select the required 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, compression quality will be 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 seconds between keyframes in the neighboring field.

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 will contain 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 required number of kilobytes per second in the neighboring field.

If the check box is not available, or not selected, data rate will be determined entirely by the selected codec.

4. Click **OK**.

Outgoing SMTP Mail Server Settings

You are able to specify settings for the outgoing SMTP mail server you are going to use with your XProtect Corporate system. Specifying these settings is a prerequisite for using rule-triggered notification profiles (see "Manage Notification Profiles" on page 233) to send out e-mail notifications on events, etc.

Note that when using the SMTP Service with .NET 4.0, it is not possible to send attachments over 3 MB. However two hotfixes (must be run in the listed order) from Microsoft can be found at:

<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226> (see <http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226> - <http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226>)

<http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723> (see <http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723> - <http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723>)

1. Go to the Management Client's menu bar, and select **Tools > Options...**
2. In the **Options** window, select the **Mail Server** tab



3. Specify the following:
 - **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 which will be used for sending e-mail notifications for all notification profiles. Example: mailserver.organization.org.

Furthermore, if the SMTP mail server requires login, select **Server requires login**, and type the required user name and password.

4. Click **OK**.



TLS (Transport Layer Security) and its predecessor SSL (Secure Socket Layer) is not supported; if the sender belongs on a server that requires TLS or SSL, e-mail notifications will not work properly. Also, you may be required to disable any e-mail scanners that could prevent the application sending the e-mail notifications.

Tip: When you add new notification profiles, you will be able to send test e-mails and thus verify that your SMTP mail server settings are correct.

Manage local IP address ranges

When a client, such as an XProtect Smart Client (see "Installing the XProtect Smart Client" on page 22), 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 completely 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 (see "Manage Public Addresses" on page 122), i.e. 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 are able to define a list of IP ranges which the surveillance system should recognize as coming from a local network.

Working with Local IP Address ranges...

1. In the Management Client's menu bar, select **Tools > Options**. This will open the Options dialog (see "Options" on page 285).

Tip: You can also access the **Options** dialog from the **Network** tab; this can be handy if you are also configuring the public IP address of a recording server.

2. In the **Options** dialog, select the **Network** tab.

Defining Local IP Address Ranges

- a On the **Network** tab, click **Add**.
- b In the **Range Start** column, specify the first IP address in the required range. Then specify the last IP address in the range in the **Range End** column.

Tip: If required, a range may include only one IP address (example: 192.168.10.1-192.168.10.1).

- c If more ranges are required, repeat steps a - b.
- d Click **OK**.

Editing Local IP Address Ranges

- a Overwrite the existing information in the **Range Start** and **Range End** columns as required.
- b Click **OK**.



Milestone Federated Architecture

Milestone Federated Architecture Overview

Milestone Federated Architecture™ (MFA) allows multiple individual standard XProtect Corporate systems (also known as sites) to interconnect in a parent/child hierarchy of sites.

IMPORTANT: Federated hierarchy is only possible with XProtect Corporate 4.0 or newer. Before installing XProtect Corporate, see Important Prerequisites When Running Federated Sites (on page 293).

In this text, the term **parent** refers to a parent site and **child** to a child site.

Through MFA, client users—based on their user rights—have seamless access to video, audio and other resources across individual XProtect Corporate sites. In addition, through a single login, administrators can centrally manage all sites within the federated hierarchy—again based on administration rights for the individual sites.

As it provides unlimited scalability, flexibility and accessibility to video surveillance across multiple sites and has no limit to the number of sites you can add, MFA is well suited for large installations covering multiple buildings, campuses, or entire city areas.

Each site in a federated hierarchy is installed and configured as a normal stand-alone system with standard system components, settings, rules, schedules, administrators, users, and user rights. Once each site has been installed, these can be connected by requesting an MFA link from one site (the parent) to another (the child). When the link is established, the two sites automatically create an MFA hierarchy to which more sites can be added to grow the federated hierarchy.



Click this thumbnail to view an example illustration of Milestone Federated Architecture.

In the clickable example, an MFA hierarchy consists of six sites. As illustrated, each site can be both a parent and a child at the same time thus making it possible to create a hierarchy with as many levels as needed. It is also evident that a site can link to several child sites on the same level in a hierarchy.

Once an MFA hierarchy is created, it allows users and administrators logged in to a site, to access that site and any child or sub-child sites it may have. Access to child and sub-child sites in the hierarchy is not gained automatically, but dependent on appropriate user and administrator rights.

It is only relevant to speak of a parent/child setup for management servers—not for recording servers (see "The Management Server" on page 14). However, due to their relations to management servers, recording servers will automatically become part of the parent/child setup.

See Manage Milestone Federated Architecture (on page 302) for details on how to work with MFA.

Important Prerequisites When Running Federated Sites

The easiest way to make MFA work correctly is to prepare your XProtect Corporate system for this feature during installation. There are certain important prerequisites that you must ensure already at the time of installing your management server. This can be done in different ways - choose between the procedures in alternative 1-3:



Alternative 1: Connect Sites from the Same Domain (with Common Domain User) and Customize the Installation of the Management Server to MFA

Before installation of the management server, a common domain user should be created and used as the administrator on all computers involved in the MFA. Depending on whether you select **Custom** or **Typical** during installation of the management server, make sure to select the appropriate procedure. Note that a typical installation requires more configuration on all sites before MFA will work properly.

Custom installation:

1. Start the management server installation (see "Install management server" on page 28) 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 must also be used when installing the other management servers in the MFA setup.

3. Finish the installation.
4. Repeat steps 1-3 to install any other XProtect Corporate systems you want to connect in the MFA.
5. See Adding a Site to the Hierarchy (see "Manage Milestone Federated Architecture" on page 302) for details on how to proceed with the MFA.

Typical Installation - set up **Network Service** on all servers:

1. Start the management server installation (see "Install management server" on page 28) and select **Typical**, let it run till it finishes.

This will install the management server as a **Network Service**.

2. Repeat step 1 to install any other XProtect Corporate systems you want to connect with the MFA.
3. Using a Management Client, connect to the management server you want to have as your parent site.
4. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security**, click **Roles**, and in the overview pane (see "Panels overview" on page 70), click **Administrator**.
5. Add the child computer to this parent server's **Administrator** role. See Assign and Remove Users and Groups to/from Roles (on page 254) for details.
6. Log out of the parent management server and connect to the management server that you just added as a child.
7. Once again, in the overview pane (see "Panels overview" on page 70), click **Administrator**.
8. Add the parent computer to this servers **Administrator** role. See Assign and Remove Users and Groups to/from Roles (on page 254) for details.
9. Log out of the management server, connect to the parent management server, and see Manage Milestone Federated Architecture (on page 302) for details on how to proceed with MFA.

Alternative 2: Connect Sites From Different Domains

To make it possible to connect sites across domains, it is very important that these domains are trusted by each other. Setting up domains to trust each other has nothing to do with MFA but is entirely a matter of Microsoft Windows Domain configuration.



For further information on how to set up trusted domains, see Microsoft website:
<http://technet.microsoft.com/en-us/library/cc961481.aspx> (<http://technet.microsoft.com/en-us/library/cc961481.aspx>).

1. When the domains, on which the sites you want to connect to each other in an MFA, are trusted correctly, follow the same instructions as if only one domain was present (see Alternative 1).

Alternative 3. Connect Sites in Workgroup(s)

When you connect sites inside workgroups, it is an important prerequisite for MFA to work correctly that the same administrator account is present on all computers you want connected in the MFA. This must be in place before installing XProtect Corporate.

1. Log in to **Windows** using a common administrator account.
2. Start the management server installation (see "Install management server" on page 28) and click **Custom**.
3. Select to install the Management Server service using a common administrator account.
4. Finish the installation.
5. Repeat steps 1-4 to install any other XProtect Corporate systems you want to connect. They must all be installed using a common administrator account.
6. See Adding a Site to the Hierarchy (see "Manage Milestone Federated Architecture" on page 302) for details on how to proceed.

It is **not** possible to mix domain(s) and workgroup(s), i.e. connect sites from a domain to sites from a workgroup and vice versa.

Licensing of Milestone Federated Architecture

To learn about licensing in general, see Manage Licenses (on page 84).

MFA can be used - freely - within the **same legal entity** as many times as needed. In an MFA setup, all sites share the same Software License Code (see "Manage Software License Codes (SLC)" on page 86) (SLC) and device licenses are shared between all sites.

In the case of **different legal entities** running MFA, each system requires a valid set of base and device licenses. Furthermore, in order for a device to be accessible across a federated setup, one **Milestone Federated Architecture Device License** is required per device accessed in the federated site.

To get additional licenses for your XProtect Corporate system, contact your XProtect Corporate vendor, or visit www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) to log into the software registration service center.

Basic Rules of Federated Sites

One Parent-Many Children

A child can only have one parent, but a parent can have an unlimited number of children.



Parent Requests Child, Not the Other Way Around

A new parent/child link is always requested by the parent, and if necessary, authorized by the child. See Accepting Inclusion in the Hierarchy (see "Manage Milestone Federated Architecture" on page 302).

One Level at the Time

A parent knows about all its children, children's children, etc., but only controls them one level down. Furthermore a child only knows about and answers to its parent one level up.

Synchronization of Hierarchy

A parent always contains an updated list of all its currently attached children, children's children, etc. But when distant communication is needed, it takes place level by level, each level forwarding and returning communication, until it reaches the server requesting the information. Depending on the number of levels that must be updated, changes to a hierarchy might take a little time to become visible in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), see Refreshing the Site Hierarchy (see "Manage Milestone Federated Architecture" on page 302). The federated hierarchy has a regularly scheduled synchronization between sites, as well as management-triggered synchronization every time a site is added or removed. This synchronization only contains site configuration data and each time will send less than 1MB. In addition to the data sent during synchronization, video or configuration data will be sent when a user or administrator views live or recorded video or configures the system. The amount of data in this case depends on what and how much is being viewed. It is not possible to schedule your own synchronizations.

Principles for Setting Up Federated Sites

When working with MFA, the link between management servers is established from the management server wanting to become parent to another management server. Theoretically, establishment of a parent/child relationship happens as follows:

1. The parent sends a link request to the potential child.
2. Depending on administrator settings, the child might have to authorize the link request.
3. If necessary, the child authorizes the link request.
4. Relevant info is exchanged.
5. The new parent/child link is established.

The Administrator Role and Federated Sites

- **Administrator vs. Non-administrator**

In general, you must be an administrator to work with federated architecture. However, by requesting the adding of children to a top-site (to which you have administrator rights), you can (without administrator rights to the other sites) create the overall initial infrastructure of a federation. But, as described in Manage Milestone Federated Architecture (on page 302), the administrator of each individual child must later authorize the connection before it can take effect.

- **Becoming an Administrator Using Active Directory-Two Possible Scenarios**

How to become administrator of a Milestone Federated Architecture setup using Active Directory depends on how the management server is installed. If it is installed as described in either of the following two scenarios, you gain administrator rights of the entire setup. Otherwise not.



- If the management server is installed as a **Network Service**: Both/All computers involved must be added as users to each other's XProtect Corporate administrator role before a parent/child link can be established without acceptance from the administrator of the child. See Assign and Remove Users and Groups to/from Roles (on page 254) for details. This type of setup is primarily recommended if all sites in the hierarchy are not a member of the same Domain. See also Important Prerequisites When Running Federated Sites (on page 293).
 - If the management server is installed as a **user account**: This user account must be a member of the administrator group of the server being linked to before one or more parent/child link(s) can be established without acceptance from the administrator of the child. This type of user right setup is primarily recommended if the number of sites in a hierarchy is large. See also Important Prerequisites When Running Federated Sites (on page 293).
- **Becoming an Administrator Using Work Groups**

How to become administrator of a federated architecture setup using work groups depends on how accounts are created. If they are set up correctly, you gain administrator rights of the entire setup. Otherwise not. See Important Prerequisites When Running Federated Sites (on page 293) for details on how to do this.

If the previous criteria are not met, the administrator of a child must accept requests for inclusion in the hierarchy (see "Manage Milestone Federated Architecture" on page 302) manually before links can be established.

One or More Administrators?

A Milestone Federated Architecture setup can have many administrators working on it at the same time. Furthermore, the **Site Navigation** pane is dynamic and reflects changes to the federated site made both by you and possibly other administrators. This means that you might see changes here caused by other users. You might also experience that a site you are connected to is removed from the federated site by another user. In this case, your site will be removed from the **Federated Site Hierarchy** pane, but nothing will change in the **Site Navigation** pane or elsewhere, allowing you to continue working.

Possibilities and Constrains of Federated Sites

In principle, there is no limit to the number of sites you can add to MFA and how these can be linked, offering you unlimited scaling, flexibility and accessibility.

There are, however, a few issues to be aware of when working with a federated hierarchy:

- **Maps**: Can only contain cameras from the federated site to which the map is attached-not from other sites in the hierarchy.
- **Alarms**: Can only be viewed per site. In other words, it is not possible to see all alarms for all sites in the hierarchy at the same time.

Frequently Asked Questions to Federated Sites

What is a federated site? A federated site is basically just an individual XProtect Corporate system, complete with management server, SQL server, one or more recording server(s), failover server(s) and cameras. To make use of Milestone Federated Architecture, you must connect at least two individual XProtect Corporate systems. The Management Client is used to configure federated hierarchies. In principle, it lets you connect to any site in the federated hierarchy at any given time (if user rights permit) using the log in credentials for your home-site. This offers you a central overview, and, at the same time, lets you zoom in on selected sites by connecting to a specific site to have a closer look, make configurations, or carry out maintenance. Note however, that the Management Client is only able to see other sites from the level of the site you are logged into and downwards in the hierarchy.



What is a top-site? Your top-site is the top level management server of your entire Milestone Federated Architecture setup.

An example an organization could have a top-level server called **MyCorp**. Second level servers called **MyCorp/RegionalServers**. Third level servers called **MyCorp/RegionalServers/CityNames**. And so on. In this case, **MyCorp** is your top-level server. There can only be one top-level server.

Tip: In a federated hierarchy, it is always a good idea to name your servers in a recognizable way, for example, using regional names or names implying where/in what context the server is located. Using, for example, consecutive numbers only, might be confusing if you have many servers.

What is a home-site? Your home-site is the site to which you are logged in. Since you may be logged in far down in the hierarchy, this is not necessarily the same as your top-site—but it **may** be. You are only able to see children from the point at which you are logged in and downwards.

Can a site be both a parent and a child at the same time? Yes, a parent with children attached, can easily be child to another site, and vice versa. This is because the parent/child concept is relative and used only in respect to other specified servers.

See the Milestone Federated Architecture illustration (see "Illustration of Milestone Federated Architecture" on page 301), where site 7 is the parent of site 8, but the child of site 6.

What is the difference between logging into and connecting to a site? To work with Milestone Federated Architecture you must always be logged in to a site via the Management Client. You can log in to any site if you have administrator rights to that particular site. This is called your home-site. When logged in to your home-site, you can see all its children (if user rights permit). From your home-site you can also connect to its children (if user rights permit). Embedded in the connection process is an automated and seamless log-in, using the same credentials as your home-site log in. Connecting to a child allows you to see and work with that site (if user rights permit). However, even though technically you log out of your home-site when connecting to another site, you will still see the site structure as your (former) home-site sees it. This means, that any changes you make to a child might not be visible until such changes reaches your home-site via scheduled synchronization. So changes you make in your hierarchy might not be reflected in the Federated Sites Hierarchy pane until later.

For more details, see Basic Rules of Federated Sites (on page 295).

You cannot refresh via a connection to a child, this must take place directly from the home-site.

When do I need to accept link requests? Whether as the administrator of a child you must accept a link request or not (or the link request is accepted automatically) depends on your administrator settings.

See Administrator Role and Federated Sites (see "The Administrator Role and Federated Sites" on page 296).

Where is Milestone Federated Architecture configured and managed? Setting up and configuring Milestone Federated Architecture takes place in the Management Client.

Do I need more than one XProtect Smart Client to work with Milestone Federated Architecture? When working with Milestone Federated Architecture, all work in the XProtect Smart Client can be handled from one XProtect Smart Client installation, i.e. there is no need for a one-to-one relationship between sites and XProtect Smart Clients.

How do I view video from federated sites? You can view video from federated sites in any XProtect Smart Client, i.e. there is no need for a one-to-one relationship between sites and XProtect Smart Clients. You will always get the view, i.e. see the site structure as the parent you are currently logged in to.

Can I include XProtect Enterprise slave(s) in my federated hierarchy? Yes, that is possible, but only as slave(s) to an XProtect Corporate management server. In this case, the relationship with the XProtect Enterprise server will work as described in Manage XProtect Enterprise Servers.

See also Defining Alarms (on page 275) for information on working with alarms in a federated setup.

Is Milestone Federated Architecture the same as multiple management servers, a.k.a. clustering? No, Milestone Federated Architecture is not the same as clustering. Clustering is a method of obtaining failover support for a management server on a site. With clustering, 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. On the other hand, Milestone Federated Architecture is a method of combining multiple independent corporate sites into one large setup, offering flexibility and unlimited possibilities.



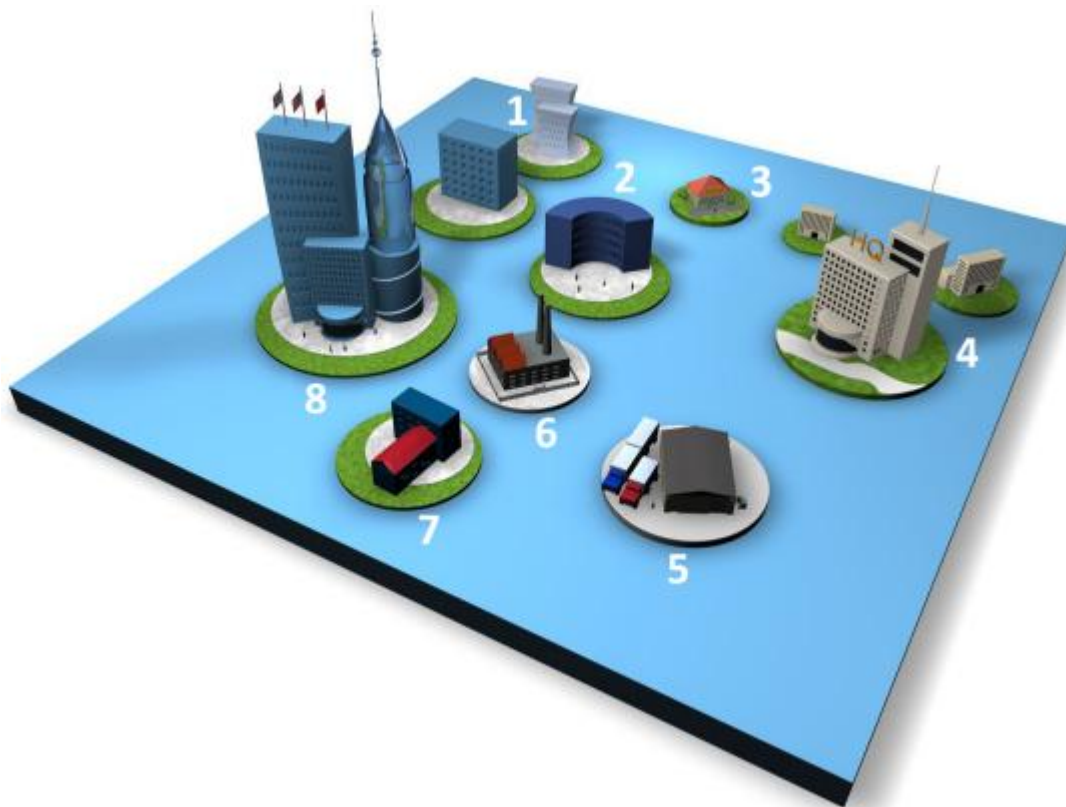
See [Manage Milestone Federated Architecture](#) (see "Milestone Federated Architecture Overview" on page 293) for more details.

Federated Sites Example Scenario—Limestone City

The following is an example of how several XProtect Corporate systems can be integrated into an MFA—in this case in a **City Surveillance** scenario.

Many surveillance integrators want to integrate several independent surveillance entities into a large scale system, where each site can still be used and managed locally and users and administrators can be given access to the entire large scale installation.

In this example, several governmental and business installations must be tied together in a large scale system offering the different entities local access and management of the system, as well as governmental (police etc.) access in case of crimes and emergencies.



1. Downtown Residential
2. City Hall - public places
3. Residential area shops
4. A.C.M.E Industries Inc & branch offices
5. Limestone Transportation Ltd.
6. MB Industries
7. Police Headquarters
8. Limestone Center Shopping Mall



All entities must be connected to the city's video surveillance so that City Hall officials and police officers can access video from their business or residential area to monitor live video or investigate recorded video in case of break-ins, thefts, vandalism, emergencies, terror etc.

In addition to being connected to the city's video surveillance, A.C.M.E Industries Inc, Downtown Residential and Limestone Center Shopping Mall also want to segment their installation in several sites as they have several physical locations that they want to monitor. The segmented architecture offers them greater flexibility during installation and daily usage.

The city uses MFA, allowing the entities independent video surveillance while being tied into the city wide surveillance system at the same time.

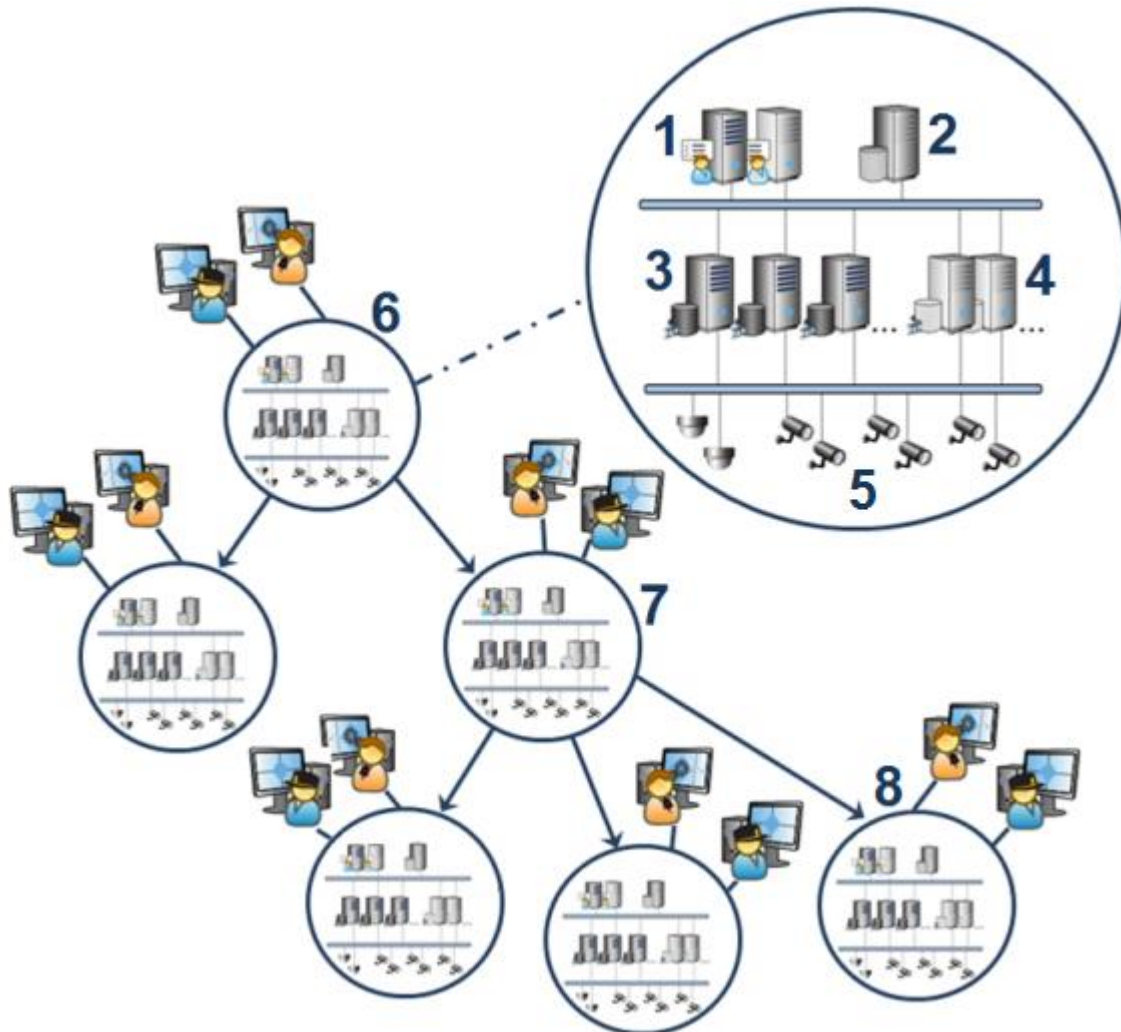
Because the police have installations that City Hall should not have access to, the Police Headquarters is selected as the top-site in the city's federated surveillance hierarchy.

Each site is then tied into Limestone city's federated hierarchy as follows:

- **Level 1:** Police Headquarters.
 - **Level 2:** Limestone City.
 - **Level 3:** City Hall and **MB Industries as one group.**
 - **Level 4:** Central Station, Streets & Intersections and Parks as one group under City Hall.
 - **Level 3:** Limestone Center Shopping, Downtown Residential, Limestone Transportation Ltd and A.C.M.E Industries Inc. as one group.
 - **Level 4:** Shops, Branch Malls and Residential area shops as one group under Limestone Center Shopping.
 - **Level 4:** Branch Office 1 and Branch Office 2 as one group under A.C.M.E Industries Inc.



Illustration of Milestone Federated Architecture



The idea behind Milestone Federated Architecture; parent and children linked as needed.

The contents of a federated site and parent/child setup:

1. Management Server and Failover Server
2. SQL Server
3. Recording Servers
4. Failover Recording Servers
5. Cameras
6. A Federated Site
7. Another Federated Site
8. Yet another Federated Site

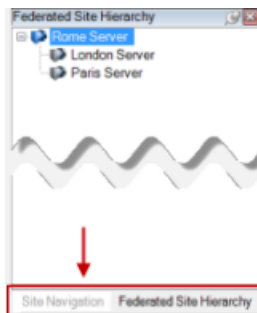


Etc.

Manage Milestone Federated Architecture

For conceptual details on Milestone Federated Architecture (MFA), see Milestone Federated Architecture Overview (on page 293).

The XProtect Corporate Management Client has a Federated Sites Hierarchy pane (see "Panels overview" on page 70) dedicated to displaying federated sites and their parent/child links. From the **View** Menu (see "Management Client menu overview" on page 75), you can show or hide the **Federated Sites Hierarchy** pane. The pane is located on the left side of the Management Client window, under the **Site Navigation** pane.



The parent server you are logged in to (your home-site), is always at the top of the site hierarchy. You can view all its linked children and downwards through the parent/child hierarchy. Settings and configurations of your home-site is always reflected in the **Overview** and **Properties** panes and its site-name visible at the top of the **Site Navigation** pane.

To connect to another site in the hierarchy (see "Connecting to Another Site in the Hierarchy" on page 305), click the wanted site in the **Federated Sites Hierarchy** pane.

What if I only have one server and don't run MFA? Your user interface looks the same, but when you view the **Federated Sites Hierarchy** pane you will only see the one server in your setup.

Federated Icons

There are a number of icons in MFA, each representing the different states a site can be in:

- Top-site in the entire hierarchy is operational:
- Top-site in the entire hierarchy is still operational but, one or more issues need attention: will be shown on top of the top-site icon.
- Normal site (not top-site) is operational:
- Normal site (not top-site) is still operational but, one or more issues need attention: will be shown on top of the normal-site icon.
- Site awaiting acceptance of inclusion in the hierarchy:
- Site being attaching, but not yet operating:

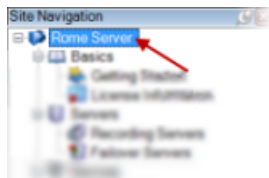


Expand/Collapse

You can expand and collapse a site in the **Site Navigation** pane, to see its children, if any.

Site Navigation Pane

The name, settings and configurations of the highlighted site (red arrow) are reflected in the **Site Navigation** pane.



Right-clicking is not Selecting!

Because you must be able to delete a site without being connected to it, **right-clicking a site does not select it**, but offers a context menu, which differs depending on where in the hierarchy you are. See Action Menu (see "Management Client menu overview" on page 75).

Context Menu

From the **Federated Site Hierarchy** pane, a context menu lets you add sites to a hierarchy, accept inclusion in a hierarchy, rename sites in a hierarchy, detach sites from hierarchy, work with site properties and refresh site hierarchy.

Due to the nature of federated sites, when the context menu is activated from a parent, you cannot accept inclusion in the hierarchy. And when it is activated from a child, it is not possible to refresh the site hierarchy.

Adding a Site to the Hierarchy

You can add children to both your home-site and to its children (when connected to them).

Prerequisites

To add a child to a parent in your hierarchy, one of the following two scenarios must be true:

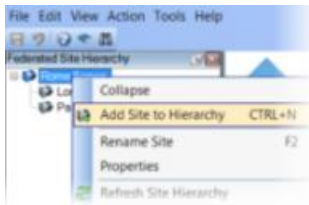
- The management server is installed as a **Network Service**: Before a parent/child link can be established without the acceptance from the administrator of the child, both computers involved (parent and child) must be added as a user to the other's XProtect Corporate administrator role. See Assign and Remove Users and Groups to/from Roles (on page 254).
- The management server is installed as a **user account**: This user account must be a member of the administrator group of the server being linked to before a parent/child link can be established without the acceptance from the administrator of the child.

If neither of these criteria are met, the administrator of the child needs to accept the request for inclusion in the hierarchy (see "Accepting Inclusion in the Hierarchy" on page 304) before the link can be established. See Milestone Federated Architecture Overview (on page 293) for more details.



To Add a Site to Hierarchy

1. In the **Management Client** window, in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), select the relevant site, right-click, and click **Add Site to Hierarchy**.



Tip: As an alternative to using the menu, press the CTRL+N keys on your keyboard.

2. Insert the URL of the requested child in the **Add Site to Hierarchy** window.
3. Click **OK**.
4. A link to the new child site is added to the **Federated Sites Hierarchy** pane.
5. If you can establish the new child link without requesting acceptance from the administrator (see **Prerequisites** described earlier), skip to step 7.

If **not**, the new child has the awaiting acceptance (see "Accepting Inclusion in the Hierarchy" on page 304)  icon and its administrator must authorize the request.

6. Make sure the child's administrator authorizes the link request (this is done from the child site).
7. The new parent/child link is established and the **Federated Sites Hierarchy** pane is updated with the  icon for the new child.

Due to synchronization issues, any changes made to children located far from your home-site might take some time to be reflected in the **Federated Sites Hierarchy** pane. See Basic Rules of Federated Sites (on page 295).

Accepting Inclusion in the Hierarchy

You must accept a child link request manually if your administrator settings require this.

- If the management server is installed as a **Network Service**: Computers involved must **not** be added as users to each other's XProtect Corporate administrator role, but should be added as another XProtect Corporate **non**-administrator role. See Assign and Remove Users and Groups to/from Roles (on page 254).
- If the management server is installed as a **user account**: This user account must **not** be a member of the administrator role of the server being linked to.

Otherwise inclusion will take place automatically.

See also Administrator Role and Federated Sites (see "The Administrator Role and Federated Sites" on page 296).

Prerequisites

The potential child must have received a link request from the potential parent. As a result, the child has the awaiting acceptance  icon.



To Accept Inclusion in a Hierarchy

1. In the Management Client window (of the potential child), in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), select the relevant site, right-click, and click Accept Inclusion in Hierarchy.
2. Click **Yes**.
3. The new parent/child link is established and the **Federated Sites Hierarchy** pane is updated with the normal site  icon for the selected site.

Due to synchronization issues, any changes made to children located far from your home-site might take some time to be reflected in the **Federated Sites Hierarchy** pane. See <FedArch Overview (see "Milestone Federated Architecture Overview" on page 293), **Basic Rules of Federated Sites, Synchronization of Hierarchy**.

Connecting to Another Site in the Hierarchy

You can connect to all sites in your MFA if your administrator settings are correct.

Prerequisites

To connect from one site in your hierarchy to another, one of the following two scenarios must be true:

- The management server is installed as a **Network Service**: Both computers involved must be added as users to each other's XProtect Corporate administrator role. See Assign and Remove Users and Groups to/from Roles (on page 254).
- The management server is installed as a **user account**: This user account must be a member of the administrator group of the server being linked to.

See Administrator Role and Federated Sites section (see "The Administrator Role and Federated Sites" on page 296).

To Connect to Another Site in Hierarchy

Simply click the wanted site in the Federated Site Hierarchy pane (see "Panels overview" on page 70). A brief dialog informs you that you are being connected to the new site. When connection is complete, your view in the **Federated Sites Hierarchy** pane will change to reflect that you are connected to a different site.

In this example, the user was logged into the home-site **Rome Server** and next connects to the child **Paris Server**:



Do I log out of my home-site when I connect to another site in the hierarchy? Both yes and no. Embedded in your home-site log-in is an automated and seamless log-in to its children as well, using the same credentials as your home-site log-in. However, even though you technically log out of your home-site when connecting to one of its children, you still see the world as your (former) home-site sees it.

Detaching a Site from the Hierarchy

Detaching/Removing a site from its hierarchy involves two different results **depending on where in the MFA you are located**.



If you are within your hierarchy-except your home-site-this will detach the selected site from the rest of the hierarchy. You will no longer be able to see the detached site.

If, on the other hand, you are located at your home-site, your home site will be detached from the rest of the hierarchy including any sites located under your home-site. Your home-site becomes the new top-site.

Detach Child from Hierarchy (Location: Any site)

Prerequisites

The site you are detaching is any site, **except** your home-site.

To Detach Child from a Hierarchy

1. In the Management Client window, in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), right-click the site you want to detach-**except** the home-site-select **Detach Site from Hierarchy**.
2. Click **Yes**.
3. The detached site is removed and the **Federated Sites Hierarchy** pane is updated.

Tip: You do not have to connect to a site to detach it. Just point your mouse to the relevant site and right click, select **Detach Site from Hierarchy**.

Detach Home-site from Parent Hierarchy (Location: Home-site, which has a parent)

Prerequisites

Your home-site must be the child of another site, i.e. have a parent.

To Detach Home-site from a Parent Hierarchy

1. In the **Management Client** window, in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), right-click the **home-site**, and click **Detach Site from Hierarchy**.
2. Click **Yes**.
3. The **Federated Sites Hierarchy** pane is updated, your home-site becomes the new top-site, and the normal site icon  changes to a top-site  icon.
4. Click **OK**.

Due to synchronization issues, changes might take a little time to be reflected in the **Federated Sites Hierarchy** pane. See Basic Rules of Federated Sites (on page 295).

Tip: As an alternative to using the menu to detach from hierarchy, press the DELETE key on your keyboard.

Refreshing the Site Hierarchy

Automatic synchronizations happen regularly through all steps of your parent/child setup. But if you want a current overview of things, and do not want to wait for the next automatic synchronization, you can refresh.

When refreshing, the home-site will display a current overview of the state of things from the home-site's point-of-view.

Note that only changes saved by the home-site since the last synchronization will be reflected—changes further down in the hierarchy will not be reflected. For this, a full scheduled synchronization is needed.

1. In the **Management Client** window, in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), right-click the home-site, and click select **Refresh Site Hierarchy**.



2. The **Federated Sites Hierarchy** pane is refreshed, reflecting any changes.

It is not possible to schedule your own synchronizations.

Renaming a Site

You can rename both your home-site and its children when connected to them.

1. In the Management Client, in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), select the relevant site, right-click, and click **Rename Site**.

Tip: As an alternative to using the menu, press the F2 key on your keyboard.

2. You can now overwrite the name of the site.
3. The **Federated Sites Hierarchy** pane is updated, reflecting the name-change.

Due to synchronization issues, any changes to remote children might take some time to be reflected in the Federated Sites Hierarchy pane. See Basic Rules of Federated Sites (on page 295).

Setting the Site Properties

You can view and, possibly, edit properties on your home-site and its children.

1. In the Management Client, in the Federated Sites Hierarchy pane (see "Panels overview" on page 70), select the relevant site, right-click, and select **Properties**.

2. If needed, change the following:

General Tab

Information related to the site you are currently connected to:

- **Name:** Enter the name of the site displayed in the Federated Sites Hierarchy pane (see "Panels overview" on page 70) and the **Site Navigation** pane.
- **Description:** Enter a description of the site.
- **URLs:** Use the list to add and remove URL(s) for this site and indicate whether they are external or not.



- **Version:** Version number of the site/management server.
- **Service account:** The service account under which the management server is running.
- **Time for last synchronization:** Last synchronization date.
- **Status for last synchronization:** Status of last synchronization. It can be either **Successful** or **Failed**. If failed, further information is offered.

Click **OK** to save changes.

Parent Site Tab (available on child sites only—marked in red)

Non-editable information regarding the parent of the child you are currently connected to:

- **Name:** Shows the name of the parent to be displayed in the Federated Sites Hierarchy pane (see "Panels overview" on page 70) and **Site Navigation** pane.
- **Description:** Shows a description of the parent.
- **URLs:** Lists URL(s) for this parent and indicates whether they are external or not.
- **Version:** Version number of the site/management server.
- **Service account:** The service account under which the management server is running.
- **Time for last synchronization:** Last synchronization date.
- **Status for last synchronization:** Status of last synchronization. It can be either **Successful** or **Failed**. If failed, further information is offered.

Due to synchronization issues, any changes made to remote children might take some time to be reflected in the **Site Navigation** pane. See Basic Rules of Federated Sites (on page 295).



Backup, restore and move system configuration

Scheduled Backup & Restore of System Configuration

Regularly backing up your XProtect Corporate database is always recommended—especially if you have a larger XProtect Corporate setup. Having a scheduled regular backup provides you with an always up to date backup. In case of a disaster recovery scenario, regular backups limit your loss of data to what was changed since last backup. Furthermore, it offers you the ability to quickly restore your XProtect Corporate configuration. However, regularly backing up also has the added benefit that it flushes your Microsoft SQL Server's transaction log.

If you have a smaller XProtect Corporate setup and do not feel the need for regular scheduled backup, see Manual Backup & Restore of System Configuration (on page 311).

The management server stores your XProtect Corporate system's configuration in a database. When backing up/restoring management server(s), make sure that this database is included in the backup/restore.

Flushing the SQL Server Transaction Log

What Is the SQL Server Transaction Log and Why Does It Need to Be Flushed? Each time a change in the XProtect Corporate data occurs, the SQL Server will 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. The SQL Server by default stores its transaction log indefinitely, and therefore the transaction log will over time 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 just grows and grows, it may in the end prevent Windows from running properly. Flushing the SQL Server's transaction log from time to time is thus a good idea; flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. XProtect Corporate 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 numerous articles on this topic, go to support.microsoft.com (see <http://support.microsoft.com/> - <http://support.microsoft.com/>) and search for SQL Server transaction log.

Prerequisites

SQL Server Express Edition users only: Microsoft® SQL Server Management Studio Express, a tool downloadable for free from www.microsoft.com/downloads (see <http://www.microsoft.com/downloads> - <http://www.microsoft.com/downloads>). Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your management server.

Scheduled Back Up of System Configuration

1. Open Microsoft SQL Server Management Studio Express from Windows' **Start** menu by selecting **All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio Express**.
2. In the tool do the following:
3. When connecting, specify the name of the required SQL Server. Use the account under which the database was created.



- Find the **Surveillance** database, containing your entire XProtect Corporate system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.

No Surveillance database? Surveillance is the default name of the database containing the system configuration. If you can find the database, but it is not called Surveillance, it could be because you gave the database another name during the management server installation.

View example... We will assume that the database uses the default name.



Example: During management server installation it is possible to change the database name from the default name Surveillance to another name

- 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**.

4. Follow the instructions in the tool to the end.

Tip: Also consider backing up the **SurveillanceLog** database, 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.

Backing Up Log Server Database

Handle the **SurveillanceLogServer** database using the same method as when handling system configuration described earlier in this topic. The **SurveillanceLogServer** database (name may be different if you renamed the system configuration database) contains all your XProtect Corporate system logs, including errors reported by recording servers and cameras.



The database is located where the Log Server Service is installed, typically the same place as your management 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.

Restoring System Configuration (From Scheduled Back Up)

Prerequisite: To prevent configurational changes being made while you restore the system configuration database, stop the:

- Management Server Service (see "Management Server Service and Recording Server Service" on page 330)
- 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) (see [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx) - [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx)).

Open Microsoft SQL Server Management Studio Express from Windows' **Start** menu by selecting **All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio Express**.

1. In the tool do the following:
 - When connecting, specify the name of the required SQL Server. Use the account under which the database was created.
 - Find the **Surveillance** database, containing your entire XProtect Corporate system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.
 - 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**.
2. Follow the instructions in the tool to the end.

If you also backed up the **SurveillanceLog** database from the old management server, restore it on the new management server using the same method.

Note that XProtect Corporate basically will not work while the Management Server Service (see "Management Server Service and Recording Server Service" on page 330) is stopped; it is thus important to remember to start the services again once you have finished restoring the database.

Manual Backup & Restore of System Configuration

Backing up your XProtect Corporate database is always recommended. In case of a disaster recovery scenario this offers you the ability to quickly restore your XProtect Corporate configuration. Furthermore, being able to easily do a manual backup of your entire system configuration via your Management Client (no need for third-party tools) offers you flexibility, security and full control of your configuration.



The type of backup described in this topic is best suited if you have a smaller XProtect Corporate setup and wish to do a one-time, non-scheduled backup. Besides manual backups, it is strongly recommended to also configure regular, scheduled system backups (see "Scheduled Backup & Restore of System Configuration" on page 309)—especially if you run a larger XProtect Corporate setup.

What is included in this type of backup and what is not? With the exception of logs, this backup type includes your full system configuration; client views, event server configuration and configuration of any Milestone published MIP plug-ins.

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

Manual Back Up of System Configuration

Important information:

- Your XProtect Corporate system stays online
- A backup cannot be used for copying configurations to other XProtect Corporate installations, see Move System Configuration to New Management Server (on page 313) for details on this.
- Depending on your XProtect Corporate configuration, your hardware, and on whether your SQL server, management server and Management Client are installed on the same machine or not, backing up configuration might take some time.
- Logs (including Audit logs (see "Manage Logs" on page 267)) are **not** part of the configuration backup.

Backing up:

All relevant XProtect Corporate configuration files will be combined into one single .cnf file, which is saved at a specified location.

1. From the Management Client's menu bar, select **File, Backup Configuration....**
2. Next, you are presented with an important note. Read the contents of the note. Click **Backup**.
3. In the file save dialog, browse to the location where you want to store the configuration backup. Specify a suitable file name, and click **Save**.
4. Let the **Backup Configuration** window finish. Click **Close**. Your backup is finished.



Restoring System Configuration (From Manual Back Up)

Important information:

- Both the user installing and the user doing the restore must be local administrator on the management server **and** on the SQL server.
- Except for your recording servers, XProtect Corporate will be completely shut down for the duration of the restore, which might take some time.
- A backup can only be restored on the XProtect Corporate installation where it was created. Furthermore, 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, it **will** be possible to start the old configuration again (since no change have been committed).
If restoring fails elsewhere in the process, rolling back to the old configuration is impossible.
As long as the backup file is not corrupted, it **will** however be possible to do another restore.
- Restoring replaces the current configuration. This means that any configurational changes since last backup is lost.
- No logs (including Audit logs (see "Manage Logs" on page 267)) are restored
- Once restoring has started, it cannot be canceled.

Restoring:

1. Right-click the notification area's Management Server service icon and select **Restore Configuration....**
2. Next, you are presented with an important note. Read the contents of the note. Click **Restore**.
3. In the file open dialog, browse to the location of the configuration backup file, select it, and click **Open**.
4. The **Restore Configuration** window will now run, showing progress and status information. Wait for it to finish and click **Close**. Your restore is finished.

Back Up/Restore Fail & Problem Scenarios

Problem: The event server or other registered services (log server, etc.) have been moved after the system configuration was backed up.

Solution: The user must choose which registered service configuration they want for the new system. In this case, it is actually possible to keep the new configuration after the system is restored to the old version. Choose by looking at the host names of the services.

Problem: If the event server is not located in the specified destination (for instance if the old registered service setup is chosen) the restore will fail.

Solution: Do another restore.

Move System Configuration to New Management Server

It can sometimes be necessary to move the XProtect Corporate management server installation from one physical server to another. The management server stores your XProtect Corporate's 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 XProtect Corporate system's configuration in a database on an existing SQL 2005 or 2008 Server on your network, you can simply 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 will connect to the hostname and IP address of the old management server. In case the new management server has been given a new hostname and/or IP address, the recording server will not be able to find the management server. Manually stop each recording server in your system, change their management server URL, and when done, restart them.

- **SQL Server Express Edition:** If you are storing your XProtect Corporate system's configuration in a SQL Server Express Edition 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 will avoid have to reconfigure your cameras, rules, time profiles, etc. after the move.

Some of this prerequisite information is only relevant for users of SQL Server Express Edition. **If you use any other SQL setup, ask your IT department for backup details.**

Prerequisites

- **Your XProtect Corporate software installation file for installation on the new management server.**
- **Your initial license (.lic) file**, i.e. the one you used when initially installing XProtect Corporate, not the .lic file which is the result of your license activation (see "Activate Licenses" on page 81). 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 XProtect Corporate software in connection with the move, you will have received a new initial .lic file together with your new Software License Code (SLC).
- **SQL Server Express Edition users only: Microsoft® SQL Server Management Studio Express**, a tool downloadable for free from www.microsoft.com/downloads. Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your existing management server **and** on the server which will be your future management server (you will need it for the entire copy process (backup as well as restoration)).

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 will connect to the hostname and IP address of the old management server. In case the new management server has been given a new hostname and/or IP address, the recording server will not be able to find the management server. Manually stop each recording server in your system, change their management server URL, and when done, restart them.

Moving System Configuration:

Moving your system configuration is in reality a three step process:

1. First you make a copy of your system configuration (identical to making a scheduled backup (see "Scheduled Backup & Restore of System Configuration" on page 309))



2. Then you install the new management server on the new server (see scheduled backup (see "Scheduled Backup & Restore of System Configuration" on page 309), step 2)
3. And finally you copy/restore your system configuration to the new system (see how to restore a scheduled backup (see "Scheduled Backup & Restore of System Configuration" on page 309))

Copying System Configuration from Old Server (Step 1)

Prerequisite: Stop the Management Server service (see "Management Server Service and Recording Server Service" on page 330) to prevent configuration changes being made. This is important since any changes made to the XProtect Corporate configuration, between the time you create a copy and the time you restore it on your new management server, will be lost. If changes are made after the copy was made, you will have to make a new copy.

Note that XProtect Corporate basically will not work while the Management Server service (see "Management Server Service and Recording Server Service" on page 330) is stopped; it is thus important to remember to start the service again once you have finished backing up the database.

Since first part of a copy is in reality identical to a scheduled backup, see Scheduled Back Up of XProtect Corporate System Configuration section (see "Scheduled Backup & Restore of System Configuration" on page 309), steps 1-3.

What Happens while the Management Server Is Unavailable?

- **Recording servers will still be able to record:** Any currently working recording servers will have received a copy of their configuration from the management server, so they will be able to work and store recordings on their own while the management server is down. Scheduled and motion-triggered recording will therefore work, and event-triggered recording will also work unless based on events related to the management server or any other recording server since these go through the management server.
- **Recording servers will temporarily store log data locally:** They will automatically send log data to the management server when the it becomes available again.
 - **Clients will not be able to log in:** Client access is authorized through the management server. Without the management server, clients will not be able to log in.
 - **Already logged in clients can remain logged in for up to an 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 will not be affected.
 - **No ability to configure the system:** Without the management server, you will not be able to change system configuration.

Even though some users might not experience loss of contact, we recommend that you inform your users about the risk of losing contact with the surveillance system while the management server is down.

Copying Log Server Database

Handle the **SurveillanceLogServer** database using the same method as when handling system configuration described earlier in this topic. The **SurveillanceLogServer** database (name may be different if you renamed the system configuration database) contains all your XProtect Corporate system logs, including errors reported by recording servers and cameras.

The database is located where the Log Server Service is installed, typically the same place as your management 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.



Installing New Management Server on New Server (Step 2)

Installing a management server (see "Install management server" on page 28) is divided into three steps. During step 2 of the installation on your new management server, make sure you select **Create a new database** for the system configuration database, even though you have a backup of the database from your old management server.

Next (see "Copying/Restoring System Configuration to New Server (Step 3)" on page 316), we must overwrite the new and empty database by restoring the backup we just created. Since we are going to overwrite the new and empty database, it is important that it has the same name as the backed-up database (if your backed-up database has the default name Surveillance, just use the default name **Surveillance** when creating the new database too).

The password for the database is not significant in this backup/restore context, but we recommend that you just use the default setting **Allow server to control password**.

Copying/Restoring System Configuration to New Server (Step 3)

Prerequisite: To prevent configurational changes being made while you restore the system configuration database, stop the:

- Management Server Service (see "Management Server Service and Recording Server Service" on page 330)
- 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) (see [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx) - [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx)).

This should all be done to the **new** management server.

Since second part of a copy is in reality identical to a restore, see Restoring XProtect Corporate System Configuration (From Scheduled Back Up) (see "Restoring System Configuration (From Manual Back Up)" on page 313), steps 1-2 and rest of the topic for details.



Device drivers

Manage and Remove Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to a recording server. The video device drivers should therefore be installed on each recording server on your XProtect Corporate system.

Video device drivers are installed automatically during the initial installation of your XProtect Corporate system. However, new versions of video device drivers are released and made available on the Milestone website (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) from time to time.

Making New Video Device Driver Versions Available for Installation

The latest version of video device drivers is available for download from www.milestonesys.com (http://www.milestonesys.com/SharePoint/XProtectEnterprise/8_0/ReleaseNotes/XPE8_Release_Notes.pdf) or from your XProtect Corporate vendor.

Once you have downloaded the latest version of video device drivers, you are able to make the latest version available for download to recording servers through the Download Manager (see "Use Download Manager" on page 60).

Installing Video Device Drivers

1. On the computer running the recording server, shut down any Milestone software, including the Recording Server service.
2. With an Internet Explorer browser, connect to the XProtect Corporate management server at the following address:

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

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

This will open the management server's web page. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.

3. On the web page, click the required video device drivers link.

Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking **Run** or similar (exact button text depends on your browser version).

4. Select required language, and click **OK**. This will open the **Video Device Driver Setup** wizard, which will guide you through the installation.
5. On the wizard's first step, click **Next**.
6. On the wizard's second step, an installation path is automatically suggested. Click **Next**.
7. On the wizard's third step, select **Device drivers for XProtect Corporate systems** from the menu, and click **Next**.



8. The wizard is now ready to install the video device drivers. Click **Install** to complete the installation of the video device drivers.
9. When ready, start the Recording Server service again.

After restarting the Recording Server service, it might take several minutes for your hardware devices to make contact with the new drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Removing Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to a recording server. When the video device drivers are removed, communication between the recording server and the camera devices will no longer be possible.

To remove video device drivers — typically prior to installing a later version of the drivers — use the following procedure on the recording server computer on which the video device drivers are installed:

1. Open Windows' **Control Panel**, and select **Add or Remove Programs**. This will open the **Add or Remove Programs** window.
2. In the **Add or Remove Programs** window, select the **Video Device Driver Vx.x** entry (where x.x indicates the relevant version number), and click **Uninstall**.
3. You will be asked to confirm that you want to remove the video device drivers. Click **OK** to remove them.



Failover servers

Failover Server Service Administration

When you have installed a failover server, you are able to check the state of the Failover Server service by looking at the Failover Server service icon in the notification area **of the computer running the failover server**. The notification area icon also lets you start and stop the Failover Server service, view status messages, etc.

Tip: The notification area is occasionally also known as the **system tray**, it is located at the far right of the management server computer's Windows taskbar.



Example: Failover Server service icon in notification area; note that failover servers also have a Recording Server service (other icon)

While the Failover Server service is stopped, the failover server will not be able to take over from regular recording servers.

Starting and Stopping the Failover Server Service

The Failover Server service starts automatically. If you have stopped the service manually, you can start and stop it the following way:

1. Right-click the notification area's failover server icon.
2. From the menu that appears, select **Start Failover Server Service** or **Stop Failover Server Service**, depending on your needs.

Changing the Management Server Address

The failover server must be able to communicate with your XProtect Corporate system's management server. You therefore specify the IP address/hostname of the management server during the installation of the failover server.

Should you later need to change the address of the management server, you do it the following way:

In order to be able to change the management server address, the Failover Server service must be stopped.

1. Stop the Failover Server Service (see Starting and Stopping the Failover Server Service (on page 319)).
2. Right-click the notification area's Failover Server service icon again.
3. From the menu that appears, select **Change Settings...** The **Failover Recording Server Settings** window appears. You are able to change the following setting:
 - o **Management server hostname / IP address:** Lets you specify the IP address (example: 123.123.123.123) or host name (example: ourserver) of the XProtect Corporate management server with which the failover server should be able to communicate.

Viewing Status Messages

1. Right-click the notification area's **Milestone Failover Server Service** icon.



- From the menu that appears, select **Show Status Messages**. The **Failover Recording Server Status Messages** window appears, listing time-stamped status messages.

Viewing Version Information

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

- Right-click the notification area's **Milestone Failover Server Service** icon.
- From the menu that appears, select **About...**
- A small dialog opens. The dialog will show the exact version of your **Failover Server Service**.

Read Failover Server Service State Icons

The following icons represent the states of the Failover Server Service:

Failover Server Service Icon	Description
	Failover Server is enabled and started. The failover server is running and able to take over from regular recording servers.
	Failover Server is stopped. The failover server is stopped and no longer taking over from regular recording servers.
	Failover Server is starting. The Failover Server Service is in the process of starting. Under normal circumstances, the icon will after a short while change to Failover Server Service is enabled and started .
	Failover Server is disabled or running offline. Typically appears if: - the failover server is not enabled through the Management Client; see Manage Failover Servers (on page 321). - the Failover Server Service is running but the Management Server Service is not. - the failover server's information about the management server address is incorrect; see Changing the Management Server Address (on page 319). - the user account under which the Failover Server Service runs has no access to your XProtect Corporate system. How to troubleshoot this...

During installation of the failover server, you specified a user account under which the **Failover Server Service** should run. For the failover server to work, it is important that the user account in question has access to your XProtect Corporate system with administrator rights.

To verify whether the user account has access to your XProtect Corporate system, do the following:



1. In the Management Client's Site Navigation pane (see "Panels overview" on page 70), expand **Security** and select **Roles**.
2. In the Overview pane (see "Panels overview" on page 70)'s roles list, select the **Administrators** role.
3. In the Properties pane (see "Panels overview" on page 70)'s role settings list, verify that the required user is listed.

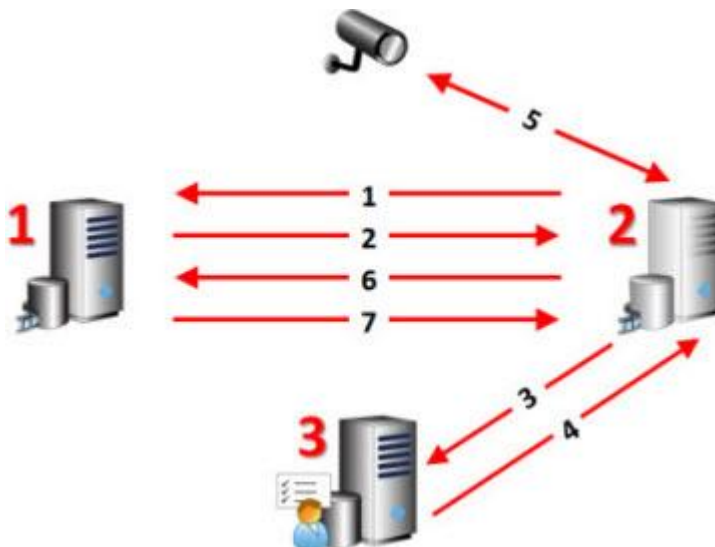
If the user is not listed, add the required user to the **Administrators** role by clicking the **Add...** button below the role settings list. For more information, see Assign Users & Groups to/from Roles (see "Assign and Remove Users and Groups to/from Roles" on page 254).

Manage Failover Servers

A failover server is a spare recording server which can take over if a regular recording server becomes unavailable. It should therefore always be installed on a separate computer. A failover server has two services:

- A Failover Server Service, which handles the processes of taking over from the regular recording server. By default, this service is always running since it constantly checks the state of relevant recording servers.
- A Recording Server Service, which enables the failover server to act as a recording server while the regular recording server is unavailable. This service is only started when required, i.e. when the failover server should take over from the regular recording server. Starting this service typically takes a couple of seconds, but may take longer depending on local security settings, etc.

A failover server **must** be able to communicate with all cameras of the recording server(s) from which it should be able to take over.



The above illustrates the failover setup:

Involved Servers:

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



Failover Steps:

1. To check whether it is running or not, failover server has a non-stop TCP connection to a recording server.
2. This connection is interrupted, i.e. the recording server is not running.
3. From the management server, the failover server requests the current configuration of the recording server.
4. The management server sends the requested configuration and the failover server starts recording instead of the recording server.
5. The failover server and the relevant camera(s) exchange video data.
6. The failover server continually tries to re-establish connection to the recording server.
7. When the connection to the recording server is reestablished, the failover server shuts down and the recording server fetches video data (if any) recorded during its down-time.

Installing Failover Servers

For information about installing failover servers, see Recording Servers (on page 36).

Adding and Grouping Failover Servers

Failover servers are installed through an installation wizard, just like regular recording servers; see Installing Failover Servers (on page 322).

Overview of Failover Servers in Management Client

Once failover servers are installed, they become visible in the Management Client: In the Site Navigation pane (see "Panels overview" on page 70), select **Servers**, then **Failover Servers** and view a list of installed failover servers in the Overview pane (see "Panels overview" on page 70).

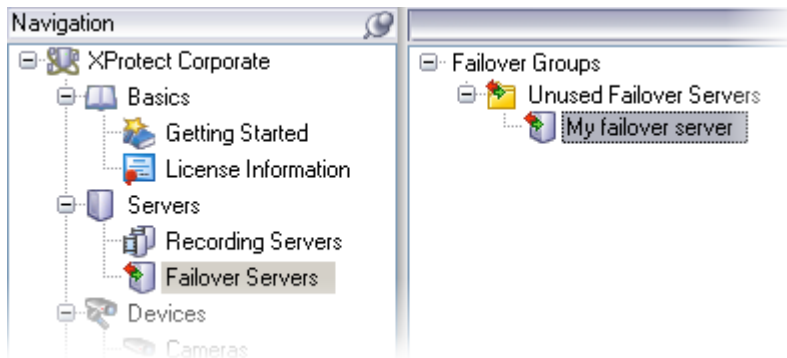
Tip: If a failover server does not become visible in the Management Client, verify that the failover server has been configured with the correct IP address/hostname of the management server. Also verify that the user account under which the Failover Server Service runs has access to your XProtect Corporate system with administrator rights.

Failover Servers Are Grouped

Failover servers are always grouped; a group can contain one or more failover servers. Grouping has a clear benefit: When you later specify which failover servers should be able to take over from a recording server, you do not select a particular failover server; rather you select a group of failover servers. If the selected group contains more than one failover server, this gives you the security of being able to have more than just one failover server ready to take over if the recording server becomes unavailable.



Initially, your failover servers will all appear in the group **Unused Failover Servers**.



A red x on a failover server icon indicates that the failover server in question is currently not in use.

Creating Failover Groups

You can create as many new failover groups as required: In the Overview pane, right-click **Failover Groups** and select **Add Group** from the menu that appears:



Specify a name and a description (optional) of your new group, then click **OK**.

Adding Failover Servers to a Group

In the Overview pane, right-click the group to which you want to add one or more failover servers, then select **Edit Group Members** from the menu that appears. This will open the **Select Group Members** window. From the **Available** box in window's left side, select the required failover server(s), then click **Add** to move the selected failover server(s) to the **Selected** box in the right side of the window:



Tip: Alternatively, drag and drop failover servers between the two boxes.

When ready, click **OK**. The required failover servers now belong to the group:





A failover server can only be a member of one group at a time.

Editing Failover Group Properties

Select the required failover group in the Overview pane.

- On the **Info** tab, you can edit the name and description of the selected failover group.
- On the **Sequence** tab, you can edit the sequence in which failover servers within the group should take over from unavailable recording servers.

Enabling Failover Servers

A failover server must be enabled before it will be able to take over from regular recording servers:

1. In the Overview pane (see "Panels overview" on page 70), select the required failover server.



2. In the Properties pane (see "Panels overview" on page 70), select **Enable this failover server**.

Editing Failover Server properties

1. In the Overview pane, select the required failover server.





2. On the **Info** tab in the Properties pane, you are able to edit the following:

The screenshot shows a 'Properties' dialog box with the 'Info' tab selected. The 'Failover server information' section contains the following fields:

- Name:** Failover Server 1
- Description:** (Empty text area)
- Host name:** sysone
- UDP port:** 8844
- Database location:** C:\MediaDatabase
- ☒ **Enable this failover server**

- **Name:** Name of the failover server, as it will appear in the Management Client, in logs, etc.
- **Description:** Optional description of the failover server, for example a description of the server's physical location.
- **Host name:** Non-editable field displaying the network address of the failover server.
- **UDP port:** The port number used for communication between failover servers. By default, port 8844 is used.

Tip: The port used by the failover server to keep a non-stop TCP connection to recording servers, is by default port number 11000. If required, you can change that port number on the recording server's **Failover** tab.

- **Database location:** This field specifies the path to the database which the failover server should use for storing recordings while taking over from a regular recording server. When the regular recording server becomes available again, recordings stored by the failover server will be transferred to the regular recording server, and merged with recordings there.

The database path cannot be changed while the failover server is taking over from a regular recording server. Changes you make will be applied when the failover server is no longer taking over from a regular recording server.

- **Enable this failover server:** A failover server must be enabled before it will be able to take over from regular recording servers. Select box to enable the failover server, clear box to disable it.

IMPORTANT: A disabled failover server will not be able to take over from regular recording servers.

3. On the **Network** tab, you are able to define the failover server's public IP address, etc. This is relevant especially if using NAT (Network Address Translation) and port forwarding. See the description of a regular recording server's **Network** tab (see "Manage Public Addresses" on page 122) for more information.
4. In the toolbar (see "Management Client Overview" on page 66), click **Save**.



Assigning Failover Servers to Recording Servers

In the Management Client, you select a recording server, then use the **Failover** tab (see "Failover Tab (Recording Server Properties)" on page 111) to specify which failover group(s) should take over from the recording server in question. On the **Failover** tab, you even have the flexibility of being able to assign a primary and a secondary failover group to each recording server.

Frequently Asked Questions

How does a failover server know when to take over? It polls (i.e. regularly check the state of) relevant recording servers every 0.5 seconds. If a recording server does not reply within 5 seconds after it was polled, the recording server is considered unavailable and the failover server takes over.

How long does it take for a failover server to take over? It takes 5 seconds plus the time it takes for the failover server's Recording Server Service to start. During this period it will not be possible to store recordings, neither will it be possible to view live video from affected cameras.

What happens when a recording server becomes available again? When it becomes available again, it will automatically take over from the failover server, and recordings stored by the failover server will automatically be merged into the regular recording server's databases.

How long the merging process takes will depend on the amount of recordings to merge, on network capacity, etc.

During the merging process, it will not be possible to browse recordings from the period during which the failover server took over.

What if the failover server must take over from another recording server during the merging process? In that case, it will postpone the merging process with recording server A, and take over from recording server B. When recording server B becomes available again, the failover server will take up the merging process with recording server A, after which it will begin merging with recording server B.

Will I lose recordings? A failover solution does not provide complete redundancy. It is, however, a very reliable way of minimizing downtime.

When the regular recording server becomes available again, the Failover Server Service will make sure that the recording server is ready to store recordings again. Only then is the responsibility for storing recordings handed back to the regular recording server. Thus, loss of recordings at this stage of the process is negligible.

How will clients experience failover? Clients should hardly notice that a failover server is taking over, although there will be a short period—usually only some seconds—with no access to video from the affected recording server while the failover server is taking over.

Clients will be able to view live video as soon as the failover server has taken over.

Clients will be able to play back recent recordings, i.e. recordings from after the failover server took over, since those recordings will be stored on the failover server. Clients will not be able to 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 server.

Clients will, however, be able to access **archived** (see "About Storage and Archiving" on page 101) recordings stored at accessible locations, such as on available network drives, but clients will not be able to access archived recordings stored at inaccessible locations, such as on the unavailable recording server itself or on an unavailable network drive.

When the recording server is functioning again, there will usually be a merging process during which recordings made by the failover server are merged back into the recording server's database. During that merging process, clients will not be able to play back recordings from the period during which the failover server took over.

Is there a failover solution for failover servers? Setting up one failover server as backup for another failover server is not necessary. This is because you do not allocate particular failover servers to take over from a regular recording server; rather you allocate failover groups.

A failover group must contain at least one failover server, but you can add as many failover servers as required to a failover group. Provided a failover group contains more than one failover server, there will be more than one failover server capable of taking over from the regular recording server.



For more information about selecting the failover groups you require for a recording server, see the description of the Management Client's Failover tab (see "Failover Tab (Recording Server Properties)" on page 111).

Will archiving work while a failover server has taken over? Any archiving (see "About Storage and Archiving" on page 101) will work even when a failover server has taken over from a regular recording server, provided the archiving destination is on a network location accessible by the failover server.

If the archiving destination is inaccessible—such as on the unavailable recording server itself or on an unavailable network drive—archiving will not work as long as the destination is unavailable.

Failover-Related Events

XProtect Corporate features two failover-related events, **Failover Started** and **Failover Stopped**, which you can use when creating rules (see "Manage Rules" on page 221). The two events are further described in the Events Overview (on page 216).



Map

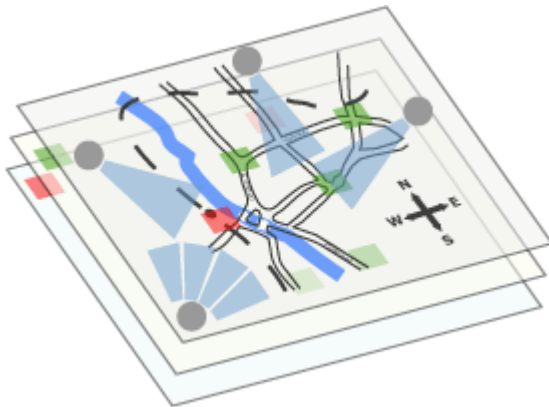
About maps

IMPORTANT: This feature will not work if you do not have the XProtect event server installed.

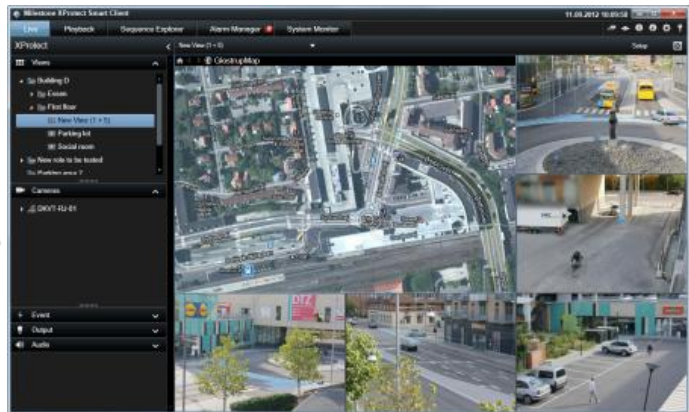
Except from installing the Event Server Service, which is a **prerequisite** for viewing and operating maps in the XProtect Smart Client, all user interaction with maps, including adding and maintenance, takes place in the XProtect Smart Client.

With maps, you get a physical overview of your surveillance system. Which cameras are placed where, and in what direction are they pointing? Maps can be used for navigation from large perspectives to small perspectives, and vice versa and a state map can have hot zones pointing to more detailed maps of cities, neighborhoods, streets, floor plans, etc. For detailed information, see the XProtect Smart Client documentation.

Can I access maps from the old XProtect map server? Maps located on your old XProtect map server is automatically accessible from your new XProtect event server, where maps are located from XProtect Corporate 4.0 and forward.



Example: Hierarchy of maps



Example: Map in XProtect Smart Client

As indicated, the Event Server Service must be installed on XProtect Corporate to handle maps in XProtect Smart Client. The event server is installed as part of the Management Server Installation (see "Install management server" on page 28), when the management server is installed with the **Typical** option. The service does not necessarily have to be installed on the management server—in fact, you can often achieve better performance by installing the Event Server Service on another server.

Administrators get the Event Server Service through the web page generated by the Download Manager (see "Use Download Manager" on page 60). This fact lets you install the Event Server Service anywhere.

Once installed, the Event Server Service is able to register itself automatically with XProtect Corporate (i.e. it automatically becomes listed by the Registered Services (see "Manage Registered Services" on page 283) feature in the Management Client). The location of the Event Server Service is thus known by XProtect Corporate, and clients logging into XProtect Corporate are thus automatically able to benefit from the Event Server Service as well.

However, if you later change the IP address or hostname of the server running the Event Server Service, you must manually edit the information under **Tools > Registered Services...** in the Management Client.

Also, if you later need to change the user under which the Event Server Service was installed, you must remove the Event Server Service and subsequently install it again under the new user.

Note that removing the Event Server Service will not in itself remove the Map configuration made through the XProtect Smart Client.



Database corruption

Protect Databases from Corruption

If a recording server's databases become corrupted, the recording server is in many cases able to repair the corrupt databases. While the ability to repair corrupt databases is highly valuable, it is of course even better to take steps to ensure that your databases do not become corrupted:

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 assessing your needs, however, do bear in mind the amount of runtime you will 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.

Windows Task Manager: Be Careful when Ending Processes

When working 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 in question will not be given the chance to save its state or data before it is terminated. This may in turn lead to corrupt camera databases.

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

Hard Disk Failure: Protect Your Drives

Hard disk drives are mechanical devices, and as such they 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 a UPS; see more information in the previous)
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water, etc. (avoid)



Services administration

About the Service Channel

The XProtect service channel enables automatic and transparent configuration communication between servers and clients in your XProtect Corporate. For example, it is the service channel that enables the fact that if a shared view is changed on one client, the change is immediately reflected on other clients using the shared view in question. 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 XProtect Corporate.

The service channel is typically installed as part of the management server installation, where it is an installation option towards the end of the management server installation process. It typically resides on the management server computer, but if required you may just as well install it on another server in your surveillance system. For installation information, see Service Channel Installation (see "Install the Service Channel" on page 42).

Once installed, the service channel is able to register itself automatically with XProtect Corporate (meaning that it automatically becomes listed by the Registered Services (see "Manage Registered Services" on page 283) feature in the Management Client). Its location is thus known by XProtect Corporate, and clients logging into XProtect Corporate are automatically able to 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 subsequently install it again under the new user.

It is important that XProtect Smart Client s are time-synchronized with the computer running the Service Channel service (see "Servers and Clients Require Time-Synchronization" on page 123); 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 the XProtect Smart Client. This means that users risk overwriting each others' configuration changes. If XProtect Smart Clients are not time-synchronized with the computer running the Service Channel service, you will see an error informing you of this.

Management Server Service and Recording Server Service

When the XProtect Corporate management server software is installed, you are able to check the state of the Management Server Service by looking at the **Management Server Service** icon in the notification area **of the computer running the management server**.

Likewise, when the XProtect Corporate recording server software is installed, you are able to check the state of the Recording Server Service by looking at the **Recording Server Service** icon in the notification area of the computer running the recording server in question.

The notification area icon also lets you start and stop the Management Server Service/Recording Server Service, view status messages, etc.

Tip: The notification area is also known as the **system tray**. It is located at the far right of the management / recording server's Windows taskbar.

IMPORTANT: When the **Recording Server Service** is running, it is **very** important that neither Windows Explorer nor other programs are accessing Media Database files or folders associated with your XProtect Corporate surveillance setup. Otherwise, the recording server might not be able to rename or move relevant media files. Unfortunately, this might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server Service, close the program accessing the media file(s) or folder(s) in question, and simply restart the Recording Server Service.



Example: **Management Server Service** and **Recording Server Service** icons in notification area

Accessing the Server Service

1. Right-click the notification area's Server Service icon.
2. From the menu that appears, depending on server type, select the needed icon.

If using multiple instances (see "Multiple recording server instances" on page 50) of the Recording Server Service, a sub-menu lets you select whether you want to start a particular instance or all instances.

Starting the Server Service

1. See Accessing the Server Service (on page 331).
2. Select either **Start Management Server Service** or **Start Recording Server Service**.

Stopping the Server Service

While the recording server service is stopped, XProtect Corporate will not be able to interact with devices connected to the recording server. Consequently, no live viewing or recording will be possible.

While the management server service is stopped, you will not be able to use the XProtect Corporate Management Client at all.

1. See Accessing the Server Service (on page 331).
2. Select either **Stop Recording Server Service** or **Stop Management Server Service**.

Changing Recording Server Settings

To change basic settings for the Recording Server Service, such as which port numbers to use, do the following:

In order to be able to change settings, the Recording Server Service must be stopped. While the Recording Server Service is stopped, XProtect Corporate will not be able to interact with devices connected to the recording server. Consequently, no live viewing or recording will be possible.

1. See Accessing the Server Service (on page 331).
2. Select **Stop Recording Server Service**.
3. Right-click the notification area's recording server icon.
4. From the menu that appears, select **Change Settings...**

The **Recording Server Settings** window appears. Change the appropriate settings.

Viewing Status Messages

1. See Accessing the Server Service (on page 331).



2. 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

Viewing Version Information

Knowing the exact version of your management server service or recording server service is an advantage if you need to contact product support.

1. In Management Client's menu bar select **Help** menu, click **About...**
2. A small dialog opens. The dialog will, depending on server type, show the exact version of your management server service or recording server service.

Work with Recording Server Settings in details

- **Management server hostname / IP address:** IP address (example: 123.123.123.123) or host name (example: ourserver) of the XProtect Corporate management server to which the recording server should be connected. This information is necessary in order for the recording server to be able to communicate with the management server.
- **Management server port:** Port number to be used when communicating with the XProtect Corporate management server. Default is port 9993, although changeable if required.
- **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 Clients. Default is port 7563, although changeable if required.
- **TCP information 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, although changeable if required.
- **SMTP server port:** Port number to be used when the recording server listens for SMTP information (some devices use SMTP (e-mail) for sending event messages). Default is port 25, although changeable if required.
- **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, although changeable if required.



Read Server Service State Icons

The following notification area icons represent the possible states of the management server service and recording server service:

Management Server Service Icon	Recording Server Service Icon	Description
		Running.
		Stopped.
		Starting. Appears when a server service is in the process of starting. Under normal circumstances, the icon will after a short while change to Management server is running or Recording server is running .
		Stopping. Appears when a server service is in the process of stopping. Under normal circumstances, the icon will after a short while change to Management server is stopped or Recording server is stopped .
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 will, under normal circumstances, change to the Recording server is starting icon, and subsequently to the Recording server is running icon.
		Running offline. Typically appears when the Recording Server Service is running but the Management Server Service is not.
		Must be authorized by administrator. Appears when the Recording Server Service is loaded for the first time. Administrators authorize the recording server through the XProtect Corporate Management Client: In the Management Client's Site Navigation pane, expand the Servers list, select the Recording Server node then in the Overview pane right-click the required recording server and select Authorize Recording Server .



Virus scanning

Virus Scanning Information

Virus scanning should in some cases be avoided—if allowed in your organization.

If you use virus scanning software on:

- recording data in databases on recording servers
- data being archived in archiving (see "About Storage and Archiving" on page 101) locations

it will most likely use a considerable amount of system resources on scanning.

This may affect system performance negatively, notably scanning of data in databases containing recordings. Some virus scanning software may furthermore temporarily lock each file it scans, which may further impact system performance negatively. Virus scanning may even corrupt recording databases, and render your surveillance system recordings useless.

Therefore:

- Do not use virus scanning on recording server directories containing recording databases (by default C:\MediaDatabase\ and all folders under that location, but note that different recording paths may have been specified in your organization).
- Do not use virus scanning on archiving locations.
- Do not use virus scanning on files with the following file extensions (which are all surveillance system-related):
 - .blk
 - .idx
 - .pic
 - .pqz
 - .sts
 - .ts
- Do not use virus scanning on the management server.

Your organization may have strict guidelines reg. virus scanning, but it is important that the mentioned locations and files are exempt from virus scanning. If allowed, you should therefore disable any virus scanning of recording servers' databases, of any archiving locations as well as on the management server. Consult your organization's IT system administrator if in doubt.



SNMP

SNMP Support

XProtect Corporate supports SNMP (Simple Network Management Protocol), a standard protocol for monitoring and controlling network devices, for managing their configuration, or collecting statistics, etc.

XProtect Corporate will act 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. The SNMP Service must therefore be installed on recording servers. This will—when the SNMP Service has been configured through its own user interface—enable recording servers to send .mib (Management Information Base) files to the SNMP management console.

Installing the SNMP Service

1. On the required recording servers, open Windows' **Add or Remove Programs** dialog (**Start > Control Panel > Add or Remove Programs**).
2. In the left side of the **Add or Remove Programs** dialog click **Add/Remove Windows Components**. This will open the **Windows Components** wizard.
3. In the wizard, select the check box next to **Management and Monitoring Tools**, then click **Details...** to open the **Management and Monitoring Tools** dialog.
4. In the **Management and Monitoring Tools** dialog, select the check box next to **Simple Network Management Protocol**, then click **OK**.
5. Back in the **Windows Components** wizard, click **Next** and follow the wizard's further steps.

Configuring the SNMP Service

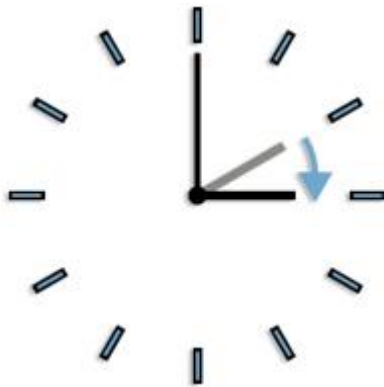
1. On the required recording servers, select **Start > Control Panel > Administrative Tools > Services**.
2. Double-click the SNMP Service.
3. Select the **Traps** tab.
4. Specify a community name, and click **Add to list**.
5. Select the **Destinations** tab.
6. Click **Add**, and specify the IP address or host name of the server running your third party SNMP management station software.
7. Click **OK**.



Daylight saving time

Daylight Saving Time

Daylight saving time (DST, also known as summer time) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. Typically, clocks are adjusted forward one hour sometime during the spring season and adjusted backward sometime during the fall season, hence the saying **spring forward, fall back**. Note that use of DST varies between countries/regions.



Clocks are adjusted forward when DST starts

When working with a surveillance system, which is inherently time-sensitive, it is important to 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 thus has 23 hours. In that case, there is simply 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 thus has 25 hours.

Server-side Handling

XProtect Corporate uses Coordinated Universal Time (UTC), which is the official world reference for time. UTC is not adjusted to reflect switches either to or from DST. Since XProtect Corporate uses UTC, no XProtect Corporate recordings are ever stored with the same timestamp twice, not even during the DST change hour.

Client-side Handling

Both of the client applications used for viewing recordings from XProtect Corporate —the XProtect Smart Client and the Remote Client —also use UTC when displaying recordings. The client simply takes local time settings (time zone and any DST) from the computer on which the client is used, and converts those time settings to UTC. This means that there is a very simple solution for viewing recordings from the DST change hour.



Viewing DST Change Hour Recordings in Clients

When you want to view recordings from the last (most recent) hour of the DST change hour, simply go ahead and view them.

When you want to view recordings from the first hour of the DST change hour, do the following:

1. On the computer on which the client is used, go to Windows' **Start** menu, and select **Control Panel**.
2. In the Control Panel, double-click **Date and Time**.
3. In the **Date and Time Properties** window, select the **Time Zone** tab.
4. Make sure the **Automatically adjust clock for daylight saving changes** check box is cleared, then click **OK**.



When the Automatically adjust clock for daylight saving changes check box is cleared, recordings from the entire DST period will be Standard Time (or one hour off compared to DST). This means that recordings from the first hour of the DST change hour can now be viewed.

IMPORTANT: When you are done viewing recordings from the first hour of the DST change hour, select the Automatically adjust clock for daylight saving changes check box again to avoid confusion. We recommend not to clear the Automatically adjust clock for daylight saving changes check box unless you specifically need to view recordings from the first hour of the DST change hour.



IPv6

IPv6 (vs. IPv4)

XProtect Corporate supports IPv6 as well as IPv4. So does the XProtect Smart Client. (see "Installing the XProtect Smart Client" on page 22)

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 thus 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 <Doc_Type> reflect use of IPv4 since this is still the most widely used IP version. IPv6 will work equally well with XProtect Corporate, provided you note the following:

Important Information if Using XProtect Corporate with IPv6

The following conditions apply when using XProtect Corporate with IPv6:

Servers

Servers are often capable of using IPv4 as well as IPv6. However, if just one server in your XProtect Corporate system (i.e. a management server, a recording server or a failover server) requires a particular IP version, all other servers in your XProtect Corporate system must communicate using the same IP version.

Example: All of the servers in your XProtect Corporate system—except one—are able to 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 in question also support the devices' IP version. See also illustration.

Clients

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

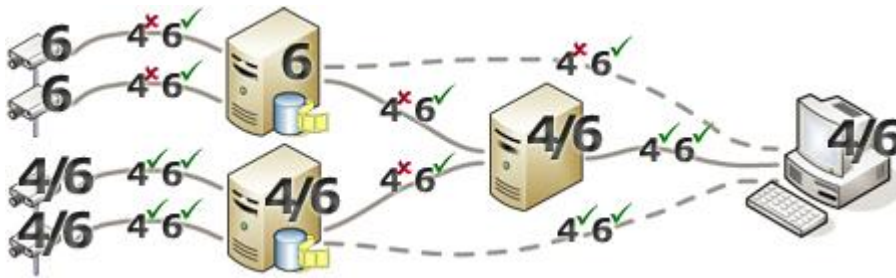
If one or more servers in the XProtect Corporate system are **only** capable of using IPv6, XProtect Smart Client users **must** use IPv6 for their communication with those servers. In this context, it is important to remember that XProtect Smart Clients technically connect to a management server for 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.

Tip: 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 XProtect Corporate system only uses IPv6, all communication with that server must naturally use IPv6. However, that server also determines the IP version for communication between all other servers in the system.

No XProtect Enterprise Integration

If using IPv6, it is not possible to integrate XProtect Enterprise servers (see "Manage XProtect Enterprise Servers" on page 279) in your XProtect Corporate system.

No Matrix Monitor Compatibility

If using IPv6, it is not possible to use the Matrix Monitor application with your XProtect Corporate system. Matrix functionality in XProtect Smart Client s is not affected.

How to Write IPv6 Addresses

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

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

Addresses may be shortened 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, addresses may be shortened 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 may 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, in order 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://\[2001:0B80:0000:0000:0000:0F80:3FA8:18AB\]](http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]), which may of course be shortened to, for example, [http://\[2001:B80::F80:3FA8:18AB\]](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](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](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.



Multi-domain with one-way trust

Setup with one-way trust

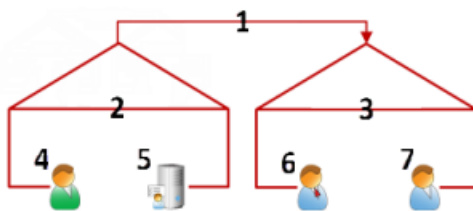
If you run XProtect Corporate in a multi-domain environment, it is possible to configure this setup with one-way trust

Prerequisites

XProtect Corporate is installed on the **Trusting** domain and users log in from **Trusting** and **Trusted** domains.

To Configure XProtect Corporate in Multi-domain Environments with One-way Trust

1. Create a service account in the **Trusted** domain. It can be named anything you want, for example, **svcMilestone**.
2. Add **svcMilestone** (example name only) to the following local Windows user groups on the server running XProtect Corporate, 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. Ensure that the **svcMilestone** (example name only) 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 **svcMilestone** (example name only) account.
5. Reboot the server to ensure all group membership and permission changes take effect.



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. XProtect Corporate Management Server
6. Milestone Service Account
7. Trusted Domain User



IMPORTANT: To add **Trusted** domain users to new or existing XProtect Corporate roles, login to Windows as a **Trusted** domain user. Next, launch the Management Client and login as user of either the **Trusting** domain or the **Trusted** domain. If you login to Windows as a **Trusting** domain user, you will be asked for credentials for the **Trusted** domain in order to browse for users.



Appendix

Ports used by XProtect Corporate

If nothing else is stated, ports are both inbound and outbound.

Port 20 and 21: Used by **recording servers** to listen for FTP information; some devices use FTP for sending event messages. FTP (File Transfer Protocol) is a standard for exchanging files across networks.

Port 25: Used by **recording servers** to listen for 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 (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers.

Port 80: While not directly used by XProtect Corporate, but by **management servers**, port 80 is typically used by the IIS (Internet Information Services) Default Web Site for running the XProtect Corporate Management Server service.

Port 554: Used by **recording servers** for RTSP traffic in connection with H.264 video streaming.

Port 1024 and above (outbound only (except ports listed in the following)): Used by **recording servers** for HTTP traffic between cameras and servers.

Port 1249: Used for communication between **event server** and **Management Client**.

Port 5210: Used for communication between **recording servers** and **failover servers** when databases are merged after a failover server has been running.

Port 5432: Used by **recording servers** to listen for TCP information; some devices use TCP for sending event messages.

Port 7563: Used by **recording servers** and **XProtect Smart Client** for handling PTZ camera control commands and for communicating.

Port 7609: Used by the **Data Collector Server service** to communicate with the server.

Port 8080: Used for internal system communication.

Port 8844: Used for communication between **failover servers**.

Port 9000: Used by **management servers** for communication between XProtect Corporate and XProtect Transact.

Port 9993: Used for communication between **recording servers** and **management servers**.

Port 11000: Used by **failover servers** for polling (i.e. regularly checking) the state of **recording servers**.

Port 12345: Used by **management servers** and **XProtect Smart Client** for communicating between XProtect Corporate and Matrix recipients.

Port 22331: Used for communication between Event Server and XProtect Smart Client.

Port 65101: Used by **recording servers** for communication between recording servers and drivers (internally, used for example when SMTP events are received).

Any other port numbers you may have selected to use. Examples: If you have changed the IIS Default Web Site port from its default port number (80) to another port number, or if you have integrated XProtect Enterprise servers into your XProtect Corporate solution, in which case a port must be allocated for use by XProtect Enterprise's Image Server service.



Index

3

360° Lens tab (camera properties) • 144

A

A Typical XProtect Corporate Setup • 13

About clients • 179

About configuration report • 264, 266

About Current Task • 264, 266

About Data Collector Server service • 265

About Device Groups • 125, 145, 147, 149, 154, 159, 175

About Devices • 125

About maps • 65, 328

About Multi-streaming • 126, 163, 175

About Remote Connect Services • 88

About Roles • 62, 73, 137, 141, 159, 233, 239, 248, 249, 250, 253, 254, 279, 280

About Rules and Events • 103, 162, 187

About Security • 248

About Storage and Archiving • 72, 101, 113, 116, 117, 220, 221, 258, 326, 327, 334

About System Dashboard • 264

About System Monitor • 264

About the Event Tab for Camera • 164

About the Event Tab for Microphone • 164

About the Service Channel • 124, 283, 330

About Updates • 14

About Upgrading • 119

Accepting Inclusion in the Hierarchy • 303, 304

Access Download Manager • 60

Accessing Registered Services Configuration • 283

Accessing the Remote Client • 24

Accessing the Server Service • 331

Action Menu items • 75

Actions and Stop Actions Overview • 173, 188, 202, 206, 207, 211, 212, 216, 267

Activate Licenses • 81, 84, 86, 96, 314

Activate licenses offline • 84

Activate Licenses Online • 82

Activating licenses after the grace day period • 84

Active Directory • 20

Active Directory User and Group Concepts • 249

Add a role and manage its Smart Client and Time Profiles • 252

Add and Configure a Smart Client Profile • 182

Add Hardware (Cameras, etc.) • 72, 90, 96, 107, 125, 145, 147, 149, 150, 154, 285

Adding a Device Group • 160

Adding a Hardware Configurable Event • 165

Adding a New Patrolling Profile • 137

Adding a New Stream • 163

Adding a New User-defined Event • 238

Adding a preset position (type 1) • 141

Adding a Site to the Hierarchy • 303

Adding a View Group • 181, 263

Adding and Editing Registered Services • 284

Adding and Grouping Failover Servers • 322

Adding Hardware (Cameras, etc.) to a Recording Server • 107

Adding Matrix recipients • 185

Adding New Notification Profiles • 234



Adding or Editing Secure Tunnel Servers • 88

Adding Users and Groups through Active Directory (Normal Way) • 249

Adding Users Not Using Active Directory • 250

Adding XProtect Enterprise Servers • 281

Address Range Scanning • 92

Adjust settings on a Smart Client Profile • 182, 184

Advanced tips for Smart Client Matrix recipients • 186

Alarms • 261, 273

Alarms Rights • 261, 274

Alternative for workgroups • 30

Appendix • 343

Application Rights • 260

Archive Structure • 104

Archiving and Virus Scanning • 105

Assign and Remove Users and Groups to/from Roles • 35, 249, 251, 252, 254, 294, 297, 303, 304, 305, 321

Assigning a default preset position • 143

Assigning Failover Servers to Recording Servers • 326

Assigning IP Address Range • 121

Assigning Users and Groups to a Role • 255

Attaching Individual Devices or a Group of Devices to a Storage Area • 101, 103

Authorizing a Recording Server • 106

Automatic and Manual Activation of Output • 155

AVI Compression Settings • 234, 287, 290

AVI Generation • 287

Axis One-Click Camera Connection Properties • 88, 89, 90

B

Back Up/Restore Fail & Problem Scenarios • 313

Backing Up Archived Recordings • 103

Backing Up Log Server Database • 310

Backup and Restore Event Server Configuration • 310

Backup, restore and move system configuration • 309

Basic Rules of Federated Sites • 295, 298, 304, 306, 307, 308

Basics • 72

Bookmarks • 287

C

Camera • 170, 175

Changing Log Language • 269

Changing Recording Server Settings • 331

Changing the Management Server Address • 319, 320

Changing Your Software License Code (SLC) • 87

Client • 179

Client settings • 127

Client Tab (Camera Properties) • 122, 126, 127

Clients overview • 20

Components controllable through the Download Manager • 65

Computer accessing Remote Client • 19

Computer running Event Server • 17

Computer running Log Server • 17

Computer running Management Client • 17

Computer running Management Server • 16



Computer running Recording Server or Failover Server • 16

Computer running Service Channel • 18

Computer running XProtect Smart Client • 19

Configuration • 128

Configuration Report Details • 266

Configuring a Speaker • 148

Configuring Individual Cameras • 126

Configuring Individual Microphones • 145

Configuring the SNMP Service • 335

Connecting to Another Site in the Hierarchy • 302, 305

Context Menu • 303

Copying a Role • 252

Copying a Smart Client Profile • 182

Copying Log Server Database • 315

Copying System Configuration from Old Server (Step 1) • 315

Copying/Restoring System Configuration to New Server (Step 3) • 316

Copyright, trademarks and disclaimer • 12

Create Many Simple or a Few Complex Rules? • 223

Create Typical Rules • 158, 194, 221, 222, 226

Creating a Configuration Report • 266

Creating a Day Length Time Profile • 233

Creating a Generic Event • 243

Creating a New Analytics Event • 240

Creating a New Rule • 223

Creating a New Storage Area • 115, 119

Creating an archive within an existing storage area • 115, 116, 119

Custom • 32

Customize the Management Client's Layout • 66, 70, 76

Customizing Transitions • 138

D

Database corruption • 329

Day Length Time Profile Properties • 233

Daylight saving time • 336

Daylight Saving Time • 336

Deactivating and Activating a Rule • 228

Default configuration of Download Manager and web page • 63

Default Goto Preset when PTZ Is Done rule • 214

Default Record on Bookmark rule • 214, 218

Default Record on Motion rule • 214

Default Record on Request rule • 215

Default Rules • 214, 221, 223

Default Start Audio Feed rule • 215

Default Start Feed rule • 215

Define Input- and Output-Related Rules • 150, 155, 157

Defining a Rule that Activates/Deactivates an Output • 158

Defining a Rule where an Input Triggers an Action • 159

Defining a Rule where an Output Triggers an Action • 158

Defining Access Roles for XProtect Enterprise Servers • 279, 280, 281

Defining Alarms • 275, 277, 298



- Defining Local IP Address Ranges • 292
- Defining Public Address and Port • 123
- Defining rules sending video to Matrix recipients • 186
- Deleting a Device Group • 162
- Deleting a Hardware Configurable Event • 165
- Deleting a Role • 253
- Deleting a Rule • 227
- Deleting a Smart Client Profile • 182
- Deleting All Hardware on a Recording Server • 99
- Deleting an Archive from within an Existing Storage • 118
- Deleting an Entire Storage Area • 118
- Deleting an Existing User-defined Event • 239
- Deleting Individual Hardware • 96
- Dependent on hardware configuration • 216
- Description of Info Tab's Fields • 167
- Detaching a Site from the Hierarchy • 305
- Device drivers • 317
- Device Rights • 256, 273, 287
- Devices • 125, 216
- Disabling/Enabling Hardware • 99
- Download Manager is not user rights management tool • 62
- E**
- Edit Menu items • 75
- Editing a Preset Position • 143
- Editing a Time Profile • 232
- Editing an Existing Analytics Event • 240
- Editing Analytics Events Settings • 242
- Editing Basic Hardware Settings (IP, etc.) • 95
- Editing Failover Server properties • 324
- Editing Local IP Address Ranges • 292
- Editing Settings for a Selected Storage Area or Archive • 119
- Editing the Axis Dispatch Service Properties • 88
- Editing the Name of an Existing User-defined Event • 239
- Editing XProtect Enterprise Servers • 282
- Editing, Copying and Renaming a Rule • 226
- Enabling and Disabling Edge Recording—Camera Only • 162, 173, 193, 235
- Enabling and Disabling Motion Detection • 130
- Enabling and Disabling Panomorph Support • 144
- Enabling and Disabling Privacy Masking • 134
- Enabling and Disabling Recording • 170
- Enabling Failover Servers • 324
- Enabling Input • 149
- Enabling Microphones • 145
- Enabling Multicasting • 121
- Enabling Multicasting for Individual Cameras • 122
- Enabling Output • 154
- Enabling PTZ on a Video Encoder • 169
- Enabling Public Access • 123
- Enabling Speakers • 147
- Enabling/Disabling Individual Devices • 100
- Enterprise • 279
- Enterprise Server rights • 261
- Event Server Settings • 288
- Events Overview • 103, 105, 163, 164, 165, 187, 193, 216, 267, 268, 276, 327
- Events Tab Overview • 126, 145, 164

**Example**

How to Create and Test a Simple Generic Event • 244

Expand/Collapse • 303

Exporting Log • 267, 270

Express • 91

External Event Rights • 260, 274

External Events • 219

F

Failover Server Service Administration • 319

Failover servers • 38, 319

Failover Service Communication Port • 112

Failover Tab (Recording Server Properties) • 111, 326, 327

Failover-Related Events • 327

Fall

Switch from DST to Standard Time • 336

FAQs

XProtect Central and Alarms - Same Thing? • 274

Federated Icons • 302

Federated Sites Example Scenario—Limestone City • 299

File Menu items • 75

Fill in Notification Profile Details • 236

Fill in Properties on the Events Tab • 151, 152

Fill in Properties on the Info Tab • 151, 155

Fill in Properties on the Settings Tab • 151, 156

Fisheye Tab (Camera Properties) • 128

Flushing the SQL Server Transaction Log • 309

Frequently Asked Questions • 326

Frequently asked questions about archiving • 105

Frequently Asked Questions to Federated Sites • 297

G

General • 285

Generic • 219

Generic Event Data Source Properties • 247

Generic Event Properties • 244

Generic Event Test Properties • 247

Generic Events • 243, 244, 247, 288

Get started • 72

Getting Additional Licenses • 83, 85, 86

H

Handling Log Settings • 267, 271

Hard Disk Failure

Protect Your Drives • 329

Hardware • 175

Hardware Configurable Events • 163, 187, 188

Help Menu items • 75

Hide and remove components • 62, 65

How a Rule Is Triggered • 222

How do I set up users and their rights? • 21

How to connect to the surveillance system? • 21

How to Write IPv6 Addresses • 339

I

If You Receive an Online Activation Error Message • 82

Illustration

How do the Alarms Feature and the Event Server work? • 274

Illustration of Milestone Federated Architecture • 298, 301



Important Information if Using XProtect Corporate with IPv6 • 338

Important Prerequisites When Running Federated Sites • 293, 297

Info Tab (Recording Server Properties) • 113

Info Tab Overview • 126, 145, 148, 166

Info Tab's Fields • 113

Install event server and log server (custom) • 32, 34, 40, 55, 63

Install management server • 27, 28, 34, 40, 42, 48, 58, 250, 294, 295, 316, 328

Install Service Channel (custom) • 44, 45

Install Service Channel (typical) • 44

Install system components • 27, 34, 40, 50, 60, 63, 66

Install the Service Channel • 32, 34, 40, 42, 330

Installation and removal • 27

Installation Overview • 27, 72

Installation troubleshooting • 30, 55

Installing an STS Environment for One-click Camera Connection • 88

Installing event server and log server • 41

Installing Failover Servers • 322

Installing multiple recording server instances • 50

Installing New Management Server on New Server (Step 2) • 316

Installing the SNMP Service • 335

Installing the XProtect Smart Client • 21, 22, 24, 27, 54, 120, 127, 140, 179, 185, 187, 262, 292, 338

Installing the XProtect Smart Client from server or DVD • 22

Installing the XProtect Smart Client silently • 23

Installing Video Device Drivers • 317

Installing XProtect Corporate in a cluster • 48, 50

Installing XProtect Corporate on virtual servers • 27

Introductions • 13

IPv6 • 122, 338

IPv6 (vs. IPv4) • 13, 22, 279, 287, 338

Issue

Automatic IIS installation for Management or Event Server fails • 55

Changes to SQL Server location prevents database access • 58

Insufficient continuous virtual memory fails installation • 58

Multi-domain environments • 59

Recording Server startup fails due to port conflict • 56

L

Licensing of Milestone Federated Architecture • 295

Limitations when Adding XProtect Enterprise Servers • 279

Local IP Ranges • 123

Log in to the Management Client • 72, 74

M

Mail Server • 286

Make new components available • 60, 65

Making New Video Device Driver Versions Available for Installation • 317

Manage Alarms • 183, 273

Manage and Remove Video Device Drivers • 27, 55, 63, 317

Manage Cameras • 73, 95, 125, 126, 130, 146, 148, 153, 157, 163, 167, 178, 187, 188

Manage Day Length Time Profiles • 229, 232

Manage Failover Servers • 73, 111, 112, 122, 173, 221, 320, 321



Manage Generic Events • 163, 187, 219, 242

Manage Hardware • 86, 95, 107, 125, 162, 167

Manage Input • 73, 95, 125, 126, 146, 148, 149, 153, 157, 163, 164, 178, 187, 188

Manage Licenses • 73, 84, 96, 295

Manage local IP address ranges • 122, 123, 287, 292

Manage Logs • 105, 192, 267, 286, 312, 313

Manage Microphones • 73, 125, 126, 144, 146, 148, 153, 157, 163, 167, 178, 187, 188

Manage Milestone Federated Architecture • 67, 71, 293, 294, 295, 296, 297, 302

Manage Multicasting • 120, 127, 128, 286

Manage Network Configuration • 282

Manage Notification Profiles • 73, 162, 187, 192, 221, 233, 287, 290, 291

Manage Output • 73, 95, 125, 126, 146, 148, 153, 154, 157, 164, 178

Manage Public Addresses • 122, 292, 325

Manage Recording Servers • 72, 106

Manage Registered Services • 283, 328, 330

Manage Roles • 21, 76, 181, 183, 229, 238, 249, 251, 255, 263

Manage Rules • 73, 105, 130, 136, 140, 143, 149, 154, 155, 158, 159, 162, 170, 172, 174, 186, 187, 188, 189, 216, 221, 229, 233, 236, 238, 239, 244, 267, 327

Manage Smart Client Profiles • 179, 182, 229, 248, 249

Manage Software License Codes (SLC) • 86, 295

Manage Speakers • 73, 125, 126, 146, 147, 148, 153, 157, 167, 178

Manage Time Profiles • 73, 162, 174, 183, 187, 201, 204, 229, 233, 248, 249, 251, 276

Manage User-defined Events • 162, 187, 220, 238, 243, 276

Manage Users and Groups • 16, 73, 76, 248, 249, 251, 254

Manage View Groups • 179, 249, 251, 253, 260, 262

Manage XProtect Enterprise Servers • 76, 261, 279, 283, 339

Manage XProtect Matrix Recipients • 179, 185, 193, 222, 261

Management client • 27, 40

Management Client • 66

Management Client menu overview • 68, 75, 302, 303

Management Client Overview • 40, 66, 88, 103, 113, 151, 152, 153, 156, 165, 166, 167, 169, 177, 228, 239, 240, 242, 276, 280, 285, 325

Management Client's Elements • 66

Management Server Service and Recording Server Service • 29, 37, 39, 46, 49, 50, 51, 108, 111, 112, 311, 315, 316, 330

Managing Analytics Events • 239

Managing Hardware on a Recording Server • 107

Manual • 93

Manual Back Up of System Configuration • 312

Manual Backup & Restore of System Configuration • 309, 311

Map • 328

Matrix rights • 261

Memory Indicator • 69

Menu and tool bars • 70



Menu Bar • 66, 67, 68

Microphone • 170

Microphone and Speaker • 175

Milestone Federated Architecture • 27, 293

Milestone Federated Architecture Overview • 14, 27,
28, 47, 68, 71, 75, 85, 194, 273, 275, 293, 299,
302, 303, 305

MIP Rights • 262

More About Administrators role • 229, 251

More About Alarms • 273

More about View Groups • 180, 262

Motion Detection Settings • 130

Motion Tab (Camera Properties) • 126, 129

Move components between web page versions • 61

Move System Configuration to New Management
Server • 312, 313

Moving Non-archived Recordings from One Storage
to Another • 119

Moving Panes • 77

Multi-domain with one-way trust • 341

Multiple management servers (clustering) • 47

Multiple recording server instances • 38, 50, 331

N

Navigating Log • 269

Navigating the Built-in Help System (online) • 25, 69

Network • 287

Network Configuration • 284

Select a Predefined Account • 33

Analytics Events • 241, 242, 287

O

Options • 76, 175, 192, 242, 243, 285, 286, 287,
288, 292

Outgoing SMTP Mail Server Settings • 234, 286,
291

Overview Pane • 70

P

Panes overview • 66, 67, 70, 76, 81, 82, 84, 85, 86,
91, 95, 96, 99, 100, 103, 106, 107, 112, 113, 114,
119, 122, 125, 127, 145, 146, 147, 149, 150, 151,
152, 154, 155, 156, 160, 161, 162, 163, 164, 168,
174, 175, 177, 178, 179, 181, 182, 185, 187, 199,
200, 204, 209, 221, 224, 226, 227, 228, 230, 232,
233, 234, 238, 239, 240, 243, 244, 248, 249, 251,
252, 253, 254, 256, 263, 264, 266, 267, 270, 275,
280, 285, 294, 296, 302, 304, 305, 306, 307, 308,
321, 322, 324

Panomorph Settings • 144

Part I—Downloading the installer • 35

Part II—Installing the component • 36

Pause PTZ Patrolling and Go to PTZ Preset on
Input • 208

Port numbers of special interest • 46

Ports used by XProtect Corporate • 46, 343

Possibilities and Constrains of Federated Sites •
297

Power outages

use a UPS • 329

Predefined events (related to devices) • 218

Predefined events (related to external events) • 219

Prerequisites • 53, 234, 249, 309

Prerequisites for Access Roles for XProtect
Enterprise Servers • 279



Prerequisites for installing XProtect Corporate in a cluster • 48

Preview • 129

Preview Pane • 70

Principles for Setting Up Federated Sites • 296

Privacy Mask Tab (Camera Properties) • 126, 133

Privacy Masking Settings • 134

Product overview XProtect Corporate • 13

Properties Pane • 70, 71

Protect Databases from Corruption • 111, 329

PTZ Patrolling Tab (Camera Properties) • 126, 136, 140, 170, 190, 191, 200, 204, 209

PTZ Presets tab (camera properties) • 136, 140, 170, 191, 199, 204, 209, 214

PTZ Rights • 258

PTZ Tab (Hardware Properties) • 126, 168

R

Read Failover Server Service State Icons • 320

Read Server Service State Icons • 89, 333

Read the Camera List's Status Icons • 126

Read the Input List's Status Icons • 153

Read the Microphone List's Status Icons • 146

Read the Output List's Status Icons • 156

Read the Recording Server Icons • 111

Read the Speaker List's Status Icons • 148

Reading and Copying Log Content • 267

Record Tab Overview • 119, 126, 145, 148, 164, 170, 188, 189, 192, 214, 215, 216, 287

Recording servers • 36, 322

Recording servers (Custom) • 36, 37

Recording servers (Typical) • 36, 37

Refreshing the Site Hierarchy • 306

Registered Services • 282

Registering a new Axis One-click Camera • 89

Registering Your Software License Code (SLC) • 86

Related to plug-ins • 217

Related to recording servers • 220

Remote Client • 21, 24, 27, 127, 179, 262

Remote Connect Hardware • 94

Remote Connect Services • 88

Remove system components • 35, 41, 43, 50, 51, 52, 53, 54, 62

Removing a Recording Server • 108

Removing a View Group • 181, 264

Removing Download Manager, Event Server and Log Server • 51

Removing Management Client or Service Channel • 51

Removing Management Server • 51

Removing non-required components from Management Server • 51, 52

Removing Recording Server • 51, 52

Removing Secure Tunnel Servers • 89

Removing the XProtect Smart Client • 23

Removing Users and Groups from a Role • 255

Removing Video Device Drivers • 318

Renaming a Recording Server • 107

Renaming a Role • 253

Renaming a Site • 307

Renaming a Smart Client Profile • 183

Renaming a View Group • 181, 264

Renaming an Existing Patrolling Profile • 140



- Renaming Hardware • 99
- Renaming Individual Devices • 100
- Replacing a Recording Server • 108
- Replacing Hardware • 85, 96
- Resetting to Default Layout • 81
- Resizing Panes • 76
- Restoring System Configuration (From Manual Back Up) • 313, 316
- Restoring System Configuration (From Scheduled Back Up) • 311
- Right-clicking is not Selecting! • 303
- Rules and Events • 187
- S**
- Scheduled Back Up of System Configuration • 309
- Scheduled Backup & Restore of System Configuration • 309, 312, 314, 315
- Searching Log • 269
- Security • 248
- Select a particular user account • 42, 44, 45, 46
- Select a Particular User Account • 33, 34, 37, 38, 39
- Select a predefined network service account • 42, 44, 45
- Select a Predefined System Account • 37, 38
- Select Shared Backup Folder • 312
- Selecting Required Failover Groups • 112
- Server Logs • 267, 286
- Servers • 90
- Servers and Clients Require Time-Synchronization • 123, 330
- Services administration • 330
- Set up a secure connection on all items in a Device Group • 177
- Set Up Alarms Using Enterprise Slaves • 278
- Setting Alarm Data • 277
- Setting Alarm Sounds • 277
- Setting Recording Frame Rate—Camera Only • 171
- Setting the Site Properties • 307
- Settings Tab Overview • 126, 130, 145, 148, 163, 174, 189, 195
- Setup with one-way trust • 59, 341
- Site Navigation Pane • 303
- Site Navigation Pane and Federated Hierarchy Pane • 67, 70, 71
- SNMP • 335
- SNMP Support • 193, 335
- Speaker • 170
- Specify Common Settings for All Items in a Device Group—Cameras, Microphones and Speakers • 175
- Specify Common Settings for All Items in a Device Group—Hardware • 177
- Specify Hardware Configurable Event Properties • 165, 166
- Specify IP Address Range • 122
- Specify recording server setup parameters • 37, 39, 40
- Specify Rights of a Role • 41, 45, 180, 181, 183, 238, 249, 251, 252, 256, 263, 264, 287
- Specifying a Time Profile • 230
- Specifying an End Position • 139
- Specifying Common Settings for All Devices in a Device Group • 161



Specifying Datagram Options • 121

Specifying How Long to Stay at Each Preset Position for • 138

Specifying Input Properties • 150

Specifying Manual PTZ Session Timeout • 140

Specifying Output Properties • 154

Specifying Preset Positions for Use in a Patrolling Profile • 137

Specifying Which Devices to Include in a Device Group • 161

Speech rights • 259

Spring

 Switch from Standard Time to DST • 336

Starting and Stopping the Failover Server Service • 319

Starting the Server Service • 331

Status Icons Overview • 178

Step 1

 Internet Information Services • 30

Step 2

 XProtect Corporate management server database • 31

Step 3

 XProtect Corporate management server • 32

Stopping the Server Service • 331

Storage Tab (Recording Server Properties) • 102, 105, 113

Storage Tab's Elements • 114

System Dashboard • 264

System requirements • 16, 22, 24, 28, 52

T

Testing a Generic Event • 243

Testing a Preset Position • 144

Testing an Analytics Event • 240

The Administrator Role and Federated Sites • 296, 298, 304, 305

The Download Manager • 15

The Management Client • 15

The Management Server • 14, 40, 283, 293

The Recording Server • 15

The XProtect Smart Client and Remote Client • 15

Toggling Preview Pane On and Off • 81

Toolbar • 68

Tools Menu items • 76

Troubleshooting

 Missing Recording Servers • 109

Typical • 14, 32

U

Unregistering an Axis One-click Camera • 89

Upgrade from previous version • 27, 28, 34, 40, 42, 52, 106

Upgrading a Management Client • 54

Upgrading Recording Servers • 54

Upgrading the Management Server • 53

Upgrading the XProtect Smart Client • 54

Upgrading Video Device Drivers • 55

Upgrading XProtect Corporate in a cluster • 50

Use Different PTZ Patrolling Profiles for Day/Night • 204

Use Download Manager • 60, 73, 317, 328

Use Higher Live Frame Rate on Motion • 194

Use Specific PTZ Patrolling Profile During Specific Part of Day • 199

User Settings • 287



User-defined events • 220

User-defined Events • 187

Using Auto-Hide • 80

Using preset positions from device (type 2) • 141, 143

Using Rules to Trigger E-mail Notifications • 235

Using Several Instances of a Hardware Configurable Event • 165, 166

V

Validating Rule(s) • 228

View examples of the two clients • 20

View Group Rights • 260

View groups from a client user's perspective • 181

View Groups from a Client User's Perspective • 263

View Menu items • 76

Viewing Archived Recordings • 103

Viewing Current State of a Microphone • 146

Viewing Current State of a Speaker • 148

Viewing Effective Roles • 254

Viewing Log • 267

Viewing Status Messages • 319, 331

Viewing the Current State of an Input • 150

Viewing Version Information • 320, 332

Viewing Your License Information • 85

Viewing/Editing a Recording Server's Properties • 107

Virus scanning • 334

Virus Scanning Information • 65, 334

Virus scanning on the Management Server not recommended • 60, 65

W

What Are the Requirements? • 121

What Happens while the Management Server Is Unavailable? • 315

What Is Multicasting? • 120

What to Know about Licenses and Milestone Federated Architecture? • 85

What to Know When Replacing Cameras? • 85

What You Can Cover in a Rule • 222

What You Can Do with Rules • 221

What's next? • 34

Where can I find more information? • 21

Which client should I choose? • 20

Which Devices Require a License? • 84

Why Clients Require Time-synchronization • 124

Why Servers Require Time-Synchronization • 123

Why Use a Public Address? • 122

Windows Task Manager

Be Careful when Ending Processes • 329

Work with Recording Server Settings in details • 332

Working with clients • 20

Working with Prebuffering • 171

Working with Smart Client Profiles, Roles and Time Profiles • 182, 183, 229

Working with Storage Area • 172

Working with System Monitor • 265

X

XProtect Enterprise Server network configuration • 282



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.