

MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2020 R2

Administrator manual

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+
XProtect Essential+



Contents

Copyright, trademarks, and disclaimer	21
Overview	22
Product overview	22
Main system components	22
Management server	22
Recording server	23
Event server	23
Log server	24
SQL Servers and databases	24
Mobile server	24
Active Directory	24
Management Client (explained)	25
Optional system components	25
Failover recording server	25
Failover management server	25
Clients	25
XProtect Smart Client (explained)	25
XProtect Mobile client (explained)	26
XProtect Web Client (explained)	27
A distributed system setup	28
Add-on products	29
XProtect Access (explained)	29
XProtect LPR (explained)	30
XProtect Smart Wall (explained)	30
XProtect Transact (explained)	31
Milestone ONVIF Bridge (explained)	31
XProtect DLNA Server (explained)	32
Ports used by the system	32

Product comparison chart	43
Licensing	47
Licenses (explained)	47
Change the Software License Code	48
Requirements and considerations	49
Daylight saving time (explained)	49
Time servers (explained)	49
Limit size of database	50
IPv6 and IPv4 (explained)	50
Writing IPv6 addresses (explained)	52
Using IPv6 Addresses in URLs	52
Virtual servers	53
Multiple management servers (clustering) (explained)	53
Requirements for clustering	53
Protect recording databases from corruption	54
Hard disk failure: protect your drives	54
Windows Task Manager: be careful when you end processes	54
Power outages: use a UPS	54
SQL database transaction log (explained)	55
Minimum system requirements	55
Before you start installation	55
Prepare your servers and network	55
Prepare Active Directory	56
Installation method	56
Decide on a SQL Server edition	59
Select service account	60
Kerberos authentication (explained)	60
Virus scanning exclusions (explained)	62
Register Software License Code	63
Device drivers (explained)	64

Requirements for offline installation	64
Secure communication(explained)	64
Management server encryption(explained)	65
Encryption from the management server to the recording server(explained)	66
Encryption between the management server and the Data Collector Server(explained)	68
Encryption to clients and servers that retrieve data from the recording server(explained)	69
Mobile server data encryption(explained)	71
Mobile server encryption requirements for clients	72
Installation	73
Install a new XProtect system	73
Install XProtect Essential+	73
Install your system - Single computer option	76
Install your system - Custom option	80
Install new XProtect components	84
Installing through Download Manager(explained)	84
Install a recording server through Download Manager	84
Install a failover recording server through Download Manager	86
Installing silently through a command line shell(explained)	88
Install a recording server silently	89
Install XProtect Smart Client silently	90
Installation for workgroups	91
Install in a cluster	92
Download Manager/download web page	94
Download Manager's default configuration	96
Download Manager's standard installers(user)	98
Add/publish Download Manager installer components	98
Hide/remove Download Manager installer components	99
Device pack installer - must be downloaded	100
Installation log files and troubleshooting	101

Configuration	102
Navigating the Management Client	102
Login overview	102
Management Client window overview	103
Panels overview	105
Menu overview	106
File menu	107
Edit menu	107
View menu	107
Action menu	107
Tools menu	108
Help menu	108
Setting options for the system	108
General tab (options)	109
Server Logs tab (options)	111
Mail Server tab (options)	112
AVI Generation tab (options)	113
Network tab (options)	114
Bookmark tab (options)	114
User Settings tab (options)	115
Customer Dashboard tab (options)	115
Evidence Lock tab (options)	115
Audio messages tab (options)	116
Access Control Settings tab (options)	117
Analytics Events tab (options)	117
Alarms and Events tab (options)	118
Generic Events tab (options)	120
Initial configuration tasks list	122
Configuring the system in the Site Navigation pane	124
Site Navigation: Basics	124

License information	124
Device changes without activation (explained)	127
How the number of device changes without activation is calculated	127
View license overview	128
Automatic license activation (explained)	129
Enable automatic license activation	129
Disable automatic license activation	129
Activate licenses online	130
Activate licenses offline	130
Activate licenses after grace period	130
Get additional licenses	131
Licenses and hardware device replacement	131
Site information	131
Edit site information	132
Site Navigation: Servers and hardware	132
Site Navigation: Servers and hardware: Recording servers	132
Recording servers (explained)	132
Register a recording server	133
Change or verify the basic configuration of a recording server	135
View encryption status to clients	136
Recording server status icons	137
Info tab (recording server)	138
Info tab properties (recording server)	139
Storage tab (recording server)	140
Storage and archiving (explained)	141
Specify behavior when recording storage is unavailable	144
Add a new storage	145
Create an archive within a storage	146
Attach a device or group of devices to a storage	146
Edit settings for a selected storage or archive	146

Enable digital signing for export	147
Encrypt your recordings	148
Back up archived recordings	151
Archive structure (explained)	152
Delete an archive from a storage	153
Delete a storage	154
Move non-archived recordings from one storage to another	154
Storage and Recording Settings properties	155
Archive Settings properties	156
Failover tab (recording server)	157
Assign failover recording servers	158
Failover tab properties	159
Multicast tab (recording server)	160
Multicasting (explained)	161
Enable multicasting for the recording server	162
Assign IP address range	162
Specify datagram options	163
Enable multicasting for individual cameras	163
Network tab (recording server)	164
Why use a public address?	164
Define public address and port	164
Assign local IP ranges	165
Site Navigation: Servers and hardware: Failover servers	165
Failover recording servers (explained)	165
Failover steps (explained)	167
Failover recording server functionality (explained)	168
Set up and enable failover recording servers	169
Group failover recording servers for cold standby	170
Read failover recording server status icons	170
Multicast tab (failover server)	171

Info tab properties (failover server)	172
Info tab properties (failover group)	173
Sequence tab properties (failover group)	173
Failover recording server services (explained)	173
Change the management server address	174
View encryption status on a failover recording server	174
View status messages	175
View version information	175
Site Navigation: Servers and hardware: Hardware	176
Hardware (explained)	176
Add hardware	176
Disable/enable hardware	177
Edit Hardware	178
Enable/disable individual devices	181
Set up a secure connection to the hardware	182
Enable PTZ on a video encoder	182
Manage hardware	183
Info tab (hardware)	183
Settings tab (hardware)	184
PTZ tab (video encoders)	185
Device password management (explained)	185
Change passwords on hardware devices	186
Site Navigation: Servers and hardware: Manage remote servers	187
Info tab (remote server)	187
Settings tab (remote server)	188
Events tab (remote server)	189
Remote Retrieval tab	189
Site Navigation: Devices: Working with devices	190
Devices (explained)	190
Camera devices (explained)	191

Microphone devices (explained)	191
Speaker devices (explained)	192
Metadata devices (explained)	193
Input devices (explained)	194
Activate input manually for test	195
Output devices (explained)	195
Activate output manually for test	196
Enable/disable devices via device groups	196
Status icons of devices	197
Site Navigation: Devices: Working with device groups	198
Add a device group	199
Specify which devices to include in a device group	200
Specify common properties for all devices in a device group	200
Site Navigation: Devices tabs	201
Info tab (devices)	201
Info tab (explained)	201
Info tab properties	201
Settings tab (devices)	203
Settings tab (explained)	203
Camera settings (explained)	204
Streams tab (devices)	205
Streams tab (explained)	205
Multi-streaming (explained)	206
Add a stream	207
Record tab (devices)	208
Record tab (explained)	208
Enable/disable recording	209
Enable recording on related devices	210
Pre-buffering (explained)	210
Devices that support pre-buffering	211

Storage of the temporary pre-buffer recordings	211
Manage pre-buffering	211
Manage manual recording	212
Specify recording frame rate	212
Enable keyframe recording	213
Storage (explained)	213
Moving devices from one storage to another	215
Remote recording (explained)	215
Motion tab (devices)	215
Motion tab (explained)	215
Enable and disable motion detection	218
Specify motion detection settings	218
Hardware acceleration (explained)	218
Enable manual sensitivity	219
Specify threshold	220
Select keyframes settings	220
Select image processing interval	220
Specify detection resolution	221
Generating motion data for smart search	221
Specify exclude regions	221
Presets tab (devices)	222
Presets tab (explained)	222
Add a preset position (type 1)	224
Use preset positions from the camera (type 2)	226
Assign a default preset position	226
Edit a preset position (type 1 only)	226
Rename a preset position (type 2 only)	228
Lock a preset position	228
Test a preset position (type 1 only)	229
Reserved PTZ sessions (explained)	229

Release PTZ session	229
Specify PTZ session timeouts	229
PTZ session properties	230
Patrolling tab (devices)	231
Patrolling tab (explained)	231
Add a patrolling profile	233
Specify preset positions in a patrolling profile	233
Specify the time at each preset position	234
Customize transitions (PTZ)	234
Specify an end position	235
Manual patrolling (explained)	235
Manual patrolling properties	236
Fisheye lens tab (devices)	236
Fisheye Lens tab (explained)	236
Enable and disable fisheye lens support	237
Specify fisheye lens settings	237
Events tab (devices)	237
Events tab (explained)	237
Add an event	238
Specify event properties	239
Use several instances of an event	239
Event tab (properties)	239
Client tab (devices)	240
Client tab (explained)	240
Client tab properties	241
Privacy masking tab (devices)	242
Privacy masking tab (explained)	242
Privacy masking (explained)	243
Enable/disable privacy masking	245
Define privacy masks	245

Give users permission to lift privacy masks	247
Change the timeout for lifted privacy masks	247
Create a report of your privacy masking configuration	248
Privacy masking tab (properties)	249
Site Navigation: Clients	251
Clients (explained)	251
Site Navigation: Clients: Configuring Smart Wall	251
XProtect Smart Wall licensing	252
Configure Smart Walls	252
Set up user rights for XProtect Smart Wall	254
Using rules with Smart Wall presets (explained)	255
Smart Wall properties	255
Info tab (Smart Wall properties)	255
Presets tab (Smart Wall properties)	255
Layout tab (Smart Wall properties)	256
Monitor properties	257
Info tab (monitor properties)	257
Presets tab (monitor properties)	258
Site Navigation: Clients: View groups	258
View groups and roles (explained)	258
Add a view group	259
Site Navigation: Clients: Smart Client profiles	259
Add and configure a Smart Client profile	260
Copy a Smart Client profile	260
Create and set up Smart Client profiles, roles and time profiles	260
Set simplified mode as the default mode	261
Prevent operators from switching between simple and advanced mode	263
Smart Client profile properties	264
Info tab (Smart Client profiles)	264
General tab (Smart Client profiles)	264

Advanced tab (Smart Client profiles)	265
Live tab (Smart Client profiles)	265
Playback tab (Smart Client profiles)	266
Setup tab (Smart Client profiles)	266
Exports tab (Smart Client profiles)	266
Timeline tab (Smart Client profiles)	267
Access Control tab (Smart Client profiles)	267
Alarm Manager tab (Smart Client profiles)	267
Smart map tab (Smart Client profiles)	268
View Layout tab (Smart Client profiles)	268
Site Navigation: Clients: Management Client profiles	268
Add and configure a Management Client profile	269
Copy a Management Client profile	269
Management Client profile properties	269
Info tab (Management Client Profiles)	269
Profile tab (Management Client Profiles)	270
Site Navigation: Clients: Configuring Matrix	273
Add Matrix recipients	273
Define rules sending video to Matrix-recipients	274
Send the same video to several XProtect Smart Client views	274
Site Navigation: Rules and events	274
Rules and events (explained)	274
Actions and stop actions (explained)	276
Events overview	288
Rules	298
Rules (explained)	298
Default rules (explained)	299
Rule complexity (explained)	302
Validating rules (explained)	303
Add a rule	304

Edit, copy and rename a rule	305
Deactivate and activate a rule	305
Recurring time	306
Time profiles	306
Specify a time profile	307
Edit a time profile	309
Day length time profiles (explained)	309
Create a day length time profile	310
Day length time profile properties	310
Notification profiles	310
Notification profiles (explained)	310
Requirements for creating notification profiles	311
Add notification profiles	311
Use rules to trigger email notifications	313
Notification profile (properties)	313
User-defined events	315
User-defined events (explained)	315
Add a user-defined event	317
Rename a user-defined event	317
Analytics events	317
Analytics events (explained)	317
Add and edit an analytics event	318
Test an analytics event	318
Test Analytics Event (properties)	319
Edit analytics events settings	321
Generic events	321
Generic events (explained)	321
Add a generic event	322
Generic event (properties)	322
Generic event data source (properties)	324

Site Navigation: Security	326
Roles (explained)	326
Rights of a role (explained)	327
Users (explained)	328
Add and manage a role	329
Copy, rename or delete a role	329
Assign/remove users and groups to/from roles	330
View effective roles	331
Roles settings	331
Info tab (roles)	331
User and Groups tab (roles)	333
Overall Security tab (roles)	333
Device tab (roles)	358
PTZ tab (roles)	366
Speech tab (roles)	367
Remote Recordings tab (roles)	367
Smart Wall tab (roles)	368
External Event tab (roles)	368
View Group tab (roles)	369
Servers tab (roles)	369
Matrix tab (roles)	370
Alarms tab (roles)	370
Access Control tab (roles)	371
LPR tab (roles)	371
MIP tab (roles)	372
Basic users (explained)	372
Create basic users	372
Site Navigation: System dashboard	372
System dashboard (explained)	372
System monitor (explained)	373

Customize dashboard	374
System monitor details (explained)	375
System monitor thresholds (explained)	376
Set system monitor thresholds	379
Evidence lock (explained)	380
Current tasks (explained)	382
Configuration reports (explained)	382
Add a configuration report	382
Configure report details	382
Site Navigation: Server logs	383
Logs (explained)	383
Filter logs	383
Export logs	384
Allow 2018 R2 and earlier components to write logs	385
System logs (properties)	386
Audit logs (properties)	386
Rule-triggered logs (properties)	387
Site Navigation: Metadata use	388
What is metadata?	388
Metadata search (explained)	388
Metadata search requirements	388
Show or hide metadata search categories and search filters in XProtect Smart Client	389
Site Navigation: Alarms	389
Alarms (explained)	389
Alarm configuration (explained)	390
Alarm Definitions	391
Add an alarm	391
Alarm Definitions (properties)	393
Alarm Data Settings	395
Sound Settings	397

Enable encryption	397
Enable encryption to and from the management server	397
Enable server encryption for recording servers or remote servers	398
Enable encryption to clients and servers	400
Enable encryption on the mobile server	401
Edit certificate	402
View encryption status to clients	402
Configuring Milestone Federated Architecture	403
Set up your system to run federated sites	407
Add site to hierarchy	408
Accept inclusion in the hierarchy	409
Set site properties	409
Refresh site hierarchy	410
Log into other sites in the hierarchy	410
Detach a site from the hierarchy	411
Federated site properties	411
General tab	411
Parent Site tab	412
Configuring Milestone Interconnect	412
Selecting Milestone Interconnect or Milestone Federated Architecture (explained)	413
Milestone Interconnect and licensing	413
Milestone Interconnect (explained)	413
Milestone Interconnect setups (explained)	415
Add a remote site to your central Milestone Interconnect site	416
Assign user rights	417
Update remote site hardware	417
Establish remote desktop connection to remote system	417
Enable playback directly from remote site camera	418
Retrieve remote recordings from remote site camera	418
Configure your central site to respond to events from remote sites	419

Configuring remote connect services	420
Install STS environment for One-Click camera connection	421
Add/edit STSs	421
Register new Axis One-Click camera	421
Axis One-Click Camera connection properties	422
Configuring smart map	423
Geographic backgrounds (explained)	423
Specify OpenStreetMap tile server	424
Acquire API key for Google Maps or Bing Maps	425
Google Maps	425
Bing Maps	426
Enable Bing Maps or Google Maps in Management Client	426
Enable Bing Maps or Google Maps in XProtect Smart Client	426
Cached smart map files (explained)	427
Enable smart map editing	427
Enable editing of cameras on smart map	428
Set camera position, direction, field of view, and depth (smart map)	428
Setting up smart map with Milestone Federated Architecture	430
Troubleshooting (smart map)	431
Error when adding camera to smart map	431
Maintenance	432
Backing up and restoring system configuration	432
Backing up and restoring your system configuration (explained)	432
Back up log server's SQL database	432
Manually backing up your system configuration (explained)	432
Backing up and restoring the event server configuration (explained)	433
Backup and restore fail and problem scenarios (explained)	433
Back up system configuration manually	433
Restore system configuration from a manual backup	433
Select shared backup folder	434

Scheduled backup and restore of system configuration (explained)	435
Back up system configuration with scheduled backup	435
Backup and restore event server configuration	436
Restore system configuration from a scheduled backup	436
Moving the management server	437
Unavailable management servers (explained)	438
Move the system configuration	438
Replace a recording server	438
Move hardware	439
Move hardware (wizard)	440
Replace hardware	443
Managing the SQL Server and databases	446
Changing the SQL Server and database addresses (explained)	446
Change the log server's SQL Server and database	447
Change the management server and event server's SQL addresses	447
Managing server services	448
Server manager tray icons (explained)	448
Start or stop the Management Server service	450
Start or stop the Recording Server service	450
View status messages for Management Server or Recording Server	451
Manage encryption with the Server Configurator	451
Start, stop, or restart the Event Server service	452
Stopping the Event Server service	452
View Event Server or MIP logs	453
Managing registered services	455
Add and edit registered services	455
Manage network configuration	455
Registered services properties	455
Removing device drivers (explained)	456
Remove a recording server	457

Delete all hardware on a recording server	457
Troubleshooting	458
Issue: Change of SQL Server and database addresses prevents database access	458
Issue: Recording server startup fails due to port conflict	458
Issue: Recording Server goes offline when switching Management Server cluster node	459
Upgrade	460
Upgrade (explained)	460
Upgrade requirements	461
Upgrade best practices	462
Upgrade in a workgroup setup	464
Upgrade in a cluster	464

Copyright, trademarks, and disclaimer

Copyright © 2020 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 reserves 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 system installation folder.

Overview

Product overview

The XProtect VMS products are video management software designed for installations of all shapes and sizes. Whether you want to protect your store from vandalism or you want to manage a multi-site, high security installation, XProtect makes it possible. The solutions offer centralized management of all devices, servers, and users, and provide an extremely flexible rule system driven by schedules and events.

Your system consists of the following main components:

- The **management server** - the center of your installation, consists of multiple servers
- One or more **recording servers**
- One or more installations of **XProtect Management Client**
- **XProtect Download Manager**
- One or more installations of **XProtect® Smart Client**
- One or more uses of **XProtect Web Client** and/or installations of **XProtect Mobile** client if needed

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

You can install your system on virtualized servers or on multiple physical servers in a distributed setup (see A distributed system setup on page 28).

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

With the most feature-rich products installed (see Product comparison chart on page 43), your system can handle an unrestricted number of cameras, servers, and users and across multiple sites if required. Your system can handle IPv4 as well as IPv6.

Main system components

Management server

The management server is the central component of the VMS system. It stores the configuration of the surveillance system in an SQL database, either on a SQL Server on the management server computer itself or on a separate SQL Server on the network. It also handles user authentication, user rights, the rule system and more. To improve system performance, you can run several management servers as a Milestone Federated Architecture™. The management server runs as a service and is typically installed on a dedicated server.

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

Recording server

The recording server is responsible for communicating with the network cameras and video encoders, recording the retrieved audio and video as well as providing client access to both live and recorded audio and video. The recording server is also responsible for communicating with other Milestone products connected via the Milestone Interconnect technology.

Device drivers

- Network cameras and video encoders communicate through a device driver developed specifically for individual devices or a series of similar devices from the same manufacturer
- From the 2018 R1 release, the device drivers are split into two device packs: the regular device pack with newer drivers and a legacy device pack with older drivers
- The regular device pack is installed automatically when you install the recording server. Later, you can update the drivers by downloading and installing a newer version of the device pack
- The legacy device pack can only be installed if the system has a regular device pack installed. The drivers from the legacy device pack are automatically installed if a previous version is already installed on your system. It is available for manual download and installation on the software download page (<https://www.milestonesys.com/downloads/>)

Media database

- The recording server stores the retrieved audio and video data in the tailor-made high-performance media database optimized for recording and storing audio and video data
- The media database supports various unique features like; multistage archiving, video grooming, encryption, and adding a digital signature to the recordings

Event server

The event server handles various tasks related to events, alarms, maps and third-party integrations via the MIP SDK.

Events

- All system events are consolidated in the event server so there are one place and interface for partners to make integrations that utilize system events
- Furthermore, the event server offers third-party access to sending events to the system via the Generic events or Analytics events interface

Alarms

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

Maps

- The event server also hosts the maps that are configured and used in XProtect Smart Client

MIP SDK

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

Log server

The log server stores all log messages for the entire system in an SQL database. This log messages SQL database can exist on the same SQL Server as the management server's system configuration SQL database or on separate SQL Server. The log server is typically installed on the same server as the management server but can be installed on a separate server for increased performance of the management and log servers.

SQL Servers and databases

The management server, the event server and the log server store, for example, the system configuration, alarms, events and log messages in SQL databases on one or more SQL Server installations. The management server and the event server share the same SQL database while the log server has its own SQL database. The system installer includes Microsoft SQL Server Express which is free edition of SQL Server.

For very large systems or systems with many transactions to and from the SQL databases, Milestone recommends that you use a Microsoft® SQL Server® Standard or Microsoft® SQL Server® Enterprise edition of the SQL Server on a dedicated computer on the network and on a dedicated hard disk drive that is not used for other purposes. Installing the SQL Server on its own drive improves the entire system performance.

Mobile server

The mobile server is responsible for giving XProtect Mobile client and XProtect Web Client users access to the system.

In addition to acting as a system gateway for the two clients, the mobile server can transcode video, since the original camera video stream in many cases are too large to fit the bandwidth available for the client users.

If you are performing a **Distributed** or **Custom** installation, Milestone recommends that you install the mobile server on a dedicated server.

Active Directory

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

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

Management Client (explained)

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

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

For a detailed overview of the Management Client, see Navigating the Management Client on page 102.

Optional system components

The following components are not mandatory to use, but components that you can add to fulfill different purposes.

Failover recording server

The failover recording server is responsible for taking over the recording task if a recording server fails.

The failover recording server can operate in two modes:

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

The difference between the cold and hot standby modes is that in the cold standby mode, the failover recording server does not know which server to take over from, so it cannot start until a recording server fails. In the hot standby mode, the failover time is significantly shorter, as the failover recording server already knows which recording server it should take over from and can preload the configuration and start up completely - except for the last step of connecting to the cameras.

Failover management server

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

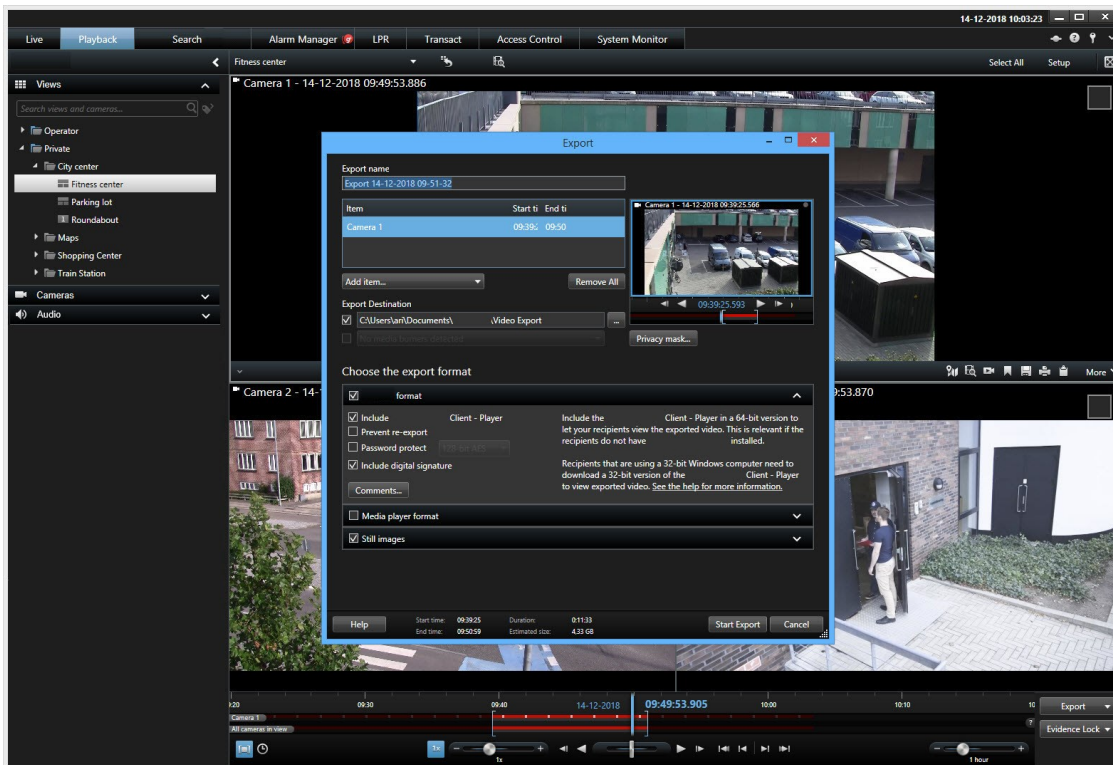
Clients

Introductions to the different clients used by the operators of a system.

XProtect Smart Client (explained)

Designed for Milestone XProtect® IP video management software, the XProtect Smart Client is an easy-to-use client application that provides intuitive control over security installations. Manage security installations with XProtect Smart Client which gives users access to live and recorded video, instant control of cameras and connected security devices, and an overview of recordings.

Available in multiple local languages, XProtect Smart Client has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.



The interface allows you to tailor your viewing experience to specific working environments by selecting a light or dark theme. It also features work-optimized tabs and an integrated video timeline for easy surveillance operation.

Using the MIP SDK, users can integrate various types of security and business systems and video analytics applications, which you manage through XProtect Smart Client.

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

XProtect Mobile client (explained)

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

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

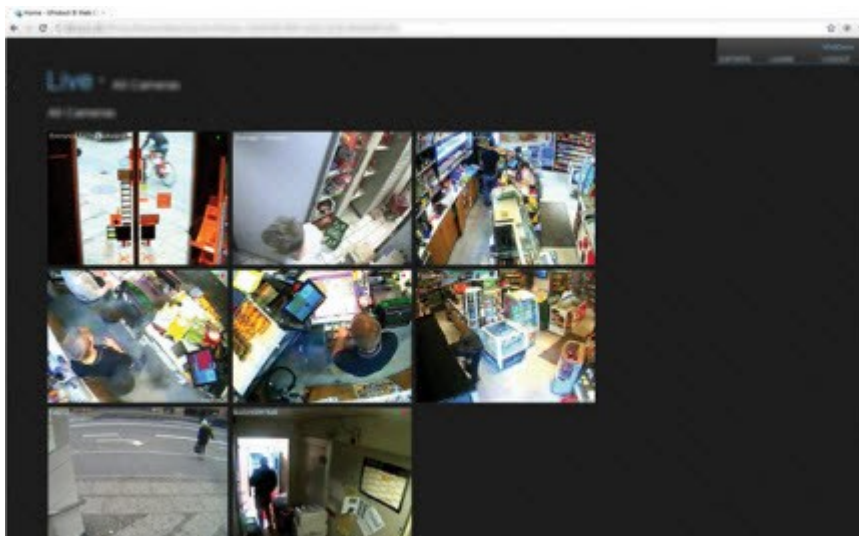


If you want to use the XProtect Mobile client with your system, you must have a XProtect Mobile server to establish the connection between the XProtect Mobile client and your system. Once the XProtect Mobile server is set up, download the XProtect Mobile client for free from Google Play or App Store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

You need one hardware device license per device that should be able to push video to your XProtect system.

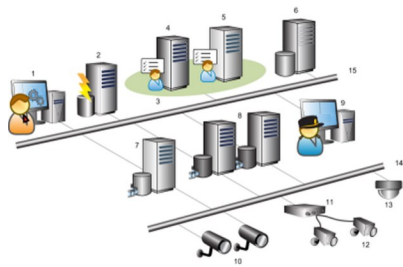
XProtect Web Client (explained)

XProtect Web Client is a web-based client application for viewing, playing back and sharing video. It provides instant access to the most commonly used surveillance functions, such as viewing live video, play back recorded video, print and export evidence. Access to features depends on individual user rights which are set up in Management Client.



To enable access to the XProtect Web Client, you must have a XProtect Mobile server to establish the connection between the XProtect Web Client and your system. The XProtect Web Client itself does not require any installation itself and works with most Internet browsers. Once you have set up the XProtect Mobile server, you can monitor your XProtect system anywhere from any computer or tablet with Internet access (provided you know the right external/Internet address, user name and password).

A distributed system setup



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

Legend:

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

Add-on products

Milestone has developed add-on products that fully integrate with XProtect to give you extra functionality. Access to add-on products are controlled by your software license code (SLC).

XProtect Access (explained)



The use of XProtect Access requires that you have purchased a base license that allows you to access this feature within your XProtect system. You also need an access control door license for each door you want to control.



You can use XProtect Access with access control systems from vendors where a vendor-specific plug-in for XProtect Access exists.

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

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

In XProtect Smart Client, the operator gets:

- Live monitoring of events at access points
- Operator aided passage for access requests
- Map integration
- Alarm definitions for access control events
- Investigation of events at access points
- Centralized overview and control of door states
- Cardholder information and management

The **Audit log** logs the commands that each user performs in the access control system from XProtect Smart Client.

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

XProtect LPR (explained)

Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

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

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

Examples of events in XProtect LPR:

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

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

XProtect Smart Wall (explained)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

XProtect Smart Wall is an advanced add-on tool that enables organizations to create video walls that meet their specific security demands. Smart Wall provides an overview of all the video data in the [VMS¹](#) system and can be shared between multiple operators.

With XProtect Smart Wall, operators can share almost any type of content available in XProtect Smart Client, for example video, images, text, alarms, and smart maps.

¹Short for "Video Management Software".



Initially, XProtect Smart Wall is configured by a system administrator in XProtect Management Client. This includes presets that control the layout of the Smart Wall and how cameras are distributed across the different monitors. In XProtect Smart Client, operators can change what is being displayed on the Smart Wall by applying different presets. Display changes can also be controlled by rules that automatically change the presets.

With the Smart Wall overview, operators can add specific content or whole views to Smart Wall monitors through simple drag-and-drop operations.

XProtect Transact (explained)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

XProtect Transact is an add-on to Milestone's IP video surveillance solutions.

XProtect Transact is a tool for observing ongoing transactions and investigating transactions in the past. The transactions are linked with the digital surveillance video monitoring the transactions, for example to help you prove fraud or provide evidence against a perpetrator. There is a 1-to-1 relationship between the transaction lines and video images.

The transaction data may originate from different types of transaction sources, typically point of sales (PoS) systems or automated teller machines (ATM).

Milestone ONVIF Bridge (explained)

ONVIF is an open, global forum that is working to standardize and secure the way that IP video surveillance products communicate. The goal is to make it easy to exchange video data. For example, to enable law enforcement, surveillance centers, or similar organizations to quickly access live and recorded video streams in any IP-based surveillance system.

Milestone Systems wants to support this goal, and has developed the Milestone ONVIF Bridge toward that end. Milestone ONVIF Bridge is a part of the Milestone Open Platform, and offers an interface that supports the parts of the ONVIF standard for retrieving live and recorded video from any Milestone VMS product.

This document provides the following:

- Information about the ONVIF standard and links to reference materials
- Instructions for installing and configuring the Milestone ONVIF Bridge in your XProtect VMS product
- Examples of how to enable various types of ONVIF clients to stream live and recorded video from XProtect VMS products

XProtect DLNA Server (explained)

DLNA (Digital Living Network Alliance) is a standard for connecting multimedia devices. Electronic manufactures get their products DLNA certified to ensure interoperability between different vendors and devices and thereby enable them to distribute multimedia content such as audio, video, and photos.

Public displays and TVs are often DLNA certified and connected to a network. They are able to scan the network for media content, connect to the device, and request a media stream to their built-in media player. XProtect DLNA Server can be discovered by certain DLNA certified devices and deliver live video streams from selected cameras to DLNA certified devices with a media player.



The DLNA devices have a live video delay of 1-10 seconds. This is caused by different buffer sizes in the devices.

XProtect DLNA Server must be connected to the same network as the XProtect system and the DLNA device must be connected to the same network as XProtect DLNA Server.

Ports used by the system

All XProtect components and the ports needed by them are listed below. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the system uses. You should only enable these ports. The lists also include the ports used for local processes.

They are arranged in two groups:

- **Server components** (services) offer their service on particular ports which is why they need to listen for client requests on these ports. Therefore, these ports need to be opened in the Windows Firewall for inbound and outbound connections
- **Client components** (clients) initiate connections to particular ports on server components. Therefore, these ports need to be opened for outbound connections. Outbound connections are typically open by default in the Windows Firewall

If nothing else is mentioned, ports for server components must be opened for inbound connections, and ports for client components must be opened for outbound connections.

Do keep in mind that server components can act as clients to other server components as well.

The port numbers are the default numbers, but this can be changed. Contact Milestone support, if you need to change ports that are not configurable through the Management Client.

Server components (inbound connections)

Each of the following sections list the ports that need to be opened for a particular service. To figure out which ports need to be opened on a particular computer, you need to consider all services running on the computer.

Management Server service and related processes

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	All XProtect components The Management Server service and Recording Server services	Main communication, for example, authentication and configurations. Handles registration of recording servers and management servers via the Authorization Server service.
443	HTTPS	IIS	XProtect Smart Client and the Management Client The Management Server service and Recording Server services	Authentication of basic users. Handles registration of recording servers and management servers via the Authorization Server service.
6473	TCP	Management Server service	Management Server Manager tray icon, local connection only.	Showing status and managing the service.
8080	TCP	Management server	Local connection only.	Communication between internal processes on the server.
9000	HTTP	Management server	Recording Server services	Web service for internal communication between servers.
9000	TCP	Management Server	Recording Server services	Authentication, configuration, token exchange.

Port number	Protocol	Process	Connections from...	Purpose
		service		
12345	TCP	Management Server service	XProtect Smart Client	Communication between the system and Matrix recipients. You can change the port number in the Management Client.
12974	TCP	Management Server service	Windows SNMP Service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect 2014 systems or older, the port number was 6475. In XProtect 2019 R2 systems and older, the port number was 7475.

SQL Server service

Port number	Protocol	Process	Connections from...	Purpose
1433	TCP	SQL Server	Management Server service	Storing and retrieving configurations.
1433	TCP	SQL Server	Event Server service	Storing and retrieving events.
1433	TCP	SQL Server	Log Server service	Storing and retrieving log entries.

Data Collector service

Port number	Protocol	Process	Connections from...	Purpose
7609	HTTP	IIS	On the management server computer: Data Collector services on all other servers. On other computers: Data Collector service on the Management Server.	System Monitor.

Event Server service

Port number	Protocol	Process	Connections from...	Purpose
1234	TCP/UDP	Event Server Service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
1235	TCP	Event Server service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
9090	TCP	Event Server service	Any system or device that sends analytics events to your XProtect system.	Listening for analytics events from external systems or devices. Only relevant if the Analytics Events feature is enabled.
22331	TCP	Event Server service	XProtect Smart Client and the Management Client	Configuration, events, alarms, and map data.
22333	TCP	Event Server service	MIP Plug-ins and applications.	MIP messaging.

Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
5210	TCP	Recording Server Service	Failover recording servers.	Merging of databases after a failover recording server had been running.
5432	TCP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7563	TCP	Recording Server Service	XProtect Smart Client, Management Client	Retrieving video and audio streams, PTZ commands.
8966	TCP	Recording Server Service	Recording Server Manager tray icon, local connection only.	Showing status and managing the service.
9001	HTTP	Recording Server Service	Management server	Web service for internal communication between servers. If multiple Recording Server instances are in use, every instance needs its own port. Additional ports will be 9002, 9003, etc.
11000	TCP	Recording Server	Failover recording	Polling the state of recording servers.

Port number	Protocol	Process	Connections from...	Purpose
		Service	servers	
12975	TCP	Recording Server Service	Windows SNMP service	<p>Communication with the SNMP extension agent.</p> <p>Do not use the port for other purposes even if your system does not apply SNMP.</p> <p>In XProtect 2014 systems or older, the port number was 6474.</p> <p>In XProtect 2019 R2 systems and older, the port number was 7474.</p>
65101	UDP	Recording Server service	Local connection only	Listening for event notifications from the drivers.



In addition to the inbound connections to the Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

Failover Server service and Failover Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Recording Server Service	Cameras, encoders, and I/O devices.	<p>Listening for event messages from devices.</p> <p>The port is disabled by default.</p>
5210	TCP	Recording Server Service	Failover recording servers	Merging of databases after a failover recording server had been running.

Port number	Protocol	Process	Connections from...	Purpose
5432	TCP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7474	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP.
7563	TCP	Recording Server Service	XProtect Smart Client	Retrieving video and audio streams, PTZ commands.
8844	UDP	Failover recording servers	Local connection only.	Communication between the servers.
8966	TCP	Failover Recording Server Service	Failover Recording Server Manager tray icon, local connection only.	Showing status and managing the service.
8967	TCP	Failover Server Service	Failover Server Manager tray icon, local connection only.	Showing status and managing the service.
8990	TCP	Failover Server Service	Management Server service	Monitoring the status of the Failover Server service.
9001	HTTP	Failover Server Service	Management server	Web service for internal communication between servers.

Log Server service

Port number	Protocol	Process	Connections from...	Purpose
22337	HTTP	Log Server service	All XProtect components except for Management Client and the recording server.	Write to, read from, and configure the log server.



In addition to the inbound connections to the Failover Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

Mobile Server service

Port number	Protocol	Process	Connections from...	Purpose
8000	TCP	Mobile Server service	Mobile Server Manager tray icon, local connection only.	SysTray application.
8081	HTTP	Mobile Server service	Mobile clients, Web clients, and Management Client.	Sending data streams; video and audio.
8082	HTTPS	Mobile Server service	Mobile clients and Web clients.	Sending data streams; video and audio.

LPR Server service

Port number	Protocol	Process	Connections from...	Purpose
22334	TCP	LPR Server Service	Event server	Retrieving recognized license plates and server status. In order to connect, the Event server

Port number	Protocol	Process	Connections from...	Purpose
				must have the LPR plug-in installed.
22334	TCP	LPR Server Service	LPR Server Manager tray icon, local connection only.	SysTray application

Milestone ONVIF Bridge service

Port number	Protocol	Process	Connections from...	Purpose
580	TCP	ONVIF Bridge Service	ONVIF clients	Authentication and requests for video stream configuration.
554	RTSP	RTSP Service	ONVIF clients	Streaming of requested video to ONVIF clients.

XProtect DLNA Server service

Port number	Protocol	Process	Connections from...	Purpose
9100	HTTP	DLNA Server Service	DLNA device	Device discovery and providing DLNA channels configuration. Requests for video streams.
9200	HTTP	DLNA Server Service	DLNA device	Streaming of requested video to DLNA devices.

XProtect Screen Recorder service

Port number	Protocol	Process	Connections from...	Purpose
52111	TCP	XProtect Screen Recorder	Recording Server Service	Provides video from a monitor. It appears and acts in the same way as a camera on the recording server. You can change the port number in the Management Client.

Server components (outbound connections)

Management Server service

Port number	Protocol	Connections to...	Purpose
443	HTTPS	Milestone Customer Dashboard via https://service.milestonesys.com/	Send status, events and error messages from the XProtect system to Milestone Customer Dashboard.
443	HTTPS	The License server that hosts the License Management service. Communication is via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Activating licenses.

Log Server service

Port number	Protocol	Connections to...	Purpose
443	HTTP	Log server	Forwarding messages to the log server.

Cameras, encoders, and I/O devices (inbound connections)

Port number	Protocol	Connections from...	Purpose
80	TCP	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
443	HTTPS	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
554	RTSP	Recording servers and failover recording servers	Data streams; video and audio.

Cameras, encoders, and I/O devices (outbound connections)

Port number	Protocol	Connections to...	Purpose
25	SMTP	Recording servers and failover recording servers	Sending event notifications (deprecated).
5432	TCP	Recording servers and failover recording servers	Sending event notifications. The port is disabled by default.
22337	HTTP	Log server	Forwarding messages to the log server.



Only a few camera models are able to establish outbound connections.

Client components (outbound connections)

XProtect Smart Client, XProtect Management Client, XProtect Mobile server

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management Server service	Authentication
443	HTTPS	Management Server service	Authentication of basic users.
7563	TCP	Recording Server service	Retrieving video and audio streams, PTZ commands.
22331	TCP	Event Server service	Alarms.

XProtect Web Client, XProtect Mobile client

Port number	Protocol	Connections to...	Purpose
8081	HTTP	XProtect Mobile server	Retrieving video and audio streams.
8082	HTTPS	XProtect Mobile server	Retrieving video and audio streams.

Product comparison chart

XProtect VMS includes the following products:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

The complete feature list is available on the product overview page on the Milestone website (<https://www.milestonesys.com/solutions/platform/product-index/>).

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

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Sites per SLC	1	1	Multi-site	Multi-site	Multi-site
Recording servers per SLC	1	1	Unrestricted	Unrestricted	Unrestricted
Hardware devices per recording server	8	48	Unrestricted	Unrestricted	Unrestricted
Milestone Interconnect™	-	Remote site	Remote site	Remote site	Central/remote site
Milestone Federated Architecture™	-	-	-	Remote site	Central/remote site
Recording server failover	-	-	-	Cold and hot standby	Cold and hot standby
Remote connect services	-	-	-	-	✓
Edge storage support	-	-	✓	✓	✓
Multi-stage video storage	Live databases + 1 archive	Live databases + 1 archive	Live databases + 1 archive	Live databases + unrestricted archives	Live databases + unrestricted archives
SNMP notification	-	-	-	✓	✓
Time controlled user access rights	-	-	-	-	✓
Reduce frame rate (grooming)	-	-	-	✓	✓
Video data encryption (recording server)	-	-	-	✓	✓

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Database signing (recording server)	-	-	-	✓	✓
PTZ priority levels	1	1	3	32000	32000
Extended PTZ (Reserve PTZ session and patrolling from XProtect Smart Client)	-	-	-	✓	✓
Evidence lock	-	-	-	-	✓
Bookmark function	-	-	Manual only	Manual and rule-based	Manual and rule-based
Live multi-streaming or multicasting / Adaptive streaming	-	-	-	✓	✓
Direct streaming	-	-	-	✓	✓
Overall security	Client user rights	Client user rights	Client user rights	Client user rights	Client user rights/ administrator user rights
XProtect Management Client profiles	-	-	-	-	✓
XProtect Smart Client profiles	-	-	3	3	Unrestricted
XProtect Smart Wall	-	-	-	optional	✓
System Monitor	-	-	-	✓	✓

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Smart map	-	-	-	✓	✓
Two-step verification	-	-	-	-	✓
DLNA support	-	✓	✓	✓	✓
Privacy masking	-	✓	✓	✓	✓
Device password management			✓	✓	✓

Licensing

Licenses (explained)

If you have installed a XProtect Essential+ system, you can run the system and eight hardware device licenses for free. Automatic license activation is enabled and hardware will be activated as you add it to the system. Only when you upgrade (see [Change the Software License Code](#) on page 48) to a more advanced XProtect product, the rest of this topic and the other licensing related topics in this documentation is relevant.

When you purchase your software and licenses, you receive:

- An order confirmation
- A software license file named after your SLC (Software License Code) and with the .lic extension

Your SLC is also printed on your order confirmation and consists of several numbers and letters grouped by hyphens like:

- Product version 2014 or earlier: xxx-xxxx-xxxx
- Product version 2016 or later: xxx-xxx-xxx-xx-xxxxxx

The software license file contains all information about your purchased VMS products and licenses. Milestone recommends that you store the information about your SLC and a copy of your software license file in a safe place from which you can find them again. In the navigation tree, you can also see your SLC if you select **Basics > License Information**. You may need the software license file or your SLC when you, for example create a My Milestone user account, contact your reseller for support and if you need to make changes to your system.

To get started, you download the software from our website (<https://www.milestonesys.com/downloads/>). While you are installing (see [Install a new XProtect system](#) on page 73) the software, you are asked to provide the software license file.

Once the installation is complete and you have activated your licenses, you can see an overview of your licenses (see [Licenses \(explained\)](#)) for all installations on the same SLC on the **Basics > License Information** page.

You have purchased at least two types of licenses:

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

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

For more information, see the list of supported hardware on the Milestone website (<https://www.milestonesys.com/supported-devices/>). If you want to use the video push feature in XProtect Mobile,

you also need one hardware device license per mobile device or tablet that should be able to push video to your system. If you are short of hardware device licenses, you can disable (see Disable/enable hardware on page 177) less important hardware devices to allow new hardware devices to run instead.

If your surveillance system is the central site of a larger system hierarchy using Milestone Interconnect, you need Milestone Interconnect camera licenses to be able to view video from hardware devices on remote sites. Only XProtect Corporate can act as a central site.

Most XProtect add-on products require additional license types. The software license file also includes information about your licenses for add-on products. Some add-on products have their own separate software license files.

Change the Software License Code

If you run your installation on a temporary Software License Code (SLC) during the first period or have upgraded to a more advanced XProtect product, you can change your SLC without any un- or reinstallation actions when you have received your new software license file.



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

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



2. Right-click the **Management Server** icon and select **Change License**.
3. Click **Import License**.
4. Next, select the software license file saved for this purpose. When done, the selected software license file location is added just below the **Import License** button.
5. Click **OK** and you are now ready to register SLC. See Register Software License Code on page 63.

Requirements and considerations

Daylight saving time (explained)

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

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



Do not change the DST setting when you are in the DST period or if you have recordings from a DST period.

Spring: Switch from Standard Time to DST

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

Example:

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

Fall: Switch from DST to Standard Time

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

Example:

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

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

Time servers (explained)

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

For information about how to configure a time server, search the Microsoft website (<https://www.microsoft.com/>) for 'time server', 'time service', or similar terms.

Limit size of database

To prevent the SQL database (see SQL Servers and databases on page 24) growing to a size that affects the performance of the system, you can specify for how many days the different types of events and alarms are stored in the database.

1. Open the **Tools** menu.
2. Click **Options>Alarms and Events** tab.

The screenshot shows the 'Options' dialog box with the 'Alarms and Events' tab selected. The dialog is divided into three main sections: Alarm settings, Log settings, and Event retention.

Alarm settings:

- Keep closed alarms for: 1 day(s)
- Keep all other alarms for: 30 day(s)

Log settings:

- Keep logs for: 30 day(s)
- ☐ Enable verbose logging

Event retention:

Event types	Retention time (days)
Default	1
System Events	0
Device Events	0
Hardware Events	0
Recording Server Events	0
Archive Disk Available	Follow group
Archive Failure: Disk Unavailable	Follow group
Database is being repaired	Follow group
System Monitor Events	0
External Events	1

Buttons at the bottom: Help, OK, Cancel.

3. Make the required settings. For more information, see Alarms and Events tab (options) on page 118.

IPv6 and IPv4 (explained)

Your system supports IPv6 as well as IPv4. So does XProtect Smart Client.

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

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

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

Using the system with IPv6 (explained)

The following conditions apply when using the system with IPv6:

Servers

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

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

Devices

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

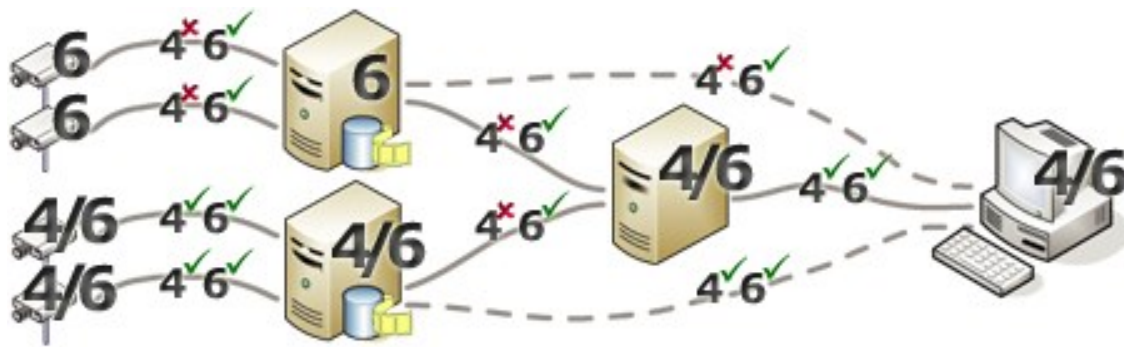
Clients

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

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

However, the XProtect Smart Client users do not have to be on an IPv6 network themselves, provided your network equipment supports communication between different IP versions, and they have installed the IPv6 protocol on their computers. See also illustration. To install IPv6 on a client computer, open a command prompt, enter *ipv6 install*, and press **ENTER**.

Example illustration



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

No Matrix Monitor compatibility

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

Writing IPv6 addresses (explained)

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

Example: `2001:0B80:0000:0000:0000:0F80:3FA8:18AB`

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

Example:

`2001:0B80:0000:0000:0000:0F80:3FA8:18AB` can be shortened to

`2001:B80:0000:0000:0000:F80:3FA8:18AB` if removing the leading zeros, or to

`2001:0B80::0F80:3FA8:18AB` if removing the 0000 blocks, or even to

`2001:B80::F80:3FA8:18AB` if removing the leading zeros as well as the 0000 blocks.

Using IPv6 Addresses in URLs

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

Example of a URL with an IPv6 address:

`http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]`, which may of course be shortened to, for example, `http://[2001:B80::F80:3FA8:18AB]`

Example of a URL with an IPv6 address and a port number:

`http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234`, which may of course be shortened to, for example, `http://[2001:B80::F80:3FA8:18AB]:1234`

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

Virtual servers

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

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

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

Multiple management servers (clustering) (explained)

The management server can be installed on multiple servers within a cluster of servers. This ensures that the system has very little downtime. If a server in the cluster fails, another server in the cluster automatically takes over the failed server's job running the management server. The automatic process of switching over the management server services to run on another server in the cluster takes up to 30 seconds.

It is only possible to have one active management server per surveillance setup, but other management servers may be set up to take over in case of failure.



The allowed number of failovers is limited to two within a six-hour period. If exceeded, management server services are not automatically started by the clustering service. The number of allowed failovers can be changed to better fit your needs.

Requirements for clustering

- Two machines with Microsoft Windows Server 2012 or newer. Make sure that:
 - All servers that you want to add as cluster nodes are running the same version of Windows Server
 - All servers that you want to add as cluster nodes are joined to the same domain
 - You have log-in access to the Windows account as the local administrator

About clusters in Microsoft Windows Servers, see Failover clusters <https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster>.

- A Microsoft SQL Server installation

Either an external SQL Server and database installed **outside** the server cluster **or** an **internal** SQL Server service (clustered) within the server cluster (creating an internal SQL Server service requires the use of the Microsoft® SQL Server® Standard or Microsoft® SQL Server® Enterprise edition, which can work as a clustered SQL Server).

Protect recording databases from corruption

Camera databases can become corrupted. Several database repair options exist to resolve such a problem. but Milestone recommends that you take steps to ensure that your camera databases do not become corrupted.

Hard disk failure: protect your drives

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

- Vibration (make sure the surveillance system server and its surroundings are stable)
- Strong heat (make sure the server has adequate ventilation)
- Strong magnetic fields (avoid)
- Power outages (make sure you use an Uninterruptible Power Supply (UPS))
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive)
- Fire, water, etc. (avoid)

Windows Task Manager: be careful when you end processes

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

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

Power outages: use a UPS

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

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

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

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

SQL database transaction log (explained)

Each time a change is written to an SQL database, the SQL database logs this change in its transaction log.

With the transaction log, you can roll back and undo changes to the SQL database through Microsoft® SQL Server Management Studio. By default, the SQL database stores its transaction log indefinitely which over time means that the transaction log has more and more entries. The transaction log is by default located on the system drive, and if the transaction log keeps growing, it may prevent Windows from running properly.

To avoid such a scenario, flushing the transaction log regularly is a good idea. Flushing it does not make the transaction log file smaller, but cleans its content and thereby prevents it from growing out of control. Your VMS system does not flush transaction logs. In SQL Server, there are ways of flushing the transaction log. Visit the Microsoft support page <https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017> and search for *Transaction log truncation*.

Minimum system requirements

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

Before you start installation

Milestone recommends that you go through the requirements described in the next sections, before you start the actual installation.

Prepare your servers and network

Operating system

Make sure that all servers have a clean installation of a Microsoft Windows operating system, and that it is updated with all the latest Windows updates.

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

Microsoft® .NET Framework

Check that all servers have Microsoft .NET Framework 4.7 or higher installed.

Network

Assign static IP addresses or make DHCP reservations to all system components and cameras. To make sure that sufficient bandwidth is available on your network, you must understand how and when the system consumes bandwidth. The main load on your network consists of three elements:

- Camera video streams
- Clients displaying video
- Archiving of recorded video

The recording server retrieves video streams from the cameras, which results in a constant load on the network. Clients that display video consume network bandwidth. If there are no changes in the content of the client views, the load is constant. Changes in view content, video search, or playback, make the load dynamic.

Archiving of recorded video is an optional feature that lets the system move recordings to a network storage if there is not enough space in the internal storage system of the computer. This is a scheduled job that you have to define. Typically, you archive to a network drive which makes it a scheduled dynamic load on the network.

Your network must have bandwidth headroom to cope with these peaks in the traffic. This enhances the system responsiveness and general user experience.

Prepare Active Directory

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

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

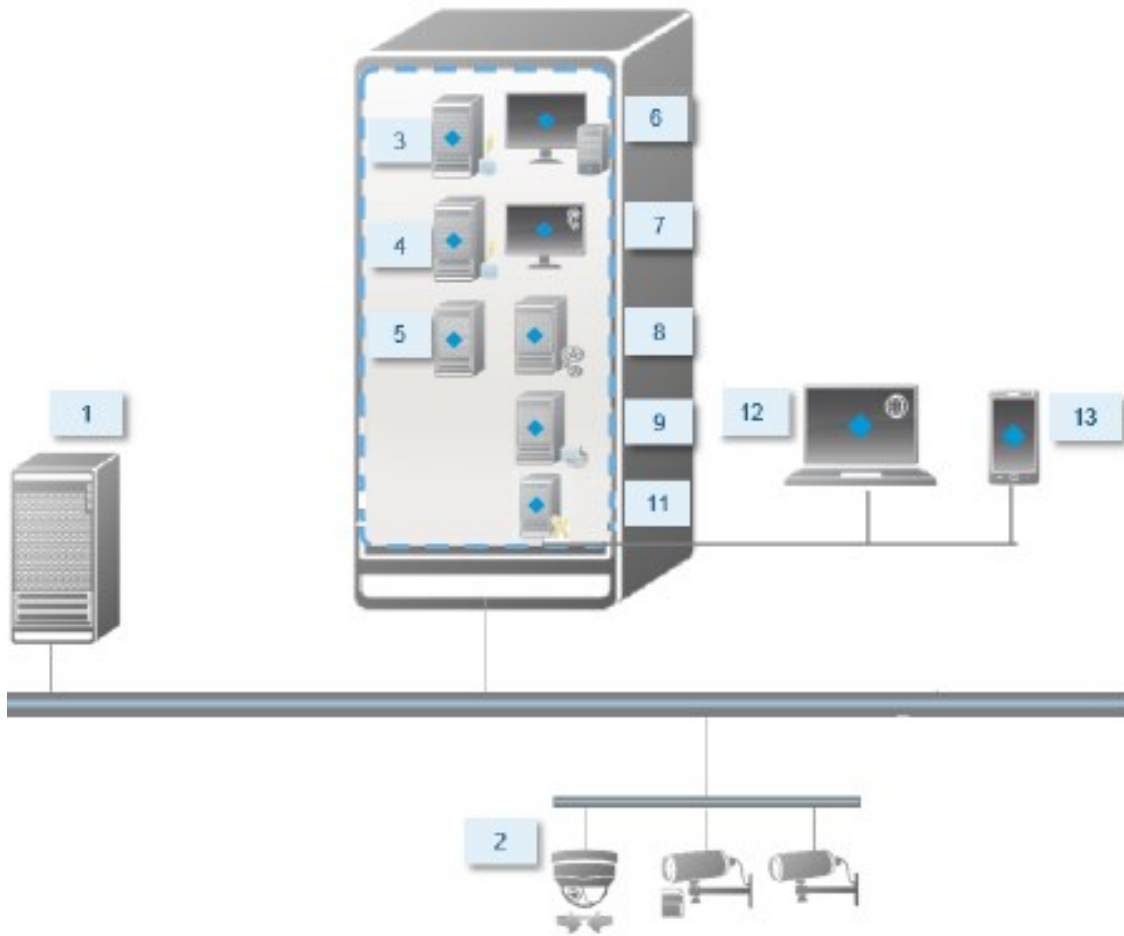
Basic users are not supported in Milestone Federated Architecture systems, so if you plan to use Milestone Federated Architecture, you must add users as Windows users through the Active Directory service. If you do not install Active Directory, follow the steps in Installation for workgroups on page 91 when you install.

Installation method

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

Options	Description
Single Computer	<p>Installs all server and client components, as well as the SQL Server on the current computer.</p> <p>When the installation completes, you get the possibility to configure your system through a wizard. If you agree to continue, the recording server scans your network for hardware, and you can select which hardware devices to add to your system. The max number of hardware devices that can be added in the configuration wizard depends on your base license. Also, cameras are preconfigured in views, and a default Operator role is created. After installation, XProtect Smart Client opens, and you are ready to use the system.</p>
Custom	<p>The management server is always selected in the system component list and is always installed, but you can select freely what to install on the current computer among the other server and client components.</p> <p>By default, the recording server is not selected in the component list, but you can change this. You can install the not selected components on other computers afterwards.</p>

Single Computer installation

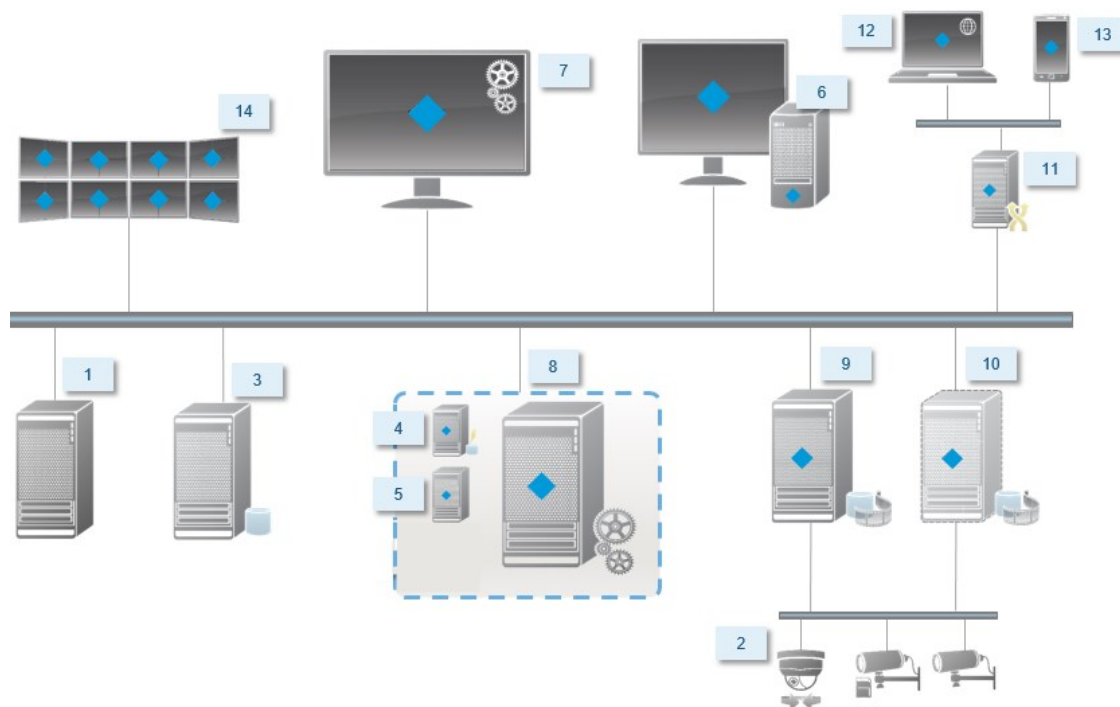


Typical system components in a system:

1. **Active Directory**
2. **Devices**
3. **Server with SQL Server**
4. **Event server**
5. **Log server**
6. **XProtect Smart Client**
7. **Management Client**
8. **Management server**
9. **Recording server**

10. **Failover recording server**
11. **XProtect Mobile server**
12. **XProtect Web Client**
13. **XProtect Mobile client**
14. **XProtect Smart Client with XProtect Smart Wall**

Custom installation - example of distributed system components



Decide on a SQL Server edition

Microsoft® SQL Server® Express is a free edition of SQL Server and is easy to install and prepare for use compared to the other SQL Server editions. During a **Single computer** installation, Microsoft SQL Server Express is installed unless a SQL Server is already installed on the computer.

The XProtect VMS installation includes Microsoft SQL Server Express version 2019. Not all Windows operating systems support this edition of SQL Server. Before you install XProtect VMS, verify that your operating system supports SQL Server 2019. If your operating system does not support this edition of SQL Server, install a supported edition of SQL Server before you start the XProtect VMS installation. For information about supported SQL Server editions, see <https://www.milestonesys.com/systemrequirements/>.

For very large systems or systems with many transactions to and from the SQL databases, Milestone recommends that you use a Microsoft® SQL Server® Standard or Microsoft® SQL Server® Enterprise edition of the SQL Server on a dedicated computer on the network and on a dedicated hard disk drive that is not used for other purposes. Installing the SQL Server on its own drive improves the entire system performance.

Select service account

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

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

Domain environment

In a domain environment:

- Milestone recommends that you use the built-in Network Service account
It is easier to use even if you need to expand the system to multiple computers.
- You can also use domain user accounts, but they are potentially more difficult to configure

Workgroup environment

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



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

Kerberos authentication (explained)

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

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

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

To make mutual authentication possible in your XProtect VMS you must register Service Principal Names (SPN) in the active directory. An SPN is an alias that uniquely identifies an entity such as a XProtect server service. Every service that uses mutual authentication must have an SPN registered so that clients can identify the service on the network. Without correctly registered SPNs, mutual authentication is not possible.

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

Service	Port number
Management Server - IIS	80 - Configurable
Management Server - Internal	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334



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

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

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

This is the Milestone SPN naming scheme:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

The following is an example of SPNs for the Recording Server service running on a computer with the following details:

```
Hostname: Record-Server1  
Domain: Surveillance.com
```

SPNs to register:

```
VideoOS/Record-Server1:7609  
VideoOS/Record-Server1.Surveillance.com:7609
```

Virus scanning exclusions (explained)

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

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

Create the following additional exclusions:

- File types: .blk, .idx, .pic
- Folders and subfolders:
 - C:\Program Files\Milestone or C:\Program Files (x86)\Milestone
 - C:\ProgramData\Milestone\MIPSDK
 - C:\ProgramData\Milestone\XProtect Mobile Server\Logs
 - C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
 - C:\ProgramData\Milestone\XProtect Event Server\Logs
 - C:\ProgramData\Milestone\XProtect Log Server
 - C:\ProgramData\Milestone\XProtect Management Server\Logs
 - C:\ProgramData\Milestone\XProtect Recording Server\Logs
 - C:\ProgramData\Milestone\XProtect Report Web Server\Logs

- Exclude network scanning on the following TCP ports:

Product	TCP ports
XProtect VMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

or

- Exclude network scanning of the following processes:

Product	Processes
XProtect VMS	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

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

Register Software License Code

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

You can install a free version of XProtect Essential+. This version provides you with limited capabilities of the XProtect VMS for a limited number of cameras. You must have internet connection to install XProtect Essential+.

The Software License Code (SLC) is printed on your order confirmation and the software license file is named after your SLC.

Milestone recommends that you register your SLC on our website (<https://online.milestonesys.com/>) before installation. Your reseller may have done that for you.

Device drivers (explained)

Your system uses video device drivers to control and communicate with the camera devices connected to a recording server. You must install device drivers on each recording server on your system.

From the 2018 R1 release, the device drivers are split into two device packs: the regular device pack with newer drivers and a legacy device pack with older drivers.

The regular device pack is installed automatically when you install the recording server. Later, you can update the drivers by downloading and installing a newer version of the device pack. Milestone releases new versions of device drivers regularly and makes them available on the download page (<https://www.milestonesys.com/downloads/>) on our website as device packs. When you update a device pack, you can install the latest version on top of any version you may have installed.

The legacy device pack can only be installed if the system has a regular device pack installed. The drivers from the legacy device pack are automatically installed if a previous version is already installed on your system. It is available for manual download and installation on the software download page (<https://www.milestonesys.com/downloads/>).

Stop the Recording Server service before you install, otherwise you need to restart the computer.

To ensure best performance, always use the latest version of device drivers.

Requirements for offline installation

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

- The Milestone XProtect VMS Products 2020 R2 System Installer.exe file
- The software license file (SLC) for your XProtect system
- OS installation media including the required .NET version (<https://www.milestonesys.com/systemrequirements/>)

Secure communication (explained)

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL).

In XProtect VMS, the secure communication is obtained by using SSL/TLS with asymmetric encryption (RSA).

SSL/TLS uses a pair of keys—one private, one public—to authenticate, secure, and manage secure connections.

A certificate authority (CA) can issue certificates to web services on servers using a CA certificate. This certificate contains two keys, a private key and public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server. Whenever a service client calls the web service, the web service sends the server certificate

including the public key to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificate to exchange a secret key and thereby establish a secure SSL/TLS connection.

For more information about TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security



Certificates have an expiry date. XProtect VMS will not warn you when a certificate is about to expire. If a certificate expires:

- The clients will no longer trust the recording server with the expired certificate and thus cannot communicate with it.
- The recording servers will no longer trust the management server with the expired certificate and thus cannot communicate with it.
- The mobile devices will no longer trust the mobile server with the expired certificate and thus cannot communicate with it.

To renew the certificates, follow the steps in this guide as you did when you created certificates.

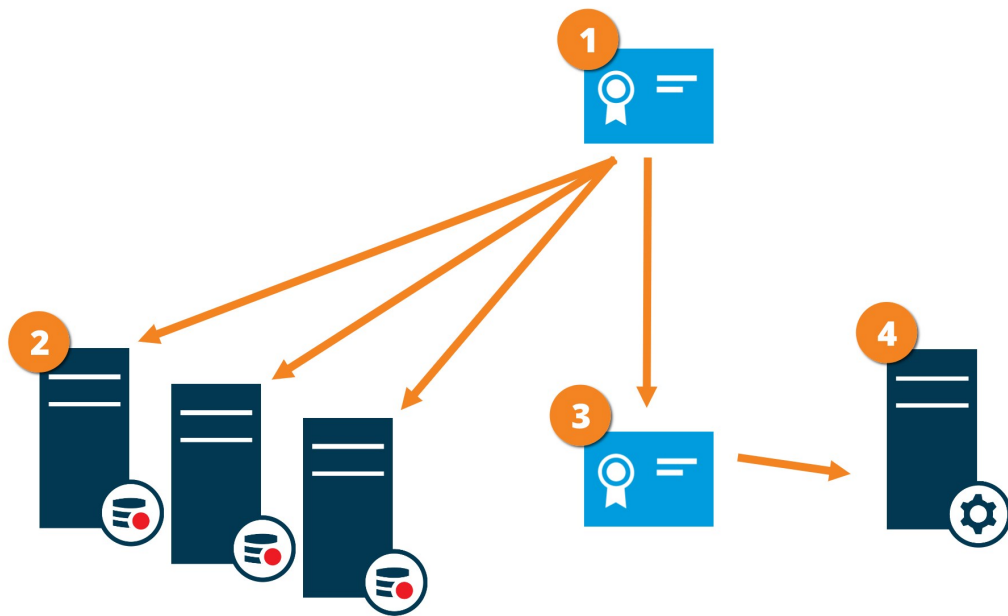
When you renew a certificate with the same subject name and add it to the Windows Certificate Store, the servers will automatically pick up the new certificate. This makes it easier to renew certificates for many servers without having to re-select the certificate for each server and without restarting the services.

Management server encryption (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. If you enable encryption on the management server, you must also enable encryption on all of the recording servers. Before you enable encryption, you must install security certificates on the management server and all recording servers.

Certificate distribution for management servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the management server.



- ❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (management server) and by the party that verifies the certificate (recording servers)
- ❷ The CA certificate must be trusted on all recording servers. In this way the recording servers can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the management server and the recording servers
- ❹ The CA certificate must be installed on the computer on which the management server is running

Requirements for the private management server certificate:

- Issued to the management server so that the management server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server itself, by trusting the CA certificate that was used to issue the management server certificate
- Trusted on all recording servers connected to the management server, by trusting the CA certificate that was used to issue the management server certificate

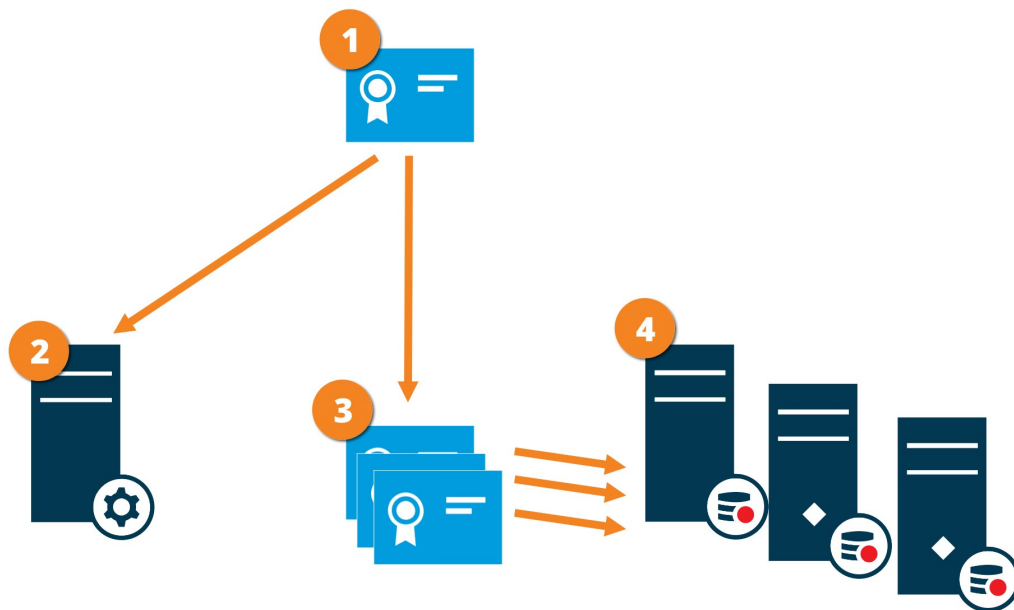
Encryption from the management server to the recording server (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. Encryption of this communication must follow the encryption setting on the

management server. So, if management server encryption is enabled, this must also be enabled on the recording servers, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all recording servers, including failover recording servers.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.



- ❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (management server)
- ❷ The CA certificate must be trusted on the management server. In this way the management server can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the recording servers and the management server
- ❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server, by trusting the CA certificate that was used to issue the recording server certificate

Encryption between the management server and the Data Collector Server (explained)

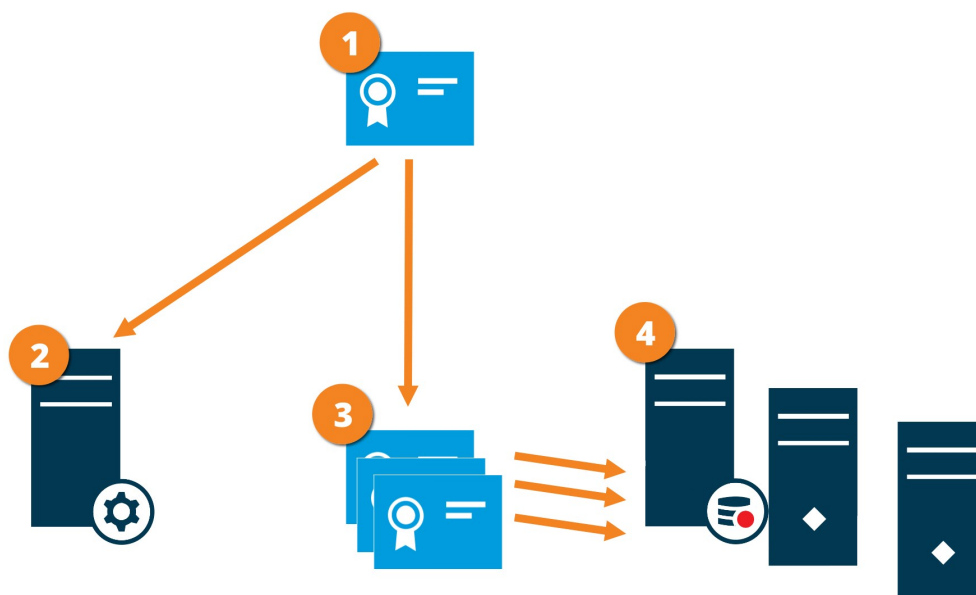
You can encrypt the two-way connection between the management server and the Data Collector affiliated when you have an external server of the following type:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

When you enable encryption on the management server, it applies to connections from all the Data Collector servers that connect to the management server. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the Data Collector servers affiliated with each external server, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all Data Collector servers affiliated with the external servers.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.



- ❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (data collector server) and by the party that verifies the certificate (management server)
- ❷ The CA certificate must be trusted on the management server. In this way the management server can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the data collector servers and the management server
- ❹ The CA certificate must be installed on the computers on which the data collector servers are running

Requirements for the private data collector server certificate:

- Issued to the data collector server so that the data collector server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server, by trusting the CA certificate that was used to issue the data collector server certificate

Encryption to clients and servers that retrieve data from the recording server (explained)

When you enable encryption on a recording server, communication to all clients, servers, and integrations that retrieve data streams from the recording server are encrypted. In this document referred to as 'clients':

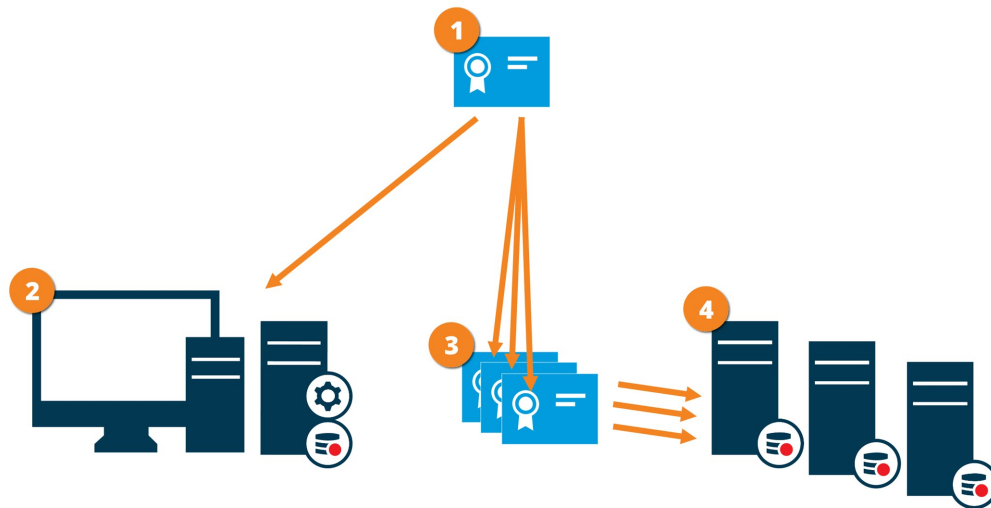
- XProtect Smart Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server through Milestone Interconnect
- Some third-party MIP SDK integrations



For solutions built with MIP SDK 2018 R3 or earlier that accesses recording servers: If the integrations are made using MIP SDK libraries, they need to be rebuilt with MIP SDK 2019 R1; if the integrations communicate directly with the Recording Server APIs without using MIP SDK libraries, the integrators must add HTTPS support themselves.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the recording server.



- 1** A CA certificate acts as a trusted third-party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (all clients)
- 2** The CA certificate must be trusted on all clients. In this way the clients can verify the validity of the certificates issued by the CA
- 3** The CA certificate is used to establish secure connection between the recording servers and all clients and services
- 4** The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on all computers running services that retrieve data streams from the recording servers, by trusting the CA certificate that was used to issue the recording server certificate
- The service account that runs the recording server must have access to the private key of the certificate on the recording server.



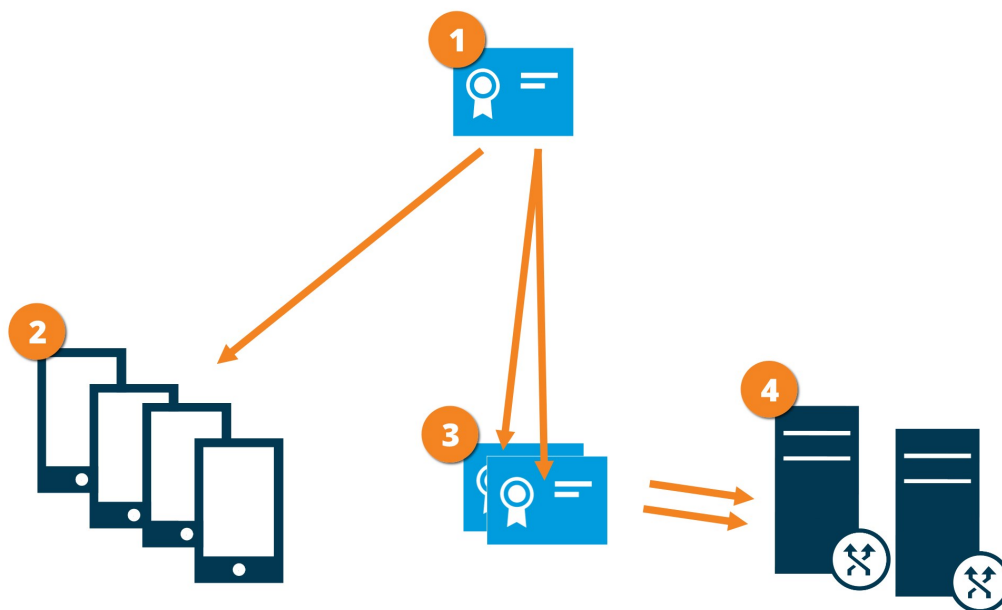
If you enable encryption on the recording servers and your system applies failover recording servers, Milestone recommends that you also prepare the failover recording servers for encryption.

Mobile server data encryption (explained)

In XProtect VMS, encryption is enabled or disabled per mobile server. When you enable encryption on a mobile server, you will have the option to use encrypted communication with all clients, services, and integrations that retrieve data streams.

Certificate distribution for mobile servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication with the mobile server.



- ❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (mobile server) and by the party that verifies the certificate (all clients)
- ❷ The CA certificate must be trusted on all clients. In this way clients can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the mobile server and clients and services
- ❹ The CA certificate must be installed on the computer on which the mobile server is running

Requirements for the CA certificate:

- The mobile server's host name must be included in the certificate, either as subject/owner or in the list of DNS names that the certificate is issued to
- The certificate must be trusted on all devices that are running services that retrieve data streams from the mobile server
- The service account that runs the mobile server must have access to the private key of the CA certificate

Mobile server encryption requirements for clients

If you do not enable encryption and use an HTTP connection, the push-to-talk feature in XProtect Web Client will not be available.

If you select a self-signed certificate for the encryption of the mobile server, XProtect Mobile client will not be able to connect with the mobile server.

Installation

Install a new XProtect system

Install XProtect Essential+

You can install a free version of XProtect Essential+. This version provides you with limited capabilities of the XProtect VMS for a limited number of cameras. You must have internet connection to install XProtect Essential+.

This version is installed on a single computer, using the **Single computer** installation option. The **Single computer** option installs all server and client components on the current computer.



Milestone recommends that you read the following section carefully before you install:
Before you start installation on page 55.

After initial installation, you can continue with the configuration wizard. Depending on your hardware and configuration, the recording server scans your network for hardware. You can then select which hardware devices to add to your system. Cameras are preconfigured in views, and you have the option to enable other devices such as microphones and speakers. You also have the option of adding users to the system with either an operator role or an administrator role. After installation, XProtect Smart Client opens, and you are ready to use the system.

Otherwise, if you close the installation wizard, XProtect Management Client opens, where you can make manual configurations such as add hardware devices and users to the system.



If you upgrade from a previous version of the product, the system does not scan for hardware or create new views and user profiles.

1. Download the software from the internet (<https://www.milestonesys.com/downloads/>) and run the **Milestone XProtect VMS Products 2020 R2 System Installer.exe** file.
2. The installation files unpack. Depending on the security settings, one or more Windows® security warnings appear. Accept these and the unpacking continues.
3. When done, the **Milestone XProtect VMS** installation wizard appears.
 1. Select the **Language** to use during the installation (this is not the language that your system uses once installed; this is selected later). Click **Continue**.
 2. Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box and click **Continue**.

3. Click the **XProtect Essential+** link to download a free license file.

The free license file is downloaded and appears in the **Enter or browse to the location of the license file** field. Click **Continue**.

4. Select **Single computer**.

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

5. On the **Select encryption** page, you can secure the communication flows:

- Between the recording servers, data collectors, and the management server

To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate.



If you encrypt the connection from the recording server to the management server, the system requires that you also encrypt the connection from the management server to the recording server.

- Between the recording servers and clients

To enable encryption between recording servers and client components that retrieve data streams from the recording server, in the **Streaming media certificate** section, select a certificate.

You can use the same certificate file for all system components or use different certificate files depending on the system components.

For more information about preparing your system for secure communication, see *Secure communication (explained)* on page 64 and the *Milestone Certificate guide* (English only).

You can also enable encryption after installation from the Server Configurator in the Management Server Manager tray icon in the notification area.

6. On the **Specify recording server settings** page, specify the different recording server settings:

1. In the **Recording server name** field, enter the name of the recording server. The default is the name of the computer.
2. The **Management server address** field shows the address and port number of the management server: localhost:80.
3. In the **Select your media database location** field, select the location where you want to save your video recording. Milestone recommends that you save your video recordings in a separate location from where you install the software and not on the system drive. The default location is the drive with the most space available.
4. In **Retention time for video recordings** field, define for how long you want to save the video recordings. You can enter from between 1 and 999 days, where 7 days is the default retention time.
5. Click **Continue**.

7. On the **Specify mobile server encryption** page, you can secure the communication between the mobile server and the clients and services.



If you do not enable encryption, some features in some clients will not be available. For more information, see Mobile server encryption requirements for clients on page 72.

Select a valid certificate in the list. For more information about establishing secure communication in your system, see Mobile server data encryption (explained) on page 71 or the *Milestone Certificate guide* (English only).

You can also enable encryption after the installation completes from the Mobile Server Manager tray icon in the taskbar of your operating system (see Enable encryption on the mobile server on page 401).

8. On the **Select file location and product language** page, do the following:
 1. In the **File location** field, select the location where you want to install the software.
 2. In **Product language**, select the language in which to install your XProtect product.
 3. Click **Install**.

The software now installs. If not already installed on the computer, Microsoft® SQL Server® Express and Microsoft IIS are automatically installed during the installation.

9. You may be prompted to restart the computer. After restarting your computer, depending on the security settings, one or more Windows security warnings may appear. Accept these and the installation completes.
10. When the installation completes, a list shows the components that are installed on the computer.

Click **Continue** to add hardware and users to the system.



If you click **Close** now, you bypass the configuration wizard and XProtect Management Client opens. You can configure the system, for example add hardware and users to the system, in Management Client.

11. On the **Enter user names and passwords for hardware** page, enter the user names and passwords for hardware that you have changed from the manufacturer defaults.

The installer scans the network for this hardware as well as hardware with manufacturer default credentials.

Click **Continue** and wait while the system scans for hardware.

12. On the **Select the hardware to add to the system** page, select the hardware that you want to add to the system. Click **Continue** and wait while the system adds the hardware.

13. On the **Configure the devices** page, you can give the hardware descriptive names by clicking the edit icon next to the hardware name. This name is then prefixed to the hardware devices.

Expand the hardware node to enable or disable the hardware devices, such as cameras, speakers, and microphones.



Cameras are enabled by default, and speakers and microphones are disabled by default.

Click **Continue** and wait while the system configures the hardware.

14. On the **Add users** page, you can add users to the system as Windows users or basic users. The users can have either the Administrators role or the Operators role.

Define the user and click **Add**.

When you are done adding users, click **Continue**.

15. When the installation and initial configuration are done, the **Configuration is complete** page appears, where you see:
 - A list of hardware devices that are added to the system
 - A list of users who are added to the system
 - Addresses to the XProtect Web Client and XProtect Mobile client, which you can share with your users

When you click **Close**, XProtect Smart Client opens and is ready to use.

Install your system - Single computer option

The **Single computer** option installs all server and client components on the current computer.



Milestone recommends that you read the following section carefully before you install:
Before you start installation on page 55.

After initial installation, you can continue with the configuration wizard. Depending on your hardware and configuration, the recording server scans your network for hardware. You can then select which hardware devices to add to your system. Cameras are preconfigured in views, and you have the option to enable other devices such as microphones and speakers. You also have the option of adding users to the system with either an operator role or an administrator role. After installation, XProtect Smart Client opens, and you are ready to use the system.

Otherwise, if you close the installation wizard, XProtect Management Client opens, where you can make manual configurations such as add hardware devices and users to the system.



If you upgrade from a previous version of the product, the system does not scan for hardware or create new views and user profiles.

1. Download the software from the internet (<https://www.milestonesys.com/downloads/>) and run the `Milestone XProtect VMS Products 2020 R2 System Installer.exe` file.
2. The installation files unpack. Depending on the security settings, one or more Windows® security warnings appear. Accept these and the unpacking continues.
3. When done, the **Milestone XProtect VMS** installation wizard appears.
 1. Select the **Language** to use during the installation (this is not the language that your system uses once installed; this is selected later). Click **Continue**.
 2. Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box and click **Continue**.
 3. In the **Enter or browse to the location of the license file**, enter your license file from your XProtect provider. Alternatively, browse to the file location or click the **XProtect Essential+** link to download a free license file. For limitations to the free XProtect Essential+ product, see the Product comparison chart on page 43. The system verifies your license file before you can continue. Click **Continue**.
4. Select **Single computer**.

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

5. On the **Select encryption** page, you can secure the communication flows:

- Between the recording servers, data collectors, and the management server

To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate.



If you encrypt the connection from the recording server to the management server, the system requires that you also encrypt the connection from the management server to the recording server.

- Between the recording servers and clients

To enable encryption between recording servers and client components that retrieve data streams from the recording server, in the **Streaming media certificate** section, select a certificate.

You can use the same certificate file for all system components or use different certificate files depending on the system components.

For more information about preparing your system for secure communication, see *Secure communication (explained)* on page 64 and the *Milestone Certificate guide* (English only).

You can also enable encryption after installation from the Server Configurator in the Management Server Manager tray icon in the notification area.

6. On the **Specify recording server settings** page, specify the different recording server settings:

1. In the **Recording server name** field, enter the name of the recording server. The default is the name of the computer.
2. The **Management server address** field shows the address and port number of the management server: localhost:80.
3. In the **Select your media database location** field, select the location where you want to save your video recording. Milestone recommends that you save your video recordings in a separate location from where you install the software and not on the system drive. The default location is the drive with the most space available.
4. In **Retention time for video recordings** field, define for how long you want to save the video recordings. You can enter from between 1 and 999 days, where 7 days is the default retention time.
5. Click **Continue**.

7. On the **Specify mobile server encryption** page, you can secure the communication between the mobile server and the clients and services.



If you do not enable encryption, some features in some clients will not be available. For more information, see Mobile server encryption requirements for clients on page 72.

Select a valid certificate in the list. For more information about establishing secure communication in your system, see Mobile server data encryption (explained) on page 71 or the *Milestone Certificate guide* (English only).

You can also enable encryption after the installation completes from the Mobile Server Manager tray icon in the taskbar of your operating system (see Enable encryption on the mobile server on page 401).

8. On the **Select file location and product language** page, do the following:
 1. In the **File location** field, select the location where you want to install the software.
 2. In **Product language**, select the language in which to install your XProtect product.
 3. Click **Install**.

The software now installs. If not already installed on the computer, Microsoft® SQL Server® Express and Microsoft IIS are automatically installed during the installation.

9. You may be prompted to restart the computer. After restarting your computer, depending on the security settings, one or more Windows security warnings may appear. Accept these and the installation completes.
10. When the installation completes, a list shows the components that are installed on the computer.

Click **Continue** to add hardware and users to the system.



If you click **Close** now, you bypass the configuration wizard and XProtect Management Client opens. You can configure the system, for example add hardware and users to the system, in Management Client.

11. On the **Enter user names and passwords for hardware** page, enter the user names and passwords for hardware that you have changed from the manufacturer defaults.

The installer scans the network for this hardware as well as hardware with manufacturer default credentials.

Click **Continue** and wait while the system scans for hardware.

12. On the **Select the hardware to add to the system** page, select the hardware that you want to add to the system. Click **Continue** and wait while the system adds the hardware.

13. On the **Configure the devices** page, you can give the hardware descriptive names by clicking the edit icon next to the hardware name. This name is then prefixed to the hardware devices.

Expand the hardware node to enable or disable the hardware devices, such as cameras, speakers, and microphones.



Cameras are enabled by default, and speakers and microphones are disabled by default.

Click **Continue** and wait while the system configures the hardware.

14. On the **Add users** page, you can add users to the system as Windows users or basic users. The users can have either the Administrators role or the Operators role.

Define the user and click **Add**.

When you are done adding users, click **Continue**.

15. When the installation and initial configuration are done, the **Configuration is complete** page appears, where you see:
 - A list of hardware devices that are added to the system
 - A list of users who are added to the system
 - Addresses to the XProtect Web Client and XProtect Mobile client, which you can share with your users

When you click **Close**, XProtect Smart Client opens and is ready to use.

Install your system - Custom option

The **Custom** option installs the management server, but you can select which other server and client components you want to install on the current computer. By default, the recording server is not selected in the component list. Depending on your selections, you can install the not selected system components on other computers afterwards. For more information about each system component and their role, see Main system components on page 22. Installation on other computers is done through the management server's download web page named Download Manager. For more information about installation through the Download Manager, see Install new XProtect components on page 84.

1. Download the software from the internet (<https://www.milestonesys.com/downloads/>) and run the `Milestone XProtect VMS Products 2020 R2 System Installer.exe` file.
2. The installation files unpack. Depending on the security settings, one or more Windows® security warnings appear. Accept these and the unpacking continues.
3. When done, the **Milestone XProtect VMS** installation wizard appears.

1. Select the **Language** to use during the installation (this is not the language that your system uses once installed; this is selected later). Click **Continue**.
2. Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box and click **Continue**.
3. In the **Enter or browse to the location of the license file**, enter your license file from your XProtect provider. Alternatively, browse to the file location or click the **XProtect Essential+** link to download a free license file. For limitations to the free XProtect Essential+ product, see the Product comparison chart on page 43. The system verifies your license file before you can continue. Click **Continue**.
4. Select **Custom**. A list of components to be installed appears. Apart from the management server, all components in the list are optional. The recording server is by default not selected. Click **Continue**.



In the steps below, all system components are installed. For a more distributed system, install fewer system components on this computer and the remaining components on other computers. If you cannot recognize an installation step, it is likely because you have not selected to install the system component that this page belongs to. In that case, continue to the next step. See also Install new XProtect components on page 84, Install new XProtect components on page 84, and Install new XProtect components on page 84.

5. The **Select a website on the IIS to use with your XProtect system** page is shown only if you have more than one IIS website available on the computer. You must select which website you will use with your XProtect system. If possible, select a website with HTTPS binding because this protocol is a more advanced and secure version of HTTP. Click **Continue**.

If Microsoft® IIS is not installed on the computer, it is installed.

6. On the **Select Microsoft SQL Server** page, select the SQL Server that you want to use. See also SQL Server options during custom installation on page 83. Click **Continue**.



If you do not have a SQL Server on your local computer, you can install Microsoft SQL Server Express, but in a larger distributed system you would typically use a dedicated SQL Server on your network.

7. On the **Select database** page (only shown if you have selected an existing SQL Server), select or create an SQL database for storing your system configuration. If you choose an existing SQL database, decide whether to **Keep** or **Overwrite** existing data. If you are upgrading, select to keep existing data so you do not lose your system configuration. See also SQL Server options during custom installation on page 83. Click **Continue**.

8. On the **Select service account** page, select either **This predefined account** or **This account** to select the service account for all system components except for the recording server. If needed, enter a password. Click **Continue**.
9. On the **Select service account for recording server**, select either **This predefined account** or **This account** to select the service account for the recording server. If needed, enter a password. Click **Continue**.
10. On the **Select encryption** page, you can secure the communication flows:

- Between the recording servers, data collectors, and the management server

To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate.



If you encrypt the connection from the recording server to the management server, the system requires that you also encrypt the connection from the management server to the recording server.

- Between the recording servers and clients

To enable encryption between recording servers and client components that retrieve data streams from the recording server, in the **Streaming media certificate** section, select a certificate.

You can use the same certificate file for all system components or use different certificate files depending on the system components.

For more information about preparing your system for secure communication, see *Secure communication (explained)* on page 64 and the *Milestone Certificate guide* (English only).

You can also enable encryption after installation from the Server Configurator in the Management Server Manager tray icon in the notification area.

11. On the **Specify recording server settings** page, specify the different recording server settings:
 1. In the **Recording server name** field, enter the name of the recording server. The default is the name of the computer.
 2. The **Management server address** field shows the address and port number of the management server: localhost:80.
 3. In the **Select your media database location** field, select the location where you want to save your video recording. Milestone recommends that you save your video recordings in a separate location from where you install the software and not on the system drive. The default location is the drive with the most space available.
 4. In **Retention time for video recordings** field, define for how long you want to save the video recordings. You can enter from between 1 and 999 days, where 7 days is the default retention time.
 5. Click **Continue**.

12. On the **Specify mobile server encryption** page, you can secure the communication between the mobile server and the clients and services.



If you do not enable encryption, some features in some clients will not be available. For more information, see Mobile server encryption requirements for clients on page 72.

Select a valid certificate in the list. For more information about establishing secure communication in your system, see Mobile server data encryption (explained) on page 71 or the *Milestone Certificate guide* (English only).

You can also enable encryption after the installation completes from the Mobile Server Manager tray icon in the taskbar of your operating system (see Enable encryption on the mobile server on page 401).

13. On the **Select file location and product language** page, select the **File location** for the program files. In the **Product language** field, select the language in which to install your XProtect product. Click **Install**.
14. The software now installs. When the installation completes, you see a list of successfully installed system components. Click **Close**.
15. You may be prompted to restart the computer. After restarting your computer, depending on the security settings, one or more Windows security warnings may appear. Accept these and the installation completes.
16. Configure your system in Management Client. See Initial configuration tasks list on page 122.
17. Depending on your selections, install the remaining system components on other computers through the Download Manager. See Install new XProtect components on page 84.

SQL Server options during custom installation

Decide which SQL Server and database to use with the below options.

SQL Server options:

- **Install Microsoft® SQL Server® Express on this computer:** This option is shown only if you do not have a SQL Server installed on the computer
- **Use the SQL Server on this computer:** This option is shown only if a SQL Server is already installed on the computer
- **Select a SQL Server on your network through search:** Enables you to search for all SQL Servers that are discoverable on your network subnet
- **Select a SQL Server on your network:** Enables you to enter the address (host name or IP address) of a SQL Server that you might not be able to find through search

SQL database options:

- **Create new database:** Mainly for new installations
- **Use existing database:** Mainly for upgrades of existing installations. Milestone recommends that you reuse the existing SQL database and keep the existing data in it, so you do not lose your system configuration. You can also choose to overwrite the data in the SQL database

Install new XProtect components

Installing through Download Manager (explained)

If you want to install system components on computers other than where the management server is installed, you must install these system components through the Management Server's download website Download Manager.

1. From the computer where Management Server is installed, go to the Management Server's download web page. In Windows' **Start** menu, select **Programs > Milestone > Administrative Installation Page** and write down or copy the internet address for later use when installing the system components on the other computers. The address is typically *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Log in to each of the other computers to install one or more of the other system components:
 - Recording Server (see also Install a recording server through Download Manager on page 84 or Install a recording server silently on page 89)
 - Management Client
 - Smart Client
 - Event Server
 - Log Server
 - Mobile Server
3. Open an internet browser, enter the address of the Management Server's download web page into the address field, and download the relevant installer.
4. Run the installer.

See Install your system - Custom option on page 80 if in doubt about the selections and settings in the different installation steps.

Install a recording server through Download Manager

If your system components are distributed on separate computers, you can install the recording servers by following the instructions below.



The recording server is already installed if you made a **Single Computer** installation, but you can use the same instructions to add more recording servers if you need more capacity.



If you need to install a failover recording server, see Install new XProtect components on page 84.

1. From the computer where Management Server is installed, go to the Management Server's download web page. In Windows' **Start** menu, select **Programs > Milestone > Administrative Installation Page** and write down or copy the internet address for later use when installing the system components on the other computers. The address is typically *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Log into the computer where you want to install the recording server.
3. Open an internet browser and enter the address of the Management Server's download web page into the address field and press Enter.
4. Download the recording server installer by selecting **All Languages** below the **Recording Server Installer**. Save the installer or run it directly from the web page.
5. Select the **Language** you want to use during the installation. Click **Continue**.
6. On the **Select an installation type page**, select:
Typical to install a recording server with default values, or
Custom to install a recording server with custom values.
7. On the **Specify recording server settings** page, specify the different recording server settings:
 1. In the **Recording server name** field, enter the name of the recording server. The default is the name of the computer.
 2. The **Management server address** field shows the address and port number of the management server: localhost:80.
 3. In the **Select your media database location** field, select the location where you want to save your video recording. Milestone recommends that you save your video recordings in a separate location from where you install the software and not on the system drive. The default location is the drive with the most space available.
 4. In **Retention time for video recordings** field, define for how long you want to save the video recordings. You can enter from between 1 and 999 days, where 7 days is the default retention time.
 5. Click **Continue**.
8. The **Recording servers IP addresses** page is shown only if you selected **Custom**. Specify the number of recording servers that you want to install on this computer. Click **Continue**.
9. On the **Select service account for recording server**, select either **This predefined account** or **This account** to select the service account for the recording server. If needed, enter a password. Click **Continue**.

10. On the **Select encryption** page, you can secure the communication flows:

- Between the recording servers, data collectors, and the management server

To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate.



If you encrypt the connection from the recording server to the management server, the system requires that you also encrypt the connection from the management server to the recording server.

- Between the recording servers and clients

To enable encryption between recording servers and client components that retrieve data streams from the recording server, in the **Streaming media certificate** section, select a certificate.

You can use the same certificate file for all system components or use different certificate files depending on the system components.

For more information about preparing your system for secure communication, see *Secure communication (explained)* on page 64 and the *Milestone Certificate guide* (English only).

You can also enable encryption after installation from the Server Configurator in the Management Server Manager tray icon in the notification area.

11. On the **Select file location and product language** page, select the **File location** for the program files. In the **Product language** field, select the language in which to install your XProtect product. Click **Install**.
12. The software now installs. When the installation completes, you see a list of successfully installed system components. Click **Close**.
13. When you have installed the recording server, you can check its state from the Recording Server Manager tray icon and configure it in Management Client. For more information, see Initial configuration tasks list on page 122.

Install a failover recording server through Download Manager



If you run workgroups, you must use the alternative installation method for failover recording servers (see Installation for workgroups on page 91).

1. From the computer where Management Server is installed, go to the Management Server's download web page. In Windows' **Start** menu, select **Programs > Milestone > Administrative Installation Page** and write down or copy the internet address for later use when installing the system components on the other computers. The address is typically `http://[management server address]/installation/Admin/default-en-US.htm`.
2. Log into the computer where you want to install the failover recording server.

3. Open an internet browser, enter the address of the Management Server's download web page into the address field and download the recording server installer. Save the installer or run it directly from the web page.
4. Download the recording server installer by selecting **All Languages** below the **Recording Server Installer**. Save the installer or run it directly from the web page.
5. Select the **Language** you want to use during the installation. Click **Continue**.
6. On the **Select an installation type** page, select **Failover** to install a recording server as a failover recording server.
7. On the **Specify recording server settings** page, specify the different recording server settings. The name of the failover recording server, the address of the management server, and the path to the media database. Click **Continue**.
8. On the **Select service account for recording server** page and when installing a failover recording server, you must use the particular user account named **This account**. This creates the failover user account. If needed, enter a password and confirm this. Click **Continue**.
9. On the **Select encryption** page, you can secure the communication flows:

- Between the recording servers, data collectors, and the management server

To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate.



If you encrypt the connection from the recording server to the management server, the system requires that you also encrypt the connection from the management server to the recording server.

- Between the recording servers and clients

To enable encryption between recording servers and client components that retrieve data streams from the recording server, in the **Streaming media certificate** section, select a certificate.

You can use the same certificate file for all system components or use different certificate files depending on the system components.

For more information about preparing your system for secure communication, see *Secure communication (explained)* on page 64 and the *Milestone Certificate guide* (English only).

You can also enable encryption after installation from the Server Configurator in the Management Server Manager tray icon in the notification area.

10. On the **Select file location and product language** page, select the **File location** for the program files. In the **Product language** field, select the language in which to install your XProtect product. Click **Install**.
11. The software now installs. When the installation completes, you see a list of successfully installed system components. Click **Close**.

12. When you have installed the failover recording server, you can check its state from the Failover Server service tray icon and configure it in Management Client. For more information, see Initial configuration tasks list on page 122.

Installing silently through a command line shell (explained)

With silent installation, system administrators can install and upgrade the Recording Server and Smart Client software over a large network with no user interactions from their part and with as little disturbance to the end users as possible.

The Recording Server and Smart Client installers (.exe files) have different command line arguments. They each have their own set of command line parameters that can be invoked directly in a command line shell or through an arguments file. In the command line shell, you can also use command line options with the installers.

You can combine the XProtect installers, their command line parameters and command line options with tools for silent distribution and installation of software, like Microsoft System Center Configuration Manager (SCCM, also known as ConfigMgr). For more information about such tools, visit the manufacturer's website. You can also use Milestone Software Manager for remote installing and updating of Recording Server, device packs, and Smart Client. For more information, see the Milestone Software Manager documentation.

Command line parameters and arguments files

During silent installation, you can specify settings that are closely linked to the different VMS system components and their internal communication with command line parameters and arguments files. Command line parameters and arguments files should only be used for new installations because you cannot change the settings that the command line parameters represent during an upgrade.

To see the available command line parameters and to generate an arguments file for an installer, in the command line shell, navigate to the directory where the installer is located and enter the following command:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Example:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

In the saved arguments file (Arguments.xml), each command line parameter has a description that explains its purpose. You can modify and save the arguments file so that the command line parameter values suit your installation needs.

When you want to use an arguments file with its installer, use the `--arguments` command line option by entering the following command:

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Example:


```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=C:\temp\arguments.xml
```

Command line options

In the command line shell, you can also combine installers with command line options. The command line options generally modify the behavior of a command.

To see the full list of command line options, in the command line shell, navigate to the directory where the installer is located and enter `[NameOfExeFile].exe --help`. For the installation to be successful, you must specify a value for command line options that require a value.

You can use both command line parameters and command line options in the same command. Use the `--parameters` command line option and divide each command line parameter with a colon (:). In the example below, `--quiet`, `--showconsole`, and `--parameters` are command line options, and `ISFAILOVER` and `RECORDERNAME` are command line parameters:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

Install a recording server silently

When you install silently, you are not notified when the installation is completed. To get notified, include the `--showconsole` command line option in the command. The Milestone XProtect Recording Server tray icon appears when the installation is completed.

In the command examples below, the text inside square brackets ([]) and the square brackets themselves must be replaced with real values. Example: instead of "[path]" you could enter "**d:\program files\, d:\record\, or \\network-storage-02\surveillance**". Use the `--help` command line option to read about the legal formats of each command line option value.

1. Log in to the computer where you want to install the Recording Server component.
2. Open an internet browser and enter the address of the Management Server's download web page that is targeted at the administrators into the address field and press Enter.

The address is typically `http://[management server address]:[port]/installation/Admin/default-en-US.htm`.
3. Download the recording server installer by selecting **All Languages** below **Recording Server Installer**.
4. Open your preferred command line shell. To open Windows Command Prompt, open the Windows Start menu and enter **cmd**.
5. Navigate to the directory with the downloaded installer.
6. Continue the installation depending on one of the two scenarios below:

Scenario 1: Upgrade an existing installation, or install on server with the Management Server component with default values

- Enter the following command and the installation starts.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

Scenario 2: Install in a distributed system

1. Enter the following command to generate an arguments file with command line parameters.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=  
[path]
```

2. Open the arguments file (Arguments.xml) from the specified path and modify the command line parameter values if needed.



Make sure that you give the command line parameters SERVERHOSTNAME and SERVERPORT valid values. If not, the installation cannot complete.

4. Save the arguments file.
5. Return to the command line shell and enter the command below to install with the command line parameter values specified in the arguments file.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --arguments=  
[path]\[filename]
```

Install XProtect Smart Client silently

When you install silently, you are not notified when the installation is completed. To get notified, include the `--showconsole` command line option in the command. A shortcut to XProtect Smart Client appears on the desktop when the installation is completed.

In the command examples below, the text inside square brackets ([]) and the square brackets themselves must be replaced with real values. Example: instead of "[path]" you could enter **"d:\program files\"**, **d:\record**, or **\\network-storage-02\surveillance**. Use the `--help` command line option to read about the legal formats of each command line option value.

1. Open an internet browser and enter the address of the Management Server's download web page that is targeted at the end users into the address field and press Enter.

The address is typically `http://[management server address]:[port]/installation/default-en-US.htm`.

2. Download the XProtect Smart Client installer by selecting **All Languages** below **XProtect Smart Client Installer**.
3. Open your preferred command line shell. To open Windows Command Prompt, open the Windows Start menu and enter **cmd**.
4. Navigate to the directory with the downloaded installer.
5. Continue the installation depending on one of the two scenarios below:

Scenario 1: Upgrade an existing installation, or install with default command line parameter values

- Enter the following command and the installation starts.

```
XProtect Smart Client 2020 R2 Installer.exe --quiet
```

Scenario 2: Install with customized command line parameter values using an xml arguments file as input

1. Enter the following command to generate an arguments xml file with command line parameters.

```
XProtect Smart Client 2020 R2 Installer.exe --generateargsfile=[path]
```

2. Open the arguments file (Arguments.xml) from the specified path and modify the command line parameter values if needed.
3. Save the arguments file.
4. Return to the command line shell and enter the command below to install with the command line parameter values specified in the arguments file.

```
XProtect Smart Client 2020 R2 Installer.exe --quiet --arguments=[path]\  
[filename]
```

Installation for workgroups

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

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



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

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

3. Depending on what you selected in step 2, select to install the Management Server or Recording Server service using a common administrator account.
4. Finish the installation.
5. Repeat steps 1-4 to install any other systems you want to connect. They must all be installed using a common administrator account.

You cannot use this approach when you upgrade workgroup installations. See instead Upgrade in a workgroup setup on page 464.

Install in a cluster

Before you install in a cluster, see Multiple management servers (clustering) (explained) on page 53 and Requirements for clustering on page 53.



Descriptions and illustrations might differ from what you see on your screen.

Installation and change of URL address:

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



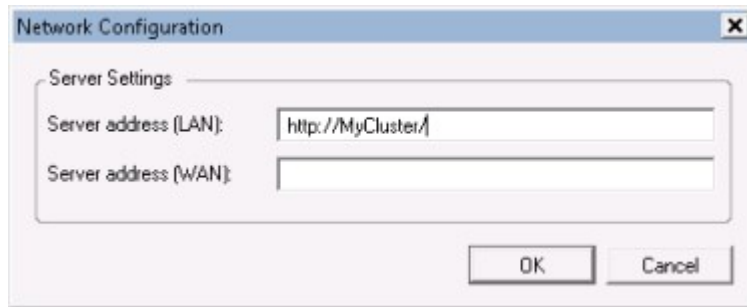
The management server must be installed with a specific user and not as a network service. This requires that you use the **Custom** install option. Also, the specific user must have access to the shared network drive and preferably a non-expiry password.

2. After you have installed the management server and Management Client on the first server in the cluster, open Management Client, and in the **Tools** menu, select **Registered Services**.
 1. In the **Add/Remove Registered Services** window, select **Log Service** in the list, click **Edit**.
 2. In the **Edit Registered Service** window, change the URL address of the log service to the URL address of the cluster.



3. Repeat these steps for all services listed in the **Add/Remove Registered Services** window. Click **Network**.

4. 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**.



5. In the **Add/Remove Registered Services** window, click **Close**. Exit the Management Client.
6. Stop the Management Server service and the IIS. Read about how to stop the IIS on the Microsoft website ([https://technet.microsoft.com/library/cc732317\(Ws.10\).aspx](https://technet.microsoft.com/library/cc732317(Ws.10).aspx)).
7. Repeat these steps for all subsequent servers in the cluster, this time pointing to the existing SQL Server and database. However, for the last server in the cluster on which you install the management server, do not stop the Management Server service.

Configure the Management Server service as a generic service in the failover cluster:

1. On the last server on which you have installed the management server, go to **Start > Administrative Tools**, open Windows' **Failover Cluster Management**. In the **Failover Cluster Management** window, expand your cluster, right-click **Services and Applications**, and select **Configure a Service or Application**.



2. In the **High Availability** dialog box click **Next**.
3. Select **Generic Service** and click **Next**.
4. Do not specify anything on the third page of the dialog box and click **Next**.
5. Select the **Milestone XProtect Management Server** service, click **Next**. Specify the name (host name of the cluster) that clients use when accessing the service, click **Next**.

6. No storage is required for the service, click **Next**. No registry settings should be replicated, click **Next**. Verify that the cluster service is configured according to your needs, click **Next**. The management server is now configured as a generic service in the failover cluster. Click **Finish**.
7. In the cluster setup, the event server and the Data Collector should be set as a dependent service of the management server, so the event server stops when the management server is stopped.
8. To add the **Milestone XProtect Event Server** service as a resource to the **Milestone XProtect Management Server Cluster** service, right-click the cluster service and click **Add a resource > 4 - Generic Service** and select **Milestone XProtect Event Server**.

Modify the following configuration settings:

On the Management Server nodes:

- In C:\ProgramData\Milestone\XProtectManagement Server\ServerConfig.xml:

```
<AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
```

- In C:\Program Files\Milestone\XProtectManagement Server\IIS\IDP\appsettings.json:

```
"Authority": "http://ClusterRoleAddress/IDP"
```

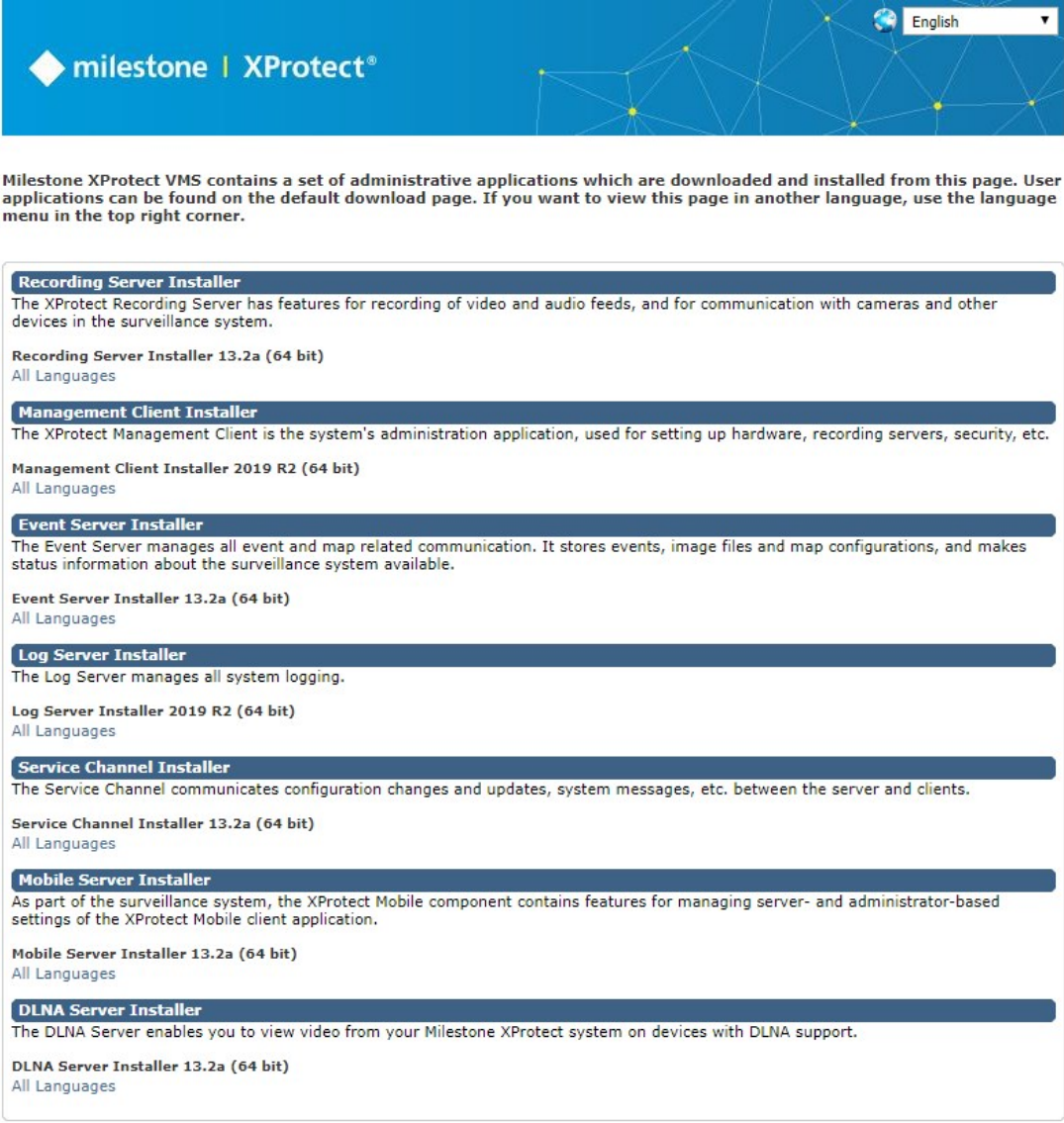
On the Recording Servers, verify that the authorizationserveraddress is also set to the cluster role address:

In C:\ProgramData\Milestone\XProtectRecording Server\RecorderConfig.xml:

```
<authorizationserveraddress>http://ClusterRoleAddress/IDP</authorizationserveraddress>
```

Download Manager/download web page

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



Milestone XProtect VMS contains a set of administrative applications which are downloaded and installed from this page. User applications can be found on the default download page. If you want to view this page in another language, use the language menu in the top right corner.

Recording Server Installer
The XProtect Recording Server has features for recording of video and audio feeds, and for communication with cameras and other devices in the surveillance system.
Recording Server Installer 2019 R2 (64 bit)
[All Languages](#)

Management Client Installer
The XProtect Management Client is the system's administration application, used for setting up hardware, recording servers, security, etc.
Management Client Installer 2019 R2 (64 bit)
[All Languages](#)

Event Server Installer
The Event Server manages all event and map related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.
Event Server Installer 2019 R2 (64 bit)
[All Languages](#)

Log Server Installer
The Log Server manages all system logging.
Log Server Installer 2019 R2 (64 bit)
[All Languages](#)

Service Channel Installer
The Service Channel communicates configuration changes and updates, system messages, etc. between the server and clients.
Service Channel Installer 2019 R2 (64 bit)
[All Languages](#)

Mobile Server Installer
As part of the surveillance system, the XProtect Mobile component contains features for managing server- and administrator-based settings of the XProtect Mobile client application.
Mobile Server Installer 2019 R2 (64 bit)
[All Languages](#)

DLNA Server Installer
The DLNA Server enables you to view video from your Milestone XProtect system on devices with DLNA support.
DLNA Server Installer 2019 R2 (64 bit)
[All Languages](#)

© Milestone Systems A/S

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

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

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

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

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

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

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

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

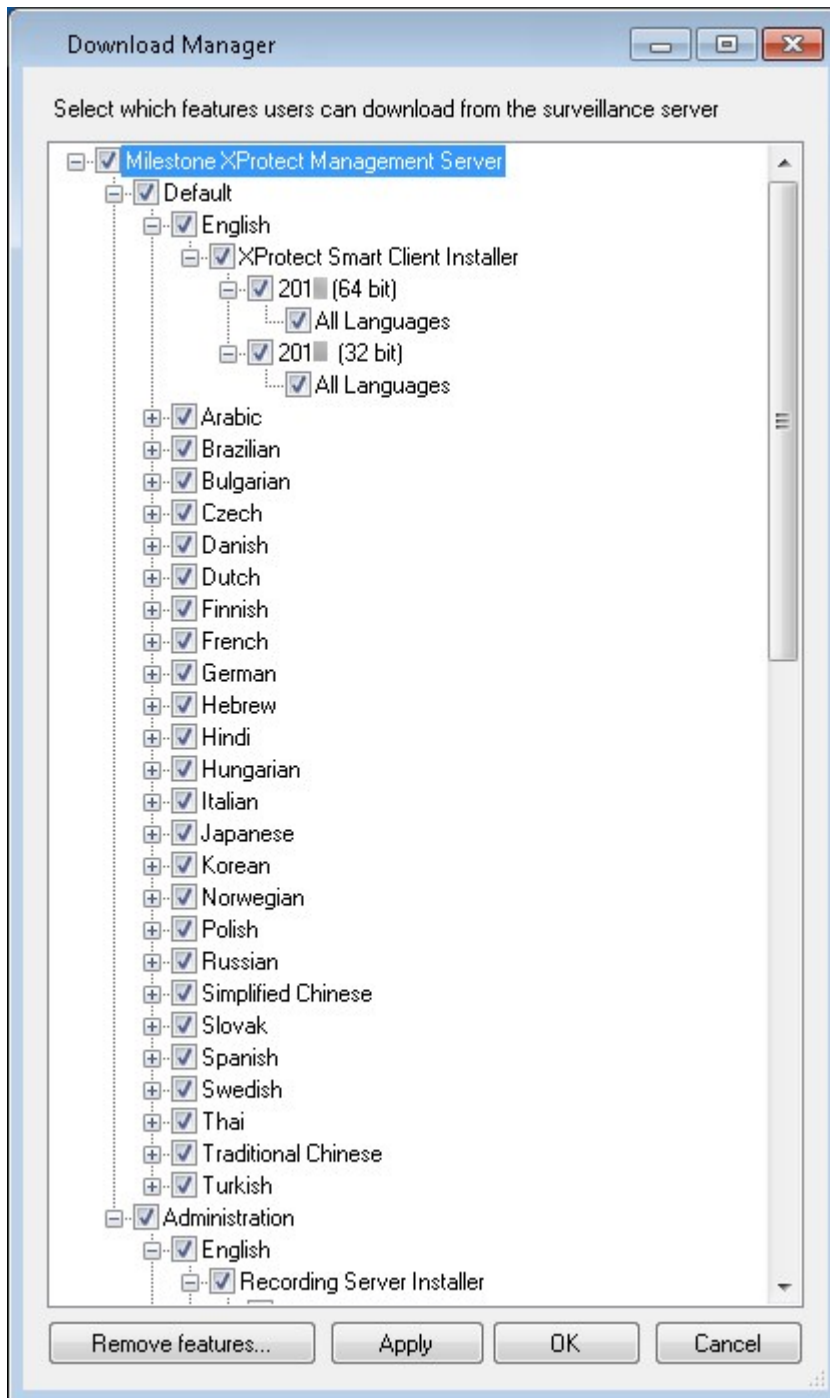
Even though you can control which components users can download and install in Download Manager, you cannot use it as a users' rights management tool. Such rights are determined by roles defined in the Management Client.

On the management server, you can access the XProtect Download Manager from Windows' **Start** menu, select **Programs > Milestone > XProtect Download Manager**.

Download Manager's default configuration

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

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



- The first level: Refers to your XProtect product
- The second level: Refers to the two targeted versions of the web page. **Default** refers to the web page version viewed by end users. **Administration** refers to the web page version viewed by system administrators
- The third level: Refers to the languages in which the web page is available

- The fourth level: Refers to the components which are - or can be made - available to users
- The fifth level: Refers to particular versions of each component, which are - or can be made - available to users
- The sixth level: Refers to the language versions of the components which are - or can be made - available to users

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

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

Download Manager's standard installers (user)

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

- Recording servers, including failover recording servers. Failover recording servers are initially downloaded and installed as recording servers, during the installation process you specify that you want a failover recording server.
- Management Client
- XProtect Smart Client
- Event server, used in connection with map functionality
- Log server, used for providing the necessary functionality for logging system information
- XProtect Mobile server
- More options may be available in your organization.

For installation of device packs, see Device pack installer - must be downloaded on page 100.

Add/publish Download Manager installer components

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

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

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

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

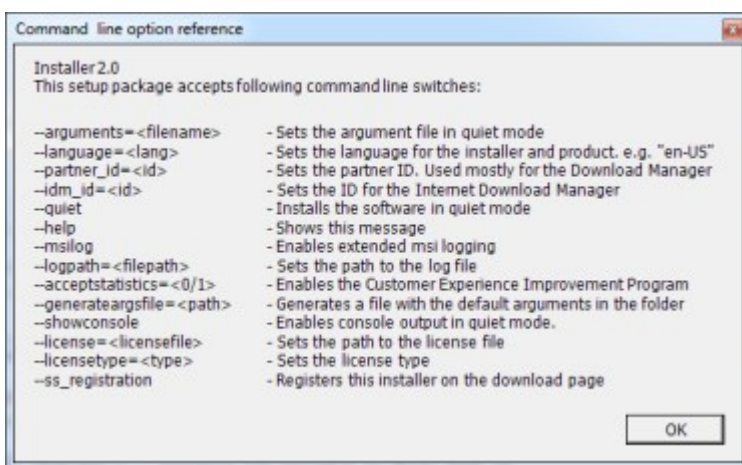
1. On the computer where you downloaded the component(s), go to Windows' **Start**, enter a *Command Prompt*
2. In the *Command Prompt*, execute the name of the file (.exe) with: [space]--ss_registration

Example: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

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



To get an overview of installer commands, in the *Command Prompt*, enter [space]--help and the following window appears:



When you have installed new components, they are by default selected in the Download Manager and are immediately available to users via the web page. You can always show or hide features on the web page by selecting or clearing check boxes in the Download Manager's tree structure.

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

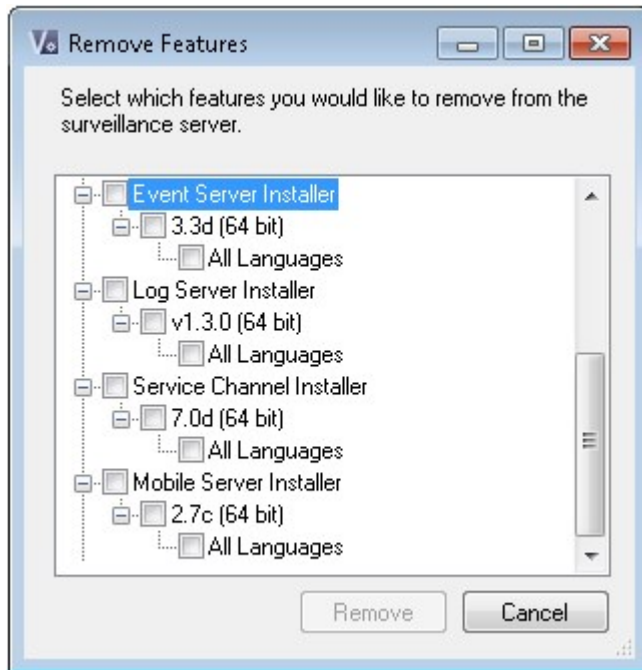
Hide/remove Download Manager installer components

You have three options:

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

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

1. In the Download Manager, click **Remove features**.
2. In the **Remove Features** window, select the feature(s) you want to remove.



3. Click **OK** and **Yes**.

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

Device pack installer - must be downloaded

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

1. Get the latest regular device pack from the download page on the Milestone website (<https://www.milestonesys.com/downloads/>).
2. On the same page, you can download the legacy device pack with older drivers. To check if your cameras use drivers from the legacy device pack, go to this website (<https://www.milestonesys.com/community/business-partner-tools/device-packs/>).
3. Add/publish it to the Download Manager by calling it with the `--ss_registration` command.

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

Installation log files and troubleshooting

During an installation, upgrade or uninstallation, log entries are written to various installation log files: To the main installation log file `installer.log` and to the log files belonging to the different system components you are installing. All log entries have a time stamp and the most recent log entries are at the end of the log files.

You can find all installation log files in the `C:\ProgramData\Milestone\Installer\` folder. Log files that are named `*I.log` or `*I[integer].log` are log files about new installations or upgrades while log files named `*U.log` or `*U[integer].log` are about uninstallations. If you have bought a server with an already installed XProtect system through a Milestone partner, there might not be any installation log files.

The log files contain information about the command-line parameters and command-line options and their values used during an installation, upgrade or uninstallation. To find the used command-line parameters in the log files, search for **Command Line:** or **Parameter** ' depending on the log file.

For troubleshooting, the main installation log file is the first place to look. If there were any exceptions, errors, or warnings during the installation, these have been logged. Try to search for **exception**, **error**, or **warning**. "Exit code: 0" means a successful installation and "Exit code: 1" the opposite. Your findings in the log files may enable you to find a solution on https://supportcommunity.milestonesys.com/s/knowledgebase?language=en_US/. If not, contact your Milestone partner and share the relevant installation log files.

Configuration

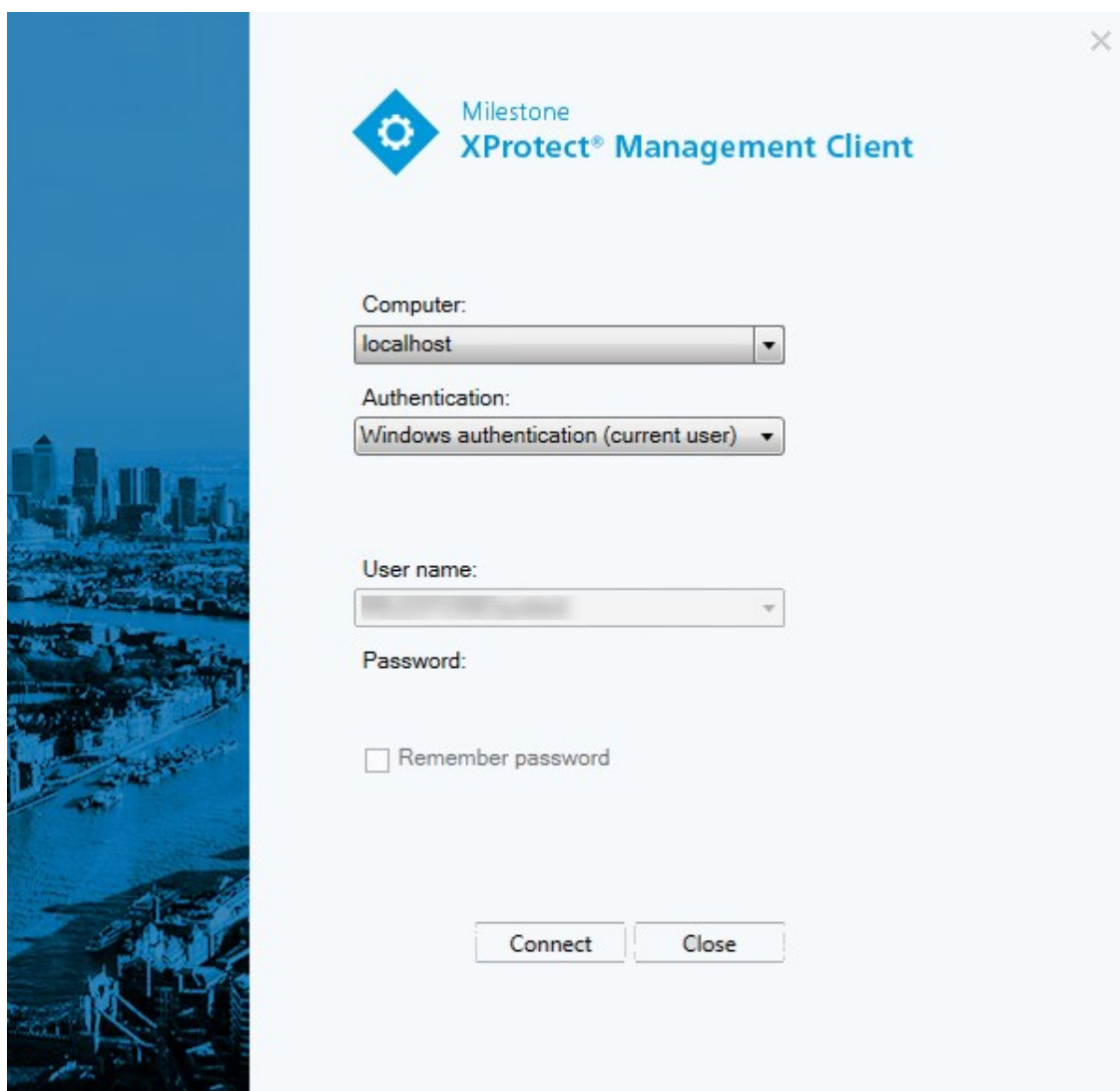
Navigating the Management Client

This section provides an introduction to the Management Client user interface.

Login overview

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

With XProtect Corporate 2016 or XProtect Expert 2016 or newer installed, you can log into systems that run older versions of the product after installing a patch. The supported versions are XProtect Corporate 2013 and XProtect Expert 2013 or newer.



Milestone
XProtect® Management Client

Computer:
localhost

Authentication:
Windows authentication (current user)

User name:
[Redacted]

Password:
[Redacted]

☐ Remember password

Connect Close

Login authorization (explained)

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

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

To associate login authorization with a role:

- Set **Login authorization required** for the selected role on the **Info** tab (see Roles settings on page 331) under **Roles**, so that the user is asked for additional authorization during login
- Set **Authorize users** for the selected role on the **Overall Security** tab (see Roles settings on page 331) under **Roles**, so that the user can authorize other users' logins

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

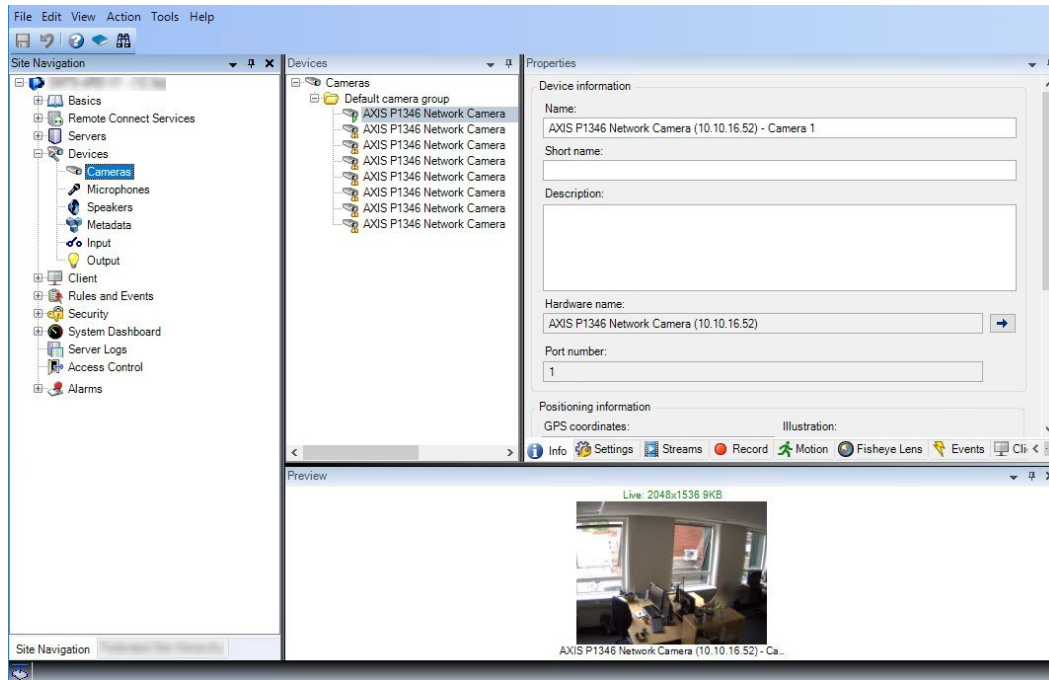
Management Client window overview

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

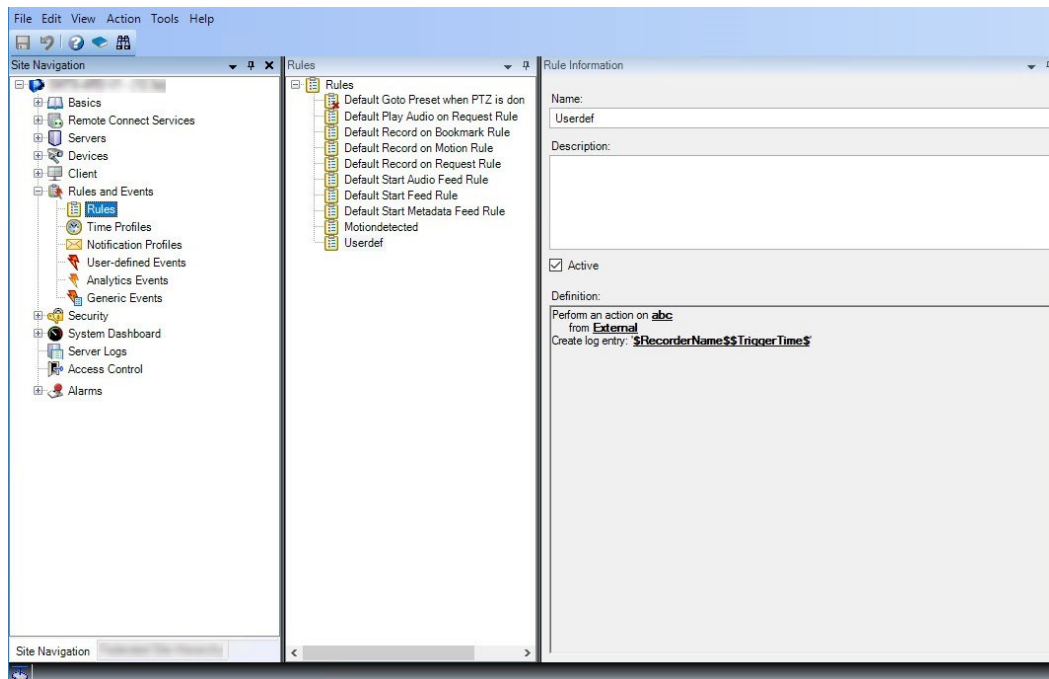
- System configuration
- Task
- Available functions

Below are some examples of typical layouts:

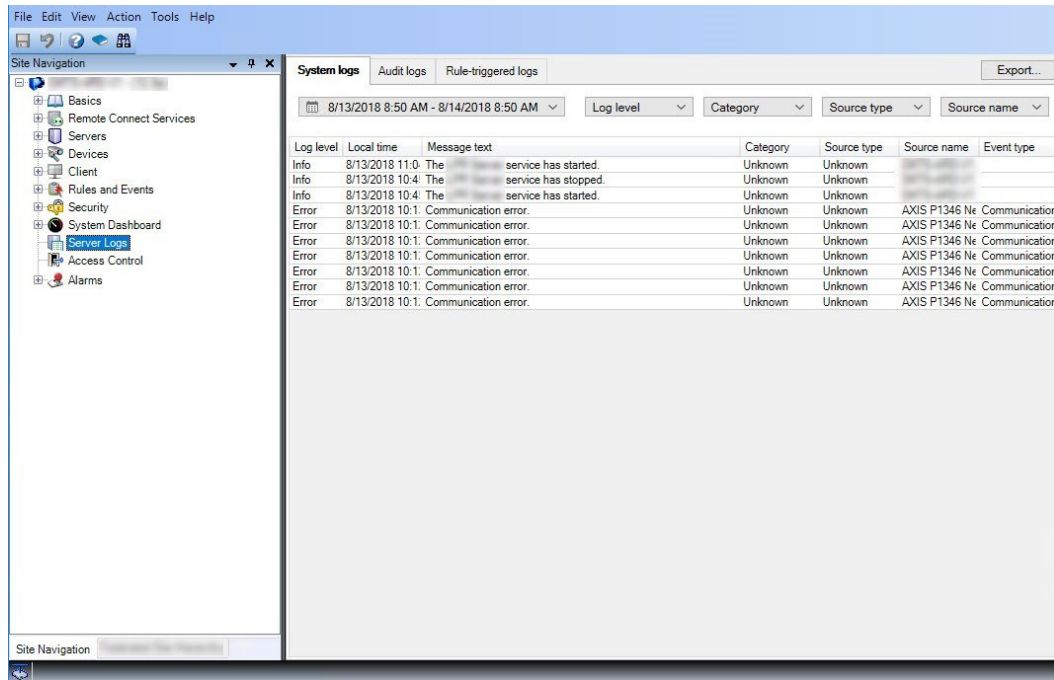
- When you work with recording servers and devices:



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



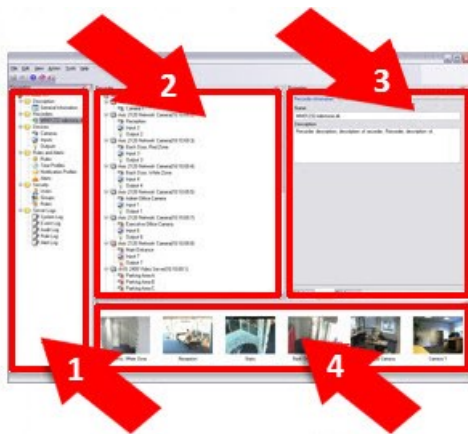
- When you view logs:



Panes overview



The illustration outlines a typical window layout. You can customize the layout so it may look different on your computer.



1. Site Navigation pane and Federated Site Hierarchy pane
2. Overview pane
3. Properties pane

4. Preview pane

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

Federated Site Hierarchy pane: This is your navigation element that displays all Milestone Federated Architecture sites in a parent/child site hierarchy.

You can select any site, log into it and the Management Client for that site launches. The site that you are logged into, is always at the top of the hierarchy.

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

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



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



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

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

Menu overview



Example only - some menus change depending on context.

File menu

You can save changes to the configuration and exit the application. You can also back up your configuration, see Backing up and restoring your system configuration (explained) on page 432.

Edit menu

You can undo changes.

View menu

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

Action menu

The content of the **Action** menu differs depending on the element you have selected in the **Site Navigation** pane. The actions you can choose from are the same as when you right-click the element. The elements are described in Configuring the system in the Site Navigation pane on page 124.

The pre-buffer period for each camera, see Devices that support pre-buffering on page 211

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

Tools menu

Name	Description
Registered Services	Manage registered services. See Managing registered services on page 455.
Effective Roles	View all roles of a selected user or group.
Options	Opens the Options dialog box, which lets you define and edit global system settings.

Help menu

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

Setting options for the system

In the **Options** dialog box, you can specify a number of settings related to the general appearance and functionality of the system.

Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

Options

General

Server Logs

Mail Server

AVI Generation

Network

Bookmark

User Settings

Evidence Lock

Audio I < >

Management Client

Max number of previews (*):

64

When adding new camera devices automatically enable:

☒ Motion detection

☒ Generate smart search motion data

☐ Multicast

Language (**):

English (United States)

(**) Restart required for setting to take effect.

Recording Server

Timeout for manual PTZ sessions:

15

Seconds

Timeout for pause patrolling sessions:

10

Minutes

Timeout for reserved PTZ sessions:

1

Hours

Ignore device communication errors if communication reestablished before:

0 sec

Help

OK

Cancel

General tab (options)

On the General tab, you can specify general settings for the Management Client and the recording server.

Management Client

Name	Description
Max number of previews	<p>Select the maximum number of thumbnail images displayed in the Preview pane. Default is 64 thumbnail images.</p> <p>Select Action > Refresh from the menu for the change to take effect.</p>

Name	Description
	A large number of thumbnail images in combination with a high frame rate may slow the system down.
When adding new camera devices automatically enable: Motion detection	<p>Select the check box to enable motion detection on new cameras, when you add them to the system with the Add Hardware wizard.</p> <p>This setting does not affect motion detection settings on existing cameras.</p> <p>You enable and disable motion detection for a camera on the Motion tab for the camera device.</p>
When adding new camera devices automatically enable: Generate motion data for smart search	<p>Generation of motion data for smart search requires that motion detection is enabled for the camera.</p> <p>Select the check box to enable generation of smart search motion data on new cameras, when you add them to the system with the Add Hardware wizard.</p> <p>This setting does not affect motion detection settings on existing cameras.</p> <p>You enable and disable the generation of smart search motion data for a camera on the Motion tab for the camera device.</p>
When adding new camera devices automatically enable: Multicast	<p>Select the check box to enable multicast on new cameras when you add them with the Add Hardware wizard.</p> <p>This setting does not affect multicast settings on existing cameras.</p> <p>You enable and disable live multicasting for a camera on the Client tab for the camera device.</p>
Language	<p>Select the language of the Management Client.</p> <p>Restart the Management Client to use the new language.</p>

Recording server

Name	Description
Timeout for manual PTZ sessions	<p>Client users with the necessary user rights can manually interrupt the patrolling of PTZ cameras. Select how much time should pass before regular patrolling is resumed after a manual interruption. The setting applies for all PTZ cameras on your system. Default setting is 15 seconds.</p> <p>If you want individual timeouts on the cameras, you specify this on the Presets tab for the camera.</p>
Timeout for pause patrolling sessions	<p>Client users with a sufficient PTZ priority can pause patrolling on PTZ cameras. Select how much time should pass before regular patrolling is resumed after a pause. The setting applies for all PTZ cameras on your system. Default setting is 10 minutes.</p> <p>If you want individual timeouts on the cameras, you specify this on the Presets tab for the camera.</p>
Timeout for reserved PTZ sessions	<p>Set the default timeout period for reserved PTZ sessions. When a user runs a reserved PTZ session, the PTZ camera cannot be used by others before it is released either manually or when the period has timed out. Default setting is 1 hour.</p> <p>If you want individual timeouts on the cameras, you specify this on the Presets tab for the camera.</p>
Ignore device communication errors if communication reestablished before	<p>The system logs all communication errors on hardware and devices, but here you select for how long a communication error must exist before the rule engine triggers the Communication Error event.</p>

Server Logs tab (options)

On the **Server Logs** tab, you can specify settings for the system's management server logs.

For more information, see Logs (explained) on page 383.

Name	Description
Logs	<p>Select the log type that you want to configure:</p> <ul style="list-style-type: none"> • System logs • Audit logs • Rule-triggered logs
Settings	<p>Disable or enable the logs and specify the retention period.</p> <p>Allow 2018 R2 and earlier components to write logs. For more information, see Allow 2018 R2 and earlier components to write logs on page 385</p> <p>For System logs, specify the level of messages that you want to log:</p> <ul style="list-style-type: none"> • All (includes undefined messages) • Information, warnings, and errors • Warnings and errors • Errors (default setting) <p>For Audit logs, enable user access logging if you want the system to log all user actions in XProtect Smart Client. These are, for example, exports, activating outputs, and viewing cameras live or in playback.</p> <p>Specify:</p> <ul style="list-style-type: none"> • The length of a playback sequence <p>This means that as long as the user plays back within this period, the system only generates one log entry. When playing back outside the period, the system creates a new log entry.</p> <ul style="list-style-type: none"> • The number of records (frames) a user has seen before the system creates a log entry

Mail Server tab (options)

On the **Mail Server** tab, you can specify the settings for your system's mail server. For more information, see Notification profiles on page 310.

Name	Description
Sender e-mail address	Enter the email address that you want to appear as the sender of email notifications for all notification profiles. Example: sender@organization.org .
Mail server address	Enter the address of the SMTP mail server that sends e-mail notifications. Example: mailserver.organization.org .
Mail server port	The TCP port used for connecting to the mail server. Default port is 25 for unencrypted connections, Encrypted connections typically use port 465 or 587.
Encrypt the connection to the server	<p>If you want to secure the communication between the management server and the SMTP mail server, select this check box.</p> <p>The connection is secured using the STARTTLS email protocol command. In this mode, the session begins on an unencrypted connection, then a STARTTLS command is issued by the SMTP mail server to the management server to switch to secure communication using SSL.</p>
Server requires login	If enabled, you must specify a user name and password for the users to log in to the mail server.

AVI Generation tab (options)

On the **AVI Generation** tab, you can specify compression settings for the generation of AVI video clip files. The settings are required if you want to include AVI files in e-mail notifications sent by rule-triggered notification profiles.

See also Notification profiles on page 310.

Name	Description
Compressor	<p>Select the codec (compression/decompression technology) that you want to apply. To have more codecs available in the list, install them on the management server.</p> <p>Not all cameras support all codecs.</p>

Name	Description
Compression quality	<p>(Not available for all codecs). Use the slider to select the degree of compression (0-100) to be performed by the codec.</p> <p>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.</p> <p>If the slider is not available, the compression quality is determined entirely by the selected codec.</p>
Keyframe every	<p>(Not available for all codecs). If you want to use keyframes, select the check box and specify the required number of frames between keyframes.</p> <p>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.</p> <p>If the check box is not available, or not selected, every frame contains the entire view of the camera.</p>
Data rate	<p>(Not available for all codecs). If you want to use a particular data rate, select the check box and specify the number of kilobytes per second.</p> <p>The data rate specifies the size of the attached AVI file.</p> <p>If the check box is not available, or not selected, the data rate is determined by the selected codec.</p>

Network tab (options)

On the **Network** tab, you can specify the IP addresses of the local clients, if the clients are to connect to the recording server via the Internet. The surveillance system then recognizes them as coming from the local network.

You can also specify the IP version of the system: IPv4 or IPv6. Default value is IPv4.

Bookmark tab (options)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

Name	Description
Bookmark ID prefix	Specify a prefix for all the bookmarks that is made by the users of XProtect Smart Client.
Default bookmark time	<p>Specify the default start and end time of a bookmark is set in XProtect Smart Client.</p> <p>This setting needs to be aligned with:</p> <ul style="list-style-type: none"> • The default bookmark rule, see Rules on page 298 • The pre-buffer period for each camera, see Devices that support pre-buffering on page 211

To specify the bookmark rights of a role, see Device tab (roles) on page 358.

User Settings tab (options)

On the **User Settings** tab, you can specify user preference settings, for example, if a message should be shown when remote recording is enabled.

Customer Dashboard tab (options)

On the **Customer Dashboard** tab, you can enable or disable Milestone Customer Dashboard.

Customer Dashboard is an online monitoring service that provides a graphical overview of the current status of your system, including possible technical issues such as camera failures, to system administrators or other people that have been given access to information about your system installation.

You can select or clear the check box to change your Customer Dashboard settings at any time.

Evidence Lock tab (options)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

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

To specify the evidence lock access rights of a role, see the Device tab (roles) on page 358 for role settings.

Audio messages tab (options)

On the **Audio messages** tab, you can upload files with audio messages that are used for broadcasting messages, triggered by rules.

The maximum number of uploaded files is 50 and the maximum size allowed for each file is 1 MB.

Name	Description
Name	Provides the name of a message. You enter the name when you add a message. To upload a message to the system, click Add .
Description	<p>Provides a description of the message.</p> <p>You enter the description when you add a message. You can use the description field to describe the purpose or the actual message.</p>
Add	<p>Lets you upload audio messages to the system.</p> <p>Supported formats are standard Windows audio file formats:</p> <ul style="list-style-type: none"> • .wav • .wma • .flac
Edit	Lets you modify the name and description, or you can replace the actual file.

Name	Description
Remove	Delete the audio message from the list.
Play	Click this button to listen to the audio message from the computer that runs the Management Client.

To create a rule that triggers playback of audio messages, see [Rules](#) on page 298.

To learn more about actions in general that you can use in rules, see [Actions and stop actions \(explained\)](#) on page 276.

Access Control Settings tab (options)



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

Name	Description
Show development property panel	<p>If selected, additional developer information appears for Access Control > General Settings.</p> <p>This setting is only meant to be used by developers of access control system integrations.</p>

Analytics Events tab (options)

On the **Analytics Events** tab, you can enable and specify the analytics events feature.



Name	Description
Enable	Specify if you want to use analytics events. As default, the feature is disabled.
Port	Specify the port used by this feature. The default port is 9090.



Name	Description
	Make sure that relevant VCA tool providers also use this port number. If you change the port number, remember to change the port number of the providers.
All network addresses or Specified network addresses	Specify if events from all IP addresses/hostnames are allowed, or only events from IP addresses/hostnames that are specified in the Address list (see below).
Address list	<p>Specify a list of trusted IP addresses/hostnames. The list filters incoming data so that only events from certain IP addresses/hostnames are allowed. You can use both Domain Name System (DNS), IPv4 and IPv6 address formats.</p> <p>You can add addresses to your list by manually entering each IP address or host name, or by importing an external list of addresses.</p> <ul style="list-style-type: none"> • Manual entering: Enter the IP address/hostname in the address list. Repeat for each required address • Import: Click Import to browse for the external list of addresses. The external list must be a .txt file and each IP address or host name must be on a separate line

Alarms and Events tab (options)

On the **Alarms and Events** tab, you can specify settings for alarms, events and logs. Related to these settings, see also Limit size of database on page 50.

Name	Description
Keep closed alarms for	Specify the number of days for storing alarms with the state Closed in the database. If you set the value to 0 , the alarm is deleted after it has been closed.

Name	Description
	<div>  <p>Alarms always have timestamps. If the alarm is triggered by a camera, the timestamp has an image from the time of the alarm. The alarm information itself is stored on the event server, while the video recordings corresponding to the attached image are stored on the relevant surveillance system server.</p> <p>To be able to see the images of your alarms, keep video recordings for at least as long as you intend to keep alarms on the event server.</p> </div>
Keep all other alarms for	<p>Specify the number of days for storing alarms with the state New, In progress, or On hold. If you set the value to 0, the alarm appears in the system, but will not be stored.</p> <div>  <p>Alarms always have timestamps. If the alarm is triggered by a camera, the timestamp has an image from the time of the alarm. The alarm information itself is stored on the event server, while the video recordings corresponding to the attached image are stored on the relevant surveillance system server.</p> <p>To be able to see the images of your alarms, keep video recordings for at least as long as you intend to keep alarms on the event server.</p> </div>
Keep logs for	<p>Specify the number of days for keeping the event server logs. If you keep the logs for longer periods of time, ensure that the machine where the event server is installed has enough disk space.</p>
Enable verbose logging	<p>To keep a more detailed log for event server communication, select the check box. It will be stored for the number of days specified in the Keep logs for field.</p>
Event types	<p>Specify the number of days for storing events in the database. There are two ways of doing this:</p> <ul style="list-style-type: none"> You can specify the retention time for an entire event group. Event types with the value Follow group will inherit the value of the event group

Name	Description
	<ul style="list-style-type: none"> Even if you set a value for an event group, you can specify the retention time for individual event types. <div>  If the value is 0, the events will not be stored in the database. </div> <div>  The external events (user-defined events, generic events, and input events) are set to 0 by default, and you cannot change that value. The reason is that these types of events occur so frequently that storing them in the database may cause performance issues. </div>

Generic Events tab (options)

On the **Generic Events** tab, you can specify generic events and data source related settings.

For more information about how to configure actual generic events, see Generic events on page 321.

Name	Description
Data source	<p>You can choose between two default data sources and define a custom data source. What to choose depends on your third party program and/or the hard- or software you want to interface from:</p> <p>Compatible: Factory default settings are enabled, echoes all bytes, TCP and UDP, IPv4 only, port 1234, no separator, local host only, current code page encoding (ANSI).</p> <p>International: Factory default settings are enabled, echoes statistics only, TCP only, IPv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10).</p> <p>[Data source A]</p> <p>[Data source B]</p> <p>and so on.</p>

Name	Description
New	Click to define a new data source.
Name	Name of the data source.
Enabled	Data sources are by default enabled. Clear the check box to disable the data source.
Reset	Click to reset all settings for the selected data source. The entered name in the Name field remains.
Port	The port number of the data source.
Protocol type selector	<p>Protocols which the system should listen for, and analyze, in order to detect generic events:</p> <p>Any: TCP as well as UDP.</p> <p>TCP: TCP only.</p> <p>UDP: UDP only.</p> <p>TCP and UDP packages used for generic events may contain special characters, such as @, #, +, ~, and more.</p>
IP type selector	Selectable IP address types: IPv4, IPv6 or both.
Separator bytes	Select the separator bytes used to separate individual generic event records. Default for data source type International (see Data sources earlier) is 13,10 . (13,10 = <CR><IF>).
Echo type selector	<p>Available echo return formats:</p> <ul style="list-style-type: none"> • Echo statistics: Echoes the following format: [X],[Y],[Z],[Name of generic event] [X] = request number. [Y] = number of characters. [Z] = number of matches with a generic event. [Name of generic event] = name entered in the Name field. • Echo all bytes: Echoes all bytes • No echo: Suppresses all echoing

Name	Description
Encoding type selector	By default, the list only shows the most relevant options. Select the Show all check box to display all available encodings.
Allowed external IPv4 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.
Allowed external IPv6 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.

Initial configuration tasks list

The checklist below lists the initial tasks for configuring your system. Some of them, you may already have completed during installation.


A completed checklist does not in itself guarantee that the system matches the exact requirements of your organization. To make the system match the needs of your organization, Milestone recommends that you monitor and adjust the system continuously.

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

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

Step	Description
<input checked="" type="checkbox"/>	You have finished the initial installation of your system. See Install a new XProtect system on page 73.
<input checked="" type="checkbox"/>	Change the trial SLC to a permanent SLC (if required). See Change the Software License Code on page 48.

Step	Description
<input checked="" type="checkbox"/>	Log in to the Management Client. See Login overview on page 102.
<input type="checkbox"/>	Verify that each recording server's storage settings meet your needs. See Storage tab (recording server) on page 140.
<input type="checkbox"/>	Verify that each recording server's archiving settings meet your needs. See Storage tab (recording server) on page 140.
<input type="checkbox"/>	Detect the hardware, cameras or video encoders to add to each recording server. See Add hardware on page 176.
<input type="checkbox"/>	Configure each recording server's individual cameras. See Camera devices (explained) on page 191.
<input type="checkbox"/>	Enable storage and archiving for individual cameras or for a group of cameras. This is done from the individual cameras or from the device group. See Storage tab (recording server) on page 140.
<input type="checkbox"/>	Enable and configure devices. See Site Navigation: Devices: Working with devices on page 190.
<input type="checkbox"/>	Rules determine the system's behavior to a large extent. You create rules to define when cameras should record, when pan-tilt-zoom (PTZ) cameras should patrol, and when notifications should be sent, for example. Create rules. See Rules and events (explained) on page 274.
<input type="checkbox"/>	Add roles to the system. See Roles (explained) on page 326.
<input type="checkbox"/>	Add users or groups of users to each of the roles.

Step	Description
	See Assign/remove users and groups to/from roles on page 330.
	Activate licenses. See License information on page 124 or License information on page 124.

See also Configuring the system in the Site Navigation pane on page 124.

Configuring the system in the Site Navigation pane

In the **Site Navigation** pane, you can configure and manage your system so it matches your needs. If your system is not a single-site system, but includes federated sites, note that you manage these sites on the **Federated Site Hierarchy** pane.

Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

Site Navigation: Basics

This article describes how to view and manage licenses and how to add information about the site.

License information

You can keep track of all licenses that share the same software license file both on this site and on all other sites, your Milestone Care subscriptions and decide how you want to activate your licenses. For basic information about the different XProtect licenses, see Licenses (explained) on page 47.

Licensed to

Lists the contact details of the license owner that you entered during the software registration. Click **Edit details** to edit the license owner information. Here you can also find a link to the end user license agreement, which you accepted prior to the installation.

Milestone Care

Here you can see information about your current Milestone Care™ level. When you bought your system, you also entered a two-year Milestone Care Plus subscription. Your installation is always covered by Milestone Care Basic which gives you access to different types of self-help material like knowledge base articles, guides and tutorials on our Support website (<https://www.milestonesys.com/support/>). The expiration date of your Milestone Care Plus

subscription is visible in the **Installed Products** table. If you decide to buy or renew a Milestone Care subscription after you have installed your system, you must activate your licenses before the correct Milestone Care information appear.

A Milestone Care Plus subscription gives you access to upgrades. You also get access to the Customer Dashboard service, the Smart Connect feature, and the full Push Notification functionality. If you have a Milestone Care Premium subscription, you can also contact Milestone support for help. Please remember to include information about your Milestone Care ID when contacting Milestone support. Again, the expiry date for your Milestone Care Premium subscription is visible. To learn more about Milestone Care, follow the links.

Installed Products

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

- Products and versions
- The products' software license code (SLC)
- The expiration date of your SLC. Typically, unlimited
- The expiration date of your Milestone Care Plus subscription
- The expiration date of your Milestone Care Premium subscription



Some licenses, such as XProtect Essential+, are installed with the automatic license activation enabled, and it is not possible to disable this setting.

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2016	M01-C01-100-01- HC4288	Unlimited	01-10-2016	01-10-2016
Milestone XProtect Smart Wall	M01-P03-023-01- HC4284	Unlimited	Unlimited	
Milestone XProtect Access 2016 v10.0a	M01-P01-011-01- HC428F	Unlimited	Unlimited	
Milestone XProtect Transact 2016	M01-P08-100-01- HC42E1	Unlimited	Unlimited	

License Overview - All sites

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

For a detailed overview of the status of your licenses activated on other sites, click the **License Details - All sites** link. See the **License Details - Current site** section below for the available information.

License Overview - All sites[License Details - All Sites...](#)

License Type	Activated
Hardware Device	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

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

License Details - Current Site

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

You can also see the number of used device changes without activation (see Device changes without activation (explained) on page 127) and how many you have available per year in the **Changes without activation** column.

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

If you forget to activate licenses before the grace period expires, they will stop sending video to the system. These licenses are shown in the **Grace Period Expired** column. For more information, see Activate licenses after grace period on page 130.

If you have used more licenses than you have available, these are listed in the **Without License** column and cannot be used in your system. For more information, see Get additional licenses on page 131.

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

License Details - Current Site: SYS TESTED VM

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

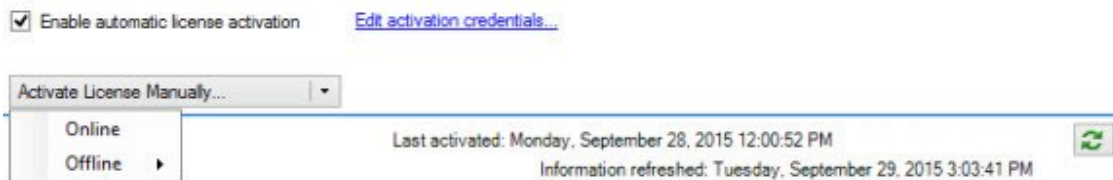
Hardware devices without licenses are identified by an exclamation mark in the Management Client. The exclamation mark is also used for other purposes. Place your mouse over the exclamation mark to see the purpose.

Features for activating licenses

Below the three tables are:

- A check box for enabling automatic license activation and a link to edit the user credentials for automatic activation. For more information, see Automatic license activation (explained) on page 129 and Enable automatic license activation on page 129. If the automatic activation has failed, a failed message will appear in red. For more information, click the **Details** link

- A drop-down list for manually activating licenses online or offline. For more information, see [Activate licenses online](#) on page 130 and [Activate licenses offline](#) on page 130
- In the lower right corner of the page, you can see when your licenses were activated last (automatically or manually) and when the information on the page were refreshed. The time stamps are from the server and not from the local computer



Device changes without activation (explained)

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

One year after your last license activation, your number of used **device changes without activation** is automatically reset to zero. Once the reset happens, you can continue to add and replace hardware devices without activating the licenses.

The number of device changes without activation differs from installation to installation and is calculated based on several variables. For a detailed description, see [License information](#) on page 124.

If your surveillance system is offline for longer periods of time, for example in cases with a surveillance system on a ship on a long cruise or a surveillance system in a very remote place without any Internet access, you can contact your Milestone reseller and request a higher number of device changes without activation.

You must explain why you think you qualify for a higher number of device changes without activation. Milestone decides each request on an individual basis. Should you be granted a higher number of device changes without activation, you must activate your licenses to register the higher number on your XProtect system.

How the number of device changes without activation is calculated

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

- **C%** that is a fixed percentage of the total amount of activated licenses
- **Cmin** that is a fixed minimum value of the number of device changes without activation
- **Cmax** that is a fixed maximum value of the number of devices changes without activation

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

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

For more information about the current default values for your product, go to My Milestone (<https://www.milestonesys.com/device-change-calculation/>).

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

A customer buys 100 hardware device licenses. He adds 100 cameras to his system. Unless he has enabled automatic license activation, his device changes without activation is still zero. He activates his licenses and he now has 15 device changes without activation.

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

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

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

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

View license overview

You can access a license overview that lists licenses that are activated, in a grace period, expired and missing for all sites licensed via the same software license file.

- Click **License Overview**

If the connection is down, you can only view the number of activated licenses. N/A appears for licenses in a grace period, expired licenses, and missing licenses.

Automatic license activation (explained)

For easy maintenance and flexibility, Milestone recommends that you enable automatic license activation (see [Enable automatic license activation on page 129](#)) because it means less maintenance for you. Automatic license activation requires the management server to be online.

When the requirements above are met, the system activates your hardware devices or other licenses a few minutes after you have added, removed or replaced hardware devices or made other changes that affect the use of your licenses. Therefore, you never have to manually start a license activation. The number of used device changes without activation is always zero. No hardware devices are within a grace period and at risk of expiring. If one of your base licenses expires within a period of 14 days, your XProtect system will also - as an extra precaution - automatically try to activate your licenses every night.

The only time you have to manually activate your licenses is when you:

- Purchase additional licenses (see [Get additional licenses on page 131](#))
- Want to upgrade (see [Upgrade requirements on page 461](#))
- Buy or renew a Milestone Care subscription (see [Automatic license activation \(explained\)](#))
- Receive allowance for more device changes without activation (see [Device changes without activation \(explained\) on page 127](#))

Enable automatic license activation

1. On the **License Information** page, select **Enable automatic license activation**.
2. Enter the user name and password that you want to use with automatic license activation:
 - If you are an existing user, enter your user name and password to log into the software registration system
 - If you are a new user, click the **Create new user** link to set up a new user account and then follow the registration procedure. If you have not yet registered your Software License Code (SLC), you must do so

The credentials are saved in a file on the management server.
3. Click **OK**.

If you later want to change your user name and/or the password for automatic activation, click the **Edit activation credentials** link.

Disable automatic license activation

Disable automatic license activation but keep the password for later use:

1. On the **License Information** page, clear **Enable automatic license activation**. The user name and password are still saved on the management server.

Disable automatic license activation and delete password:

1. On the **License Information** page, click **Edit activation credentials**.
2. Click **Delete password**.
3. Confirm that you want to delete the user name and password from the management server.

Activate licenses online

Activate your licenses online if the computer that runs the management server has Internet access.

1. On the **License Information** node, select **Activate License Manually** and then **Online**.
2. The **Activate Online** dialog box opens:
 - If you are an existing user, enter your user name and password
 - If you are a new user, click the **Create new user** link to set up a new user account. If you have not yet registered your Software License Code (SLC), you must do so
3. Click **OK**.

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

Activate licenses offline

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

1. On the **License Information** node, select **Activate License Manually > Offline > Export License for Activation** to export a license request file (.lrq) with information about your added hardware devices.
2. The license request file (.lrq) is automatically given the same name as your SLC. If you have several sites, remember to make the name unique so you can easily identify which file belongs to which site.
3. Copy the license request file to a computer with internet access and log into our website (<https://online.milestonesys.com/>) to obtain the activated software license file (.lic).
4. Copy the .lic file that has the same name as your license request file to your computer with Management Client.
5. In the Management Client on the **License Information** page, select **Activate License Offline > Import Activated License**, and select the activated software license file to import it and thereby activate your licenses.
6. Click **Finish** to end the activation process.

Activate licenses after grace period

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

- Configuration of the camera and other settings are not removed from the Management Client
- The license is not removed from the system configuration
- To enable the unavailable devices again, activate the licenses as usual. For more information, see [Activate licenses offline on page 130](#) or [Activate licenses online on page 130](#)

Get additional licenses

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

- To get additional licenses for your system, contact your XProtect product reseller

New licenses to your existing surveillance system version:

- Simply activate your licenses manually to get access to the new licenses. For more information, see [Activate licenses offline on page 130](#) or [Activate licenses online on page 130](#)

New licenses and an upgraded surveillance system version:

- You receive an updated software license file (.lic) (see [Licenses \(explained\) on page 47](#)) with the new licenses and the new version. You must use the new software license file during the installation of the new version. For more information, see [Upgrade requirements on page 461](#)

Licenses and hardware device replacement

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

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

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

If you replace a hardware device with a different model, you must use the **Replace Hardware** wizard (see [Replace hardware on page 443](#)) to map all relevant databases of cameras, microphones, inputs, outputs, and settings.

If you have enabled automatic license activation (see [Enable automatic license activation on page 129](#)), the new hardware device is automatically activated.

If you have used all your device changes without activation (see [Device changes without activation \(explained\) on page 127](#)), you must manually activate your licenses. For more information about activating licenses, see [Activate licenses offline on page 130](#) or [Activate licenses online on page 130](#).

Site information

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

- Address/location
- Administrator(s)
- Additional information

Edit site information

To update site information:

1. Select **Edit**.
2. Select a tag.
3. Enter information in the **Value** field.
4. Click **OK**.

Site Navigation: Servers and hardware

This section describes how to install and configure recording servers and failover recording servers. You also learn how to add new hardware to the system and interconnect other sites.

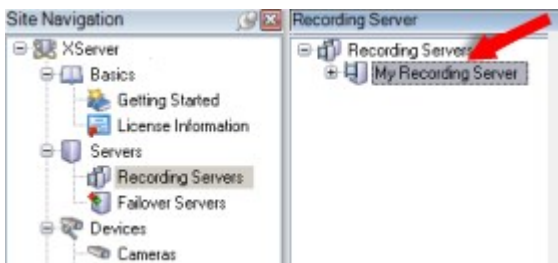
- Site Navigation: Servers and hardware: Recording servers on page 132
- Site Navigation: Servers and hardware: Failover servers on page 165
- Site Navigation: Servers and hardware: Hardware on page 176
- Site Navigation: Servers and hardware: Manage remote servers on page 187

Site Navigation: Servers and hardware: Recording servers

Recording servers (explained)

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

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



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

The recording server supports encryption of data streams to the clients and services. For more information, see [Before you start installation](#) on page 55:

- [Enable encryption to clients and servers](#) on page 400
- [View encryption status to clients](#) on page 136

The recording server also supports encryption of the connection with the management server. For more information, see [Before you start installation](#) on page 55:

- [Enable encryption](#) on page 397
- [Enable server encryption for recording servers or remote servers](#) on page 398

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

- [Add hardware](#) on page 176
- [Move hardware](#) on page 439
- [Delete all hardware on a recording server](#) on page 457
- [Remove a recording server](#) on page 457



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

Register a recording server

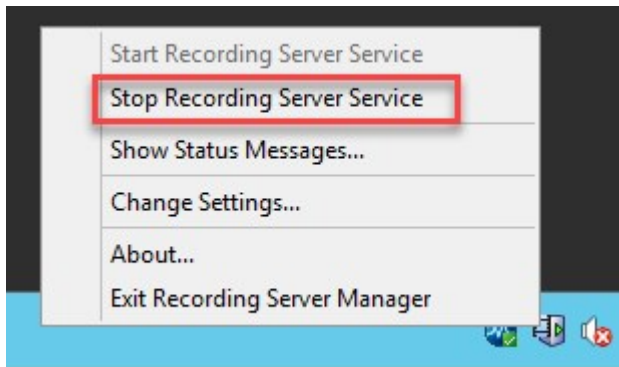
When you install a recording server, it is automatically registered in most cases. But you need to do the registration manually if:

- The recording server was installed offline and then added to the management server afterward
- Your management server does not use the default ports. Port 80 is the default port in a system with no encryption between the recording server and the management server. If encryption is enabled, the default port is 443

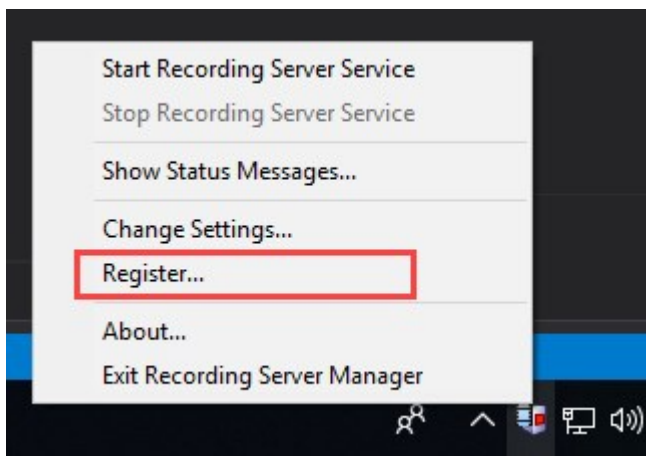
- You have replaced the recording server
- You change the address of the management server
- You disable or enable encryption from the management server to the recording server

When you register a recording server, you configure it to connect to your management server. The part of the management server that handles registration is the Authorization Server service.

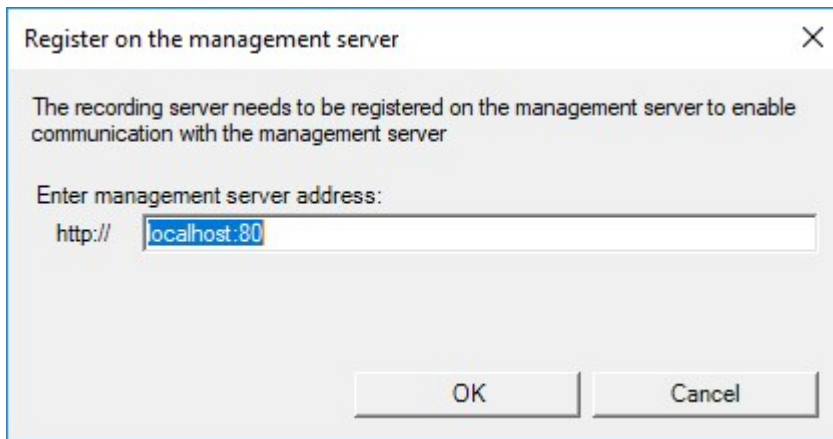
1. On the recording server, right-click the Recording Server Manager tray icon in the notification area and stop the Recording Server service.



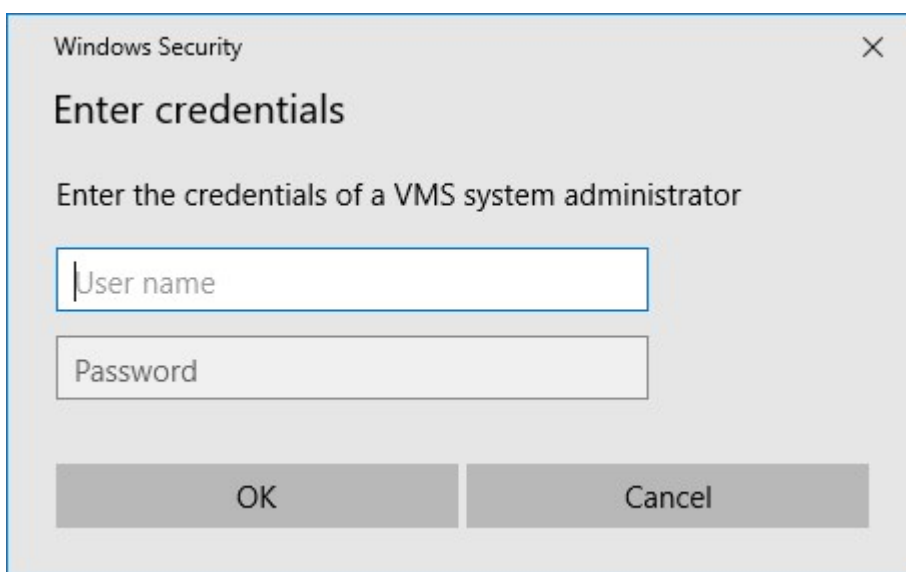
2. When the recording server is not running, right-click the Recording Server Manager tray icon and select **Register**.



3. Enter the address of the management server that you want the recording server to connect to and click **OK**.



4. Enter the user name and password of a system administrator of XProtect and click **OK**.



5. A confirmation window pops up and the recording server is registered. Right-click the Recording Server Manager tray icon in the notification area and start the Recording Server service.

See also Replace a recording server on page 438.

Change or verify the basic configuration of a recording server

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

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

1. On the computer that runs the recording server, right-click the **Recording Server** icon in the notification area.
2. Select **Stop Recording Server service**.
3. Right-click the **Recording Server** icon again and select **Change Settings**.

The **Recording Server Settings** window appears.

4. Verify/change, for example, the following settings:
 - **Management server hostname/IP address:** Specify the IP address or host name of the management server to which the recording server should be connected
 - **Management server port:** Specify the port number to be used when communicating with the management server. Default is port 9000. You can change this if required, but the port number must always match the port number set up on the management server
5. Click **OK**.
6. To start the Recording Server service again, right-click the **Recording Server** icon, and select **Start Recording Server service**.

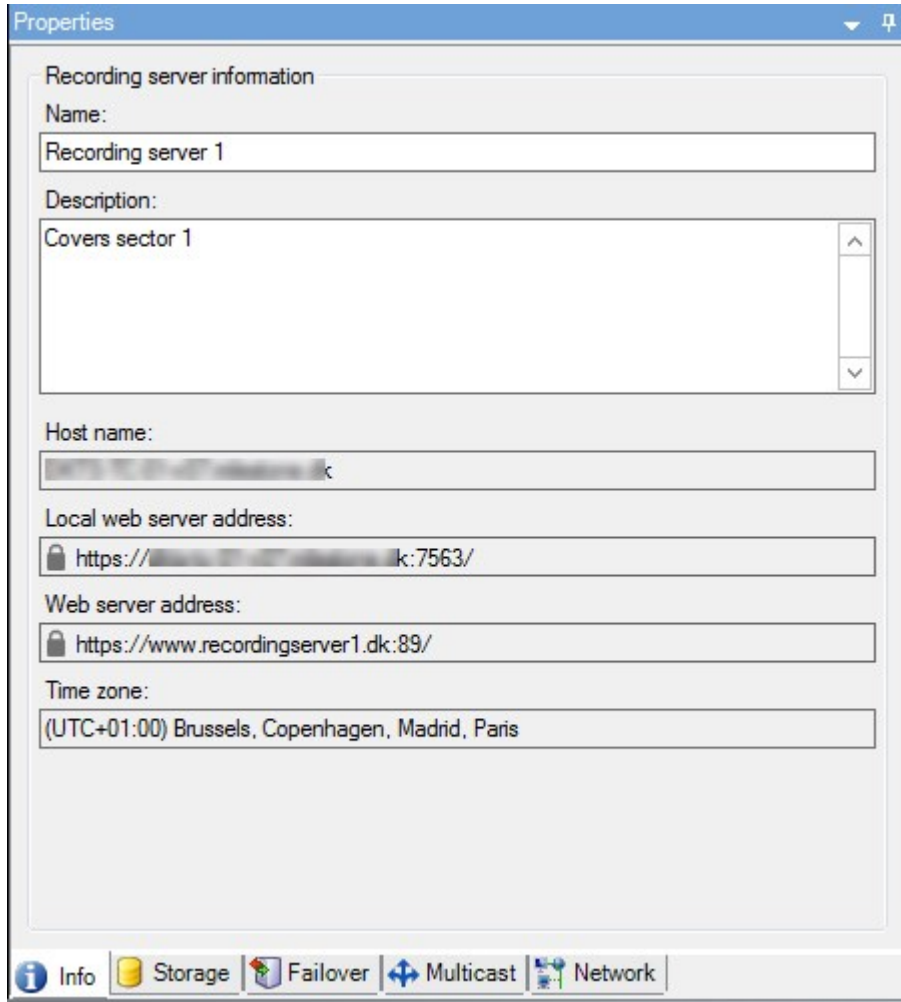


Stopping the Recording Server service means that you cannot record and view live video while you verify/change the recording server's basic configuration.

View encryption status to clients

To verify if your recording server encrypt connections:

1. Open the Management Client.
2. In the **Site Navigation** pane, select **Servers > Recording Servers**. This opens a list of recording servers.
3. In the **Overview** pane, select the relevant recording server and go to the **Info** tab.
If encryption is enabled to clients and servers that retrieve data streams from the recording server, a padlock icon appears in front of the local web server address and the optional web server address.



The screenshot shows a 'Properties' dialog box with a blue title bar. It contains several fields for configuring a recording server. The 'Name' field is 'Recording server 1'. The 'Description' field is 'Covers sector 1'. The 'Host name' field is partially obscured. The 'Local web server address' field shows a padlock icon followed by 'https://[redacted].dk:7563/'. The 'Web server address' field shows a padlock icon followed by 'https://www.recordingserver1.dk:89/'. The 'Time zone' field is '(UTC+01:00) Brussels, Copenhagen, Madrid, Paris'. At the bottom, there is a tab bar with icons and labels for 'Info', 'Storage', 'Failover', 'Multicast', and 'Network'.

Properties

Recording server information

Name:
Recording server 1

Description:
Covers sector 1

Host name:
[redacted].dk

Local web server address:
🔒 https://[redacted].dk:7563/






Web server address:
🔒 https://www.recordingserver1.dk:89/

Time zone:
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris

Info Storage Failover Multicast Network

Recording server status icons

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

Icon	Description
	Recording server is running
	<p>Recording server requires attention: Either the recording server is not running or it is running with errors.</p> <ol style="list-style-type: none"> 1. Hover over the recording server icon to view the status message. 2. If you need to start or stop the recording server, right-click the Recording Server Manager tray icon.
	<p>Ongoing database repair: Appears when databases are corrupted, for example due to a power failure, and the recording server is repairing them. The repair process may take some time if the databases are large.</p> <p>See Protect recording databases from corruption on page 54 for information about how to avoid corrupt databases.</p> <div>  <p>During a database repair at startup, you cannot record video from cameras connected to the recording server. Only live viewing is available.</p> </div> <div>  <p>A database repair at normal operation does not affect any recordings.</p> </div>

Info tab (recording server)

On the **Info** tab, you can verify or edit the name and description of the recording server.

You can view the host name and addresses. The padlock icon in front of the web server address indicates encrypted communication with the clients and services that retrieve data streams from this recording server.

Properties

Recording server information

Name:
Recording server 1

Description:
Covers sector 1

Host name:
[Redacted]

Local web server address:
https://[Redacted]:7563/

Web server address:
https://www.recordingserver1.dk:89/

Time zone:
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris

Info | Storage | Failover | Multicast | Network

Info tab properties (recording server)

Name	Description
Name	<p>You can choose to enter a name for the recording server. The name is used in the system and clients when the recording server is listed. The name does not have to be unique.</p> <p>When you rename a recording server, the name is changed globally in the Management Client.</p>
Description	<p>You can choose to enter a description that appears in a number of listings within the system. A description is not mandatory.</p>

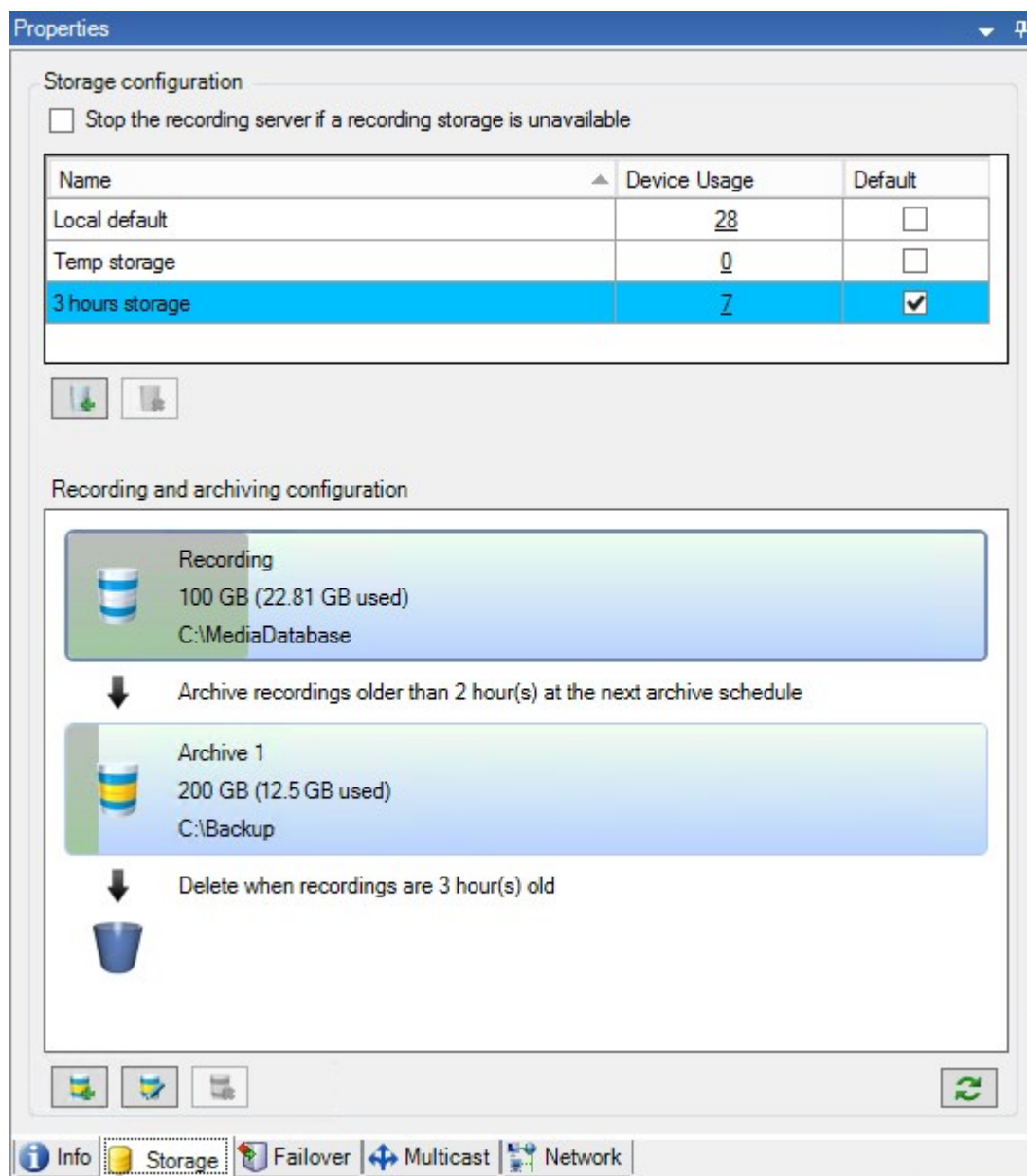
Name	Description
Host name	Displays the recording server's host name.
Local web server address	<p>Displays the local address of the recording server's web server. You use the local address, for example, for handling PTZ camera control commands, and for handling browsing and live requests from XProtect Smart Client.</p> <p>The address includes the port number that is used for web server communication (typically port 7563).</p> <p>If you enable encryption to clients and servers that retrieve data streams from the recording server, a padlock icon appears, and the address includes https instead of http.</p>
Web server address	<p>Displays the public address of the recording server's web server over the internet.</p> <p>If your installation uses a firewall or NAT router, enter the address of the firewall or NAT router so that clients that access the surveillance system on the internet can connect to the recording server.</p> <p>You specify the public address and port number on the Network tab.</p> <p>If you enable encryption to clients and servers that retrieve data streams from the recording server, a padlock icon appears, and the address includes https instead of http.</p>
Time zone	Displays the time zone that the recording server is located in.

Storage tab (recording server)

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

For recording storages and archives, the horizontal bar shows the current amount of free space. You can specify the behavior of the recording server in case recording storages become unavailable. This is mostly relevant if your system includes failover servers.

If you are using **Evidence lock**, there will be a vertical red line showing the space used for evidence locked footage.



Storage and archiving (explained)

Available functionality depends on the system you are using. See

<https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

To avoid that the recording database runs full, you can create additional storages (see [Storage and archiving \(explained\)](#)). You can also create archives (see [Create an archive within a storage](#)) within each storage and start an archiving process to store data.



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

You configure storage and archiving on each recording server.

As long as you store archived recordings locally or on accessible network drives, you can use XProtect Smart Client to view them.

If a disk drive breaks and the recording storage becomes unavailable, the horizontal bar turns red. It is still possible to view live video in XProtect Smart Client, but recording and archiving stops until the disk drive is restored. If your system is configured with failover recording servers, you can specify the recording server to stop running, to let the failover servers take over (see [Storage and archiving \(explained\)](#)).

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



Milestone recommends that you use a dedicated hard disk drive for recording storages and archives to prevent low disk performance. When you format the hard disk, it is important to change its **Allocation unit size** setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help on the Microsoft website (<https://support.microsoft.com/help/140365/default-cluster-size-for-ntfs-fat-and-exfat/>).



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

Attaching devices to a storage

Once you have configured the storage and archiving settings for a recording server, you can enable storage and archiving for individual cameras or a group of cameras. You do this from the individual devices or from the device group. See [Attach a device or group of devices to a storage](#).

Effective archiving

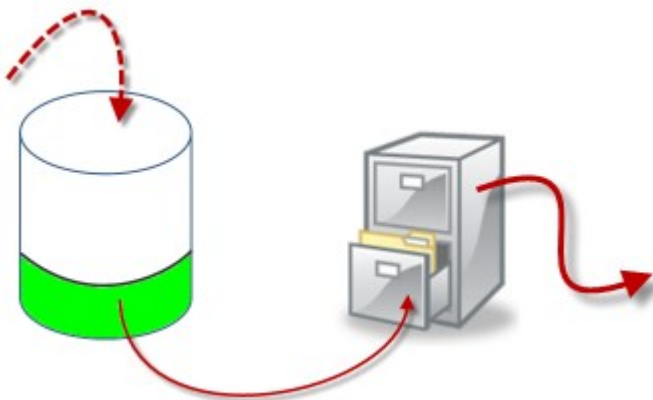
When you enable archiving for a camera or a group of cameras, the content of the recording storage is automatically moved to the first archive at intervals that you define.

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

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

- Recording storage retention
- Recording storage size
- Archive retention
- Archive size
- Archive schedule
- Encryption
- Frames Per Second (FPS).

The size fields define the size of the recording storage, exemplified by the cylinder, and its archive(s) respectively:



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

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

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

FPS determines the size of the data in the databases.

To archive your recordings, you must set all these parameters up in accordance with each other. This means that the retention period of the next archive must always be longer than the retention period of a current archive or recording database. This is because the number of retention days stated for an archive includes all retention

stated earlier in the process. Archiving must also always take place more frequently than the retention period, otherwise you risk losing data. If you have a retention time of 24 hours, any data older than 24 hours is deleted. Therefore, to get your data safely moved to the next archive, it is important to run archiving more often than every 24 hours.

Example: These storages (image to the left) have a retention time of 4 days and the following archive (image to the right) a retention time of 10 days. Archiving is set to occur every day at 10:30, ensuring a much more frequent archiving than retention time.

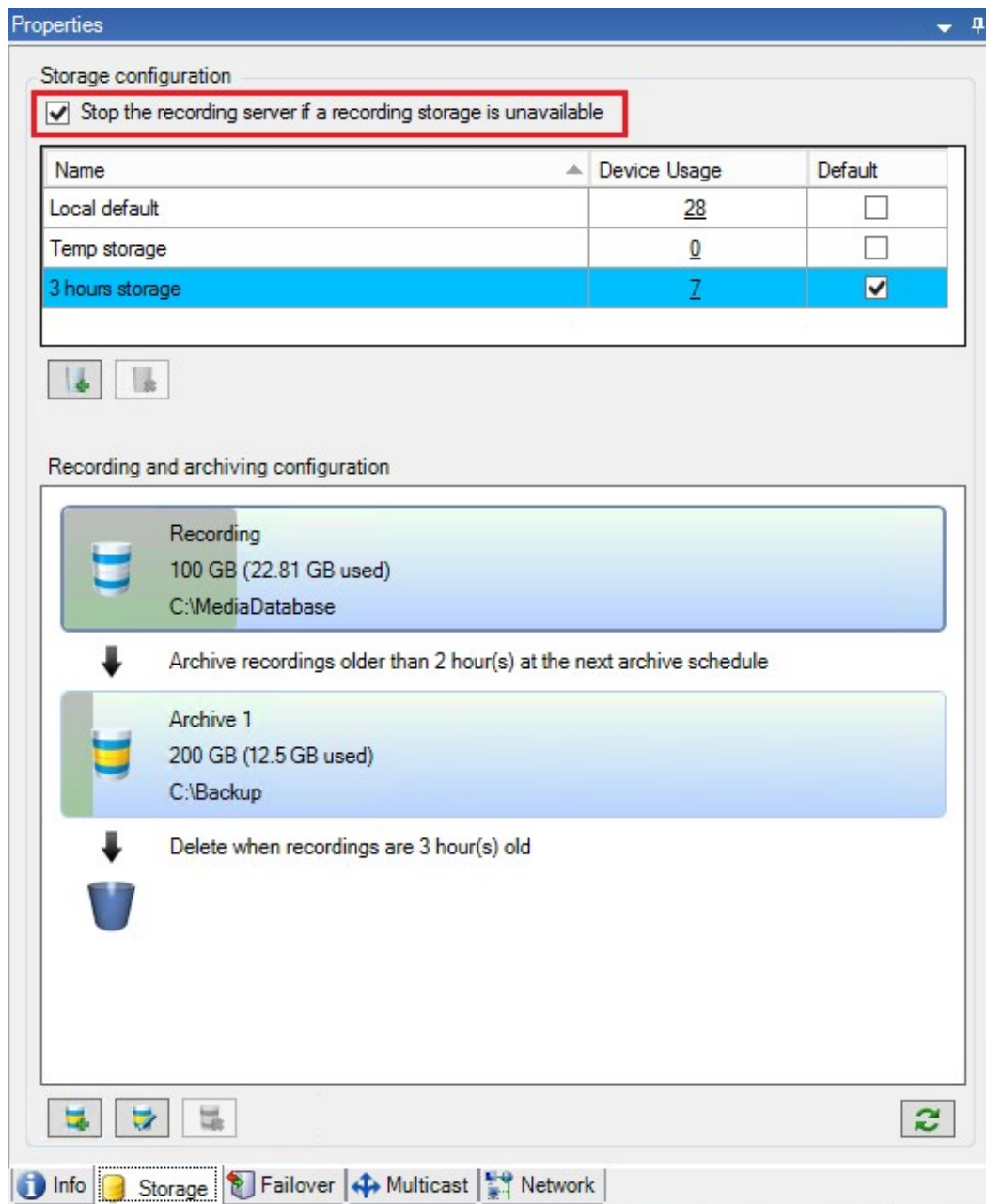


You can also control archiving by use of rules and events.

Specify behavior when recording storage is unavailable


By default, the recording server keeps running if a recording storage becomes unavailable. If your system is configured with failover recording servers, you can specify the recording server to stop running, to make the failover servers take over:

1. On the relevant recording server, go to the **Storage** tab.
2. Select the **Stop the recording server if a recording storage is unavailable** option.



Add a new storage


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

1. To add an extra storage to a selected recording server, click the  button located below the **Storage configuration** list. This opens the **Storage and Recording Settings** dialog box.
2. Specify the relevant settings (see [Storage and Recording Settings properties](#)).
3. Click **OK**.

If needed, you are now ready to create archive(s) within your new storage.

Create an archive within a storage

A storage has no default archive, but you can create archives as needed.

1. Select the relevant storage in the **Recording and archiving configuration** list.
2. Click the  button below the **Recording and archiving configuration** list.
3. In the **Archive Settings** dialog box, specify the required settings (see [Archive Settings properties](#)).
4. Click **OK**.


Attach a device or group of devices to a storage

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

1. Expand **Devices** and select either **Cameras**, **Microphones** or **Speakers** as required.
2. Select the device or a device group.
3. Select the **Record** tab.
4. In the **Storage** area, select **Select**.
5. In the dialog box that appears, select the database that should store the recordings of the device and then click **OK**.
6. In the toolbar, click **Save**.

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

Edit settings for a selected storage or archive

1. To edit a storage, select its recording database in the **Recording and archiving configuration** list. To edit an archive, select the archive database.
2. Click the **Edit Recording Storage** button  located below the **Recording and archiving configuration** list.
3. Either edit a recording database or edit an archive.



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

Enable digital signing for export



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

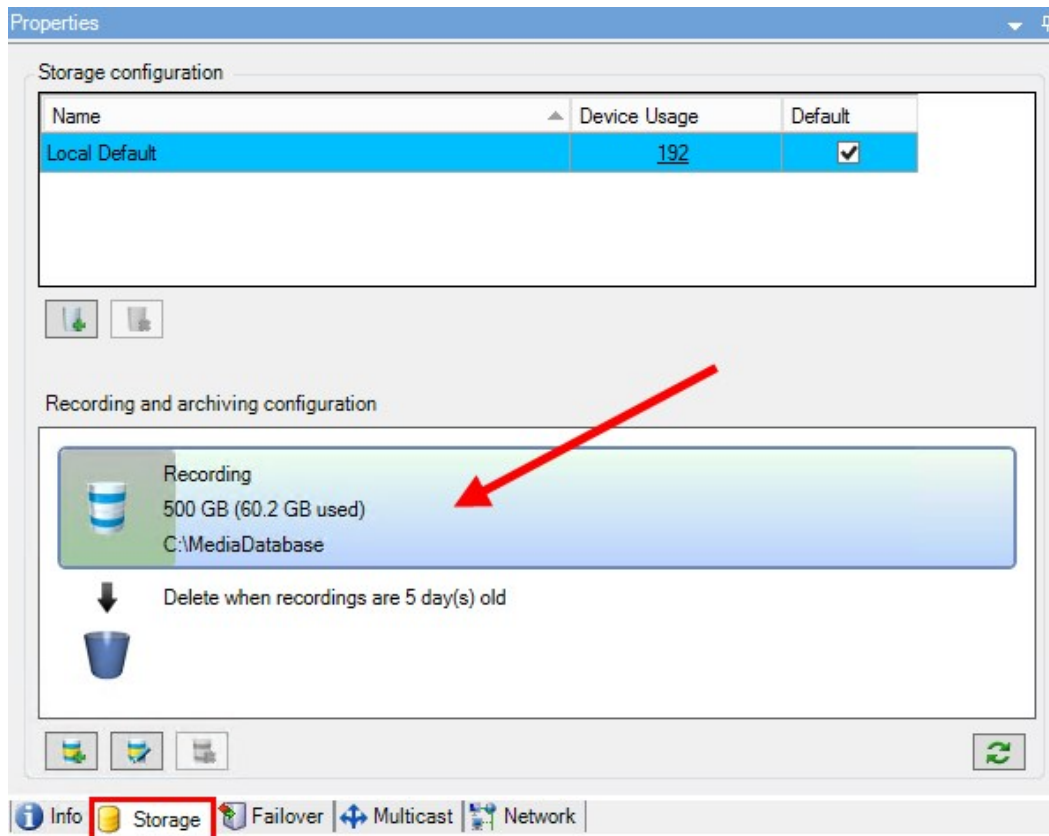
You can enable digital signing for recorded video, so that client users can verify that the recorded video has not been tampered with since it was recorded. Verifying the authenticity of the video is something that the user does in XProtect Smart Client – Player after the video has been exported.



Signing must also be activated in XProtect Smart Client in the **Export** dialog. Otherwise, the **Verify Signatures** button in XProtect Smart Client – Player is not displayed.

1. In the **Site Navigation** pane, expand the **Servers** node.
2. Click **Recording Servers**.
3. In the overview pane, click the recording server you want to enable signing for.

- At the bottom of the **Properties** pane, click the **Storage** tab.



- In the **Recording and archiving configuration** section, double-click the horizontal bar that represents the recording database. The **Storage and Recording Settings** window appears.
- Select the **Signing** check box.
- Click **OK**.

Encrypt your recordings



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

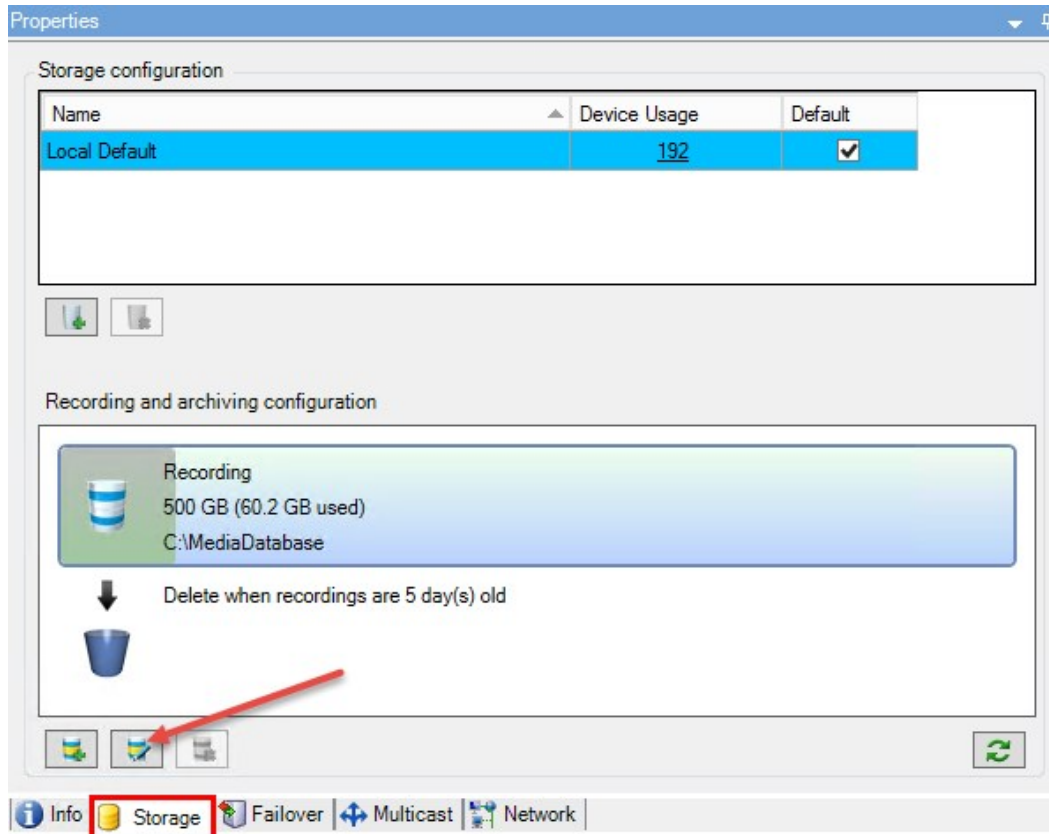
You can secure your recordings by enabling encryption on your recording servers' storage and archives. You can choose between light and strong encryption. When you enable encryption, you must also specify a related password.



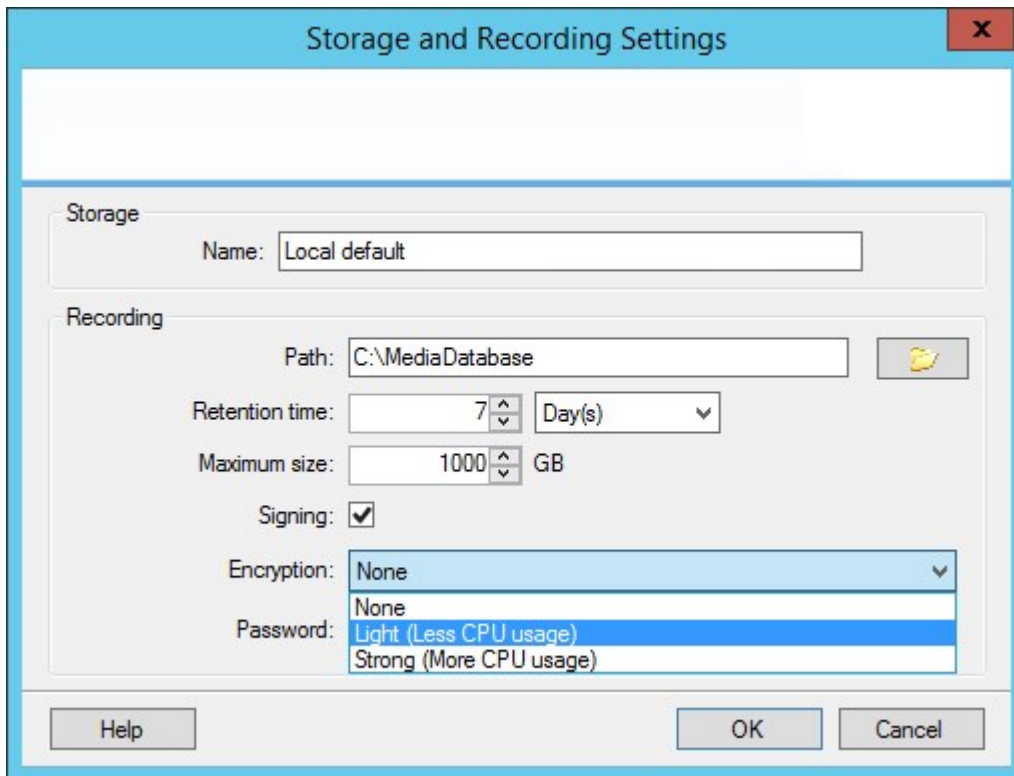
Enabling or changing encryption settings or password can potentially be time consuming, depending on the size of the database and performance of the drive. You can follow the progress under **Current Tasks**.

Do not stop the recording server while this task is ongoing.

1. Click the **Edit Recording Storage** button below the **Recording and archiving configuration** list.



2. In the dialog box that appears, specify encryption level.



3. You are automatically directed to **Set Password** dialog box. Enter password and click **OK**.

Back up archived recordings

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

Back up archives rather than camera databases

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

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

Know your archive structure so that you can target backups

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

During all regular use of your system, the sub-directory structure is completely transparent to the system's users when they browse recordings with XProtect Smart Client. This is true both with archived and non-archived recordings. It is relevant to know the sub-directory structure (see [Archive structure \(explained\)](#)) if you want to back up your archived recordings (see Backing up and restoring system configuration on page 432).

Archive structure (explained)

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



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

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

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

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

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

Naming structure

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

If from edge storage:

```
...[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 Encoder(10.100.50.137) - 2011-10-05T11:23:47+02:00\
```

Sub-directories

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

- **Media:** This folder contains the actual media that is either video or audio (not both)
- **MotionLevel:** This folder contains motion level grids generated from the video data using our motion detection algorithm. This data allows the Smart Search feature in XProtect Smart Client to do very fast searches
- **Motion:** In this folder, the system stores motion sequences. A motion sequence is a time slice for which motion has been detected in the video data. This information is, for example, used in the time line in XProtect Smart Client
- **Recording:** In this folder, the system stores recording sequences. A recording sequence is a time slice for which there are coherent recordings of media data. This information is, for example, used to draw the time line in XProtect Smart Client
- **Signature:** This folder holds the signatures generated for the media data (in the Media folder). With this information, you can verify that the media data has not been tampered with since it was recorded

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

Examples of backup

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

```
...F:\OurArchive\
```

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

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

Delete an archive from a storage

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



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

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

3. Click **Yes**.



If the archive is unavailable, for example, offline, you need to restore the connection before you can delete the archive.

Delete a storage

You cannot delete the default storage or storages that devices use as the recording storage for live recordings. This means that you may need to move devices (see [Move hardware on page 439](#)) and any not yet archived recordings to another storage before you delete the storage.


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



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

2. Follow the steps in [Move non-archived recordings from one storage to another](#).
3. Continue until you have moved all devices.
4. Select the storage that you want to delete.

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

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

Move non-archived recordings from one storage to another

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


1. Select the device type. In the **Overview** pane, select the device.
2. Click the **Record** tab. In the upper part of the **Storage** area, click **Select**.
3. In the **Select Storage** dialog box, select the database.
4. Click **OK**.
5. In the **Recordings Action** dialog box, select if you want to remove already existing - but **non-archived** - recordings to the new storage or if you want to delete them.
6. Click **OK**.

Storage and Recording Settings properties

Available functionality depends on the system you are using. See

<https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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


Name	Description
Name	Rename the storage if needed. Names must be unique.
Path	Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer. If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\server\volume\directory\.
Retention time	Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings). The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process.
Maximum size	Select the maximum number of gigabytes of recording data to save in the recording database. Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted.  When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.
Signing	Enables a digital signature to the recordings. This means, for example, that the system confirms that exported video has not been modified or tampered with when played back. The system uses the SHA-2 algorithm for digital signing.

Name	Description
Encryption	<p>Select the encryption level of the recordings:</p> <ul style="list-style-type: none"> • None • Light (less CPU usage) • Strong (more CPU usage) <p>The system uses the AES-256 algorithm for encryption.</p> <p>If you select Light, a part of the recording is encrypted. If you select Strong, the whole recording is encrypted.</p> <p>If you choose to enable encryption, you must also specify a password below.</p>
Password	<p>Enter a password for the users allowed to view encrypted data.</p> <p>Milestone recommends that you use strong passwords. Strong passwords do not contain words that can be found in a dictionary or are part of the user's name. They include eight or more alpha-numeric characters, upper and lower cases, and special characters.</p>

Archive Settings properties

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

Name	Description
Name	Rename the storage if needed. Names must be unique.
Path	<p>Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer.</p> <p>If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\server\volume\directory\.</p>
Retention time	Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings).

Name	Description
	The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process.
Maximum size	<p>Select the maximum number of gigabytes of recording data to save in the recording database. Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted.</p> <div>  <p>When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.</p> </div>
Schedule	Specify an archiving schedule that outlines the intervals with which the archiving process should start. You can archive very frequently (in principle every hour all year round), or very infrequently (for example, every first Monday of every 36 months).
Reduce frame rate	<p>To reduce FPS when archiving, select the Reduce frame rate check box and set a frame per second (FPS).</p> <p>Reduction of frame rates by a selected number of FPS makes your recordings take up less space in the archive, but it also reduces the quality of your archive. MPEG-4/H.264/H.265 reduces automatically to key-frames as a minimum.</p> <p>0.1 = 1 frame per 10 seconds.</p>

Failover tab (recording server)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

If your organization uses failover recording servers, use the **Failover** tab to assign failover servers to recording servers, see [Failover tab properties](#).

The screenshot shows the 'Properties' dialog box for a recording server, specifically the 'Failover' tab. The 'Failover server' section has three radio button options: 'None', 'Primary failover server group:', and 'Hot standby server:'. The 'Primary failover server group:' option is selected, and it has a dropdown menu below it. The 'Hot standby server:' option also has a dropdown menu below it. There is a button labeled 'Advanced failover settings...'. The 'Port' section has a text label 'Failover service communication port (TCP):' and a text box containing '11000'. Below the text box is a note: 'Changing the port requires a restart of the recording server'. At the bottom of the dialog is a tab bar with five tabs: 'Info', 'Storage', 'Failover' (which is active), 'Multicast', and 'Network'.

For details on failover recording servers, installation and settings, failover groups and their settings, see Failover recording servers (explained) on page 165.

Assign failover recording servers

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

- No failover setup
- A primary/secondary failover setup (cold standby)
- A hot standby setup

If you select **b** and **c**, you must select the specific server/groups. With **b**, you can also select a secondary failover group. If the recording server becomes unavailable, a failover recording server from the primary failover group takes over. If you have also selected a secondary failover group, a failover recording server from the secondary

group takes over in case all failover recording servers in the primary failover group are busy. In this way, you only risk not having a failover solution in the rare case when all failover recording servers in the primary, as well as in the secondary, failover group are busy.

1. In the **Site Navigation** pane, select **Servers > Recording Servers**. This opens a list of recording servers.
2. In the **Overview** pane, select the wanted recording server, go to the **Failover** tab.
3. To choose failover setup type, select between:
 - **None**
 - **Primary failover server group/Secondary failover sever group**
 - **Hot standby server**

You cannot select the same failover group as both primary and secondary failover group nor select regular failover servers already part of a failover group as hot standby servers.

4. Next, click **Advanced failover settings**. This opens the **Advanced Failover Settings** window, listing all devices attached to the selected recording server. If you selected **None**, the advanced failover settings are also available. The system keeps any selections for later failover setups.
5. To specify the level of failover support, select **Full Support**, **Live Only** or **Disabled** for each device in the list. Click **OK**.
6. In the **Failover service communication port (TCP)** field, edit the port number if needed.



If you enable failover support and the recording server is configured to keep running if a recording storage is unavailable, the failover recording server will not take over. To make the failover support work, you must select the **Stop the recording server if a recording storage is unavailable** option on the **Storage** tab.

Failover tab properties

Name	Description
None	Select a setup without failover recording servers.
Primary failover server group / Secondary failover server group	Select a regular failover setup with one primary and possibly one secondary failover server group.

Name	Description
Hot standby server	Select a hot standby setup with one dedicated recording server as hot standby server.
Advanced failover settings	<p>Opens the Advanced Failover Settings window:</p> <ul style="list-style-type: none"> • Full Support: Enables full failover support for the device • Live Only: Enables only failover support for live streams on the device • Disabled: Disables failover support for the device
Failover service communication port (TCP)	By default, the port number is 11000. You use this port for communication between recording servers and failover recording servers. If you change the port, the recording server must be running and must be connected to the management server.

Multicast tab (recording server)

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

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



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



If you are using failover servers, remember to also specify the IP address of the network interface card on the failover servers (see Multicast tab (failover server) on page 171).



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

Properties

☒ Multicast

Address range
An address from this range is assigned to new multicast streams that are started on the recording server.

IP address
Start: 232.0.1.0
End: 232.0.1.0

Port
Start: 6000
End: 7000

Source IP address for all multicast streams:
0.0.0.0
(IPv4: '0.0.0.0' = Use default interface)
(IPv6: '::' = Use default interface)

Datagram options
MTU: 1500
TTL: 32

Info Storage Camera **Multicast** Network

Multicasting (explained)

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

- When you use **unicasting**, the source must transmit one data stream for each recipient
- When you use **multicasting**, only a single data stream is required on each network segment

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

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



Multicast streams are not encrypted, even if the recording server uses encryption.

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

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

Enable multicasting for the recording server

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

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

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



Multicast streams are not encrypted, even if the recording server uses encryption.

Assign IP address range

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

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

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

Name	Description
IP address	In the Start field, specify the first IP address in the required range. Then specify the last IP address in the range in the End field.
Port	In the Start field, specify the first port number in the required range. Then specify the last port number in the range in the End field.
Source IP address for all multicast streams	<p>You can only multicast on one network interface card, so this field is relevant if your recording server has more than one network interface card or if it has a network interface card with more than one IP address.</p> <p>To use the recording server's default interface, leave the value 0.0.0.0 (IPv4) or :: (IPv6) in the field. If you want to use another network interface card, or a different IP address on the same network interface card, specify the IP address of the required interface.</p> <ul style="list-style-type: none"> IPv4: 224.0.0.0 to 239.255.255.255. IPv6, the range is described on the IANA website (https://www.iana.org/).

Specify datagram options

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

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

Enable multicasting for individual cameras

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

1. Select the recording server and select the required camera in the **Overview** pane.
2. On the **Client** tab, select the **Live multicast** check box. Repeat for all relevant cameras.



Multicast streams are not encrypted, even if the recording server uses encryption.

Network tab (recording server)

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

Why use a public address?

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

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

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

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

Define public address and port

1. To enable public access, select the **Enable public access** check box.
2. Define the recording server's public address. Enter the address of the firewall or NAT router so clients that access the surveillance system from the Internet can connect to the recording servers.
3. Specify a public port number. It is always a good idea that port numbers used on the firewall or NAT router are different from the ones used locally.



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

Assign local IP ranges

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

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

Site Navigation: Servers and hardware: Failover servers

Failover recording servers (explained)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

You install failover recording servers like standard recording servers (see Install new XProtect components on page 84). Once you have installed failover recording servers, they are visible in the Management Client. Milestone recommends that you install all failover recording servers on separate computers. Make sure that you configure failover recording servers with the correct IP address/host name of the management server. The user rights for the user account under which the Failover Server service runs are provided during the installation process. They are:

- Start/Stop permissions to start or stop the failover recording server
- Read and Write access permissions to read or write the RecorderConfig.xml file

If a certificate is selected for encryption, then the administrator must grant read access permission to the failover user on the selected certificate private key.



If the failover recording server takes over from a recording server that uses encryption, Milestone recommends that you also prepare the failover recording server for using encryption. For more information, see Before you start installation on page 55 and Install new XProtect components on page 84.

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



While your system is in failover mode, you cannot replace or move hardware, update the recording server, or change device configurations such as storage settings or video stream settings.

Cold standby failover recording servers

In a cold standby failover recording server setup, you group multiple failover recording servers in a failover group. The entire failover group is dedicated to take over from any of several preselected recording servers, if one of these becomes unavailable. You can create as many groups as you want (see [Group failover recording servers for cold standby](#)).

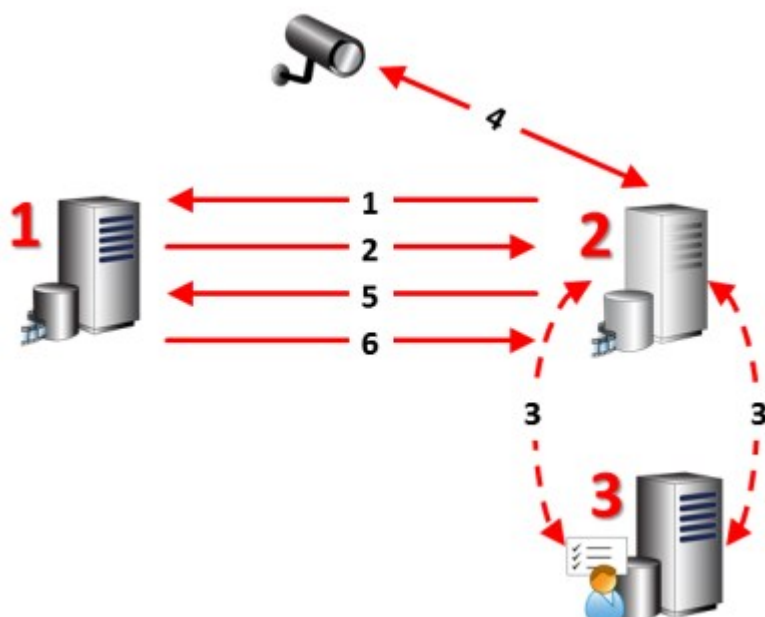
Grouping has a clear benefit: when you later specify which failover recording servers should take over from a recording server, you select a group of failover recording servers. If the selected group contains more than one failover recording server, this offers you the security of having more than one failover recording server ready to take over if a recording server becomes unavailable. You can specify a secondary failover server group that takes over from the primary group if all the recording servers in the primary group are busy. A failover recording server can only be a member of one group at a time.

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

Hot standby failover recording servers

In a hot standby failover recording server setup, you dedicate a failover recording server to take over from **one** recording server only. Because of this, the system can keep this failover recording server in a "standby" mode which means that it is synchronized with the correct/current configuration of the recording server it is dedicated to and can take over much faster than a cold standby failover recording server. As mentioned, you assign hot standby servers to one recording server only and cannot group it. You cannot assign failover servers that are already part of a failover group as hot standby recording servers.

Failover steps (explained)



Description

Involved servers (numbers in red):

1. Recording Server
2. Failover Recording Server
3. Management Server

Failover steps for **Cold standby** setups:

1. To check whether it is running or not, a failover recording server has a non-stop TCP connection to a recording server.
2. This connection is interrupted.
3. The failover recording server requests the current configuration of the recording server from the management server. The management server sends the requested configuration, the failover recording server receives the configuration, starts up, and starts recording on behalf of the recording server.
4. The failover recording server and the relevant camera(s) exchange video data.

Description
<ol style="list-style-type: none"> 5. The failover recording server continually tries to re-establish connection to the recording server. 6. When the connection to the recording server is re-established, the failover recording server shuts down and the recording server fetches video data (if any) recorded during its down-time and the video data is merged back in to the recording server database.
<p>Failover steps for Hot standby setups:</p> <ol style="list-style-type: none"> 1. To check whether it is running or not, a hot standby server has a non-stop TCP connection to its assigned recording server. 2. This connection is interrupted. 3. From the management server, the hot standby server already knows the current configuration of its assigned recording server and starts recording on its behalf. 4. The hot standby server and the relevant camera(s) exchange video data. 5. The hot standby server continually tries to re-establish connection to the recording server. 6. When the connection to the recording server is re-established and the hot standby server goes back to hot standby mode, the recording server fetches video data (if any) recorded during its down-time and the video data is merged back in to the recording server database.

Failover recording server functionality (explained)

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

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

Set up and enable failover recording servers



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

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

1. In the **Site Navigation** pane, select **Servers > Failover Servers**. This opens a list of installed failover recording servers and failover groups.
2. In the **Overview** pane, select the required failover recording server.
3. Right-click and select **Enabled**. The failover recording server is now enabled.
4. To edit failover recording server properties, go to the **Info** tab.
5. When done, go to the **Network** tab. Here you can define the failover recording server's public IP address and more. This is relevant if you use NAT (Network Address Translation) and port forwarding. See the standard recording server's **Network** tab for more information.
6. In the **Site Navigation** pane, select **Servers > Recording Servers**. Select the recording server that you want failover support for and assign failover recording servers (see Failover tab (recording server) on page 157).

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






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

Group failover recording servers for cold standby

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

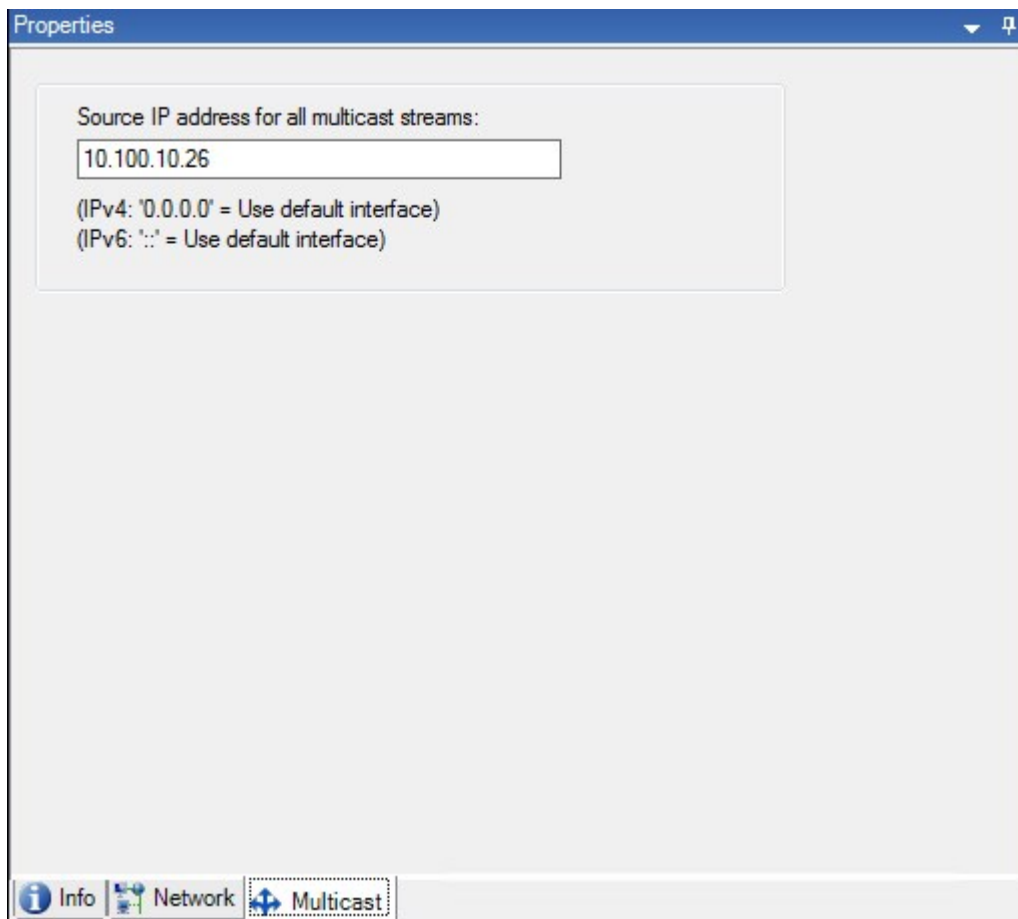
Read failover recording server status icons

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

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

Multicast tab (failover server)

If you are using failover servers, and you have enabled multicasting of live streaming, you must specify the IP address of the network interface card you are using, on both the recording servers and the failover servers.





For more information about multicasting, see Multicast tab (recording server) on page 160 or Multicast tab (recording server) on page 160.

Info tab properties (failover server)

Specify the following failover recording server properties:

Name	Description
Name	The name of the failover recording server as it appears in the Management Client, logs and more.
Description	An optional field that you can use to describe the failover recording server, for example which recording server it takes over from.
Host name	Displays the failover recording server's host name. You cannot change this.
Local web server address	<p>Displays the local address of the failover recording server's web server. You use the local address, for example, for handling PTZ camera control commands, and for handling browsing and live requests from XProtect Smart Client.</p> <p>The address includes the port number that is used for web server communication (typically port 7563).</p> <p>If the failover recording server takes over from a recording server that uses encryption, you also need to prepare the failover recording server to use encryption.</p> <p>If you enable encryption to clients and servers that retrieve data streams from the recording server, a padlock icon appears, and the address includes https instead of http.</p>
Web server address	<p>Displays the public address of the failover recording server's web server on the internet.</p> <p>If your installation uses a firewall or NAT router, enter the address of the firewall or NAT router so that clients that access the surveillance system on the internet can connect to the failover recording server.</p> <p>You specify the public address and port number on the Network tab.</p> <p>If you enable encryption to clients and servers that retrieve data streams from the recording server, a padlock icon appears, and the address includes https instead of http.</p>

Name	Description
UDP port	The port number used for communication between failover recording servers. Default port is 8844.
Database location	Specify the path to the database used by the failover recording server for storing recordings. You cannot change the database path while the failover recording server is taking over from a recording server. The system applies the changes when the failover recording server is no longer taking over from a recording server.
Enable this failover server	Clear to disable the failover recording server (selected by default). You must disable failover recording servers before they can take over from recording servers.

Info tab properties (failover group)

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

Sequence tab properties (failover group)

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

Failover recording server services (explained)

A failover recording server has two services installed:

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

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

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

Change the management server address

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

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

View encryption status on a failover recording server

To verify if your failover recording server uses encryption, do the following:

1. In the **Site Navigation** pane, select **Servers > Failover Servers**. This opens a list of failover recording servers.
2. In the **Overview** pane, select the relevant recording server and go to the **Info** tab.
If encryption is enabled to clients and servers that retrieve data streams from the recording server, a

padlock icon appears in front of the local web server address and the optional web server address.

Properties

Failover server information

Name:
Failover recording server 1

Description:
Failover for Recording server 1

Host name:
hostname.local

Local web server address:
https://hostname.local:7563/

Web server address:
https://www.failoverrecordingserver1:89/

UDP port:
8844

Database location:
C:\MediaDatabase

☒ Enable this failover server

Info Network Multicast

View status messages

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

View version information

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

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

Site Navigation: Servers and hardware: Hardware

Hardware (explained)

Hardware represents either:

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

For more information about how to add hardware to your system, see [Add hardware](#) on page 176.

Add hardware

You have several options for adding hardware to each recording server in your system.




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

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

1. To access **Add Hardware**, right-click the required recording server and select **Add Hardware**.
2. Select one of the wizard options (see below) and follow the instruction on the screen.
3. After installation, you can see the hardware and its devices in the **Overview** pane.


Name	Description
Express (Recommended)	The system scans automatically for new hardware on the recording server's local network. Select the Show hardware running on other recording servers check box to see if detected hardware is running on other recording servers.

Name	Description
	<p>You can select this option every time you add new hardware to your network and want to use it in your system.</p> <p>You cannot use this option to add remote systems in Milestone Interconnect setups.</p> <div>  <p>To add both HTTP and HTTPS hardware, run Express detection with the HTTPS (Secure) radio button selected, and then with the HTTP (Unsecure) radio button selected.</p> </div>
Address range scanning	<p>The system scans your network for relevant hardware and Milestone Interconnect remote systems based on your specifications of:</p> <ul style="list-style-type: none"> • hardware user names and passwords. Not needed if your hardware uses the factory default user names and passwords • drivers • IP ranges (IPv4 only) • port number (default = 80) <p>You can select this option when you only want to scan a part of your network, for example, when you expand your system.</p>
Manual	<p>Specify details about each hardware and Milestone Interconnect remote systems separately. This can be a good choice if you want to add only a few pieces of hardware, and you know their IP addresses, relevant user names and passwords or if a camera does not support the automatic discovery function.</p>
Remote connect hardware	<p>The system scans for hardware connected via a remotely connected server.</p> <p>You can use this option if you have installed servers for, for example, the Axis One-click Camera Connection.</p> <p>You cannot use this option to add remote systems in Milestone Interconnect setups.</p>

Disable/enable hardware

Added hardware is by default **enabled**.

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

 Enabled

 Disabled

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

1. Expand the recording server, right-click the hardware you want to disable.
2. Select **Enabled** to clear or select it.


Edit Hardware



Right-click on added hardware and select **Edit Hardware** to modify the network configuration and user authentication settings of hardware in Management Client.



For some hardware, the **Edit Hardware** dialog also lets you apply settings directly to the hardware device.

If the **Edit Management Client settings** radio button is selected, the **Edit Hardware** dialog displays the settings which Management Client uses to connect to the hardware. To ensure the hardware device is added to the system properly, enter the same settings you use to connect to the manufacturer's hardware configuration interface:

Name	Description
Name	Displays the name of the hardware alongside its detected IP address (in parenthesis).
Hardware URL	The web address of the manufacturer's hardware configuration interface, typically containing the IP address of the hardware.
User name	<p>The user name used to connect to the hardware.</p> <div>  <p>The user name that you enter here does not change the user name on the actual hardware device. Select the Edit Management Client and hardware settings radio button to modify settings on supported hardware devices.</p> </div>
Password	The password used to connect to the hardware.






Name	Description
	<div>  <p>The password that you enter here does not change the password on the actual hardware device. Select the Edit Management Client and hardware settings radio button to modify settings on supported hardware devices.</p> </div> <div>  <p>For information about how to change passwords on multiple hardware devices, see Change passwords on hardware devices on page 186.</p> </div> <p>As a system administrator, you need to give other users permission to view the password in Management Client. For more information, see Roles settings on page 331 under Hardware.</p>





If the **Edit Management Client and hardware settings** radio button is selected (for supported hardware), the **Edit Hardware** dialog displays settings which are also applied directly to the hardware device:



Applying the settings with this radio button selected will overwrite the current settings on the hardware device. The hardware will momentarily lose connection to the recording server while the settings are applied.

Name	Description
Name	Displays the name of the hardware alongside its detected IP address (in parenthesis).
Network Configuration	The network settings of the hardware. To adjust the network settings, select Configure on page 179.
Configure	<p>Specify the Internet Protocol (for supported hardware devices) using the IP version dropdown list.</p> <ul style="list-style-type: none"> For IPv4, the values must be in the format: (0-999).(0-999).(0-999).(0-999) For IPv6, the values must be in the format of eight groups of hexadecimal digits each separated by a colon. The subnet mask must be a number between 0-128.

Name	Description
	<p>The Check button tests whether there is currently another hardware device in the system that is using the entered IP address.</p> <div>  <p>Check cannot detect conflicts with hardware devices that are turn off, outside of the XProtect VMS system, or otherwise momentarily not responding.</p> </div>
User name	<p>The user name and level used to connect to the hardware. Select another user from the dropdown list, and add a new password using the Password field described below.</p> <p>Add or delete users using the underlined actions at the bottom of the Authentication section (see Add a user on page 180 or Delete users on page 181).</p> <div>  <p>Selecting a user that does not have the highest user level specified by the manufacturer could result in some features not being available.</p> </div>
Password	<p>The password used to connect to the hardware. View the currently entered text using the Reveal  icon.</p> <p>When changing the password, consult the manufacturer's documentation for the password rules for the specific hardware device, or use the Generate Password  icon to automatically generate a password that matches the requirements.</p> <div>  <p>For information about how to change passwords on multiple hardware devices, see Change passwords on hardware devices on page 186.</p> </div> <p>As a system administrator, you need to give other users permission to view the password in Management Client. For more information, see Roles settings on page 331 under Hardware.</p>
Add a user	<p>Select the underlined Add link to open the Add a User dialog and add a user to the hardware device.</p>

Name	Description
	<div>  Adding a user will automatically set it as the currently active user and overwrite the previously entered credentials. </div> <p>When creating the password, consult the manufacturer's documentation for the password rules for the specific hardware device, or use the Generate Password  icon to automatically generate a password that matches the requirements.</p> <p>The highest user level detected on the hardware device will automatically be preselected. It is not recommended to modify the User level from its default value.</p> <div>  Selecting a User level that is not the highest specified by the manufacturer could result in some features not being available. </div>
Delete users	<p>Select the underlined Delete link to open the Delete Users dialog and remove users from the hardware device.</p> <div>  You cannot delete the currently active user. To set a new user, use the Add a User dialog described above, then remove the old user using this interface. </div>

See also [Manage Hardware](#).

Enable/disable individual devices

Cameras are by default **enabled**.

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

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

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



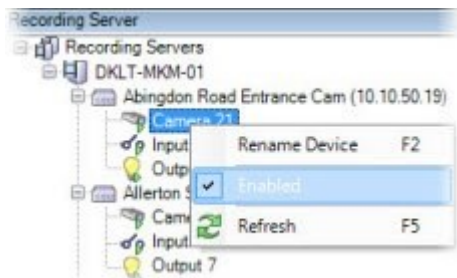
Disabled



Enabled

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

1. Expand the recording server and the device. Right-click the device you want to enable.
2. Select **Enabled** to clear or select it.

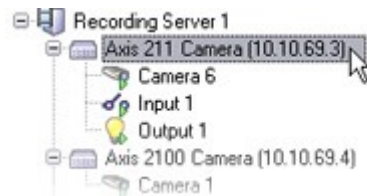


Set up a secure connection to the hardware

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

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

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



2. On the **Settings** tab, enable HTTPS. This is not enabled by default.
3. Enter the port on the recording server to which the HTTPS connection is connected. The port number must correspond with the port set up on the device's homepage.
4. Make changes as needed and save.

Enable PTZ on a video encoder

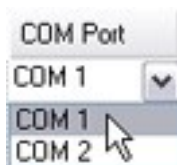
To enable the use of PTZ cameras on a video encoder, do the following on the **PTZ** tab:

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

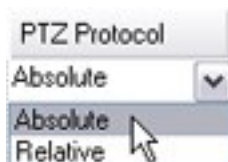


2. In the **PTZ Device ID** column, verify the ID of each camera.

3. In the **COM Port** column, select which video encoder's COM (serial communications) ports to use for control of the PTZ functionality:



4. In the **PTZ Protocol** column, select which positioning scheme you want to use:



- **Absolute:** When operators use PTZ controls for the camera, the camera is adjusted relative to a fixed position, often referred to as the camera's home position
- **Relative:** When operators use PTZ controls for the camera, the camera is adjusted relative to its current position

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

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

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

- Add a preset position (type 1) on page 224
- Add a patrolling profile on page 233


Manage hardware

Info tab (hardware)

For information about the **Info** tab for remote servers, see Info tab (remote server) on page 187.

Info tab (hardware)

Name	Description
Name	Enter a name. The system uses the name whenever the hardware is listed in the system and

Name	Description
	<p>in the clients. The name does not have to be unique.</p> <p>When you rename hardware, the name is changed globally in the Management Client.</p>
Description	<p>Enter a description of the hardware (optional). The description appears in a number of listings within the system. For example, when moving the mouse pointer over the hardware name in the Overview pane:</p> 
Model	Identifies the hardware model.
Serial number	Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
Driver	Identifies the driver that handles the connection to the hardware.
IE	Opens the default home page of the hardware vendor. You can use this page for administration of the hardware.
Address	The host name or IP address of the hardware.
MAC address	Specifies the Media Access Control (MAC) address of the system hardware. A MAC address is a 12-character hexadecimal number uniquely identifying each piece of hardware on a network.
Password last changed	The Password last changed field shows the time stamp of the latest password change based on the local time settings of the computer that the password was changed from.

Settings tab (hardware)

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



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

For information about the **Settings** tab for remote servers, see Settings tab (remote server) on page 188.

PTZ tab (video encoders)

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

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



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



PTZ tab, with PTZ enabled for two channels on a video encoder.

Device password management (explained)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

You can change passwords on multiple hardware devices in one operation.

Initially, the supported devices are models from Axis, Bosch, Hanwa, Panasonic, Hikvision, and ONVIF compatible hardware devices, but the user interface shows you directly if a model is supported or not. You can also go to our website to find out if a model is supported: <https://www.milestonesys.com/community/business-partner-tools/supported-devices/>



For devices that do not support device password management, you must change the password of a hardware device from its web page and then manually enter the new password in Management Client. For more information, see Edit Hardware on page 178.

You can choose to let the system generate individual passwords for each hardware device or to use a single user-defined password for all hardware devices. In passwords, only ASCII printable characters are supported.

The system generates passwords based on the requirements from the manufacturer of the hardware devices.

When you apply the new passwords, the hardware devices lose connection to the recording server momentarily.

After you have applied new passwords, the result for each hardware device appears on the screen. For unsuccessful changes, the reason for failure appears if the hardware device supports such information. From within the wizard, you can create a report of successful and failed password changes, but the results are also logged under **Server logs**.



For hardware devices with ONVIF drivers and multiple user accounts, only an administrator of XProtect with administrative rights of the hardware device can change passwords from the VMS.

For information about how to change passwords in one operation, see Change passwords on hardware devices on page 186.

Change passwords on hardware devices



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

You can change passwords on multiple hardware devices in one operation. For more information about the feature and supported models, see Device password management (explained) on page 185.

Requirements:

- The hardware device model supports device password management by Milestone.

Steps:

1. In the **Site Navigation** pane, select the **Recording Servers** node.
2. Right-click the relevant recording server or hardware in the overview pane.
3. Select **Change Hardware Password**. A wizard appears.
4. Follow the instructions on the screen to complete the changes.



The **Password last changed** field shows the time stamp of the latest password change based on the local time settings of the computer that the password was changed from.

5. The last page shows the result. If the system could not update a password, click **Failed** next to the hardware device to see the reason.
6. You can also click the **Print report** button to see the full list of successful and unsuccessful updates.
7. In case you want to change the password on the hardware devices that failed, click **Retry**, and the wizard starts over with the failed hardware devices.



If you click **Retry**, you can no longer access the report from the first time you completed the wizard.



Due to security restrictions, some hardware devices might become unavailable for a certain period if you fail to change password several times in a row. Security restrictions vary for different manufacturers.

Site Navigation: Servers and hardware: Manage remote servers

Info tab (remote server)

Name	Description
Name	<p>The system uses the name whenever the remote server is listed in the system and clients. The name does not have to be unique.</p> <p>When you rename a server, the name is changed globally in the Management Client.</p>

Name	Description
Description	Enter a description of the remote server (optional). The description appears in a number of listings within the system. For example, when pausing the mouse pointer over the hardware name in the Overview pane.
Model	Displays the XProtect product installed at the remote site.
Version	Displays the version of the remote system.
Software license code	The software license code of the remote system.
Driver	Identifies the driver that handles the connection to the remote server.
Address	The host name or IP address of the hardware.
IE	Opens the default home page of the hardware vendor. You can use this page for administration of the hardware or system.
Remote system ID	The unique system ID of the remote site used by XProtect to, for example, manage licenses.
Windows user name	Enter the Windows user name for access through the remote desktop.
Windows password	Enter the Windows password for access through the remote desktop.
Connect	Opens a remote connection to the remote site (if Windows credentials are approved).

Settings tab (remote server)

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

Events tab (remote server)

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

If the list appears to be incomplete:

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

Remote Retrieval tab

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

Specify the following properties:

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

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



None of the above applies to direct playback of remote recordings.
All cameras set to be played back directly is available for direct playback and use bandwidth as needed.

Site Navigation: Devices: Working with devices

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

You can manage devices via the device groups if they have the same properties, see Site Navigation: Devices: Working with device groups on page 198.

You can also manage the devices individually:

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

Devices (explained)

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

- A physical camera has devices that represent the camera part (lenses) as well as microphones, speakers, metadata, input and output either attached or built-in
- A video encoder has multiple analog cameras connected that appear in one list of devices that represent the camera part (lenses) as well as microphones, speakers, metadata, input and output either attached or built-in
- An I/O module has devices that represent the input and output channels for, for example, lights
- A dedicated audio module has devices that represent microphones and speaker inputs and outputs
- In a Milestone Interconnect setup, the remote system appears as hardware with all devices from the remote system listed in one list

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



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

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

Camera devices (explained)

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

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



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

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

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See [Enable/disable devices via device groups](#) on page 196.

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

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

1. Configure camera settings (see Settings tab (devices) on page 203).
2. Configure streams (see Streams tab (devices) on page 205).
3. Configure motion (see Motion tab (devices) on page 215).
4. Configure recording (see Record tab (devices) on page 208).
5. Configure the remaining settings as needed.

Microphone devices (explained)

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

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

You can use microphones completely independently of cameras.

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



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

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

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

Enabling/disabling and renaming of individual devices take place on the recording server hardware. For more information, see [Enable/disable devices via device groups](#) on page 196.

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

You can configure microphone devices on these tabs:

- Info tab (see [Info tab \(devices\)](#) on page 201)
- Settings tab (see [Settings tab \(devices\)](#) on page 203)
- Record tab (see [Record tab \(devices\)](#) on page 208)
- Events tab (see [Events tab \(devices\)](#) on page 237)

Speaker devices (explained)

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

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

You can use speakers completely independently of cameras.



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

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

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

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

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See [Enable/disable devices via device groups](#) on page 196.

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

You can configure speaker devices on these tabs:

- Info tab (devices) on page 201
- Settings tab (devices) on page 203
- Record tab (devices) on page 208

Metadata devices (explained)

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

Metadata can be generated by:

- The device itself delivering the data, for example a camera that is delivering video
- A third-party system or integration via a generic metadata driver

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



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

Roles determine the users' right to view metadata.

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

Enabling/disabling and renaming of individual devices take place on the recording server hardware. For more information, see [Enable/disable devices via device groups](#) on page 196.

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

You can configure metadata devices on these tabs:

- Info tab (see Info tab (devices) on page 201)
- Settings tab (see Settings tab (devices) on page 203)
- Record tab (see Record tab (devices) on page 208)

Input devices (explained)

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

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

You can use input devices completely independently of cameras.



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

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



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups on page 196.

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

You can configure input devices on these tabs:

- Info tab (see Info tab (devices) on page 201)
- Settings tab (see Settings tab (devices) on page 203)
- Events tab (see Events tab (devices) on page 237)

Activate input manually for test

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

1. In the **Overview** pane, select the relevant input device.
2. Activate the input on the physical device.
3. In the **Preview** pane, see if the indicator lights up green. Then the input device works.



Output devices (explained)

On many devices, you can attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through the system.

You can use output when creating rules. You can create rules that automatically activate or deactivate outputs, and rules that trigger actions when the state of an output is changed.

Output can be triggered manually from the Management Client and XProtect Smart Client.



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

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



For information about supported hardware, see the supported hardware page on the Milestone website (<https://www.milestonesys.com/supported-devices/>).

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See *Enable/disable devices via device groups* on page 196.

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

You can configure output devices on these tabs:

- Info tab (devices) on page 201
- Settings tab (devices) on page 203

Activate output manually for test

With the rules feature, you define rules that automatically activate or deactivate output or you can activate them manually from a client.


You can activate an output manually from the Management Client to test the functionality:

1. In the **Overview pane**, select the relevant output device.
2. Typically, the following elements are shown for each output in the **Preview** pane:



3. Select/clear the check box ☒  to activate/deactivate the selected output. When an output is activated, the indicator lights up green:



4. Alternatively, click the rectangular button  to activate the output for the duration defined in the **Output Trigger Time** setting on the **Settings** tab (this feature/setting may not be available for all outputs). After the defined duration, the output is automatically deactivated.

Enable/disable devices via device groups

You can enable/disable devices only via the configured hardware. Unless manually enabled/disabled in the add hardware wizard, camera devices are by default enabled and all other devices are by default disabled.























To locate a device via the device groups to enable or disable:





















1. In the **Site Navigation** pane, select the device.
2. In the **Overview** pane expand the relevant group and find the device.
3. Right-click the device, and select **Go To Hardware**.
4. Click the plus node to see all devices on the hardware.
5. Right-click the device you want to enable/disable, and select **Enabled**.

Status icons of devices

When you select a device, information about the current status appears in the **Preview** pane.

The following icons indicate the status of the devices:

Camera	Microphone	Speaker	Metadata	Input	Output	Description
						Device enabled and retrieving data: The device is enabled and you retrieve a live stream.
						Device recording: The device is recording data on the system.
						Device temporarily stopped or has no feed: When stopped, no information is transferred to the system. If it is a camera, you cannot view live video. A stopped device can still communicate with the recording server for retrieving events, setting settings etc., as opposed to when a device is disabled.
						Devices disabled: Cannot be started automatically through a rule and cannot communicate with the recording server. If a camera is disabled, you cannot view live or recorded video.

Camera	Microphone	Speaker	Metadata	Input	Output	Description
						Device database being repaired.
						Device requires attention: The device does not function correctly. Pause the mouse pointer over the device icon to get a description of the problem in the tooltip.
						Status unknown: Status of the device is unknown, for example, if the recording server is offline.
						Some icons can be combined, as in this example where Device enabled and retrieving data is combined with Device recording .

Site Navigation: Devices: Working with device groups

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

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

- Device groups help you maintain an intuitive overview of devices on your system
- Devices can exist in several groups
- You can create subgroups and subgroups in subgroups
- You can specify common properties for all devices within a device group in one go
- Device properties set via the group are not stored for the group but on the individual devices
- When dealing with roles, you can specify common security settings for all devices within a device group in one go
- When dealing with rules, you can apply a rule for all devices within a device group in one go

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



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

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

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

Add a device group on page 199

Specify which devices to include in a device group on page 200

Specify common properties for all devices in a device group on page 200

Add a device group

1. In the **Overview** pane, right-click the device type under which you want to create a device group.
2. Select **Add Device Group**.
3. In the **Add Device Group** dialog box, specify a name and description of the new device group:

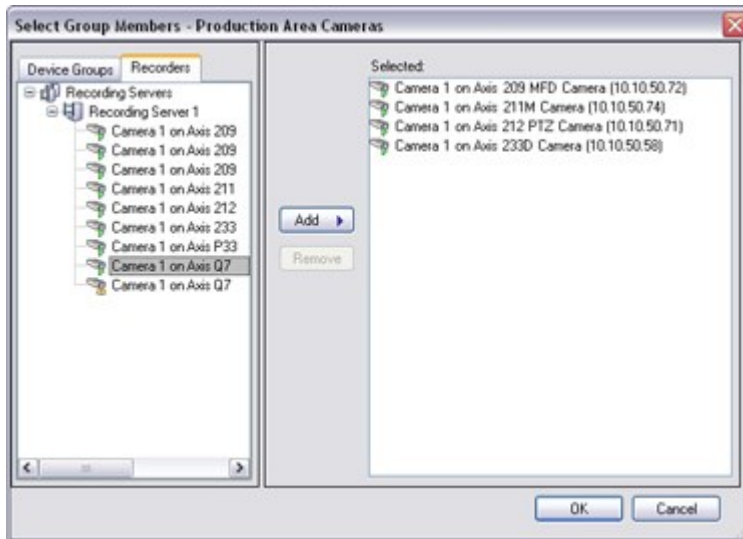


The description appears when you pause the mouse pointer over the device group in the device group list.

4. Click **OK**. A folder representing the new device group appears in the list.
5. Continue with Specify which devices to include in a device group (see Specify which devices to include in a device group on page 200).

Specify which devices to include in a device group

1. In the **Overview** pane, right-click the relevant device group folder.
2. Select **Edit Device Group Members**.
3. In the **Select Group Members** window, select one of the tabs to locate the device.
A device can be a member of more than one device group.
4. Select the devices you want to include, and click **Add** or double-click the device:



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



Specify common properties for all devices in a device group

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

1. In the **Overview** pane, click the device group.
In the **Properties** pane, all properties **which are available on all of the device group's devices** are listed and grouped on tabs.
2. Specify the relevant common properties.
On the **Settings** tab, you can switch between settings for **all** devices and settings for individual devices.
3. In the toolbar, click **Save**. The settings are saved on the individual devices, not in the device group.

Site Navigation: Devices tabs

Info tab (devices)

Info tab (explained)

On the **Info** tab, you can view and edit basic information about a device in a number of fields. All devices have an **Info** tab.

Properties

Device information

Name:

Axis 211W Camera (10.100.50.65) - Camera 1

Description:

Hardware name:

Axis 211W Camera (10.100.50.65)



➔




Port number:

1

Info tab properties

Name	Description
Name	The name is used whenever the device is listed in the system and clients.

Name	Description
	When you rename a device, the name is changed globally in the Management Client.
Description	<p>Enter a description of the device (optional).</p> <p>The description appears in a number of listings within the system. For example, when you pause the mouse pointer over the name in the Overview pane.</p>
Hardware name	Displays the name of the hardware, with which the device is connected. The field is non-editable from here, but you can change it by clicking Go To next to it. This takes you to hardware information where you can change the name.
Port number	<p>Displays the port on which the device is attached on the hardware.</p> <p>For single-device hardware, the port number is typically 1. For multi-device hardware, such as video servers with several channels, the port number typically indicates the channel on which the device is attached, for example 3.</p>
Short name	<p>To apply a short name for the camera, enter it here. The maximum length of characters is 128.</p> <p>If you are using smart map, automatically the short name is displayed with the camera on the smart map. Otherwise the full name is displayed.</p>
Geo coordinates	<p>Enter the geographic location of the camera in the format latitude, longitude. The value you enter determines the position of the camera icon on the smart map in XProtect Smart Client.</p> <div>  The field is mainly for smart map and third party integrations. </div>
Direction	<p>Enter the viewing direction of the camera measured against a due north point on a vertical axis. The value you enter determines the direction of the camera icon on the smart map in XProtect Smart Client.</p> <p>The default value is 0.0.</p> <div>  The field is mainly for smart map and third party integrations. </div>
Field of view	<p>Enter the field of view in degrees. The value you enter determines the field of view of the camera icon on the smart map in XProtect Smart Client.</p> <p>The default value is 0.0.</p>

Name	Description
	 The field is mainly for smart map and third party integrations.
Depth	<p>Enter the depth of the camera in meters or feet. The value you enter determines the depth of the camera icon on the smart map in XProtect Smart Client.</p> <p>The default value is 0.0.</p>  The field is mainly for smart map and third party integrations.
Preview position in browser	<p>To verify that you have entered the correct geographic coordinates, click the button. Google Maps will open in your standard Internet browser on the position you specify.</p>  The field is mainly for smart map and third party integrations.

Settings tab (devices)

Settings tab (explained)

On the **Settings** tab, you can view and edit settings for a device in a number of fields.

All devices have a **Settings** tab.

The values appear in a table as changeable or read-only. When you change a setting to a non-default value, the value appears in bold.

The content of the table depends on the device driver.

Allowed ranges appear in the information box below the settings table:

Properties	
Axis 211W Camera	
General	
Brightness	50
Include Date	No
Include Time	No
Rotation	0
Saturation	50
Sharpness	0
JPEG - streamed	
Compression	30
Frames per second	8
Resolution	640x480
JPEG 2 - streamed	
Compression	30
Frames per second	8
Resolution	640x480
JPEG 3 - streamed	
Compression	30
Frames per second	8
Resolution	640x480
MPEG-4 - streamed	
Bit rate control priority	Framerate
Frames per second	30
Maximum bit rate	3000
Maximum compression	100
Minimum compression	0
Resolution	640x480
Target bit rate	9900
Saturation A numeric value between 0 and 100.	

Camera settings (explained)

You can view or edit settings, such as:

- Default frame rate
- Resolution
- Compression
- The maximum number of frames between keyframes
- On-screen date/time/text display for a selected camera, or for all cameras within a device group

The drivers for the cameras determine the content of the **Settings** tab. The drivers vary depending on the type of camera.

For cameras that support more than one type of stream, for example MJPEG and MPEG-4/H.264/H.265, you can use multi-streaming, see Multi-streaming (explained) on page 206.

When you change a setting, you can quickly verify the effect of your change if you have the **Preview** pane enabled. You cannot use the **Preview** pane to judge the effect of frame rate changes because the **Preview** pane's thumbnail images use another frame rate defined in the **Options** dialog box.

If you change the settings for **Max. frames between keyframes** and **Max. frames between keyframes mode**, it may lower the performance of some functionalities in XProtect Smart Client. For example, XProtect Smart Client requires a keyframe to start up showing video, so a longer period between keyframes, prolongs the XProtect Smart Client start up.

Streams tab (devices)

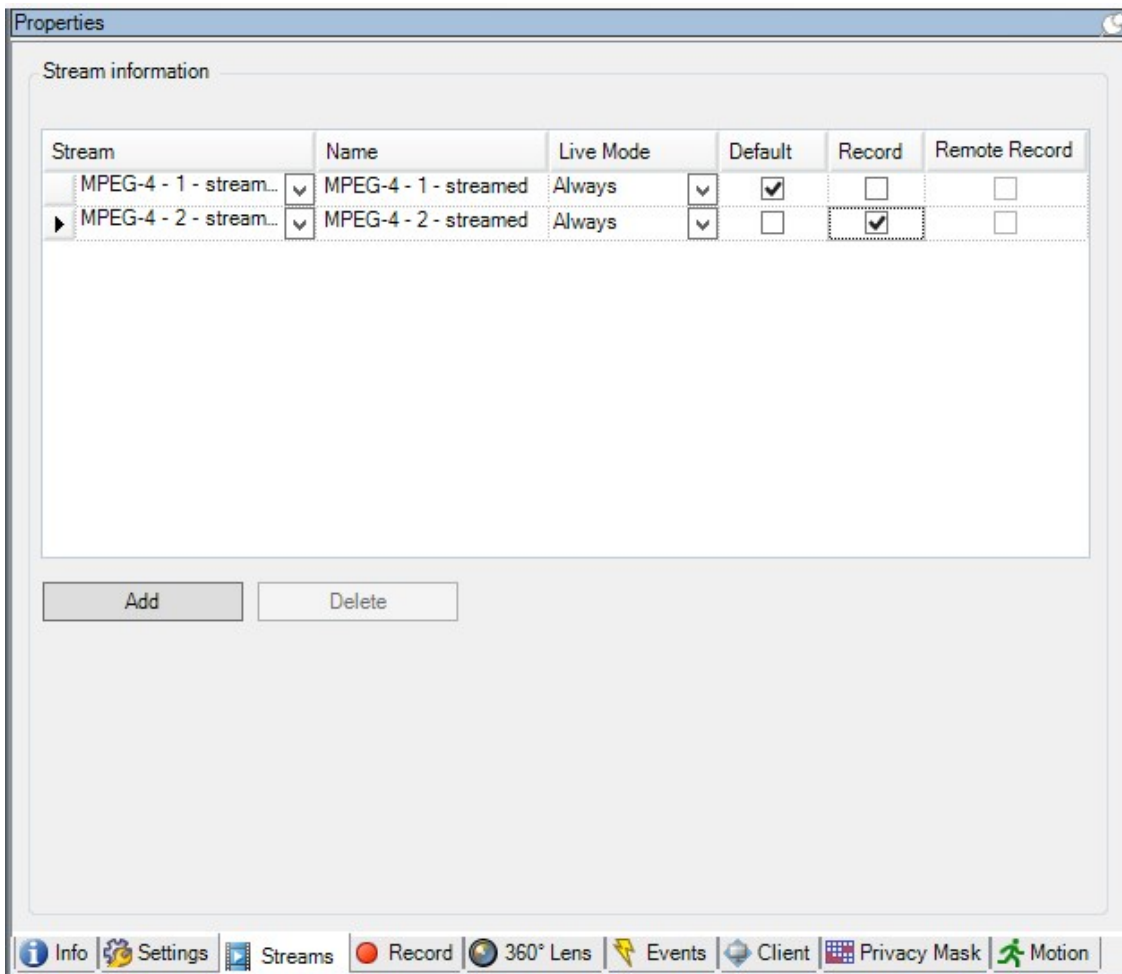
Streams tab (explained)

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

- Cameras

The **Streams** tab lists by default a single stream. It is the selected camera's default stream, used for live and recorded video.

For live streaming, you can set up and use as many live streams as the camera supports, but you can only select one stream for recording at a time. To change which stream to use for recording, select the **Record** box for the stream to be recorded.



Multi-streaming (explained)

Viewing live video and playing back recorded video do not necessarily require the same video quality and frame rate. You can have **either** one stream for live viewing and another stream for playback purposes **or** multiple separate live streams with different resolution, encoding, and frame rate settings.

To manage streaming and limit unnecessary data transmission, streaming does not start when the following conditions are met:

- On the **Streams** tab, **Live Mode** is set to When needed
- On the **Record** tab, **Recording** is disabled
- On the **Motion** tab, **Motion detection** is disabled

If these conditions are met, video streams will only run when viewed by a client.

Example 1, live and recorded video:

- For viewing **live** video, your organization may prefer H.264 at a high frame rate
- For playing back **recorded** video, your organization may prefer MJPEG at a lower frame rate to preserve disk space

Example 2, local and remote live video:

- For viewing **live video from a local connected operating point**, your organization may prefer H.264 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 to preserve network bandwidth

Example 3, adaptive streaming:

- For viewing **live video and decreasing the load on the CPU and GPU of the XProtect Smart Client computer**, your organization may prefer multiple high frame rate H.264/H.265 but with different resolutions to match the resolution requested by XProtect Smart Client when using adaptive streaming. For more information, see Smart Client profile properties on page 264.



If you enable **Live multicast** on the camera's **Client** tab, it only works on the default video stream.

Even when cameras support multi-streaming, individual multi-streaming capabilities may vary between different cameras. See the camera's documentation for more information.

To see if a camera offers different types of streams, see the **Settings** tab.

Add a stream

1. On the **Streams** tab, click **Add**. This adds a second stream to the list.
2. In the **Name** column, edit the name of the stream. The name appears in XProtect Smart Client.
3. In the **Live Mode** column, select when live streaming is needed:
 - **Always**: the stream runs even if no XProtect Smart Client users request the stream
 - **Never**: the stream is off. Only use this for recording streams, for example, if you want recordings in high quality and need the bandwidth
 - **When needed**: the stream starts when a user of XProtect Smart Client requests for it
4. In the **Default** column, select which stream is default.
5. In the **Record** column, select the check box if you want to record this stream or leave it cleared if you only want to use it for live video.
6. Click **Save**.



If you set a stream to **Default** or **Record**, the stream is always running independent of the



Live Mode setting. Selecting **When needed** and **Always** have the same effect in the system and if you select **Never**, the stream is running, but cannot be viewed live.



If you do not want the streams to run at all unless someone is viewing live video, you can modify the **Default Start Feed Rule** to start on request with the predefined **Live Client Feed Requested** event.

Record tab (devices)

Record tab (explained)

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

- Cameras
- Microphones
- Speakers
- Metadata

Recordings from a device are only saved in the database when you have enabled recording and the recording-related rule criteria are met.

Parameters that cannot be configured for a device are grayed out.

Properties

Recording settings

☒ **Recording**

☒ Record on related devices

☒ Stop manual recording after: minutes

☒ **Pre-buffer**

Location:

Time: seconds

Recording frame rate


JPEG: FPS

MPEG-4/H.264/H.265: ☐ Record keyframes only

Storage










Status:

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

Total used space: 

Remote recordings

☐ Automatically retrieve remote recordings when connection is restored

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

Enable/disable recording

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

1. In the **Site Navigation** pane, select **Recording Servers**.
2. Select the relevant device in the **Overview** pane.
3. On the **Record** tab, select or clear the **Recording** check box.



You must enable recording for the device before you can record data from the camera. A rule that specifies the circumstances for a device to record does not work if you have disabled recording for the device.

Enable recording on related devices

For camera devices, you can enable recording for related devices, for example, microphones that are connected to the same recording server. It means that the related devices record when the camera records.

Recording on related devices are enabled by default for new camera devices, but you can disable and enable as you want. For existing camera devices in the system, the check box is cleared by default.

1. In the **Site Navigation** pane, select **Recording Servers**.
2. Select the relevant camera device in the **Overview** pane.
3. On the **Record** tab, select or clear the **Record on related devices** box.
4. On the **Client** tab, specify the devices that relate to this camera.

If you want to enable recording on related devices that are connected to another recording server, you must create a rule.

Pre-buffering (explained)

Pre-buffering is the ability to record audio and video before the actual triggering event occurs. This is useful when you want to record the audio or video that leads up to an event that triggers recording, for example, opening a door.

Pre-buffering is possible because the system continuously receives audio and video streams from the connected devices and temporarily stores them for the defined pre-buffer period.

- If a recording rule is triggered, the temporary recordings are made permanent for the rule's configured pre-recording time
- If no recording rule is triggered, the temporary recordings in the pre-buffer are automatically deleted after the defined pre-buffer time



To use the pre-buffer function, the devices must be enabled and sending a stream to the system.

Devices that support pre-buffering

Cameras, microphones and speakers support pre-buffering. For speakers, the streams are only sent when the XProtect Smart Client user uses the **Talk to speaker** function. This means that depending on how your speaker streams are triggered to be recorded there is little or no pre-buffering available.

In most cases, you set up speakers to record when the XProtect Smart Client user uses the **Talk to speaker** function. In such cases, no speaker pre-buffer is available.

Storage of the temporary pre-buffer recordings

You can choose the storage location of the temporary pre-buffer recordings:

- In the memory; the pre-buffer period is limited to 15 seconds.
- On the disk (in the media database); you can choose all values.

Storage to the memory instead of to disk improves system performance, but is only possible for shorter pre-buffer periods.

When recordings are stored in the memory, and you make some of the temporary recordings permanent, the remaining temporary recordings are deleted and cannot be restored. If you need to be able to keep the remaining recordings, store the recordings on the disk.

Manage pre-buffering

Enable and disable pre-buffering

Pre-buffering is enabled by default with a pre-buffer size of three seconds and storage to the memory.

1. To enable/disable pre-buffering, select/clear the **Pre-buffer** check box.

Specify storage location and pre-buffer period

Temporary pre-buffer recordings are stored either in the memory or on the disk:

1. For **Location**, select **Memory** or **Disk** and specify the number of seconds.

The number of seconds you specify must be sufficiently large to accommodate your requirements in the various recording rules you define.

If you require a pre-buffer period of more than 15 seconds, select **Disk**.

2. If you change the location to **Memory**, the system reduced the period to 15 seconds automatically.

Use pre-buffer in rules

When you create rules that trigger recording, you can select that recordings should start some time before the actual event (pre-buffer).

Example: The below rule specifies that recording should start on the camera 5 seconds before motion is detected on the camera.

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



To use the pre-buffer recording function in the rule, you must enable pre-buffering on the device being recorded and you must set the pre-buffer length to at least the same length as specified in the rule.

Manage manual recording

Stop manual recording after is enabled by default with a recording time of five minutes. This is to ensure that the system automatically stops all recordings started by the XProtect Smart Client users.

☒ Stop manual recording after: minutes

1. To enable and disable manual recording to be stopped automatically by the system, select/clear the **Stop manual recording after** check box.
2. When you enable it, specify a recording time. The number of minutes you specify must be sufficiently large to accommodate the requirements of the various manual recordings without overloading the system.

Add to roles:

You must grant the right to start and stop manual recording to the client users on each camera in **Roles** on the **Device** tab.

Use in rules:

The events you can use when you create rules related to manual recording are:

- Manual Recording Started
- Manual Recording Stopped

Specify recording frame rate

You can specify the recording frame rate for JPEG.

- Select or enter the recording frame rate (in FPS, frames per second) in the **Recording frame rate: (JPEG)** box.

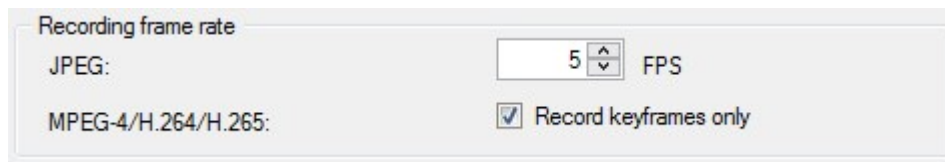
Recording frame rate:
JPEG: FPS

Enable keyframe recording

You can enable keyframe recording for MPEG-4/H.264/H.265 streams. It means that the system switches between recording keyframes only and recording all frames depending on your rule settings.

You can, for example, let the system record keyframes when there is no motion in the view and switch to all frames only in case of motion detection to save storage.

1. Select the **Record keyframes only** box.



2. Set up a rule that activates the function, see Actions and stop actions (explained) on page 276.

Storage (explained)

Under **Storage**, you can monitor and manage the databases for a device or a group of devices added to the same recording server.


Above the table, you can see the selected database and its status. In this example, the selected database is the default **Local Default** and the status is **Recordings also located on other recording servers**. The other server is the recording server in building A.

Storage

Local Default Select...

Status: Recordings also located on other recording servers

Status	Database	Location	Used space
OK	Local Default	C:\MediaDB	288 MB
OK	Local Default	Recording server - Building A	42.2 MB

Total used space: 330 MB Delete All Recordings 

Possible statuses for selected database

Name	Description
Recordings also located on other recording servers	The database is active and running and has recordings located in storages on other recording servers as well.
Archives also located in old storage	The database is active and running and has archives located in other storages as well.
Active	The database is active and running.
Data for some of the devices chosen is currently moving to another location	The database is active and running and the system is moving data for one or more selected devices in a group from one location to another.
Data for the device is currently moving to another location	The database is active and running and the system is moving data for the selected device from one location to another.
Information unavailable in failover mode	The system cannot collect status information about the database when the database is in failover mode.

Further down in the window, you can see the status of each database (**OK**, **Offline** or **Old Storage**), the location of each database and how much space each database uses.

If all servers are online, you can see the total space used for the entire storage in the **Total used space** field.

With the **Delete All Recordings** button, you can delete all recordings for the device or device group if you have added all devices in the group to the same server. Protected data is not deleted.

For information about configuration of storage, see Storage tab (recording server) on page 140.

Moving devices from one storage to another

You can select a new storage location for your devices by selecting **Select....** under **Storage**.

This way you can choose another recording storage for your devices to record in, and they will archive according to the configuration for that storage.

When you select a new location to store recordings, the existing recordings will not be moved. They will remain in the current location, with the conditions defined by the configuration of the storage they belong to.

Remote recording (explained)



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

To ensure that all recordings are saved in case of network issues, select **Automatically retrieve remote recordings when connection is restored**. This enables automatic retrieval of recordings once connection is re-established.

The type of hardware selected determines where recordings are retrieved from:

- For a camera with local recording storage, recordings are retrieved from the camera's local recording storage
- For a Milestone Interconnect remote system, recordings are retrieved from the remote systems' recording servers

You can use the following functionality independently of the automatic retrieval:

- Manual recording
- The **Retrieve and store remote recordings from <devices>** rule
- The **Retrieve and store remote recordings between <start and end time> from <devices>** rule

Motion tab (devices)

Motion tab (explained)

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

- Cameras

On the **Motion** tab, you can enable and configure motion detection for the selected camera. Motion detection configuration is a key element in your system: Your motion detection configuration determines when the system generates motion events and typically also when video is recorded.

Time spent on finding the best possible motion detection configuration for each camera helps you later avoid, for example, unnecessary recordings. Depending on the physical location of the camera, it may be a good idea to test motion detection settings under different physical conditions such as day/night and windy/calm weather.

Before you configure motion detection for a camera, Milestone recommends that you have configured the camera's image quality settings, for example resolution, video codec and stream settings on the **Settings** tab. If you later change image quality settings, you should always test any motion detection configuration afterwards.

If you have defined areas with permanent privacy masks on the **Privacy masking** (see Privacy masking tab (devices) on page 242) tab, you can choose to display the privacy masks on the **Motion** tab by selecting the **Show privacy masks** check box.




There is no motion detection within areas covered by permanent privacy masks.

☒ Motion detection

Hardware acceleration:

☒ Automatic
 ☐ Off

Motion preview



☒ Show privacy masks

☐ Manual sensitivity

< 33

Threshold:

< 2000

☒ Keyframes only (MPEG-4/H.264/H.265)

Process image every (msec):

500

Detection resolution:

12%

☒ Generate motion data for smart search

☐ Use exclude regions

16x16

☒ Show grid
 ☒ Show regions

Clear

Pen size:

Info
 Settings
 Streams
 Record
 Motion
 Fisheye Lens
 Events

You can configure all the settings for a group of cameras, but you would typically set the exclude regions per camera.

Enable and disable motion detection

You specify the default setting of motion detection for cameras on the **Tools > Options > General** tab.

To enable or disable motion detection afterwards for a camera:

- Select or clear the **Motion** tab's **Motion detection** check box



When you disable motion detection for a camera, motion detection-related rules for the camera do not work.

Specify motion detection settings

You can specify settings related to the amount of changes required in a camera's view in order for the change to be regarded as motion. You can for example specify intervals between motion detection analysis and areas of a view in which motion should be ignored. You can also adjust the accuracy of the motion detection and thereby the load on system resources.

Hardware acceleration (explained)

Select **Automatic** to enable hardware accelerated video motion detection. This is the default setting when you add a camera. The recording server is now using GPU resources if they are available. This will reduce the CPU load during video motion analysis and improve the general performance of the recording server.

Hardware accelerated video motion detection uses GPU resources on:

- Intel CPUs that support Intel Quick Sync
- NVIDIA® display adapters connected to your recording server

The load balancing between the different resources is done automatically. In the **System Monitor** node you can verify if the current motion analysis load on the NVIDIA GPU resources is within the specified limits from the **System Monitor Thresholds** node. The NVIDIA GPU load indicators are:

- NVIDIA decoding
- NVIDIA memory
- NVIDIA rendering



If the load is too high, you can add GPU resources to your recording server by installing multiple NVIDIA display adapters. Milestone does not recommend the use of Scalable Link Interface (SLI) configuration of your NVIDIA display adapters.

NVIDIA products have different compute capabilities. To verify that your NVIDIA product supports hardware acceleration for the codecs used in your Milestone XProtect system, look up the supported codecs for the compute capability version in the table below.

To find out the compute capability version for your NVIDIA product, visit the NVIDIA website (<https://developer.nvidia.com/cuda-gpus/>).

Compute capability	Architecture	H.264	H.265
3.x	Kepler	✓	-
5.x	Maxwell	✓	-
6.x	Pascal	✓	✓
7.x	Volta	✓	✓

To see if video motion detection is hardware accelerated for a specific camera, enable logging on the recoding server log file. Set level to **Debug** and diagnostics is logged to the DeviceHandling.log. The log follows the pattern: [time] [274] DEBUG – [guid] [name] Configured decoding: Automatic: Actual decoding: Intel/NVIDIA

The OS version of the recording server and CPU generation may impact performance of hardware accelerated video motion detection. GPU memory allocation is often the bottleneck with older versions (typical limit is between 0.5 GB and 1.7 GB).

Systems based on Windows 10 / Server 2016 and 6th generation CPU (Skylake) or newer can allocate 50% of system memory to GPU and thereby removing or reducing this bottleneck.

6th generation Intel CPUs does provide hardware accelerated decoding of H.265, so the performance is comparable with H.264 for these versions of CPU.

Enable manual sensitivity

The sensitivity setting determines **how much each pixel** in the image must change before it is regarded as motion.

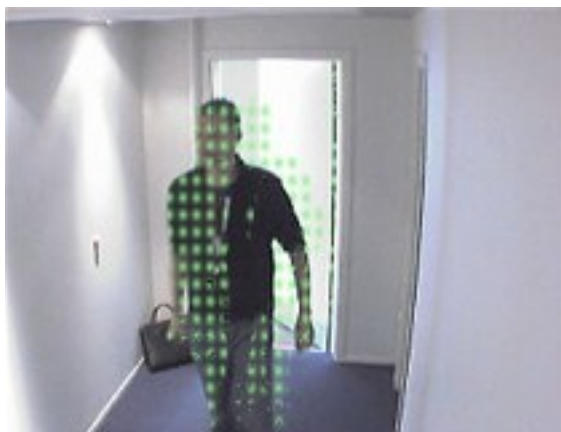
1. Select the **Motion** tab's **Manual Sensitivity** check box.
2. Drag the slider to the left for a higher sensitivity level, and to the right for a lower sensitivity level.

The **higher** the sensitivity level, the less change is allowed in each pixel before it is regarded as motion.

The **lower** the sensitivity level, the more change in each pixel is allowed before it is regarded as motion.

Pixels in which motion is detected are highlighted in green in the preview image.

3. Select a slider position in which only detections you consider motion are highlighted.



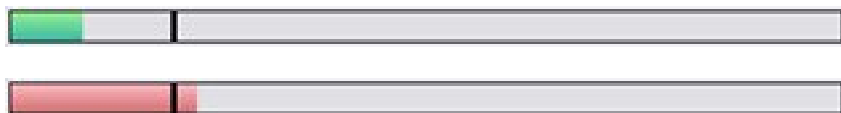
You can compare and set the exact sensitivity setting between cameras by the number in the right side of the slider.

Specify threshold

The motion detection threshold determines **how many pixels** in the image must change before it is regarded as motion.

1. Drag the slider to the left for a higher motion level, and to the right for a lower motion level.
2. Select a slider position in which only detections that you consider motion are detected.

The black vertical line in the motion indication bar shows the motion detection threshold: When detected motion is above the selected detection threshold level, the bar changes color from green to red, indicating a positive detection.



Motion indication bar: changes color from green to red when above the threshold, indicating a positive motion detection.

Select keyframes settings

Determines if motion detection is done on keyframes only instead of on the entire video stream. Only applies to MPEG-4/H.264/H.265.

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

Select **Keyframes only (MPEG-4/H.264/H.265)** box to do motion detection on keyframes only.

Select image processing interval

You can select how often the system performs the motion detection analysis.

From the **Process image every (msec)** list:

- Select the interval. For example, every 1000 milliseconds are once every second. Default value is every 500 milliseconds.

The interval is applied if the actual frame rate is higher than the interval you set here.

Specify detection resolution

Lets you optimize motion detection performance by analyzing only a selected percentage of the image, for example 25%. By analyzing 25%, only every fourth pixel in the image is analyzed instead of all pixels.

Using optimized detection reduces the amount of processing power used to carry out the analysis, but also means a less accurate motion detection.

- In the **Detection resolution** list, select the wanted detection resolution.

Generating motion data for smart search

With **Generate motion data for smart search** enabled, the system generates motion data for the images used for motion detection. For example, if you select motion detection on keyframes only, the motion data is also produced for keyframes only.

The extra motion data enables the client user, via the smart search function, to quickly search for relevant recordings based on motion in the selected area of the image. The system does not generate motion data within areas covered by permanent privacy masks, but only for areas with liftable privacy masks (see Privacy masking tab (devices) on page 242).

Motion detection threshold and exclude regions do not influence the generated motion data.

You specify the default setting of generating smart search data for cameras on the **Tools > Options > General** tab.

Specify exclude regions

You can exclude motion detection from specific areas of a camera view.



Areas with permanent privacy masks, are also excluded from motion detection. Select the **Show privacy masks** check box to display them.

Excluding motion detection from specific areas helps you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

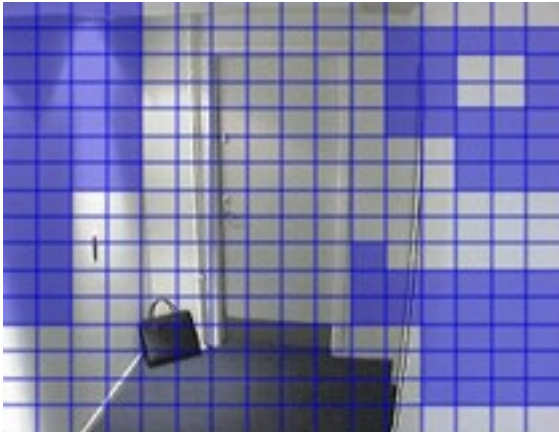
When you use exclude regions with PTZ cameras and you pan-tilt-zoom the camera, the excluded area does **not** move accordingly because the area is locked to the camera image, and not the object.

1. To use exclude regions, select the **Use exclude regions** check box.

A grid divides the preview image into selectable sections.

2. To define exclude regions, drag the mouse pointer over the required areas in the preview image while you press the left mouse button. Right mouse button clears a grid section.

You can define as many exclude regions as needed. Excluded regions appear in blue:



The blue exclude areas only appear in the preview image on the **Motion** tab, not in any other preview images in the Management Client or access clients.

Presets tab (devices)


Presets tab (explained)

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

- PTZ cameras that support preset positions

On the **Presets** tab, you can create or import preset positions, for example:

- In rules for making a PTZ (pan-tilt-zoom) camera move to a specific preset position when an event occurs
- In patrolling, for the automatic movement of a PTZ camera between a number of preset positions
- For manual activation by the XProtect Smart Client users

You can lock a preset position if you want to prevent users in XProtect Smart Client or users with limited security rights from updating this preset. Locked presets are indicated with this icon .

Administrators with security rights to run a reserved PTZ session (see Reserved PTZ sessions (explained) on page 229) can run the PTZ camera in this mode. This prevents other users from taking control over the camera. With sufficient rights, you can release other users' reserved PTZ sessions (see Release PTZ session on page 229).


You assign PTZ permission to roles on the Overall Security tab (see Overall Security tab (roles) on page 333) or the PTZ tab (see PTZ tab (roles) on page 366).

You can monitor if the system is currently patrolling or a user has taken control, in the **PTZ session** area. (see PTZ session properties on page 230)

You also change the PTZ session timeouts for the camera.

Properties

Preview



Preset positions

☐ Use presets from device

↕ Dairy products

↕ Store entrance

↕ Canned foods

↕ Soft drinks

↕ Fresh products

↕ Delicatessen

↕ Check-out

↕ Frozen products

Add New...

Edit...

Delete

Activate

☐ Default preset

↑

↓

PTZ session

User	Priority	Timeout	Reserved
	0	00:00:00	False

Release

Reserve

☐ Timeout for manual PTZ session:

15

↑

↓

Seconds

☐ Timeout for pause patrolling session:

10

↑

↓

Minutes

☐ Timeout for reserved PTZ session:

1

↑

↓

Hours

Info

Settings

Streams

Record

Motion

Presets

Patrolling

◀

▶

Add a preset position (type 1) on page 224

Use preset positions from the camera (type 2) on page 226

Assign a default preset position on page 226

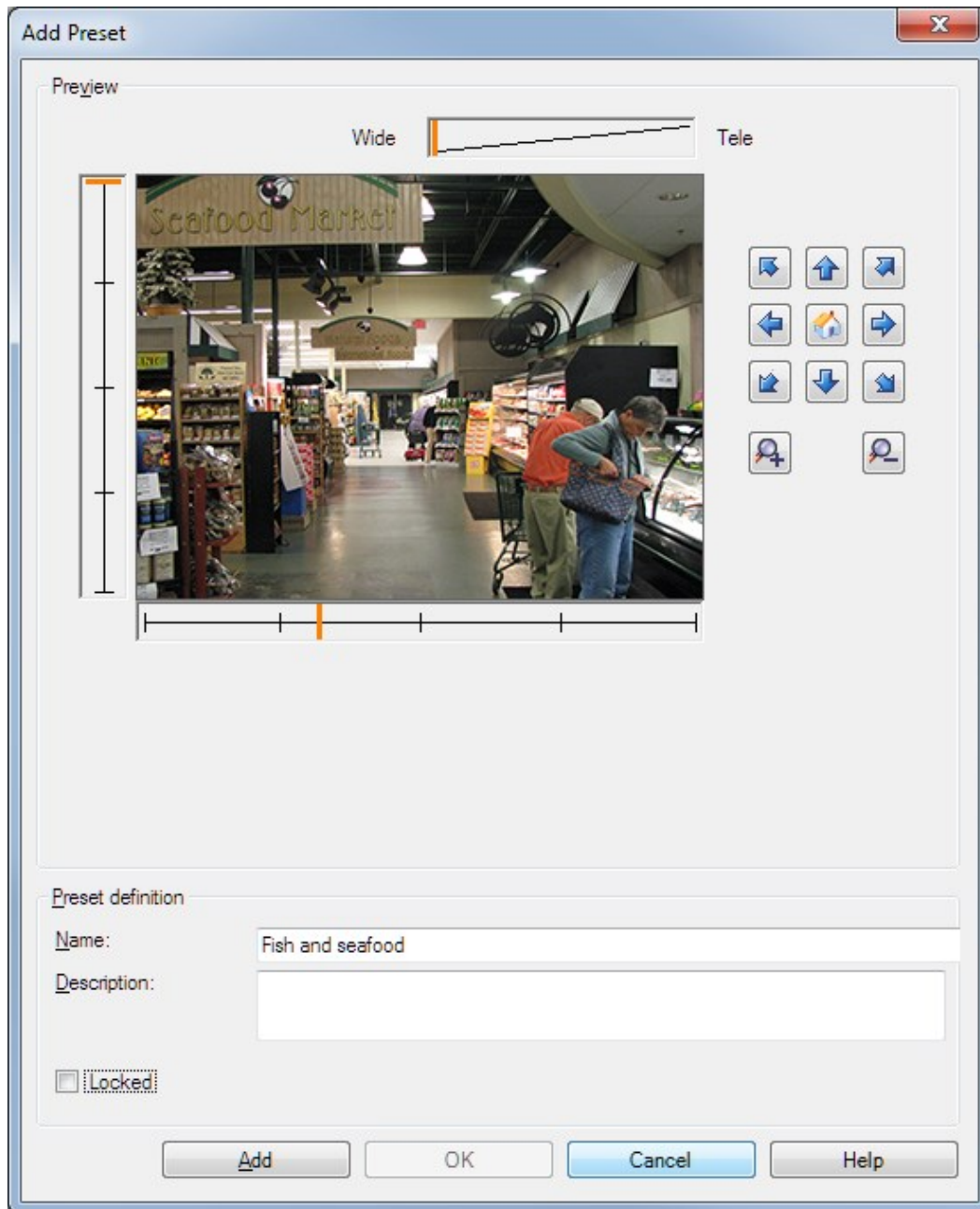
Edit a preset position (type 1 only) on page 226

Test a preset position (type 1 only) on page 229

[Add a preset position \(type 1\)](#)

To add a preset position for the camera:

1. Click **Add New**. The **Add Preset** window appears:



2. The **Add Preset** window displays a live preview image from the camera. Use the navigation buttons and/or sliders to move the camera to the required position.
3. Specify a name for the preset position in the **Name** field.
4. Optionally, enter a description of the preset position in the **Description** field.
5. Select **Locked** if you want to lock the preset position. Only users with sufficient rights can unlock the position afterwards.

6. Click **Add** to specify presets. Keep adding until you have the presets you want.
7. Click **OK**. The **Add Preset** window closes, and adds the position to the **Presets** tab's list of available preset positions for the camera.

Use preset positions from the camera (type 2)

As an alternative to specifying preset positions in the system, you can specify preset positions for some PTZ cameras on the camera itself. You can typically do this by accessing a product-specific configuration web page.

1. Import the presets into the system by selecting **Use presets from device**.
Any presets you have previously defined for the camera are deleted and affect any defined rules and patrolling schedules as well as remove the presets available for the XProtect Smart Client users.
2. Click **Delete** to delete presets that your users do not need.
3. Click **Edit** if you want to change the display name of the preset (see Rename a preset position (type 2 only) on page 228).
4. If you later want to edit such device-defined presets, edit on the camera and then re-import.

Assign a default preset position

If required, you can assign one of a PTZ camera's preset positions as the camera's default preset position.

It can be useful to have a default preset position because it allows you to define rules that specify that the PTZ camera should go to the default preset position under particular circumstances, for example after you have operated the PTZ camera manually.

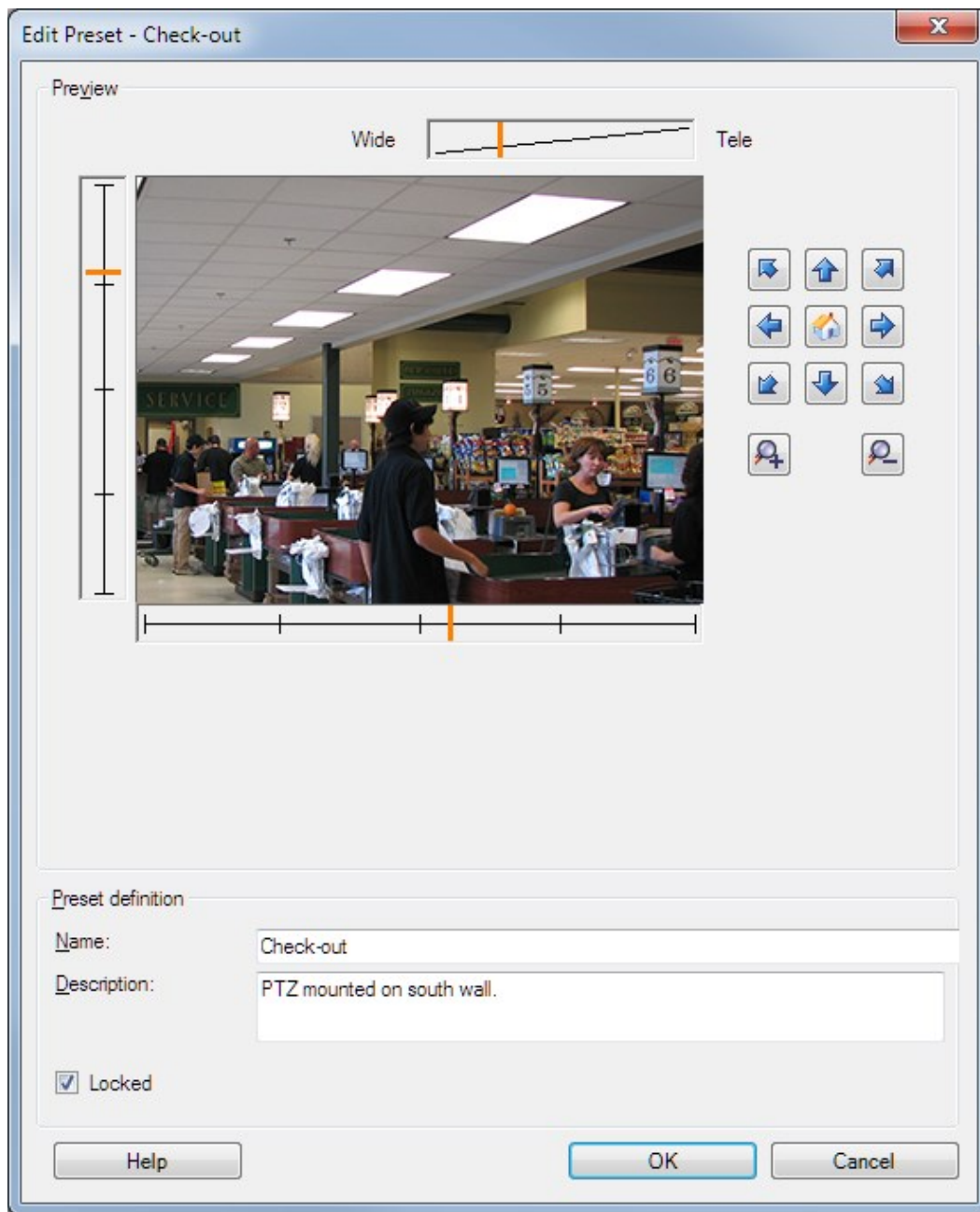
1. To assign a preset position as the default, select the preset in your list of defined preset positions.
2. Select the **Default preset** check box below the list.

You can only define one preset position as the default preset position.

Edit a preset position (type 1 only)

To edit an existing preset position defined in the system:

1. Select the preset position in the **Presets** tab's list of available preset positions for the camera.
2. Click **Edit**. This opens the **Edit Preset** window:



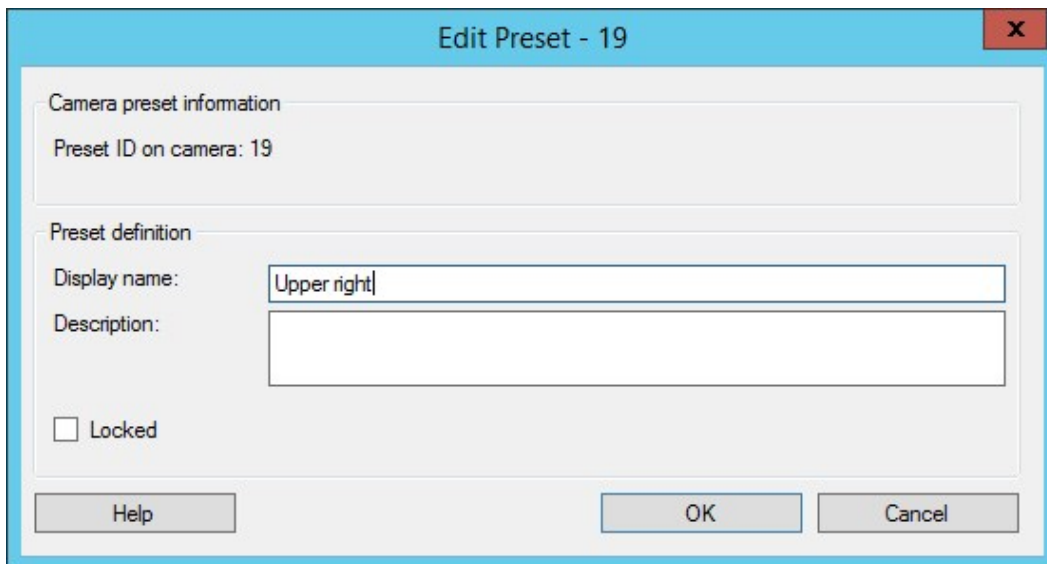
3. The **Edit Preset** window displays live video from the preset position. Use the navigation buttons and/or sliders to change the preset position as required.
4. Change the name/number and description of the preset position if needed.
5. Select **Locked** if you want to lock the preset position. Only users with sufficient rights can unlock the position afterwards.

- Click **OK**.


Rename a preset position (type 2 only)

To edit the name of a preset position defined in the camera:


- Select the preset position in the **Presets** tab's list of available presets for the camera.
- Click **Edit**. This opens the **Edit Preset** window:



The screenshot shows the 'Edit Preset - 19' window. It has a light blue title bar with a close button (X) in the top right corner. The window is divided into two main sections. The top section, 'Camera preset information', has a light gray background and contains the text 'Preset ID on camera: 19'. The bottom section, 'Preset definition', also has a light gray background and contains three input fields: 'Display name:' with the text 'Upper right', 'Description:' which is empty, and a 'Locked' checkbox which is currently unchecked. At the bottom of the window are three buttons: 'Help', 'OK', and 'Cancel'.

- Change the name and add a description of the preset position if needed.
- Select **Locked** if you want to lock the preset name. You can lock a preset name if you want to prevent users in XProtect Smart Client or users with limited security rights from updating the preset name or deleting the preset. Locked presets are indicated with this icon . Only users with sufficient rights can unlock the preset name afterwards.
- Click **OK**.

Lock a preset position

You can lock a preset position if you want to prevent users in XProtect Smart Client or users with limited security rights from updating or deleting a preset. Locked presets are indicated with this icon .

You lock presets as part of adding (see Add a preset position (type 1) on page 224) and editing (see Edit a preset position (type 1 only) on page 226).

Test a preset position (type 1 only)

1. Select the preset position in the **Presets** tab's list of available preset positions for the camera.
2. Click **Activate**.
3. The camera moves to the selected preset position.

Reserved PTZ sessions (explained)

Depending on your surveillance system, you can reserve PTZ sessions.

Administrators with security rights to run a reserved PTZ session can run the PTZ camera in this mode. This prevents other users from taking control over the camera. In a reserved PTZ session, the standard PTZ priority system is disregarded to avoid that users with a higher PTZ priority interrupt the session.

You can operate the camera in a reserved PTZ session both from XProtect Smart Client and the Management Client.

To reserve a PTZ session can be useful, if you need to make urgent updates or maintenance to a PTZ camera or its presets without being interrupted by other users.



You cannot start a reserved PTZ session, if a user with a higher priority than yours controls the camera or if another user has already reserved the camera.

Release PTZ session

The **Release** button allows you to release your current PTZ session so another user can control the camera. When you click **Release**, the PTZ session ends immediately and will be available for the first user to operate the camera.

Administrators assigned with the security permission **Release PTZ session** has the rights to release other users' reserved PTZ session at any time. This can, for example, be useful in occasions where you need to maintain the PTZ camera or its presets, or if other users have accidentally blocked the camera in urgent situations.

Specify PTZ session timeouts

Management Client and XProtect Smart Client users with the necessary user rights can manually interrupt the patrolling of PTZ cameras.

You can specify how much time should pass before regular patrolling is resumed for all PTZ cameras on your system:

1. Select **Tools > Options**.
2. On the **Options** window's **General** tab, select the amount of time in the:
 - **Timeout for manual PTZ sessions** list (default is 15 seconds).
 - **Timeout for pause patrolling sessions** list (default is 10 minutes).
 - **Timeout for reserved PTZ sessions** list (default is 1 hour).

The settings apply for all PTZ cameras on your system.

You can change the timeouts individually for each camera.

1. In the **Site Navigation** pane, click **Camera**.
2. In the Overview pane, select the camera.
3. On the **Presets** tab, select the amount of time in the:
 - **Timeout for manual PTZ session** list (default is 15 seconds).
 - **Timeout for pause patrolling session** list (default is 10 minutes).
 - **Timeout for reserved PTZ session** list (default is 1 hour).

The settings apply for this camera only.

PTZ session properties

The **PTZ session** table shows the current status of the PTZ camera.

Name	Description
User	Displays the user that has pressed the Reserved button and currently controls the PTZ camera. If a patrolling session is activated by the system, it displays Patrolling .
Priority	Displays the user's PTZ priority. You can only take over PTZ sessions from users with a lower priority than you.
Timeout	Displays the remaining time of the current PTZ session.
Reserved	Indicates if the current session is a reserved PTZ session or not: <ul style="list-style-type: none"> • True: Reserved • False: Not reserved

You can change the following timeouts for each PTZ camera.

Name	Description
Timeout for manual PTZ session	Specify the timeout period for manual PTZ sessions on this camera if you want the timeout to be different from the default period. You specify the default period in the Tools menu under Options .
Timeout for pause patrolling PTZ session	Specify the timeout period for pause patrolling PTZ sessions on this camera if you want the timeout to be different from the default period. You specify the default period in the Tools menu under Options .
Timeout for reserved PTZ session	Specify the timeout period for reserved PTZ sessions on this camera if you want the timeout to be different from the default period. You specify the default period in the Tools menu under Options .

Patrolling tab (devices)

Patrolling tab (explained)

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

- PTZ cameras

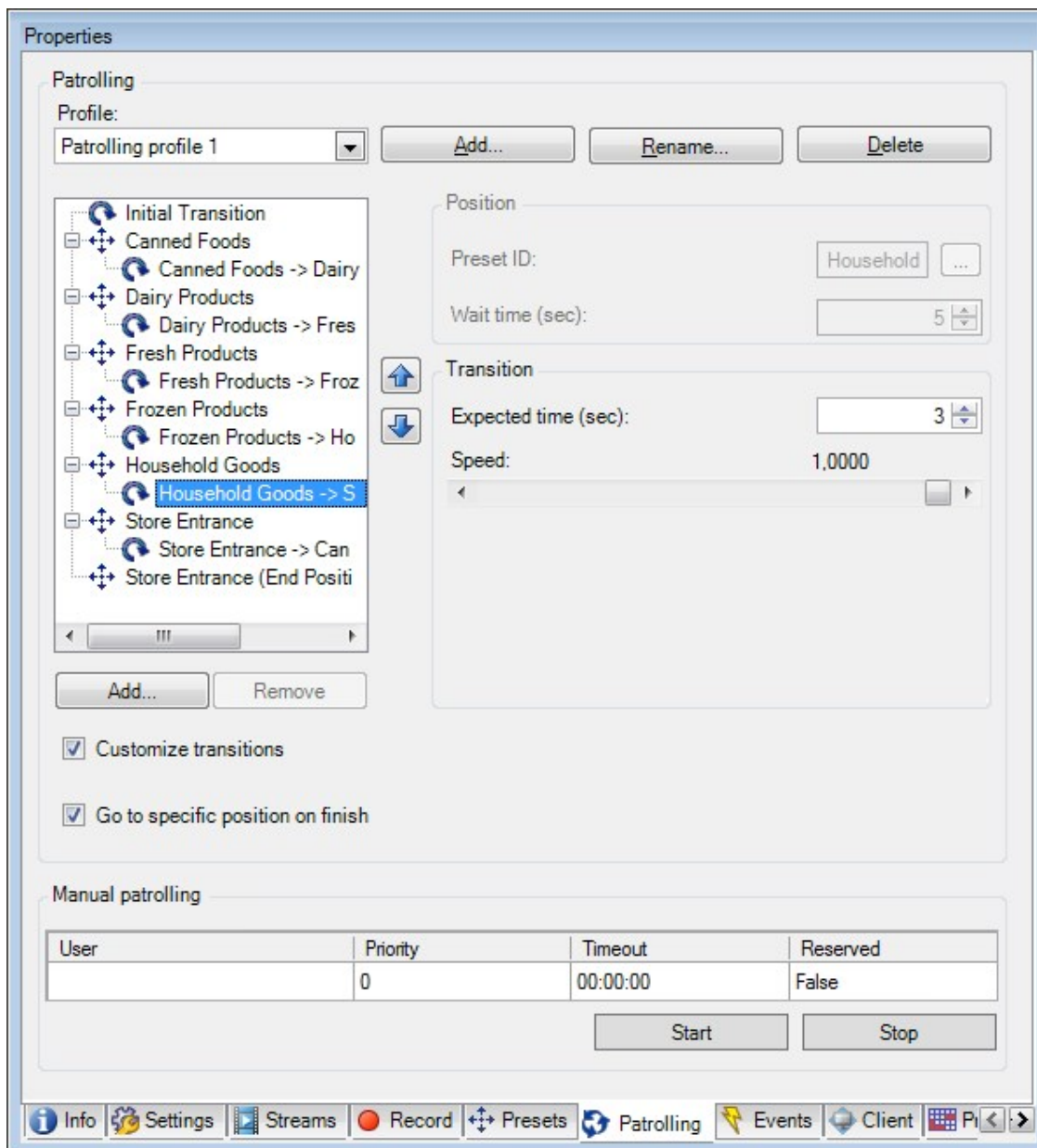
On the **Patrolling** tab, you can create patrolling profiles - the automatic movement of a PTZ (pan-tilt-zoom) camera between a number of preset positions.

Before you can work with patrolling, you must specify at least two preset positions for the camera in the **Presets** tab.

Patrolling profiles are the definitions of how patrolling should take place. This includes the order in which the camera should move between preset positions and how long it should remain at each position. You can create an unrestricted number of patrolling profiles and use them in your rules. For example, you may create a rule specifying that one patrolling profile should be used during daytime opening hours and another during nights.

Before you apply a patrolling profile in a rule, for example, you can test the patrolling profile with manual patrolling. You can also use manual patrolling to take over patrolling from another user or from a rule-activated patrolling, provided that you have a higher PTZ priority.

You can monitor if the system is currently patrolling or a user has taken control, in the **Manual patrolling** area.



Patrolling tab, displaying a patrolling profile with customized transitions.

Add a patrolling profile on page 233

Specify preset positions in a patrolling profile on page 233

Specify the time at each preset position on page 234

Customize transitions (PTZ) on page 234

Specify an end position on page 235

Specify manual PTZ session timeout (see Presets tab (devices) on page 222)

Add a patrolling profile

Add a profile that you want to use in a rule:

1. Click **Add**. The **Add Profile** dialog box appears.
2. In the **Add Profile** dialog box, specify a name for the patrolling profile.
3. Click **OK**. The button is disabled if the name is not unique.

The new patrolling profile is added to the **Profile** list. You can now specify the preset positions and other settings for the patrolling profile.

Specify preset positions in a patrolling profile

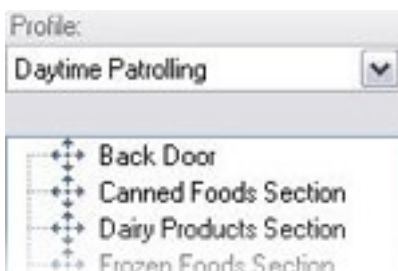
1. Select the patrolling profile in the **Profile** list:



2. Click **Add**.
3. In the **Select Preset** dialog box, select the preset positions for your patrolling profile:



4. Click **OK**. The selected preset positions are added to the list of preset positions for the patrolling profile:



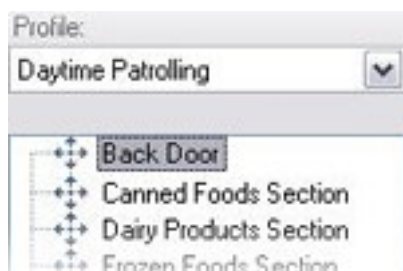
5. The camera uses the preset position at the top of the list as the first stop when it patrols according to the patrolling profile. The preset position in the second position from the top is the second stop, and so forth.

Specify the time at each preset position

When patrolling, the PTZ camera by default remains for 5 seconds at each preset position specified in the patrolling profile.

To change the number of seconds:

1. Select the patrolling profile in the **Profile** list.
2. Select the preset position for which you want to change the time:



3. Specify the time in the **Time on position (sec)** field:
4. If required, repeat for other preset positions.

Customize transitions (PTZ)

By default, the time required for moving the camera from one preset position to another, known as **transition**, is estimated to be three seconds. During this time, motion detection is by default disabled on the camera, because irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions.

You can only customize speed for transitions if your camera supports PTZ scanning and is of the type where preset positions are configured and stored on your system's server (type 1 PTZ camera). Otherwise the **Speed** slider is grayed out.

You can customize the following:

- The estimated transition time
- The speed with which the camera moves during a transition

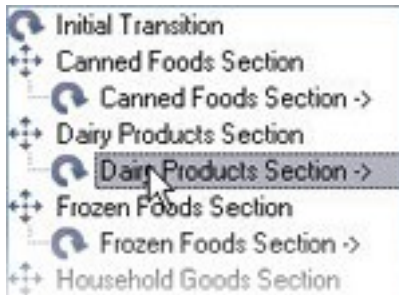
To customize transitions between the different preset positions:

1. Select the patrolling profile in the **Profile** list.
2. Select the **Customize transitions** check box.



Transition indications are added to the list of preset positions.

- In the list, select the transition.



- Specify the estimated transition time (in number of seconds) in the **Expected time (sec)** field.



- Use the **Speed** slider to specify the transition speed. When the slider is in its rightmost position, the camera moves with its default speed. The more you move the slider to the left, the slower the camera moves during the selected transition.
- Repeat as required for other transitions.

Specify an end position

You can specify that the camera should move to a specific preset position when patrolling according to the selected patrolling profile ends.

- Select the patrolling profile in the **Profile** list.
- Select the **Go to specific position on finish** check box. This opens the **Select preset** dialog box.
- Select the end position, and click **OK**.



You can select any of the camera's preset positions as the end position, you are not limited to the preset positions used in the patrolling profile.

- The selected end position is added to the profile list.

When patrolling according to the selected patrolling profile ends, the camera moves to the specified end position.

Manual patrolling (explained)

When you have designed a patrolling profile, you can test it with manual patrolling before you apply it in the system. Use the **Start** and **Stop** buttons to initiate and stop manual patrolling.

If the camera is already patrolling or controlled by another user, you can only start manual patrolling if you have a higher priority.

If you start a manual patrolling while the camera runs a rule-activated system patrolling, the system resumes this patrolling when you stop your manual patrolling. If another user runs a manual patrolling, but you have a higher priority and start your manual patrolling, the other user's manual patrolling is not resumed.

If you do not stop your manual patrolling yourself, it will continue until a rule-based patrolling or a user with a higher priority takes over. When the rule-based system patrolling stops, the system resumes your manual patrolling. If another user starts a manual patrolling, your manual patrolling stops, and will not be resumed.

When you stop your manual patrolling and you have defined an end position for your patrolling profile with **Go to specific position on finish**, the camera returns to this position.

Manual patrolling properties

The **Manual patrolling** table shows the current status of the PTZ camera.

Name	Description
User	Displays the user who has either reserved the PTZ session or started a manual patrolling and currently controls the camera. If a patrolling session is activated by the system, it displays Patrolling .
Priority	Displays the user's PTZ priority. You can only take over PTZ sessions from users or patrolling profiles with a lower priority than yours.
Timeout	Displays the remaining time of the current reserved or manual PTZ sessions.
Reserved	Indicates if the current session is a reserved PTZ session or not. <ul style="list-style-type: none">• True: Reserved• False: Not reserved

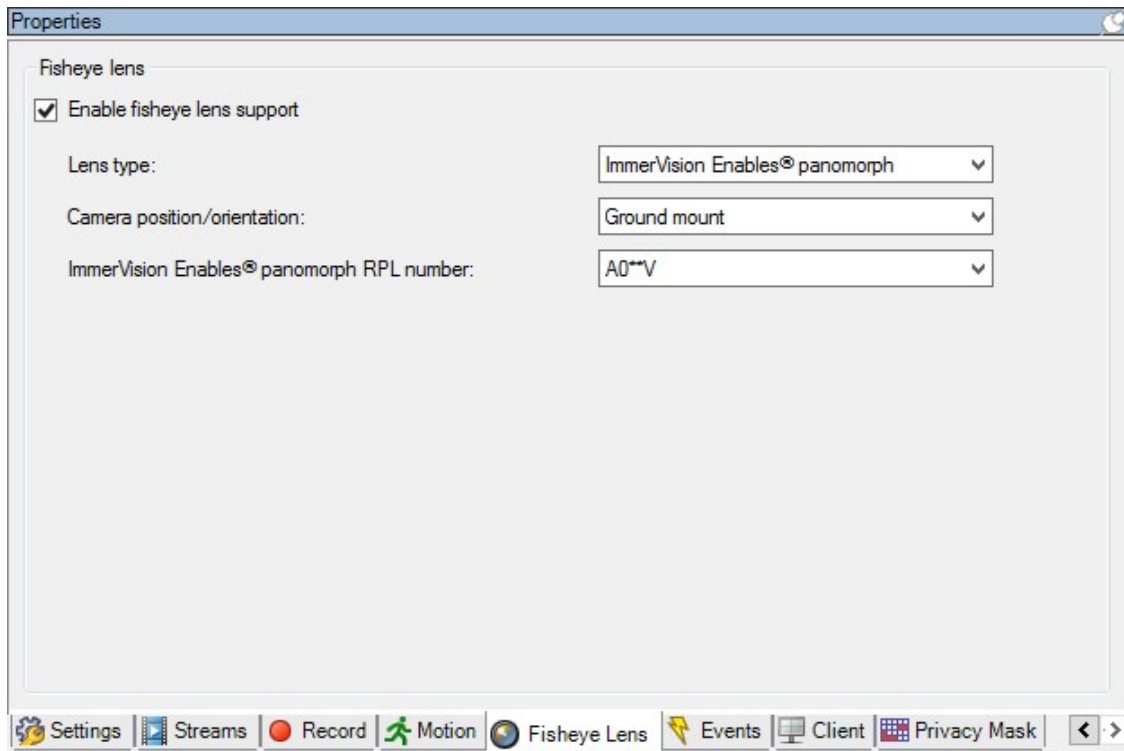
Fisheye lens tab (devices)

Fisheye Lens tab (explained)

The following devices have a **Fisheye Lens** tab:

- Fixed cameras with a fisheye lens

On the **Fisheye Lens** tab, you can enable and configure fisheye lens support for the selected camera.



Enable and disable fisheye lens support

The fisheye lens support is disabled by default.

To enable or disable it, select or clear the **Fisheye Lens** tab's **Enable fisheye lens support** check box.

Specify fisheye lens settings

When you enable the fisheye lens support:

1. Select the lens type.
2. Specify the physical position/orientation of the camera from the **Camera position/orientation** list.
3. Select a Registered Panomorph Lens (RPL) number from the **ImmerVision Enables® panomorph RPL number** list.

This ensures the identification and correct configuration of the lens used with the camera. You usually find the RPL number on the lens itself or on the box it came in. For details of ImmerVision, panomorph lenses, and RPLs, see the Immervision website (<https://www.immervisionenables.com/>).

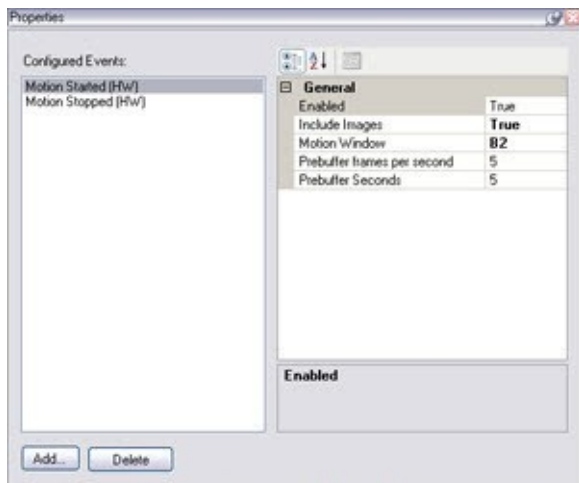
Events tab (devices)

Events tab (explained)

The following devices have an **Events** tab:

- Cameras
- Microphones
- Inputs

In addition to the system's event, some devices can be configured to trigger events. You can use these events when creating event-based rules in the system. Technically, they occur on the actual hardware/device rather than on the surveillance system.



Event tab, example from **camera**.

When you delete an event, it affects all rules that use the event.

- Add an event on page 238
- Specify event properties on page 239
- Use several instances of an event on page 239

Add an event

1. In the **Overview** pane, select a device.
2. Select the **Events** tab and click **Add**. This opens the **Select Driver Event** window.
3. Select an event. You can only select one event at a time.
4. If you want to see an entire list of all events, allowing you to add events that have already been added, select **Show already added events**.
5. Click **OK**.
6. In the toolbar, click **Save**.

Specify event properties

You can specify properties for each event you have added. The number of properties depends on the device and the event. In order for the event to work as intended, you must specify some or all of the properties identically on the device as well as on this tab.

Use several instances of an event

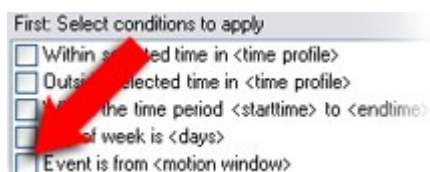
To be able to specify different properties for different instances of an event, you can add an event more than once.



The following example is specific to cameras.

Example: You have configured the camera with two motion windows, called A1, and A2. You have added two instances of the Motion Started (HW) event. In the properties of one instance, you have specified the use of motion window A1. In the properties of the other instance, you have specified the use of motion window A2.

When you use the event in a rule, you can specify that the event should be based on motion detected in a specific motion window for the rule to be triggered:



Event tab (properties)

Name	Description
Configured events	Which events you may select and add in the Configured events list is determined entirely by the device and its configuration. For some types of devices, the list is empty.
General	The list of properties depends on the device and the event. In order for the event to work as intended, you must specify some or all of the properties identically on the device as well as on this tab.

Client tab (devices)

Client tab (explained)

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

- Cameras

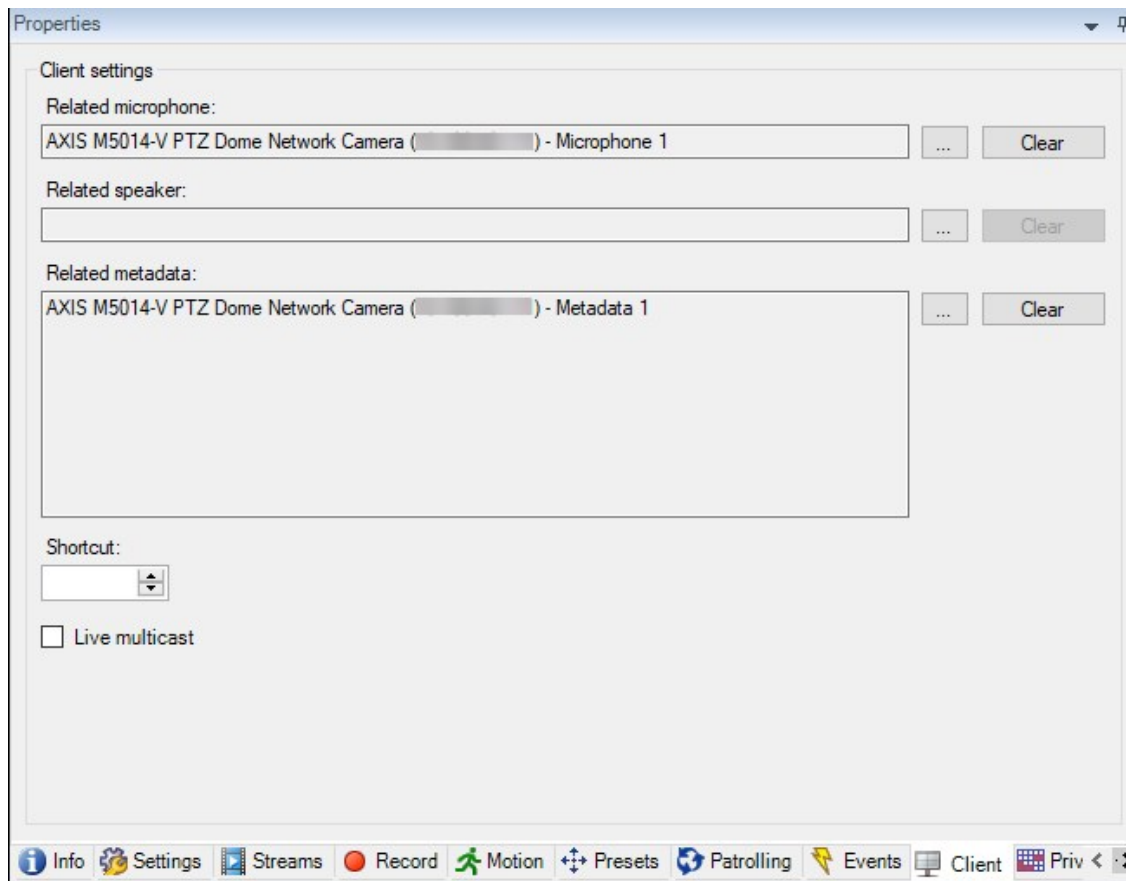
On the **Client** tab you can specify which other devices are viewed and heard when you use the camera in XProtect Smart Client.

The related devices also record when the camera records, see Enable recording on related devices on page 210.

You can also enable **Live multicast** on the camera. It means that the camera multicasts live streams to the clients via the recording server.



Multicast streams are not encrypted, even if the recording server uses encryption.





See also:

- Enable multicasting for the recording server on page 162
- Multicasting (explained) on page 161

Client tab properties

Name	Description
Related microphone	<p>Specify the microphone on the camera that XProtect Smart Client users by default listen to audio. The XProtect Smart Client user can manually select to listen to another microphone if needed.</p> <p>Specify the microphone that is related to the video push camera for streaming video with audio.</p> <p>The related microphones record when the camera records.</p>
Related speaker	<p>Specify through which speakers on the camera, that XProtect Smart Client users speak by default. The XProtect Smart Client user can manually select another speaker if needed.</p> <p>The related speakers record when the camera records.</p>
Related metadata	<p>Specify one or more metadata devices on the camera, that XProtect Smart Client users receive data from.</p> <p>The related metadata devices record when the camera records.</p>
Shortcut	<p>To ease the selection of cameras for the XProtect Smart Client users, define keyboard shortcuts to the camera.</p> <ul style="list-style-type: none">• Create each shortcut so it uniquely identifies the camera• A camera shortcut number cannot be longer than four digits

Name	Description
Live multicast	<p>The system supports multicast of live streams from the recording server to XProtect Smart Client. To enable multicast of live streams from the camera, select the check box.</p> <div>  <p>Live multicasting only works on the stream that you have specified as the camera's default stream on the Streams tab.</p> </div> <p>You must also configure multicasting for the recording server. See Multicast tab (recording server) on page 160.</p> <div>  <p>Multicast streams are not encrypted, even if the recording server uses encryption.</p> </div>

Privacy masking tab (devices)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

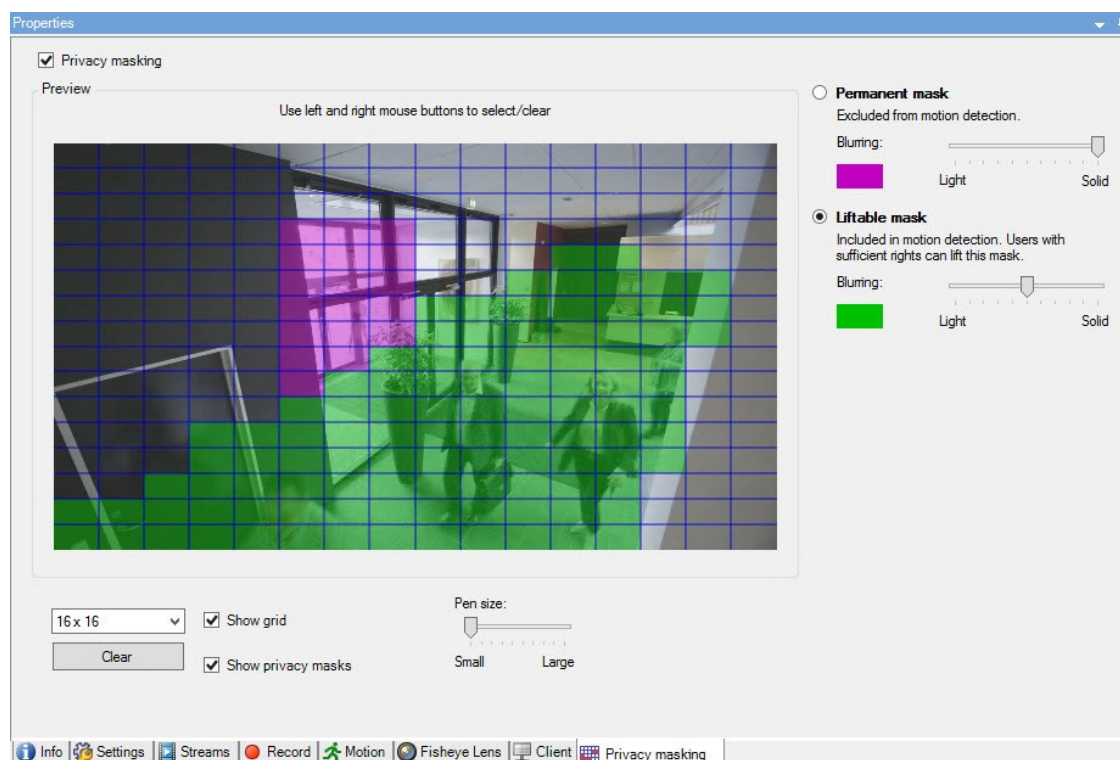
XProtect Essential+ 2018 R1 and onwards does not support privacy masking, so if you upgrade from a system with privacy masks applied, the masks will be removed.

Privacy masking tab (explained)

The following devices have a **Privacy masking** tab:

- Cameras

On the **Privacy masking** tab, you can enable and configure privacy protection for the selected camera.



Privacy masks are applied and locked to an area of the camera image, so the covered area does not follow the pan-til-zoom movements, but constantly cover the same area of the camera image. On some PTZ cameras, you can enable position based privacy masking on the camera itself.

In a Milestone Interconnect setup, the central site disregards privacy masks defined in a remote site. If you want to apply the same privacy masks, you must redefine it on the central site.

- Privacy masking (explained) on page 243
- Enable/disable privacy masking on page 245
- Define privacy masks on page 245
- Change the timeout for lifted privacy masks on page 247
- Give users permission to lift privacy masks on page 247
- Create a report of your privacy masking configuration on page 248

Privacy masking (explained)

With privacy masking, you can define which areas of the video from a camera you want to cover with privacy masks when shown in the clients. For example, if a surveillance camera covers a street, you can cover certain areas of a building (could be windows and doors) with privacy masks, to protect the privacy of residents. In some countries, this is a legal requirement.

You can specify privacy masks as either solid or blurred. The masks cover both live, recorded, and exported video.

There are two types of privacy masks:

- **Permanent privacy mask:** Areas with this type of mask are always covered in the clients. Can be used to cover areas of the video that never requires surveillance, like public areas, or areas where surveillance is not allowed. Motion detection is excluded from areas with permanent privacy masks
- **Liftable privacy mask:** Areas with this type of mask can be temporarily uncovered in XProtect Smart Client by users with permission to lift privacy masks. If the logged in XProtect Smart Client user does not have the right to lift privacy masks, the system asks for an authorized user to approve of the lift. Privacy masks are lifted until timeout or the user reapply them. Be aware that privacy masks are lifted on video from all cameras that the user has access to



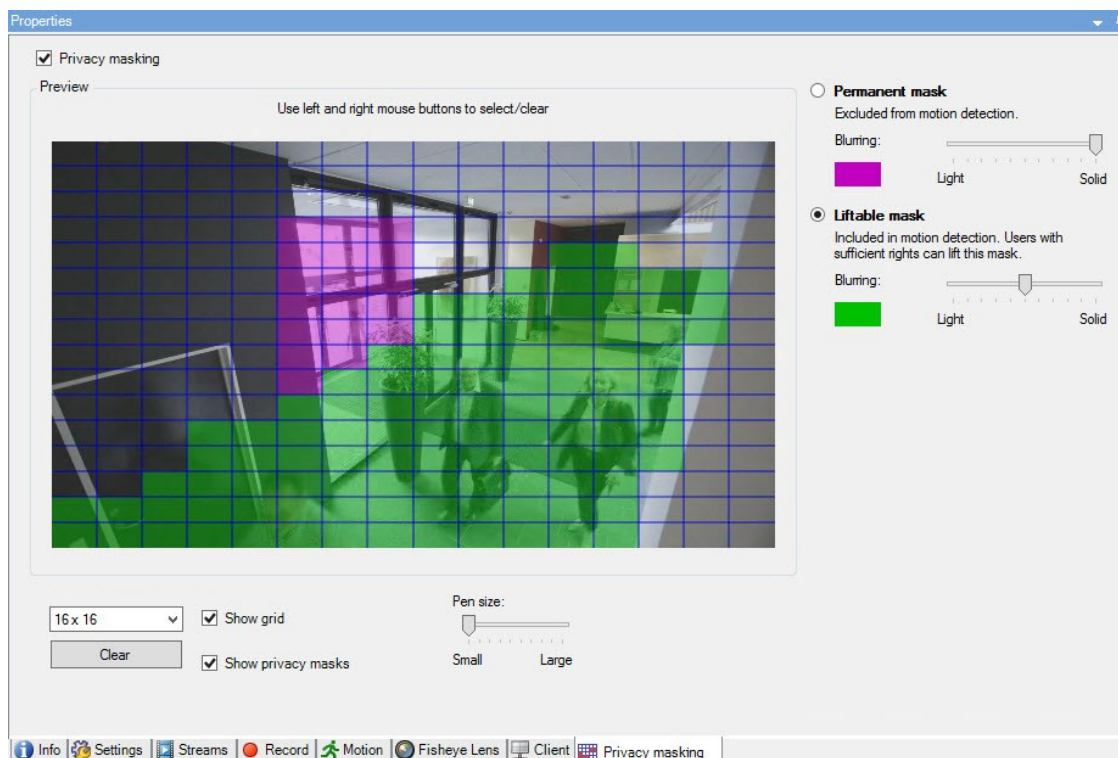
If you upgrade from a 2017 R3 system or older with privacy masks applied, the masks will be converted to liftable masks.

When a user exports or playbacks recorded video from a client, the video includes the privacy masks configured at the time of recording, even if you have changed or removed the privacy masks later. If privacy protection is lifted when exporting, the exported video does **not** include the liftable privacy masks.

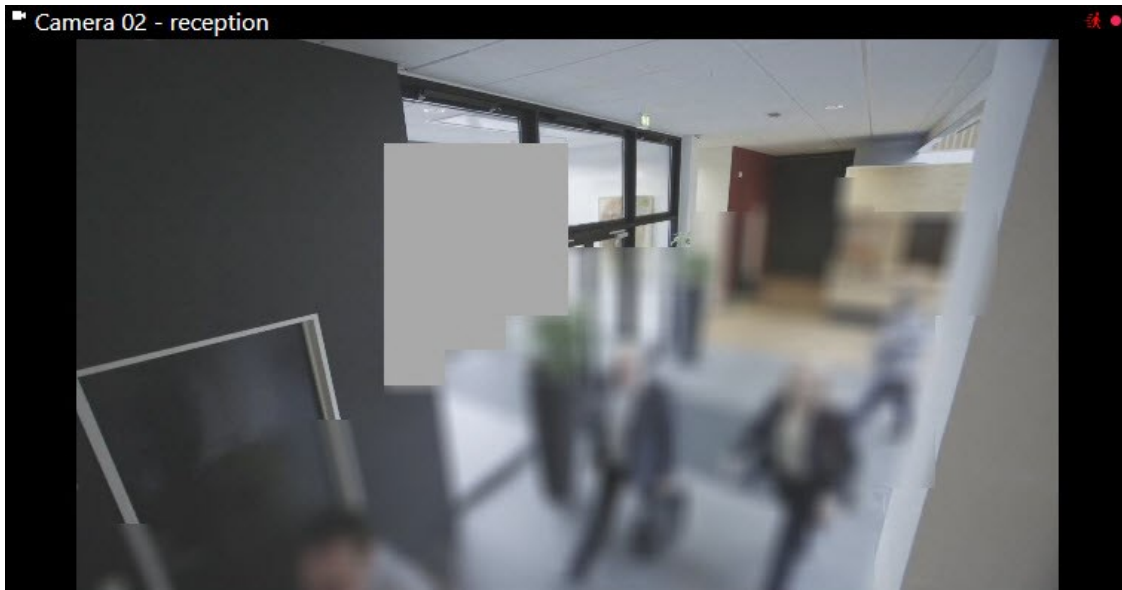


If you change privacy masking settings very often, for example once a week, your system can potentially be overloaded.

Example of the **Privacy masking** tab with privacy masks configured:



And this is how they appear in the clients:



You can inform the client users about the settings of permanent and liftable privacy masks.

Enable/disable privacy masking

The privacy masking feature is disabled by default.

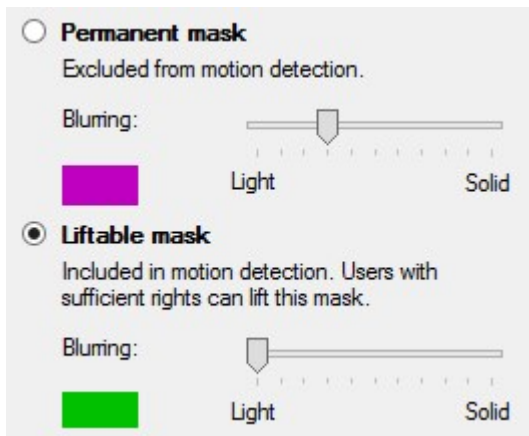
To enable/disable the privacy masking feature for a camera:

- On the **Privacy masking** tab, select or clear **Privacy masking** check box

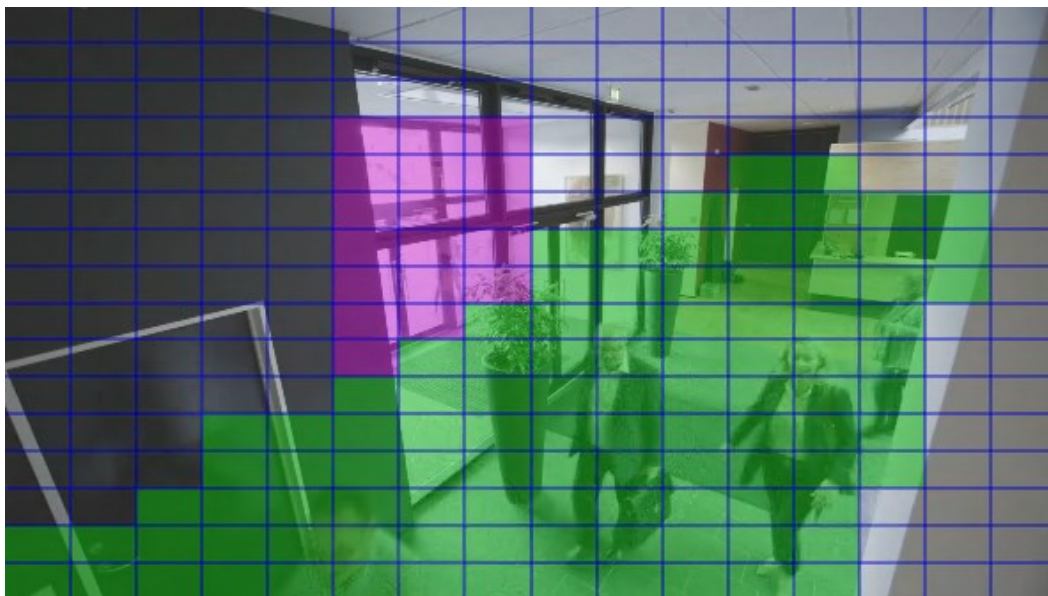
Define privacy masks

When you enable the privacy masking feature on the **Privacy masking** tab, a grid is applied to the camera preview.

1. To cover an area with a privacy mask, first select if you want a permanent or liftable privacy mask.



2. Drag the mouse pointer over the preview. Press down the left mouse button to select a grid cell. Press down the right mouse button to clear a grid cell.
3. You can define as many privacy mask areas as needed. Areas with permanent privacy masks appear in purple and areas with liftable privacy masks in green.



4. Define how the covering of the areas should appear in the video when shown in the clients. Use the sliders to go from a light blurring to a full nontransparent mask.



Permanent privacy masks also appear on the **Motion** tab.

5. In XProtect Smart Client, check that the privacy masks appear as you defined.

Give users permission to lift privacy masks

By default, no users have permissions to lift privacy masks in XProtect Smart Client.

To enable/disable the permission:

1. Under **Roles**, select the role that you want to give permission to lift privacy masks.
2. On the **Overall Security** tab, select **Cameras**.
3. Select the **Allow** check box for the **Lift privacy masks** permission.

Users that you assign to this role, can lift privacy masks configured as liftable masks for himself/herself as well as authorize the lift for other XProtect Smart Client users.

Change the timeout for lifted privacy masks

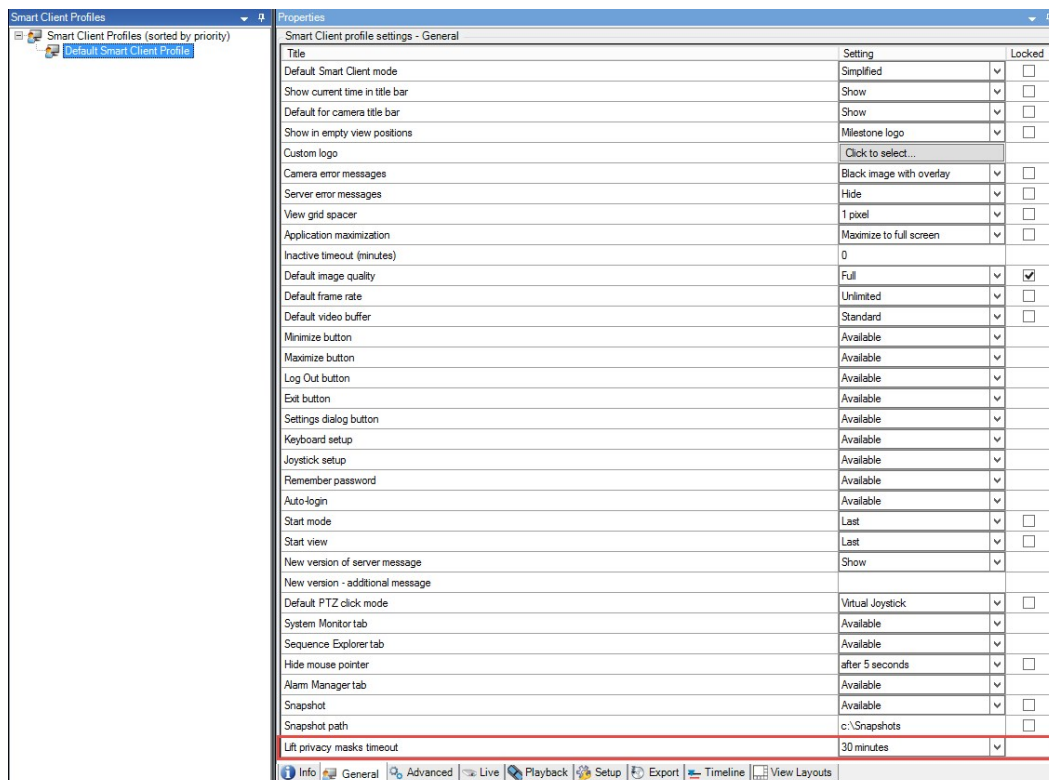
By default, privacy masks are lifted for 30 minutes in XProtect Smart Client and afterwards applied automatically, but you can change that.



When you change the timeout, remember to do it for the Smart Client profile associated with the role that has the permission to lift privacy masks.

To change the timeout:

1. Under **Smart Client Profiles**, select the relevant Smart Client profile.
2. On the **General** tab, locate **Lift privacy masks timeout**.



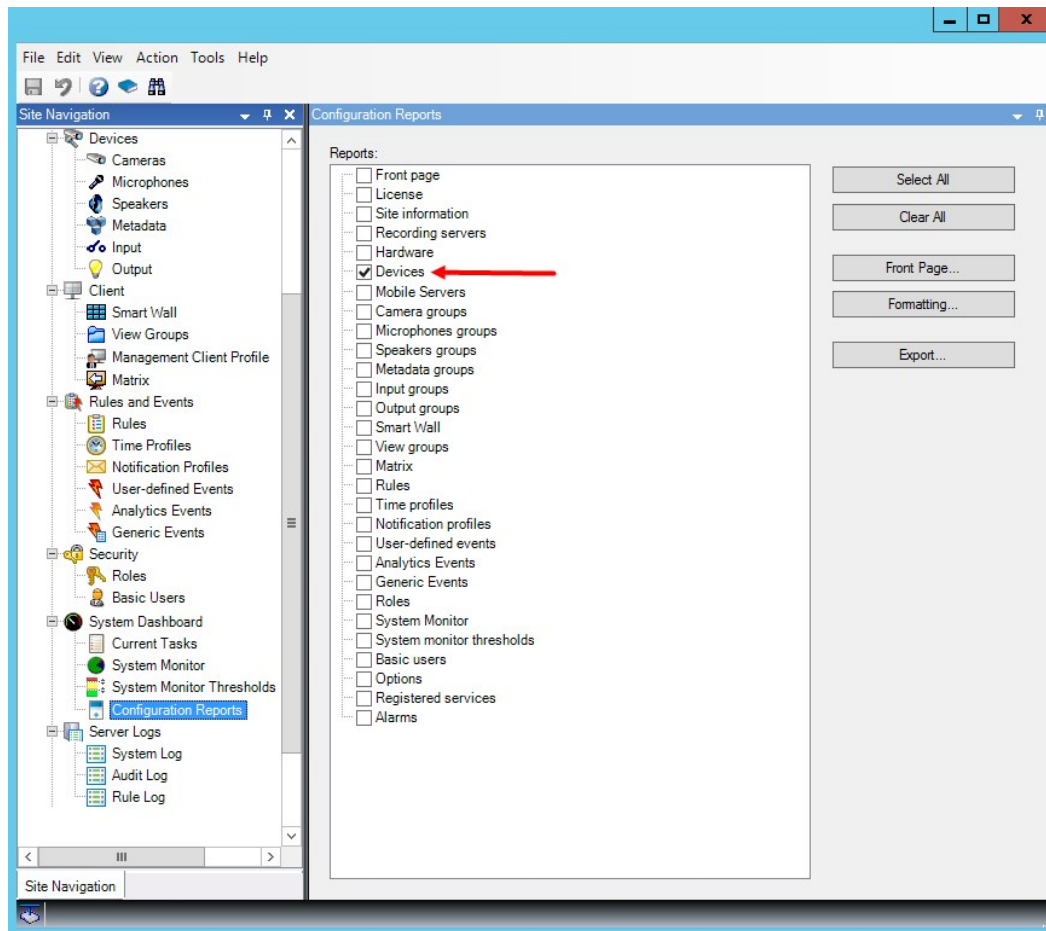
3. Select between the values:
 - 2 minutes
 - 10 minutes
 - 30 minutes
 - 1 hour
 - 2 hours
 - Until logged out
4. Click **Save**.

Create a report of your privacy masking configuration

The devices report include information about your cameras' current privacy masking settings.

To configure a report:

1. Under **Configuration Reports**, select the **Devices** report.



2. If you want to modify the report, you can change the front page and the formatting.
3. Click **Export**, and the system creates the report as a PDF file.

For more information about reports, see Configuration reports (explained) on page 382.

Privacy masking tab (properties)

Name	Description
Grid size	<p>The selected grid size determines the density of the grid, regardless whether the grid is visible in the preview or not.</p> <p>Select between the values 8×8, 16×16, 32×32 or 64×64.</p>

Name	Description
Clear	Clears all privacy masks you have specified.
Show grid	Select the Show grid check box to make the grid visible.
Show privacy masks	<p>When you select the Show privacy masks check box (default), permanent privacy masks appear in purple in the preview and liftable privacy masks in green.</p> <p>Milestone recommends that you keep the Show privacy masks box selected so that you and your colleagues can see the current privacy protection configuration.</p>
Pen size	Use the Pen size slider to indicate the size of the selections you wish to make when you click and drag the grid to select regions. Default is set to small, which is equivalent to one square in the grid.
Permanent mask	<p>Appears in purple in the preview on this tab and on the Motion tab.</p> <p>Permanent privacy masks are always visible in XProtect Smart Client and cannot be lifted. Can be used to cover areas of the video that never requires surveillance, like public areas, where surveillance is not allowed. Motion detection is excluded from permanent masks.</p> <p>You specify the coverage of privacy masks as either solid or some level of blurred. The coverage settings apply to both live and recorded video.</p>
Liftable mask	<p>Appears in green in the preview on this tab.</p> <p>Liftable privacy masks can be lifted in XProtect Smart Client by users with sufficient user rights. By default, the privacy masks are lifted for 30 minutes, or until the user apply them again. Be aware that the privacy masks are lifted on video from all the cameras that the user has access to.</p> <p>If the XProtect Smart Client user does not have the right to lift privacy masks, the system asks for a user with permission to authorize the lift.</p> <p>You specify the coverage of privacy masks as either solid or a level of blurred. The coverage settings apply to both live and recorded video.</p>
Blurring	<p>Use the slider to select the blurring level of the privacy masks in the clients or set the coverage to solid.</p> <p>By default, the coverage of areas with permanent privacy masks are solid (nontransparent). By default, liftable privacy masks are medium blurred.</p> <p>You can inform the client users about the appearance of permanent and liftable privacy masks, so they are able to distinguish.</p>

Site Navigation: Clients

This article describes how to customize the user interface for operators in XProtect Smart Client and for system administrators in the Management Client.

Clients (explained)

Available functionality depends on the system you are using. See

<https://www.milestonesys.com/solutions/platform/product-index/> for more information.

The Client section of the Management Client consists of:

Name	Description
XProtect Smart Wall	XProtect Smart Wall is an add-on that allows you to send view content from XProtect Smart Client to a dedicated video wall. For more detailed information about XProtect Smart Wall, see XProtect Smart Wall (explained (see XProtect Smart Wall (explained) on page 30).
View groups	The way in which video from cameras is presented is called a view. To control who can see what in XProtect Smart Client, you can create view groups to group views in logical entities. You can assign access to these view groups through roles and limit who can access individual view groups to specific roles. Select View Groups to design and work with view groups to fit your surveillance needs.
Smart Client profiles	To differentiate XProtect Smart Client users, you can create Smart Client profiles, prioritize these and customize their profiles as needed for the different tasks at hand.
Management Client profiles	To differentiate Management Client administrator users, you can create Management Client profiles, prioritize these and customize their profiles as needed for the different tasks at hand.
Matrix	Matrix is a feature for distributing video remotely. If you use Matrix, you can push video from any camera on your system's network to any running XProtect Smart Client.

Site Navigation: Clients: Configuring Smart Wall

This article describes how to configure XProtect Smart Wall.

XProtect Smart Wall licensing

XProtect Smart Wall requires the following video wall-related licenses:

- A **base license** for XProtect Smart Wall that covers an unrestricted number of monitors displaying video on a video wall

A base license for XProtect Smart Wall is included in the base license for XProtect Corporate. If you have XProtect Expert, you can purchase a base license for XProtect Smart Wall separately.

Configure Smart Walls

A Smart Wall configuration consists of defining the Smart Wall, adding monitors and defining the monitor layout, and optionally specifying Smart Wall presets and the layout and content of the different monitors.

You need not define Smart Wall presets, if you only want to display cameras and XProtect Smart Client views that your XProtect Smart Client users manually can push onto the video wall.

If you want to use rules to change automatically what is displayed on the video wall, or if you have typical surveillance scenarios where you want to display the same content on the video wall each time the scenario happens, you should define Smart Wall presets.

The configuration of the Smart Wall is very flexible. You can include all monitors on the video wall in one Smart Wall or group the monitors and configure a Smart Wall for each group. Smart Wall presets can change the layout and content of all monitors in a Smart Wall or only some of the monitors. Monitors can be part of several Smart Walls and Smart Wall presets. Create as many Smart Walls and Smart Wall presets you need to optimize the coverage of your typical surveillance scenarios.

a. Define the Smart Wall:

1. Expand **Client**, and select **Smart Wall**.
2. In the **Overview** pane, right-click **Smart Wall** and select **Add Smart Wall**.
3. Specify the settings for the Smart Wall.
4. In the **General View Item Properties** settings, define if you want system status information and title bars to appear above the cameras' layout items.
5. Click **OK**.

b. Add monitors and define the monitor layout:

1. Right-click the Smart Wall and select **Add Monitor**.
2. Configure the dimensions of the monitor so it resembles one of the physical monitors on the video wall.
3. Use the preset behavior settings **Empty preset** and **Empty preset item** to define what is displayed on a monitor with an empty preset layout or in a preset's empty preset items when a new Smart Wall preset is automatically triggered or manually selected in XProtect Smart Client. You can use empty presets and empty preset items for content not controlled by the Smart Wall preset.
4. Use the preset behavior setting **Element insertion** to define what should happen when a user of XProtect Smart Client drags a camera onto a layout item in the Smart Wall preset. Select **Independent** to replace the camera already in the preset item with the new camera or **Linked** to push the content of the layout items from left to right from where you inserted the new camera.
5. Add as many monitors as you have on the physical video wall.
6. Select the Smart Wall and on the **Layout** tab, click **Edit** to position the different monitors so their positions resemble the mounting of the physical monitors on the video wall.
7. Click **OK**. The same layout is used in XProtect Smart Client.

c. Add Smart Wall presets (optionally):

1. Select the Smart Wall and from the **Presets** tab, click **Add New**.
2. Enter a name and a description and click **OK**.
3. Click **Activate** to display the Smart Wall preset on the video wall.
4. Create as many Smart Wall presets as you need.

d. Add layout and cameras to the monitors (requires a Smart Wall preset):

1. Select one of the monitors you created and from the **Presets** tab, select a preset from the list to configure what you want the selected monitor to show when used with the selected Smart Wall preset.
2. Click **Edit**.
3. Click the layout button to select which layout to use with your monitor, and click **OK**.



4. Drag cameras from the **Device Groups**, **Recording Servers** or **Federated Site Hierarchy** tab onto the different layout items. The cameras on the **Federated Site Hierarchy** tab are accessible in a Milestone Federated Architecture setup. You can leave layout items blank, so they are available for other content not controlled by the Smart Wall preset.

5. If the monitor already has a layout for the selected preset, you can click **Clear** to define a new layout or to exclude the monitor from the Smart Wall preset, so the monitor is available for other content not controlled by the Smart Wall preset.
6. Click **OK**.
7. Repeat the steps, until you have added a layout and cameras on the monitors you want to include in the Smart Wall preset.

Set up user rights for XProtect Smart Wall

You can control the tasks that XProtect Smart Client users can perform in XProtect Smart Wall by specifying user rights for roles. The user rights apply to all users who are assigned to the role. For more information, see Roles with Smart Wall rights properties (see Roles settings on page 331).

Selections for the **Read**, **Edit**, and **Delete** user rights are always applied. For the **Operate** and **Playback** user rights, you can also grant the user rights for a specific period of time by selecting a time profile. For example, this is useful if you want to allow a user to change the content that is displayed on a Smart Wall, but only during their normal working hours.

To specify user rights for a role, follow these steps:

1. In the Site Navigation pane, expand **Security**, and select **Roles**.
2. In the **Roles** pane, select the role, or create a new role by right-clicking in the pane and selecting **Add Role**.
3. In the upper part of the **Role settings** pane, select the Smart Wall.
4. In the lower part of the Role Settings pane, click the **Smart Wall** tab, and then select the user rights to assign.
 - **Read** - View Smart Walls in client applications
 - **Edit** - Modify Smart Walls in client applications
 - **Delete** - Delete Smart Walls in client applications
 - **Operate** - Apply layouts on the selected monitor in client applications, and activate presets
 - **Playback** - Review and manage live and recorded video



If you do not select the **Playback** permission, users can view but not change the content that is displayed on the video wall. If a user makes a change, the system automatically disconnects from the shared state and the content on the video wall is not affected. To return to the shared view, click **Reconnect Smart Wall monitor**.

5. Optional: To grant the **Operate** or **Playback** user rights for a specific period of time, select the check box, and then select the time profile.

Using rules with Smart Wall presets (explained)

By combining rules and Smart Wall presets, you can control what is displayed on your video wall in similar way as the system uses rules to control the behavior of cameras and more. For example, a rule can trigger your video wall to display a certain Smart Wall preset during a certain day. You can even use rules to control what individual monitors in a video wall display. See Rules on page 298 for information about how to create rules.

Example of a rule triggering a Smart Wall preset:

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

Smart Wall properties

Info tab (Smart Wall properties)

On the **Info** tab for a Smart Wall, you can add and edit Smart Walls.

Name	Description
Name	The name of the Smart Wall. Displayed in XProtect Smart Client as the Smart Wall view group name.
Description	A description of the Smart Wall. The description is only used internally in the Management Client.
Status text	If selected, camera and system status information is displayed across cameras' layout items on the video wall.
No title bar	If selected, all Smart Wall layout items have no title bars on the video wall.
Title bar	If selected, all Smart Wall layout items have title bars on the video wall.
Title bar with live indicator	When selected, all Smart Wall layout items' title bars display live and motion indicators on the video wall.

Presets tab (Smart Wall properties)

On the **Presets** tab for a Smart Wall, you can add and edit Smart Wall presets.

Name	Description
Add New	Click to add a preset to your XProtect Smart Wall installation. Define a name and description for the new Smart Wall preset.
Edit	Edit the name and/or description of a Smart Wall preset.
Delete	Delete a Smart Wall preset.
Activate	Click to display the Smart Wall preset on the video wall. You must create rules with the Smart Wall preset before the system can automatically trigger the display of the Smart Wall preset. See also Using rules with Smart Wall presets (explained) on page 255.

Layout tab (Smart Wall properties)

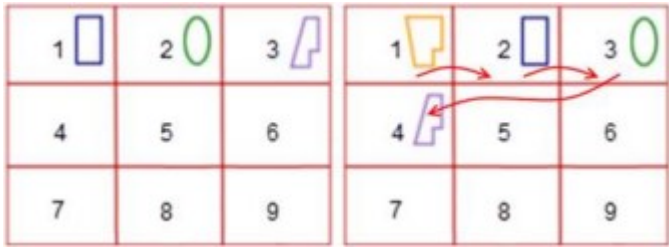
On the **Layout** tab for a Smart Wall, you position the monitors in your Smart Wall so their positions resemble the mounting of the physical monitors on the video wall. The layout is also used in the XProtect Smart Client.

Name	Description
Edit	Click to adjust the positioning of the monitors.
Movement	To move a monitor to a new position, select the relevant monitor and drag it to the desired position, or click one of the arrow buttons to move the monitor in the selected direction.
Zoom buttons	Click buttons to zoom in/out of the Smart Wall layout preview to ensure you position the monitors correctly.
Name	The name of the monitor. The name is displayed in XProtect Smart Client.
Size	The size of the physical monitor on the video wall.
Aspect ratio	The height/width relationship of the physical monitor on the video wall.

Monitor properties


Info tab (monitor properties)

On the **Info** tab for a monitor in a Smart Wall preset, you can add monitors and edit the monitors' settings.

Name	Description
Name	The name of the monitor. The name is displayed in XProtect Smart Client.
Description	A description of the monitor. The description is only used internally in the Management Client.
Size	The size of the physical monitor on the video wall.
Aspect ratio	The height/width relationship of the physical monitor on the video wall.
Empty preset	<p>Defines what should be displayed on a monitor with an empty preset layout when a new Smart Wall preset is triggered or selected in XProtect Smart Client.</p> <p>Select Preserve to keep the current content on the monitor.</p> <p>Select Clear to clear all content so nothing is displayed on the monitor.</p>
Empty preset item	<p>Defines what should be displayed in an empty preset layout item when a new Smart Wall preset is triggered or selected in XProtect Smart Client.</p> <p>Select Preserve to keep the current content in the layout item.</p> <p>Select Clear to clear the content so nothing is displayed in the layout item.</p>
Element insertion	<p>Defines how cameras are inserted in the monitor's layout when viewed in the XProtect Smart Client. When selecting Independent, only the content of the affected layout item changes, the rest of the content in the layout remain the same. When selecting Linked, the contents of the layout items are pushed from left to right. If, for instance, a camera is inserted in position 1, the previous camera of position 1 is pushed to position 2, the previous camera of position 2 is pushed to position 3, and so on as illustrated in this example.</p> 

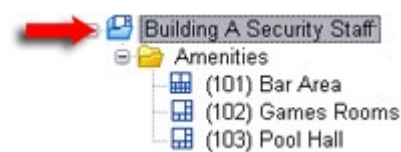
Presets tab (monitor properties)

On the **Presets** tab for a monitor in a Smart Wall preset, you can edit the layout and content of the monitor in the selected Smart Wall preset.

Name	Description
Preset	A list of Smart Wall presets for the select Smart Wall.
Edit	<p>Click Edit to edit the layout and the content of the selected monitor.</p> <p>Double-click a camera to remove a single camera.</p> <p>Click Clear to define a new layout or to exclude the monitor in the Smart Wall preset so the monitor is available for other content not controlled by the Smart Wall preset.</p> <p>Click  to select the layout you want to use with your monitor in the selected preset, and click OK.</p> <p>Drag cameras from the Device Groups, Recording Servers or Federated Sites tab onto the different layout items. You can leave layout items empty, so they are available for other content not controlled by the Smart Wall preset.</p>

Site Navigation: Clients: View groups

The way in which the system presents video from one or more cameras in clients is called a view. A view group is a container for one or more logical groups of such views. In clients, a view group is presented as an expandable folder from which users can select the group and the view they want to see:



Example from XProtect Smart Client: Arrow indicates a view group, which contains a logical group (called Amenities), which in turn contains 3 views.

View groups and roles (explained)

By default, each role you define in the Management Client is also created as a view group. When you add a role in the Management Client, the role by default appears as a view group for use in clients.

- You can assign a view group based on a role to users/groups assigned to the relevant role. You may change these view group rights by setting this up in the role afterwards
- A view group based on a role carries the role's name.

Example: If you create a role with the name **Building A Security Staff**, it appears in XProtect Smart Client as a view group called **Building A Security Staff**.

In addition to the view groups you get when adding roles, you may create as many other view groups as you like. You can also delete view groups, including those automatically created when adding roles

- Even if a view group is created each time you add a role, view groups do not have to correspond to roles. You can add, rename or remove any of your view groups if required



If you rename a View group, client users already connected must log out and log in again before the name change is visible.

Add a view group

1. Right-click **View Groups**, and select **Add View Group**. This opens the **Add View Group** dialog box.
2. Enter the name and an optional description of the new view group and click **OK**.



No roles have the right to use the newly added view group until you have specified such rights. If you have specified which roles that can use the newly added view group, already connected client users with the relevant roles must log out and log in again before they can see the view group.

Site Navigation: Clients: Smart Client profiles



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

Smart Client profiles allows system administrators to control how XProtect Smart Client should look and behave and what features and panes XProtect Smart Client users have access to. You can set up user rights for: panes and options, minimize/maximize options, inactivity time-control, remember password or not, view shown after log in, layout of print reports, export path, and more.

To manage Smart Client profiles in the system, expand **Client** and select **Smart Client Profiles**. You can also learn about the relationship between Smart Client profiles, roles and time profiles and how to use these together (see Create and set up Smart Client profiles, roles and time profiles on page 260).

Add and configure a Smart Client profile

You must create a Smart Client profile before you can configure it.

1. Right-click **Smart Client Profiles**.
2. Select **Add Smart Client Profile**.
3. In the **Add Smart Client Profile** dialog box, enter a name and description of the new profile and click **OK**.
4. In the **Overview** pane, click the profile you created to configure it.
5. Adjust settings on one, more or all of the available tabs and click **OK**.

Copy a Smart Client profile

If you have a Smart Client profile with complicated settings or rights and need a similar profile, it might be easier to copy an already existing profile and make minor adjustments to the copy than to creating a new profile from scratch.

1. Click **Smart Client Profiles**, right-click the profile in the **Overview** pane, select **Copy Smart Client Profile**.
2. In the dialog box that appears, give the copied profile a new unique name and description. Click **OK**.
3. In the **Overview** pane, click the profile you just created to configure it. This is done by adjusting settings on one, more or all of the available tabs. Click **OK**.

Create and set up Smart Client profiles, roles and time profiles

When you work with Smart Client profiles, it is important to understand the interaction between Smart Client profiles, roles and time profiles:

- Smart Client profiles deal with user right settings in XProtect Smart Client
- Roles deal with security settings in clients, MIP SDK and more
- Time profiles deal with time aspects of the two profiles-types

Together these three features provide unique control and customizing possibilities with regards to XProtect Smart Client user rights.

Example: You need a user in your XProtect Smart Client setup who should only be allowed to view live video (no playback) from selected cameras, and only during normal working hours (8.00 to 16.00). One way of setting this up could be as follows:

1. Create a Smart Client profile, and name it, for example, **Live only**.
2. Specify the needed live/playback settings on **Live only**.
3. Create a time profile, and name it, for example, **Daytime only**.
4. Specify the needed time period on **Daytime only**.
5. Create a new role and name it, for example, **Guard (Selected cameras)**.

6. Specify which cameras **Guard (Selected cameras)** can use.
7. Assign the **Live only** Smart Client profile and the **Daytime only** time profile to the **Guard (Selected cameras)** role to connect the three elements.

You now have a mix of the three features creating the wanted result and allowing you room for easy fine-tuning and adjustments. You can do the setup in a different order, for example, creating the role first and then the Smart Client profile and the time profile, or any other order you prefer.

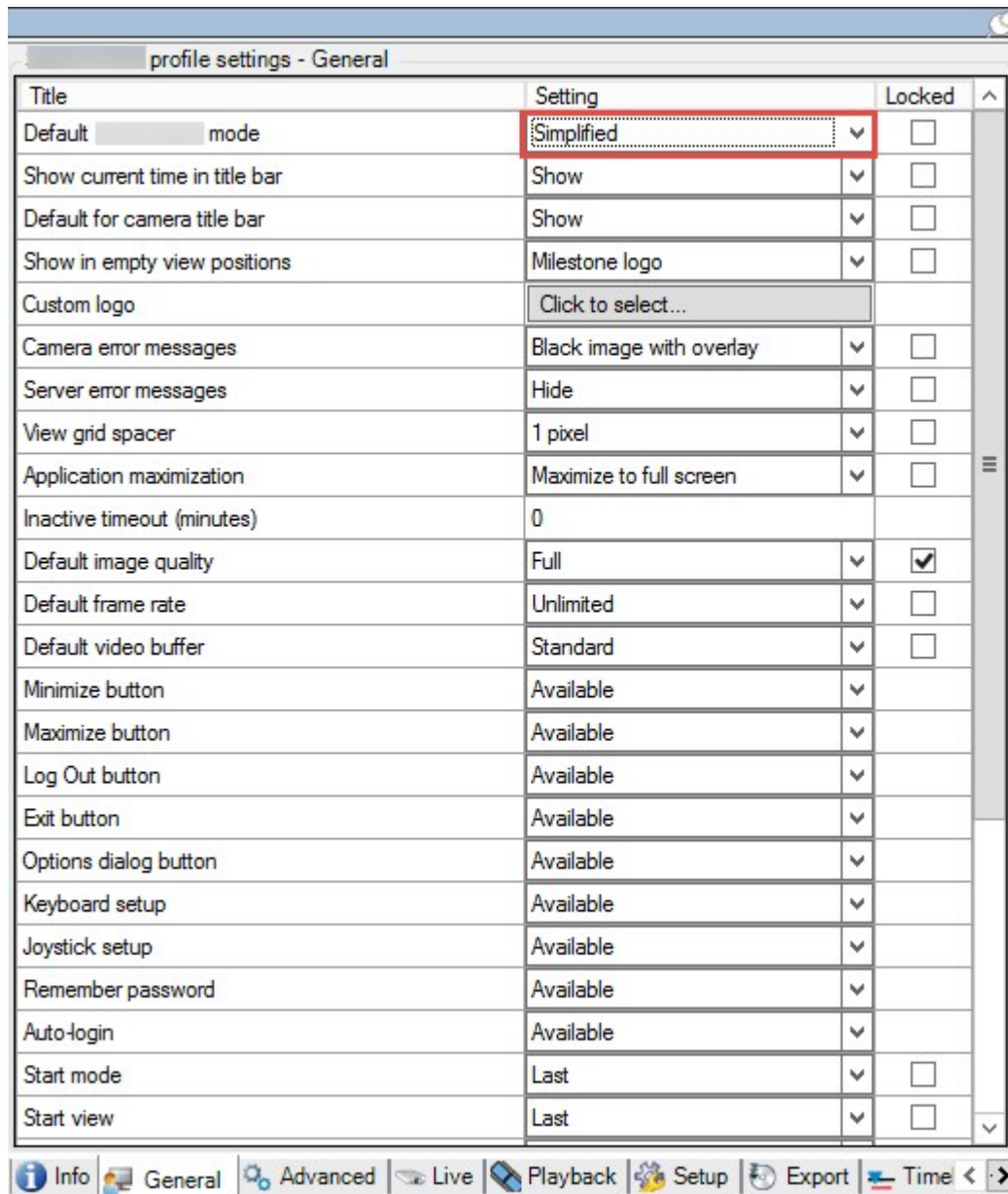
Set simplified mode as the default mode

Through the Smart Client profiles, you can configure your system to automatically open XProtect Smart Client in simplified mode with a limited set of features and tabs. By default, XProtect Smart Client opens in advanced mode with the complete set of features and tabs.



If the XProtect Smart Client operator at some point decides to switch to a different mode than the default mode, XProtect Smart Client remembers this setting the next time the operator opens the program.

1. In Management Client, expand the **Client** node.
2. Select the relevant Smart Client profile.
3. Click the **General** tab.

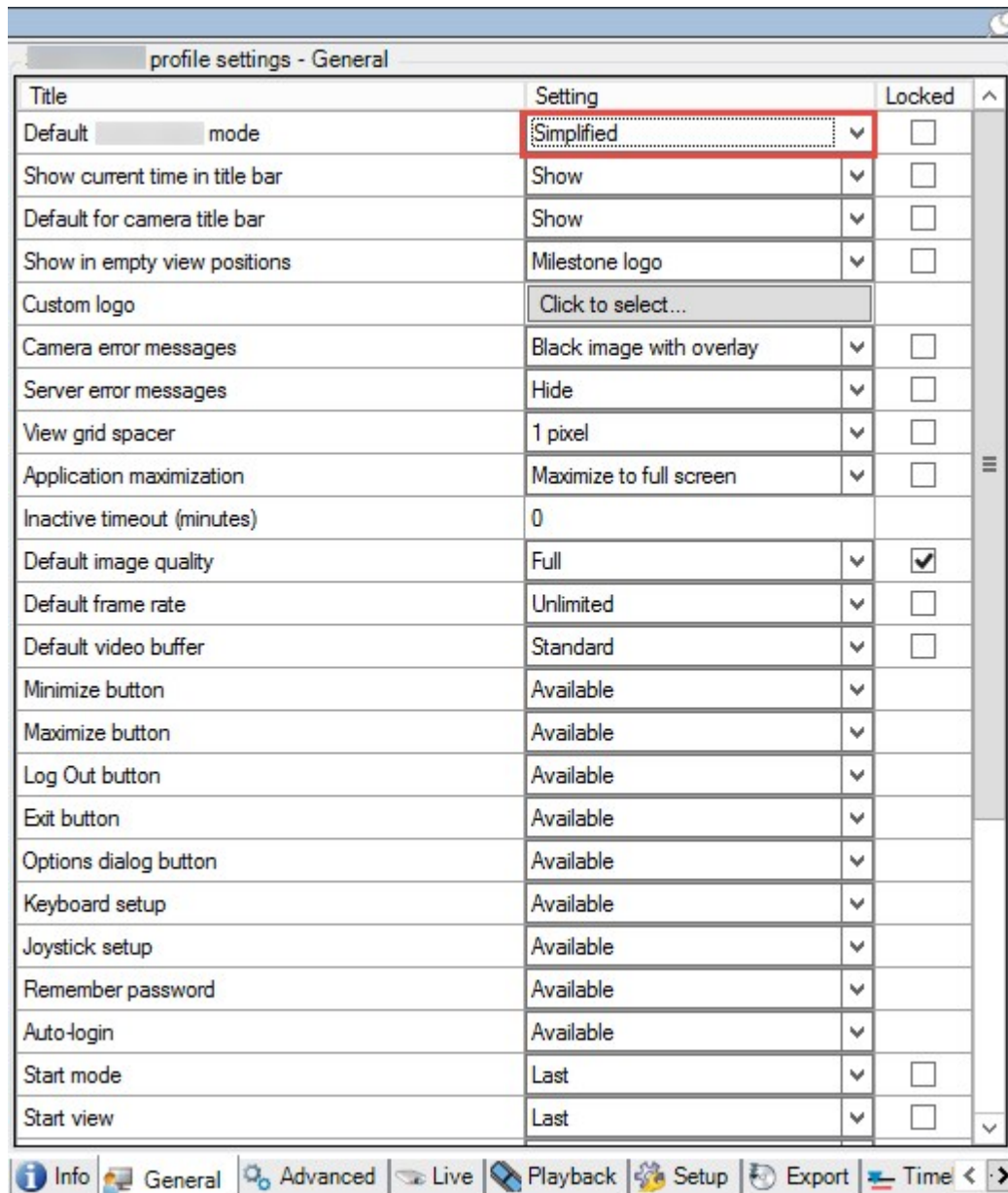


4. In the **Default Smart Client mode** list, select **Simplified**. XProtect Smart Client now opens in simplified mode for those users associated with the current Smart Client profile.

Prevent operators from switching between simple and advanced mode

In XProtect Smart Client, operators can switch between simple and advanced mode. However, you can prevent the XProtect Smart Client operators from switching between modes. Technically, you must lock the setting that determines whether XProtect Smart Client opens in simple mode or advanced mode.

1. In Management Client, expand the **Client** node.
2. Select the relevant Smart Client profile.
3. Click the **General** tab.



4. Verify that the **Default Smart Client mode** list has the proper value. If **Enabled**, XProtect Smart Client opens in simple mode.
5. Select the **Locked** check box. The mode toggling button in XProtect Smart Client is hidden.



See also, Set simplified mode as the default mode on page 261.

Smart Client profile properties

The following tabs allow you to specify the properties of each Smart Client profile. You can lock the settings in the Management Client if required, so the users of XProtect Smart Client cannot change them.


Info tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Info	<p>Name and description, priority of existing profiles and an overview of which roles use the profile.</p> <p>If a user is a member of more than one role, each with their individual Smart Client profile, the user gets the Smart Client profile with the highest priority.</p>

General tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
General	<p>Settings such as show/hide and mini- and maximize menu settings, login/-out, startup, timeout, info and messaging options, and enabling or disabling of certain tabs in XProtect Smart Client.</p> <div>  <p>If you Hide the camera error messages, there is a risk that the operator overlooks that the connection to a camera has been lost.</p> </div>

Tab	Description
	<p>The Online help setting lets you to disable the help system in XProtect Smart Client.</p> <p>The Video tutorials setting lets you disable the Video tutorials button in XProtect Smart Client. The button redirects operators to the video tutorials page: https://www.milestonesys.com/support/help-yourself/video-tutorials/</p>

Advanced tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Advanced	<p>Advanced settings such as maximum decoding threads, deinterlacing and time zone settings.</p> <p>Maximum decoding threads controls how many decoding threads are used to decode video streams. It can help improve performance on multi-core computers in live as well as playback mode. The exact performance improvement depends on the video stream. It is mainly relevant if using heavily coded high-resolution video streams like H.264/H.265, for which the performance improvement potential can be significant, and less relevant if using, for example, JPEG or MPEG-4.</p> <p>With deinterlacing, you convert video into a non-interlaced format. Interlacing determines how an image is refreshed on a screen. The image is refreshed by first scanning the odd lines in the image, then scanning the even lines. This allows a faster refresh rate because less information is processed during each scan. However, interlacing may cause flickering, or the changes in half of the image's lines may be noticeable.</p> <p>Adaptive streaming enables XProtect Smart Client to automatically select the live video streams with the best match in resolution to the streams requested by the view item. This decreases the load on the CPU and the GPU and thereby improves the decoding capability and performance of the computer. This requires multi-streaming of live video streams with different resolutions to be configured, see Streams tab (devices) on page 205.</p>

Live tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Live	Availability of live tabs/panes, camera playback and overlay buttons, bounding boxes, and live-related MIP plug-ins.

Playback tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Playback	Availability of playback tabs/panes, layout of print reports, independent playback, bookmarks, bounding boxes, and playback-related MIP plug-ins.

Setup tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Setup	Availability of general setup/panes/buttons, setup-related MIP plug-in and rights to edit a map and to edit live video buffering.

Exports tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Exports	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 tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Timeline	<p>Whether to include audio or not, visibility of indication of time and motion, and finally how to handle playback gaps.</p> <p>You can also select whether to show additional data or additional markers from other sources.</p>


Access Control tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Access Control	Select if access request notifications should pop up on the XProtect Smart Client screen when triggered by events.

Alarm Manager tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Alarm Manager	<p>Specify whether desktop notifications for alarms should be displayed on the computers where XProtect Smart Client is installed. The notifications appear only if XProtect Smart Client is running - even if minimized.</p> <div>  <p>Desktop notifications for alarms appear only when the alarms have certain priorities, for example Medium or High. To configure which alarm priorities that trigger notifications, go to Alarms > Alarm Data Settings > Alarm Data Levels. For each required alarm priority, select the Enable desktop notifications check box. See Alarm Data Settings on page 395.</p> </div>

Smart map tab (Smart Client profiles)

This tab allows you to specify the following properties:

Tab	Description
Smart map	<p>Specify settings for the smart map feature.</p> <p>You can specify whether OpenStreetMaps is available for use as a geographic background, and whether XProtect Smart Client will automatically create locations when a user adds a custom overlay to the smart map.</p> <p>You can also specify how often you want the system to delete data related to smart maps from your computer. To help XProtect Smart Client display smart map faster, the client saves map data in the cache on your computer. Over time this might slow down your computer.</p> <p>If you want to use Bing Maps or Google Maps as geographic backgrounds, enter a Bing Maps API key, or a Maps Static API key from Google.</p>

View Layout tab (Smart Client profiles)

This tab allows you to specify the following properties:

Site Navigation: Clients: Management Client profiles



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

To associate a role with a Management Client profile, see the Role Settings' Info tab (see Roles settings on page 331). Management Client profiles only handle the visual representation of system functionality, not the actual access to it. To limit the overall access to system functionality for a role, see the Role Settings' Overall Security tab (see Management ClientRoles settings on page 331).



It is important that all roles, to have access to the Management Server, enable the **Connect** security right, located in **Role Settings > Management Server > Roles settings** on page 331.

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

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



Apart from the built-in administrator role, only users associated with a role that has been granted **Manage security** permissions for the management server on the **Overall Security** tab, can add, edit, and delete Management Client profiles.

Add and configure a Management Client profile

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

1. Right-click **Management Client Profiles**.
2. Select **Add Management Client Profile**.
3. In the **Add Management Client Profile** dialog box, enter a name and description of the new profile and click **OK**.
4. In the **Overview** pane, click the profile you created to configure it.
5. On the **Profile** tab, select or clear functionality from the Management Client profile.

Copy a Management Client profile

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

1. Click **Management Client Profile**, right-click the profile in the **Overview** pane, select **Copy Management Client Profile**.
2. In the dialog box that appears, give the copied profile a new unique name and description. Click **OK**.
3. In the **Overview** pane, click the profile and go to the **Info** tab or **Profile** tab to configure the profile.

Management Client profile properties

Info tab (Management Client Profiles)

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

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

Profile tab (Management Client Profiles)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

Navigation

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

Navigation element	Description
Basics	Allows the administrator user associated with the Management Client profile to see License Information and Site Information .
Remote Connect	Allows the administrator user associated with the Management Client profile to see Axis One-click Camera Connection .

Navigation element	Description
Services	
Servers	Allows the administrator user associated with the Management Client profile to see Recording Servers and Failover Servers .
Devices	Allows the administrator user associated with the Management Client profile to see Cameras, Microphones, Speakers, Metadata, Input and Output .
Client	Allows the administrator user associated with the Management Client profile to see Smart Wall, View Groups, Smart Client Profiles, Management Client Profiles and Matrix .
Rules and Events	Allows the administrator user associated with the Management Client profile to see Rules, Time Profiles, Notification Profiles, User-defined Events, Analytics Events and Generic Events .
Security	Allows the administrator user associated with the Management Client profile to see Roles and Basic Users .
System Dashboard	Allows the administrator user associated with the Management Client profile to see System Monitor, System Monitor Thresholds, Evidence Lock, Current Tasks and Configuration Reports .
Server Logs	Allows the administrator user associated with the Management Client profile to see system, audit, and rule-triggered logs.
Access Control	Allows the administrator user associated with the Management Client profile to see Access Control features, if you have added any access control system integrations or plug-ins to your system.

Details

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

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

Tools Menu

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

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

Federated Sites

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

Site Navigation: Clients: Configuring Matrix

With Matrix, you can send video from any camera on a network operating your system to Matrix-recipients. A Matrix recipient is a computer that can display Matrix-triggered video. There are two kinds of Matrix recipients:

- computers running a dedicated Matrix application
- computers running XProtect Smart Client

To see a list of Matrix recipients configured in the Management Client, expand **Client** in the **Site Navigation** pane, then select **Matrix**. A list of Matrix configurations is displayed in the **Properties** pane.



Each Matrix recipient, regardless whether it is a computer with the Matrix Monitor or the XProtect Smart Client, must be configured to receive Matrix-triggered video. For more information, see Matrix Monitor and XProtect Smart Client.

Add Matrix recipients

To add an existing Matrix recipient, for example an existing Matrix Monitor or XProtect Smart Client installation, through the Management Client:

1. Expand **Clients**, then select **Matrix**.
2. Right-click **Matrix Configurations** and select **Add Matrix**.
3. Fill out the fields in the **Add Matrix** dialog box.
 1. In the **Address** field enter the IP address or the host name of the required Matrix recipient.
 2. In the **Port** field enter the port number used by the Matrix recipient installation. You can find the port number and password in this way: For a Matrix Monitor application, go to the Matrix Monitor **Configuration** dialog box. For XProtect Smart Client, see the XProtect Smart Client documentation.
4. Click **OK**.

You can now use the Matrix recipient in rules.



Your system does not verify that the specified port number or password is correct or that the specified port number, password, or type corresponds with the actual Matrix recipient. Make sure that you enter the correct information.

Define rules sending video to Matrix-recipients

To send video to Matrix-recipients you must include the Matrix recipient in a rule that triggers the video transmission to the related Matrix-recipient. To do so:

1. In the **Site Navigation** pane, expand **Rules and Events > Rules**. Right-click **Rules** to open the **Manage Rule** wizard. In the first step, select a rule type and in the second step, a condition.
2. In **Manage Rule**'s step 3 (**Step 3: Actions**) select the **Set Matrix to view <devices>** action.
3. Click the Matrix link in the initial rule description.
4. In the **Select Matrix Configuration** dialog box, select the relevant Matrix-recipient, and click **OK**.
5. Click the **devices** link in the initial rule description, and select from which cameras you would like to send video to the Matrix-recipient, then click **OK** to confirm your selection.
6. Click **Finish** if the rule is complete or define if required additional actions and/or a stop action.



If you delete a Matrix-recipient, any rule that includes the Matrix-recipient stops working.

Send the same video to several XProtect Smart Client views

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

1. In XProtect Smart Client, create the relevant views and Matrix positions that share the same port number and password.
2. In the Management Client, add the relevant XProtect Smart Client as a Matrix-recipient.
3. You may include the Matrix-recipient in a rule.

Site Navigation: Rules and events

This article describes how to configure events and rules to help you trigger actions and alarms in the system. It also explains how to set up email notifications and time limits on rules.

Rules and events (explained)

Rules are a central element in your system. Rules determine highly important settings, such as when cameras should record, when PTZ cameras should patrol, when notifications should be sent, etc.


Example - a rule specifying that a particular camera should begin recording when it detects motion:

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](#)

Events are central elements when using the **Manage Rule** wizard. In the wizard, events are primarily used for triggering actions. For example, you can create a rule which specifies that in the **event** of detected motion, the surveillance system should take the **action** of starting recording of video from a particular camera.

The following types of conditions can trigger rules:

Name	Description
Events	When events occur on the surveillance system, for example when motion is detected or the system receives input from external sensors.
Time interval	When you enter specific periods of time, for example: <code>Thursday 16th August 2007 from 07.00 to 07.59</code> or <code>every Saturday and Sunday</code>
Recurring time	When you set an action to be executed on a detailed, recurring schedule. For example: <ul style="list-style-type: none"> • Every week on Tuesday every 1 hour(s) between 15:00 and 15:30 • On day 15 every 3 month(s) at 11:45 • Every day every 1 hour(s) between 15:00 and 19:00 <div>  <p>The time is based on the local time settings of the server on which Management Client is installed.</p> </div> <p>For more information, see Recurring time on page 306.</p>

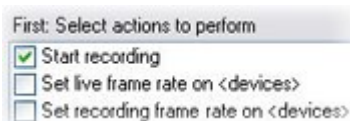
You can work with the following under **Rules and Events**:

- **Rules:** Rules are a central element in the system. The behavior of your surveillance system is to a very large extent determined by rules. When creating a rule, you can work with all types of events
- **Time profiles:** Time profiles are periods of time defined in the Management Client. You use them when you create rules in the Management Client, for example to create a rule which specifies that a certain action should take place within a certain time profile
- **Notification profiles:** You can use notification profiles to set up ready-made email notifications, which can automatically be triggered by a rule, for example when a particular event occurs
- **User-defined events:** User-defined events are custom-made events that makes it possible for users to manually trigger events in the system or react to inputs from the system
- **Analytics events:** Analytics events are data received from an external third-party video content analysis (VCA) providers. You can use analytics events as basis for alarms
- **Generic events:** Generic events allow you to trigger actions in the XProtect event server by sending simple strings via the IP network to your system

See Events overview on page 288 for a list of events.

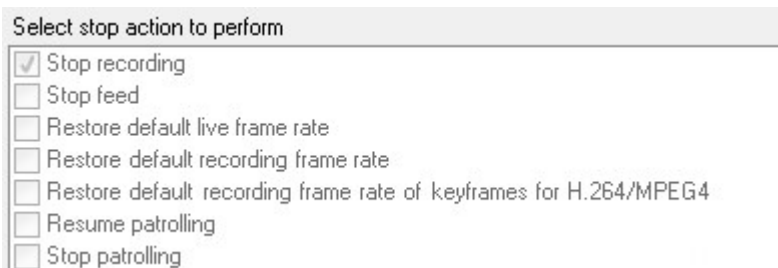
Actions and stop actions (explained)

When you add rules (see Add a rule on page 304) in the **Manage Rule** wizard, you can select between different actions:



Some of the actions require a stop action. **Example:** If you select the action **Start recording**, recording starts and potentially continues indefinitely. As a result, the action **Start recording** has a mandatory stop action called **Stop recording**.


The **Manage Rule** wizard makes sure you specify stop actions when necessary:





Selecting stop actions. In the example, note the mandatory stop action (selected, dimmed), the non-relevant stop actions (dimmed) and the optional stop actions (selectable).





Each type of action from your XProtect system is described. You may have more actions available if your system installation uses add-on products or vendor-specific plug-ins. For each type of action, stop action information is listed if relevant:


Action	Description
Start recording on <devices>	<p>Start recording and saving data in the database from the selected devices.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to specify:</p> <p>When recording should start. This happens either immediately or a number of seconds before the triggering event/beginning of the triggering time interval and on which devices the action should take place.</p> <p>This type of action requires that you have enabled recording on the devices to which the action is linked. You can only save data from before an event or time interval if you have enabled pre-buffering for the relevant devices. You enable recording and specify pre-buffering settings for a device on the Record tab.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Stop recording.</p> <p>Without this stop action, recording would potentially continue indefinitely. You also have the option of specifying further stop actions.</p>
Start feed on <devices>	<p>Begin data feed from devices to the system. When the feed from a device is started, data is transferred from the device to the system, in which case you may view and record, depending on the data type.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to specify on which devices to start the feeds. Your system includes a default rule which ensures that feeds are always started on all cameras.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Stop feed.</p> <p>You can also specify further stop actions.</p> <p>Using the mandatory stop action Stop feed to stop the feed from a device means that data is no longer transferred from the device to the system, in which case live viewing and recording of video, for example, is no longer possible. However, a device on which you have stopped the feed can still communicate with the recording server, and you can start the feed again automatically through a rule, as opposed to when you manually</p>

Action	Description
	<p>have disabled the device.</p> <div>  <p>While this type of action enables access to selected devices' data feeds, it does not guarantee that data is recorded, as you must specify recording settings separately.</p> </div>
Set <Smart Wall> to <preset>	<p>Sets the XProtect Smart Wall to a selected preset. Specify the preset on the Smart Wall Presets tab.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set <Smart Wall> <monitor> to show <cameras>	<p>Sets a specific XProtect Smart Wall monitor to display live video from the selected cameras on this site or any child site configured in Milestone Federated Architecture.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set <Smart Wall> <monitor> to show text <messages>	<p>Sets a specific XProtect Smart Wall monitor to display a user-defined text message of up to 200 characters.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Remove <cameras> from <Smart Wall> monitor <monitor>	<p>Stop displaying video from a specific camera.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set live frame rate on <devices>	<p>Sets a particular frame rate to use when the system displays live video from the selected cameras that substitutes the cameras' default frame rate. Specify this on the Settings tab.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to specify which frame rate to set, and on which devices. Always verify that the frame rate you specify is available on the relevant cameras.</p>


Action	Description
	<p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Restore default live frame rate.</p> <p>Without this stop action, the default frame rate would potentially never be restored. You also have the option of specifying further stop actions.</p>
Set recording frame rate on <devices>	<p>Sets a particular frame rate to use when the system saves recorded video from the selected cameras in the database, instead of the cameras' default recording frame rate.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to specify which recording frame rate to set, and on which cameras.</p> <p>You can only specify a recording frame rate for JPEG, a video codec with which each frame is separately compressed into a JPEG image. This type of action also requires that you have enabled recording on the cameras to which the action is linked. You enable recording for a camera on the Record tab. The maximum frame rate you can specify depends on the relevant camera types, and on their selected image resolution.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Restore default recording frame rate.</p> <p>Without this stop action, the default recording frame rate would potentially never be restored. You also have the option of specifying further stop actions.</p>
Set recording frame rate to all frames for MPEG-4/H.264/H.265 on <devices>	<p>Sets the frame rate to record all frames when the system saves recorded video from the selected cameras in the database, instead of keyframes only. Enable the recording keyframes only function on the Record tab.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to select which devices the action should apply for.</p> <p>You can only enable keyframe recording for MPEG-4/H.264/H.265. This type of action also requires that you have enabled recording on the cameras to which the action is linked. You enable recording for a camera on the Record tab.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Restore default recording frame rate of keyframes for MPEG-4/H.264/H.265</p> <p>Without this stop action, the default setting would potentially never be restored. You also have the option of specifying further stop actions.</p>


Action	Description
Start patrolling on <device> using <profile> with PTZ priority <priority>	<p>Begins PTZ patrolling according to a particular patrolling profile for a particular PTZ camera with a particular priority. This is an exact definition of how patrolling should be carried out, including the sequence of preset positions, timing settings, and more.</p> <p>If you have upgraded your system from an older version of the system, the old values (Very Low, Low, Medium, High and Very High) have been translated as follows:</p> <ul style="list-style-type: none"> • Very Low = 1000 • Low = 2000 • Medium = 3000 • High = 4000 • Very High = 5000 <p>When you select this type of action, the Manage Rule wizard prompts you to select a patrolling profile. You can only select one patrolling profile on one device and you cannot select several patrolling profiles.</p> <div>  <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> </div> <div>  <p>You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the Patrolling tab.</p> </div> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Stop patrolling</p> <p>Without this stop action, patrolling would potentially never stop. You can also specify further stop actions.</p>
Pause patrolling on <devices>	<p>Pauses PTZ patrolling. When you select this type of action, the Manage Rule wizard prompts you to specify the devices on which to pause patrolling.</p>

Action	Description
	<div>  <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> </div> <div>  <p>You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the Patrolling tab.</p> </div> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Resume patrolling</p> <p>Without this stop action, patrolling would potentially pause indefinitely. You have also the option of specifying further stop actions.</p>
Move <device> to <preset> position with PTZ priority <priority>	<p>Moves a particular camera to a particular preset position - however always according to priority. When selecting this type of action, the Manage Rule wizard prompts you to select a preset position. Only one preset position on one camera can be selected. It is not possible to select several preset positions.</p> <div>  <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> </div> <div>  <p>This action requires that you have defined at least one preset position for those devices. You define preset positions for a PTZ camera on the Presets tab.</p> </div> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Move to default preset on <devices> with	<p>Moves one or more particular cameras to their respective default preset positions - however always according to priority. When you select this type of action, the Manage Rule wizard prompts you to select which devices the action should apply for.</p>


Action	Description
PTZ priority <priority>	<div>  <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>This action requires that you have defined at least one preset position for those devices. You define preset positions for a PTZ camera on the Presets tab.</p> </div> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set device output to <state>	<p>Sets an output on a device to a particular state (activated or deactivated). When you select this type of action, the Manage Rule wizard prompts you to specify which state to set, and on which devices.</p> <p>This type of action requires that the devices to which the action is linked each have at least one external output unit connected to an output port.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Create bookmark on <device>	<p>Creates a bookmark on live streaming or recordings from a selected device. A bookmark makes it easy to retrace a certain event or period in time. Bookmark settings are controlled from the Options dialog box. When you select this type of action, the Manage Rule wizard prompts you to specify bookmark details and select devices.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Play audio <message> on <devices> with <priority>	<p>Plays back an audio message on selected devices triggered by an event. Devices are mostly speakers or cameras.</p> <p>This type of action requires that you have uploaded the message to the system on Tools > Options > Audio messages tab.</p> <p>You can create more rules to the same event and send different messages to each device, but always according to priority. The priorities that control the sequence are those set on the rule and on the device for a role on the Speech tab:</p>

Action	Description
	<ul style="list-style-type: none"> • If a message is played back and another message with the same priority is sent to the same speaker, the first message will complete and then the second one starts • If a message is played back and another message with a higher priority is sent to the same speaker, the first message is interrupted and the second one starts immediately
Send notification to <profile>	<p>Sends a notification, using a particular notification profile. When you select this type of action, the Manage Rule wizard prompts you to select a notification profile, and which devices to include pre-alarm images from. You can only select one notification profile and you cannot select several notification profiles. A single notification profile may contain several recipients.</p> <p>You can also create more rules to the same event and send different notifications to each of the notification profiles. You can copy and re-use the content of rules by right-clicking a rule in the Rules list.</p> <p>This type of action requires that you have defined at least one notification profile. Pre-alarm images are only included if you have enabled the Include images option for the relevant notification profile.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Make new <log entry>	<p>Generates an entry in the rule log. When selecting this type of action, the Manage Rule wizard prompts you to specify a text for the log entry. When you specify the log text, you can insert variables, such as \$DeviceName\$, \$EventName\$, into the log message.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Start plug-in on <devices>	<p>Starts one or more plug-ins. When you select this type of action, the Manage Rule wizard prompts you to select required plug-ins, and on which devices to start the plug-ins.</p> <p>This type of action requires that you have at least one or more plug-ins installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can</p>

Action	Description
	specify optional stop actions to be performed on either an event or after a period of time.
Stop plug-in on <devices>	<p>Stops one or more plug-ins. When you select this type of action, the Manage Rule wizard prompts you to select required plug-ins, and on which devices to stop the plug-ins.</p> <p>This type of action requires that you have at least one or more plug-ins installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Apply new settings on <devices>	<p>Changes device settings on one or more devices. When you select this type of action, the Manage Rule wizard prompts you to select relevant devices, and you can define the relevant settings on the devices you have specified.</p> <div>  <p>If you define settings for more than one device, you can only change settings that are available for all of the specified devices.</p> </div> <p>Example: You specify that the action should be linked to Device 1 and Device 2. Device 1 has the settings A, B and C, and Device 2 has the settings B, C and D. In this case, you can only change the settings that are available for both devices, namely settings B and C.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set Matrix to view <devices>	<p>Makes video from the selected cameras appear on a computer capable of displaying Matrix-triggered video such as a computer on which you have installed either XProtect Smart Client or the Matrix Monitor application.</p> <p>When you select this type of action, the Manage Rule wizard prompts you to select a Matrix recipient, and one or more devices from which to display video on the selected Matrix recipient.</p> <p>This type of action allows you to select only a single Matrix recipient at a time. If you want to make video from the selected devices appear on more than one Matrix recipient, you should create a rule for each required Matrix recipient or use the</p>

Action	Description
	<p>XProtect Smart Wall feature. By right-clicking a rule in the Rules list, you can copy and re-use the content of rules. This way, you can avoid having to create near-identical rules from scratch.</p> <div>  <p>As part of the configuration on the Matrix recipients themselves, users must specify the port number and password required for the Matrix communication. Make sure that the users have access to this information. The users must typically also define the IP addresses of allowed hosts from which commands regarding display of Matrix-triggered video is accepted. In that case, the users must also know the IP address of the management server, or any router or firewall used.</p> </div>
Send SNMP trap	<p>Generates a small message which logs events on selected devices. The text of SNMP traps is auto-generated and cannot be customized. It can contain the source type and name of the device on which the event occurred.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Retrieve and store remote recordings from <devices>	<p>Retrieves and stores remote recordings from selected devices (that support edge recording) in a specified period before and after the triggering event.</p> <p>This rule is independent of the Automatically retrieve remote recordings when connection is restored setting.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Retrieve and store remote recordings between <start and end time> from <devices>	<p>Retrieves and stores remote recordings in a specified period from selected devices (that support edge recording).</p> <p>This rule is independent of the Automatically retrieve remote recordings when connection is restored setting.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>

Action	Description
Save attached image	<p>Ensures that when an image is received from the Images Received event (sent via SMTP email from a camera), it is saved for future usage. In future, other events can possibly also trigger this action.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Activate archiving on <archives>	<p>Starts archiving on one or more archives. When you select this type of action, the Manage Rule wizard prompts you to select relevant archives.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
On <site> trigger <user-defined event>	<p>Relevant mostly within Milestone Federated Architecture, but you can also use this in a single site setup. Use the rule to trigger a user-defined event on a site, normally a remote site within a federated hierarchy.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Show <access request notification>	<p>Lets you access request notifications pop up on the XProtect Smart Client screen when the criteria for the triggering events are met. Milestone recommends that you use access control events as triggering events for this action, because access request notifications typically are configured for operating on related access control commands and cameras.</p> <p>This type of action requires that you have at least one access control plug-in installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set <camera> to <rule-based DLNA channel>	<p>Cameras are assigned to the rule-based DLNA channel based on events. This type of action requires that you have a DLNA server installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>

Action	Description
Remove <camera> from <rule-based DLNA channel>	<p>Cameras are removed from the rule-based DLNA channel based on events. This type of action requires that you have a DLNA server installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Remove current camera from <rule-based DLNA channel>	<p>The camera with the active stream is removed from the rule-based DLNA channel based on events. This type of action requires that you have a DLNA server installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Change the password on hardware devices	<p>Changes the password of selected hardware devices to a randomly-generated password based on the password requirements for that specific hardware device. For a list of supported hardware devices, see https://www.milestonesys.com/community/business-partner-tools/supported-devices/.</p> <div>  <p>This action is only available when you set up a rule using the Perform an action on a <recurring time> rule type.</p> </div> <p>The following events are available for the action:</p> <ul style="list-style-type: none"> • Scheduled password change started on page 298 • Scheduled password change completed successfully on page 298 • Scheduled password change completed with errors on page 298 <p>This type of action does not have a stop action.</p> <p>You can view the progress of this action in the Current Tasks node. For more information, see Current tasks (explained) on page 382.</p> <p>To view the action results - go to the Server Logs node, on the System logs tab. For more information, see Server Logs tab (options) on page 111.</p> <p>For more information, see System logs (properties) on page 386.</p>

Events overview

When you add an event-based rule in the **Manage Rule** wizard, you can select between a number of different event types. In order for you to get a good overview, events you can select are listed in groups according to whether they are:

Hardware:

Some hardware is capable of creating events themselves, for example to detect motion. You can use these as events but you must configure them on the hardware before you can use them in the system. You may only be able to use the events listed on some hardware as not all types of cameras can detect tampering or temperature changes.

Hardware - Configurable events:

Configurable events from hardware are automatically imported from device drivers. This means that they vary from hardware to hardware and are not documented here. Configurable events are not triggered until you have added them to the system and configured them on the **Event** tab for hardware. Some of the configurable events also require that you configure the camera (hardware) itself.

Hardware - Predefined events:

Event	Description
Communication Error (Hardware)	Occurs when a connection to the hardware is lost.
Communication Started (Hardware)	Occurs when communication with the hardware is successfully established.
Communication Stopped (Hardware)	Occurs when communication with the hardware is successfully stopped.

Devices - Configurable events:

Configurable events from devices are automatically imported from device drivers. This means that they vary from device to device and are not documented here. Configurable events are not triggered until you have added them to the system and configured them on the **Event** tab on a device.

Devices - Predefined events:

Event	Description
Bookmark Reference Requested	Occurs when a bookmark is made in live or playback mode in the clients. Also, a requirement for using the Default record on bookmark rule.
Communication Error (Device)	Occurs when a connection to a device is lost, or when an attempt is made to communicate with a device, and the attempt is unsuccessful.
Communication Started (Device)	Occurs when communication with a device is successfully established.
Communication Stopped (Device)	Occurs when communication with a device is successfully stopped.
Evidence Lock Changed	Occurs when an evidence lock is changed for devices by a client user or via the MIP SDK.
Evidence Locked	Occurs when an evidence lock is created for devices by a client user or via the MIP SDK.
Evidence Unlocked	Occurs when an evidence lock is removed for devices by a client user or via the MIP SDK.
Feed Overflow Started	<p>Feed overflow (media overflow) occurs when a recording server cannot process received data as quickly as specified in the configuration and therefore is forced to discard some recordings.</p> <p>If the server is healthy, feed overflow usually happens because of slow disk writes. You can resolve this either by reducing the amount of data written, or by improving the storage system's performance. Reduce the amount of written data by reducing frame rates, resolution or image quality on your cameras, but this may degrade recording quality. If you are not interested in that, instead improve your storage system's performance by installing extra drives to share the load or by installing faster disks or controllers.</p> <p>You can use this event to trigger actions that helps you avoid the problem, for example, to</p>

Event	Description
	lower the recording frame rate.
Feed Overflow Stopped	Occurs when feed overflow (see description of the Feed Overflow Started event) ends.
Live Client Feed Requested	Occurs when client users request a live stream from a device. The event occurs upon the request even if the client user's request later turns out to be unsuccessful, for example because the client user does not have the rights required for viewing the requested live feed or because the feed is for some reason stopped.
Live Client Feed Terminated	Occurs when client users no longer request a live stream from a device.
Manual Recording Started	Occurs when a client user starts a recording session for a camera. The event is triggered even if the device is already recording via rule actions.
Manual Recording Stopped	Occurs when a client user stops a recording session for a camera. If the rule system also has started a recording session it continues recording even after the manual recording is stopped.
Marked Data Reference Requested	Occurs when an evidence lock is made in playback mode in the clients or via the MIP SDK. An event is created that you can use in your rules.
Motion Started	Occurs when the system detects motion in video received from cameras. This type of event requires that the system's motion detection is enabled for the cameras to which the event is linked. In addition to the system's motion detection, some cameras can detect motion themselves and trigger the Motion Started (HW) event, but it depends on the configuration of the camera hardware and in the system. See Hardware - Configurable events above.
Motion Stopped	Occurs when motion is no longer detected in received video. See also the description of the Motion Started event. This type of event requires that the system's motion detection is enabled for the cameras

Event	Description
	<p>to which the event is linked.</p> <p>In addition to the system's motion detection, some cameras can detect motion themselves and trigger the Motion Stopped (HW) event, but it depends on the configuration of the camera hardware and in the system. See Hardware - Configurable events above.</p>
Output Activated	<p>Occurs when an external output port on a device is activated.</p> <p>This type of event requires that at least one device on your system supports output ports.</p>
Output Changed	<p>Occurs when the state of an external output port on a device is changed.</p> <p>This type of event requires that at least one device on your system supports output ports.</p>
Output Deactivated	<p>Occurs when an external output port on a device is deactivated.</p> <p>This type of event requires that at least one device on your system supports output ports.</p>
PTZ Manual Session Started	<p>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.</p> <p>This type of event requires that the cameras to which the event is linked are PTZ cameras.</p>
PTZ Manual Session Stopped	<p>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.</p> <p>This type of event requires that the cameras to which the event is linked are PTZ cameras.</p>
Recording Started	Occurs whenever recording is started. There is a separate event for manual recording started.
Recording Stopped	Occurs whenever recording is stopped. There is a separate event for manual recording stopped.
Settings Changed	Occurs when settings on a device are successfully changed.
Settings Changed Error	Occurs when an attempt is made to change settings on a device, and the attempt is unsuccessful.

External events - Predefined events:

Event	Description
Request Play Audio Message	Activated when play audio messages are requested via the MIP SDK. Through the MIP SDK a third-party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) for your system.
Request Start Recording	Activated when start recordings are requested via the MIP SDK. Through the MIP SDK a third-party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) for your system.
Request Stop Recording	Activated when stop recordings are requested via the MIP SDK. Through the MIP SDK a third party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) for your system.

External events - Generic events:

Generic events allow you to trigger actions in the system by sending simple strings via the IP network to the system. The purpose of generic events is to allow as many external sources as possible to interact with the system.

External events - User-defined events:

A number of events custom made to suit your system may also be selectable. You can use such user-defined events for:

- Making it possible for client users to manually trigger events while viewing live video in the clients
- Countless other purposes. For example, you may create user-defined events which occur if a particular type of data is received from a device

See User-defined events (explained) on page 315 for more information

Recording servers:

Event	Description
Archive Available	Occurs when an archive for a recording server becomes available after having been unavailable (see Archive Unavailable).
Archive Unavailable	<p>Occurs when an archive for a recording server becomes unavailable, for example if the connection to an archive located on a network drive is lost. In such cases, you cannot archive recordings.</p> <p>You can use the event to, for example, trigger an alarm or a notification profile so that an email notification is automatically sent to relevant people in your organization.</p>
Archive Not Finished	Occurs when an archive for a recording server is not finished with the last archiving round when the next is scheduled to start.
Database Deleting Recordings Before Set Retention Size	Occurs when the retention time limit is reached before the database size limit.
Database Deleting Recordings Before Set Retention Time	Occurs when database size limit is reached before the retention time limit.
Database Disk Full - Auto Archiving	<p>Occurs when a database disk is full. A database disk is considered to be full when there is less than 5GB of space is left on the disk:</p> <p>The oldest data in a database is always auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free.</p>
Database Disk Full - Deleting	Occurs when a database disk is full and less than 1GB space is free. Data is deleted even if a next archive is defined. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data is written to the database until enough space has been freed. The actual maximum size of your database is the number of gigabytes you specify, minus 5GB.
Database Full - Auto Archiving	Occurs when an archive for a recording server is full and needs to auto-archive to an archive in the storage.

Event	Description
Database Repair	Occurs if a database becomes corrupted, in which case the system automatically attempts two different database repair methods: a fast repair and a thorough repair.
Database Storage Available	Occurs when a storage for a recording server becomes available after having been unavailable (see Database Storage Unavailable). You can, for example, use the event to start recording if it has been stopped by a Database Storage Unavailable event.
Database Storage Unavailable	Occurs when a storage for a recording server becomes unavailable, for example if the connection to a storage located on a network drive is lost. In such cases, you cannot archive recordings. You can use the event to, for example, stop recording, trigger an alarm or a notification profile so an e-mail notification is automatically sent to relevant people in your organization.
Failover encrypted communication error	Occurs when there is an SSL communication error between the failover server and monitored recording servers.
Failover Started	Occurs when a failover recording server takes over from a recording server. See Failover recording servers (explained) on page 165.
Failover Stopped	Occurs when a recording server becomes available again, and can take over from a failover recording server.

System monitor events

System monitor events are triggered by exceeded thresholds values configured in the **System Monitor Thresholds** (see System monitor thresholds (explained) on page 376) node.



This functionality requires that the Data Collector service is running.

System Monitor - Server:

Event	Description
CPU usage critical	Occurs when the CPU usage exceeds the critical CPU threshold.
CPU usage normal	Occurs when the CPU usage falls back below the warning CPU threshold.
CPU usage warning	Occurs when the CPU usage exceeds the warning CPU threshold or falls back below the critical CPU threshold.
Memory usage critical	Occurs when the memory usage exceeds the critical memory threshold.
Memory usage normal	Occurs when the memory usage falls back below the warning memory threshold.
Memory usage warning	Occurs when the memory usage exceeds the warning memory threshold or falls back below the critical memory usage threshold.
NVIDIA decoding critical	Occurs when the NVIDIA decoding usage exceeds the critical NVIDIA decoding threshold.
NVIDIA decoding normal	Occurs when the NVIDIA decoding usage falls back below the warning NVIDIA decoding threshold.
NVIDIA decoding warning	Occurs when the NVIDIA decoding usage exceeds the warning NVIDIA decoding threshold or falls back below the critical NVIDIA decoding threshold.
NVIDIA memory critical	Occurs when the NVIDIA memory usage exceeds the critical NVIDIA memory threshold.
NVIDIA memory normal	Occurs when the NVIDIA memory usage falls back below the warning NVIDIA memory threshold.
NVIDIA memory warning	Occurs when the NVIDIA memory usage exceeds the warning NVIDIA memory threshold or falls back below the critical NVIDIA memory threshold.
NVIDIA rendering	Occurs when the NVIDIA rendering usage exceeds the critical NVIDIA rendering

Event	Description
critical	threshold.
NVIDIA rendering normal	Occurs when the NVIDIA rendering usage falls back below the warning NVIDIA rendering threshold.
NVIDIA rendering warning	Occurs when the NVIDIA rendering usage exceeds the warning NVIDIA rendering threshold or falls back below the critical NVIDIA rendering threshold.
Service available critical	Occurs when a server service stops running. There are no threshold values for this event.
Service available normal	Occurs when a server service status changes to running. There are no threshold values for this event.

System Monitor - Camera:

Event	Description
Live FPS critical	Occurs when the live FPS rate falls below the critical live FPS threshold.
Live FPS normal	Occurs when the live FPS rate exceeds the warning live FPS threshold.
Live FPS warning	Occurs when the live FPS rate falls below the warning live FPS threshold or exceeds the critical live FPS threshold.
Recording FPS critical	Occurs when the recording FPS rate falls below the critical recording FPS threshold.
Recording FPS normal	Occurs when the recording FPS rate exceeds the warning recording FPS threshold.
Recording FPS warning	Occurs when the recording FPS rate falls below the warning recording FPS threshold or exceeds the critical recording FPS threshold.
Used space critical	Occurs when the storage used for recordings by a specific camera exceeds the critical used space threshold.

Event	Description
Used space normal	Occurs when the storage used for recordings by a specific camera falls back below the warning used space threshold.
Used space warning	Occurs when the storage used for recordings by a specific camera exceeds the warning used space threshold or falls back below the critical used space threshold.

System Monitor - Disk:

Event	Description
Free space critical	Occurs when the disk space usage exceeds the critical free space threshold.
Free space normal	Occurs when the disk space usage falls below the warning free space threshold.
Free space warning	Occurs when the disk space usage exceeds the warning free space threshold or falls back below the critical free space threshold.

System Monitor - Storage:

Event	Description
Retention time critical	Occurs when the system predicts that the storage will be filled up faster than the critical retention time threshold value. For example, when data from video streams is filling up the storage faster than expected.
Retention time normal	Occurs when the system predicts that the storage will be filled up slower than the warning retention time threshold value. For example, when data from video streams is filling up the storage at the expected rate.
Retention time warning	Occurs when the system predicts that the storage will be filled up faster than the warning retention time threshold value or slower than the critical retention time threshold value. For example, when data from video streams is filling up the storage faster than expected due to more motion detected by the cameras configured to record on motion.

Other:

Event	Description
Automatic license activation failed	Occurs when online automatic license activation fails. There are no thresholds values for this event.
Scheduled password change started	Occurs when a scheduled password change starts.
Scheduled password change completed successfully	Occurs when a scheduled password change completes without errors.
Scheduled password change completed with errors	Occurs when a scheduled password change completes with errors..

Events from add-on products and integrations:

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

- Analytics events can also be used in the rule system

Rules

Rules (explained)

Rules specify actions to carry out under particular conditions. Example: When motion is detected (condition), a camera should begin recording (action).

The following are **examples** of what you can do with rules:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording frame rate
- Start and stop PTZ patrolling
- Pause and resume PTZ patrolling
- Move PTZ cameras to specific positions
- Set output to activated/deactivated state
- Send notifications via e-mail

- Generate log entries
- Generate events
- Apply new device settings, for example a different resolution on a camera
- Make video appear in Matrix recipients
- Start and stop plug-ins
- Start and stop feeds from devices

Stopping a device means that video is no longer transferred from the device to the system, in which case you cannot view live video nor record video. In contrast, a device on which you have stopped the feed can still communicate with the recording server, and you can start the feed from the device automatically through a rule, as opposed to when the device is manually disabled in the Management Client.



Some rule content may require that certain features are enabled for the relevant devices. For example, a rule specifying that a camera should record does not work as intended if recording is not enabled for the relevant camera. Before creating a rule, Milestone recommends that you verify that the devices involved can perform as intended.

Default rules (explained)

Your system includes a number of default rules that you can use for basic features without setting anything up. You can deactivate or modify the default rules as you need. If you modify or deactivate the default rules, your system may not work as desired nor guarantee that video feeds or audio feeds are automatically fed to the system.

Default rule	Description
Go to Preset when PTZ is done	<p>Ensures that PTZ cameras go to their respective default preset positions after you have operated them manually. This rule is not enabled by default.</p> <p>Even when you have enabled the rule, you must have defined default preset positions for the relevant PTZ cameras in order for the rule to work. You do this on the Presets tab.</p>
Play Audio on Request	<p>Ensures that video is recorded automatically when an external request occurs.</p> <p>The request is always triggered by a system integrating externally with your system, and the rule is primarily used by integrators of external systems or plug-ins.</p>

Default rule	Description
Record on Bookmark	<p>Ensures that video is recorded automatically when an operator sets a bookmark in XProtect Smart Client. This is provided you have enabled recording for the relevant cameras. Recording is enabled by default.</p> <p>The default recording time for this rule is three seconds before the bookmark is set and 30 seconds after the bookmark is set. You can edit the default recording times in the rule. The pre-buffer which you set on the Record Tab must match or be longer than the pre-recording time.</p>
Record on Motion	<p>Ensures that as long as motion is detected in video from cameras, the video is recorded, provided recording is enabled for the relevant cameras. Recording is by default enabled.</p> <p>While the default rule specifies recording based on detected motion, it does not guarantee that the system records video, as you may have disabled individual cameras' recording for one or more cameras. Even when you have enabled recording, remember that the quality of recordings may be affected by individual camera's recording settings.</p>
Record on Request	<p>Ensures that video is recorded automatically when an external request occurs, provided recording is enabled for the relevant cameras. Recording is enabled by default.</p> <p>The request is always triggered by a system integrating externally with your system, and the rule is primarily used by integrators of external systems or plug-ins.</p>
Start Audio Feed	<p>Ensures that audio feeds from all connected microphones and speakers are automatically fed to the system.</p> <p>While the default rule enables access to connected microphones' and speakers' audio feeds immediately upon installing the system, it does not guarantee that audio is recorded, as you must specify recording settings separately.</p>
Start Feed	<p>Ensures that video feeds from all connected cameras are automatically fed to the system.</p> <p>While the default rule enables access to connected cameras' video feeds immediately upon installing the system, it does not guarantee that video is recorded, as cameras' recording settings must be specified separately.</p>
Start Metadata Feed	<p>Ensures that data feeds from all connected cameras are automatically fed to the system.</p> <p>While the default rule enables access to connected cameras' data feeds immediately upon installing the system, it does not guarantee that data is recorded, as cameras' recording settings must be specified separately.</p>

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

Recreate default rules

If you accidentally delete any of the default rules, you can recreate them by entering the following content:

Default rule	Text to enter
Goto preset when PTZ is done	Perform an action on PTZ Manual Session Stopped from All Cameras Move immediately to default preset on the device on which event occurred
Play Audio on Request	Perform an action on Request Play Audio Message from External Play audio message message from metadata on the devices from metadata with priority 1
Record on Bookmark	Perform an action on Bookmark Reference Requested from All Cameras, All Microphones, All Speakers start recording three seconds before on the device on which event occurred Perform action 30 seconds after stop recording immediately
Record on Motion	Perform an action on Motion Started from All Cameras start recording three seconds before on the device on which event occurred Perform stop action on Motion Stopped from All Cameras stop recording three seconds after
Record on Request	Perform an action on Request Start Recording from External start recording immediately on the devices from metadata Perform stop action on Request Stop Recording from External stop recording immediately
Start Audio Feed	Perform an action in a time interval always start feed on All Microphones, All Speakers

Default rule	Text to enter
	Perform an action when time interval ends stop feed immediately
Start Feed	Perform an action in a time interval always start feed on All Cameras Perform an action when time interval ends stop feed immediately
Start Metadata Feed	Perform an action in a time interval always start feed on All Metadata Perform an action when time interval ends stop feed immediately
Show Access Request Notification	Perform an action on Access request (Access Control Categories) from Systems [+ units] Show built-in access request notification

Rule complexity (explained)

Your exact number of options depends on the type of rule you want to create, and on the number of devices available on your system. Rules provide a high degree of flexibility: you can combine event and time conditions, specify several actions in a single rule, and very often create rules covering several or all of the devices on your system.

You can make your rules as simple or complex as required. For example, you can create very simple time-based rules:

Example	Explanation
Very Simple Time-Based Rule	On Mondays between 08.30 and 11.30 (time condition), Camera 1 and Camera 2 should start recording (action) when the time period begins and stop recording (stop action) when the time period ends.
Very Simple Event-Based Rule	When motion is detected (event condition) on Camera 1, Camera 1 should start recording (action) immediately, then stop recording (stop action) after 10 seconds. Even if an event-based rule is activated by an event on one device, you can specify that actions should take place on one or more other devices.

Example	Explanation
Rule Involving Several Devices	When motion is detected (event condition) on Camera 1, Camera 2 should start recording (action) immediately, and the siren connected to Output 3 should sound (action) immediately. Then, after 60 seconds, Camera 2 should stop recording (stop action), and the siren connected to Output 3 should stop sounding (stop action).
Rule Combining Time, Events, and Devices	When motion is detected (event condition) on Camera 1, and the day of the week is Saturday or Sunday (time condition), Camera 1 and Camera 2 should start recording (action) immediately, and a notification should be sent to the security manager (action). Then, 5 seconds after motion is no longer detected on Camera 1 or Camera 2, the 2 cameras should stop recording (stop action).

Depending on your organization's needs, it is often a good idea to create many simple rules rather than a few complex rules. Even if it means you have more rules in your system, it provides an easy way to maintain an overview of what your rules do. Keeping your rules simple also means that you have much more flexibility when it comes to deactivating/activating individual rule elements. With simple rules, you can deactivate/activate entire rules when required.

Validating rules (explained)

You can validate the content of an individual rule or all rules in one go. When you create a rule, the **Manage Rule** wizard ensures that all of the rule's elements make sense. When a rule has existed for some time, one or more of the rule's elements may have been affected by other configuration, and the rule may no longer work. For example, if a rule is triggered by a particular time profile, the rule does not work if you have deleted that time profile or if you no longer have permissions to it. Such unintended effects of configuration may be hard to keep an overview of.

Rule validation helps you keep track of which rules have been affected. Validation takes place on a per-rule basis and each rule is validated by themselves. You cannot validate rules against each other, for example in order to see whether one rule conflicts with another rule, not even if you use the **Validate All Rules** feature.



You cannot validate whether configuration of requirements 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 is validated if the elements in the rule itself are correct, even if motion detection, which is enabled on a camera level, not through rules, has not been enabled for the relevant camera.

You validate an individual rule or all rules in one go by right-clicking the rule you want to validate and select **Validate Rule** or **Validate All Rules**. A dialog box informs you whether the rule(s) validated successfully or not. If you chose to validate more than one rule and one or more rules did not succeed, the dialog box lists the names of the affected rules.



Add a rule

When you create rules, you are guided by the wizard **Manage Rule** which only lists relevant options.

It ensures that a rule does not contain missing elements. Based on your rule's content, it automatically suggests suitable stop actions, that is what should take place when the rule no longer applies, ensuring that you do not unintentionally create a never-ending rule.

1. Right-click the **Rules** item > **Add Rule**. This opens the **Manage Rule** wizard. The wizard guides you through specifying the content of your rule.
2. Specifying a name and a description of the new rule in the **Name** and **Description** fields respectively.
3. Select the relevant type of condition for the rule: either a rule which performs one or more actions when a particular event occurs, or a rule which performs one or more actions when you enter a specific period of time.
4. Click **Next** to go to the wizard's second step. On the wizard's second step, define further conditions for the rule.

5. Select one or more conditions, for example **Day of week is <day>**:



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



Click the underlined items in **bold italics** to specify their exact content. For example, clicking the **days** link in our example lets you select one or more days of the week on which the rule should apply.

6. Having specified your exact conditions, click **Next** to move to the next step of the wizard and select which actions the rule should cover. Depending on the content and complexity of your rule, you may need to define more steps, such as stop events and stop actions. For example, if a rule specifies that a device should perform a particular action during a time interval (for example, Thursday between 08.00 and 10.30), the wizard may ask you to specify what should happen when that time interval ends.
7. Your rule is by default active once you have created it if the rule's conditions are met. If you do not want the rule to be active straight away, clear the **Active** check box.
8. Click **Finish**.

Edit, copy and rename a rule

1. In the **Overview** pane, right-click the relevant rule.
2. Select either:
Edit Rule or **Copy Rule** or **Rename Rule**. The wizard **Manage Rule** opens.
3. In the wizard, rename and/or change the rule. If you selected **Copy Rule**, the wizard opens, displaying a copy of the selected rule.
4. Click **Finish**.

Deactivate and activate a rule

Your system applies a rule as soon as the rule's conditions apply which means it is active. If you do not want a rule to be active, you can deactivate the rule. When you deactivate the rule, the system does not apply the rule even if the rule's conditions apply. You can easily activate a deactivated rule later.

Deactivating a rule

1. In the **Overview** pane, select the rule.
2. Clear the **Active** check box in the **Properties** pane.
3. Click **Save** in the toolbar.
4. An icon with a red x indicates that the rule is deactivated in the **Rules** list:



Activating a rule

When you want to activate the rule again, select the rule, select the **Activate** check box, and save the setting.

Recurring time

When you set an action to be executed on a detailed, recurring schedule.

For example:

- Every week on Tuesday every 1 hour(s) between 15:00 and 15:30
- On day 15 every 3 month(s) at 11:45
- Every day every 1 hour(s) between 15:00 and 19:00



The time is based on the local time settings of the server on which Management Client is installed.

Optionally, you can select a time profile to ensure that the rule is executed only inside, or outside of that time profile interval.

For general instructions on how to set up a new rule, see Rules on page 298.

For information about time profiles, see Time profiles on page 306.

Time profiles

Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

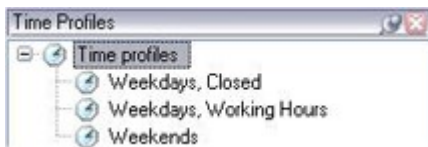
Time profiles are periods of time defined by the administrator. You can use time profiles when creating rules, for example, a rule specifying that a certain action should take place within a certain time period.

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

Time profiles are highly flexible: you can base them on one or more single periods of time, on one or more recurring periods of time, or a combination of single and recurring times. Many users may be familiar with the concepts of single and recurring time periods from calendar applications, such as the one in Microsoft® Outlook.

Time profiles always apply in local time. This means that if your system has recording servers placed in different time zones, any actions, for example recording on cameras, associated with time profiles are carried out in each recording server's local time. Example: If you have a time profile covering the period from 08.30 to 09.30, any associated actions on a recording server placed in New York is carried out when the local time is 08.30 to 09.30 in New York, while the same actions on a recording server placed in Los Angeles is carried out some hours later, when the local time is 08.30 to 09.30 in Los Angeles.

You create and manage time profiles by expanding **Rules and Events > Time Profiles**. A **Time Profiles** list opens. Example only:



For an alternative to time profiles, see Day length time profiles (explained) on page 309.

Specify a time profile

1. In the **Time Profiles** list, right-click **Time Profiles > Add Time Profile**. This opens the **Time Profile** window.
2. In the **Time Profile** window, enter a name for the new time profile in the **Name** field. Optionally, enter 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 Recurring Time**.
4. When you have specified the time periods for your time profile, click **OK** in the **Time Profile** window. Your system adds your new time profile to the **Time Profiles** list. If at a later stage you wish to edit or delete the time profile, you do that from the **Time Profiles** list as well.

Add a single time

When you select **Add Single Time**, the **Select Time** window appears:

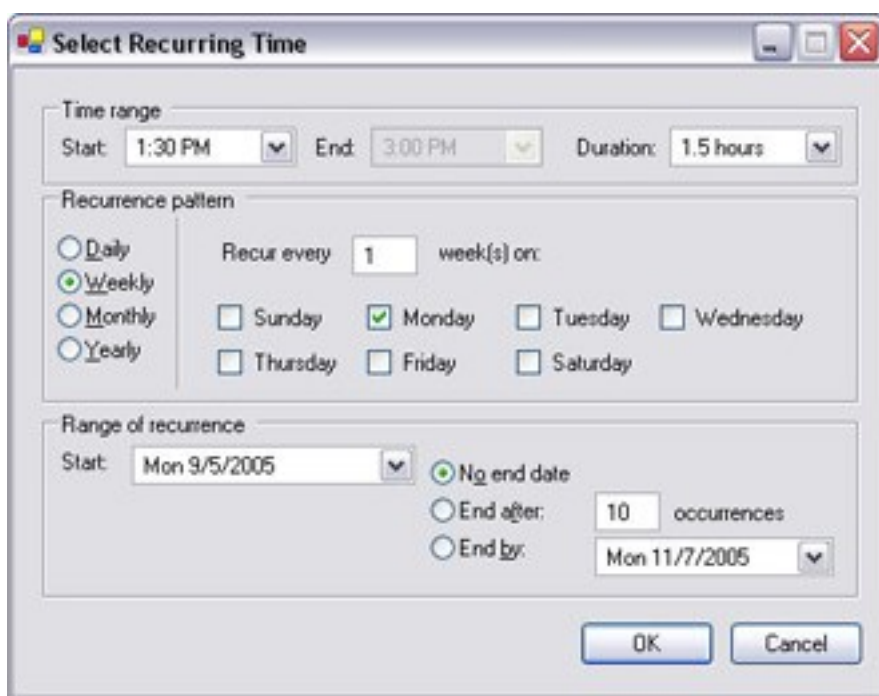


Time and date format may be different on your system.

1. In the **Select Time** window, specify **Start time** and **End time**. If the time is to cover whole days, select the **All day event** box.
2. Click **OK**.

Specify a recurring time

When you select **Add Recurring Time**, the **Select Recurring Time** window appears:



1. In the **Select Time** window, specify time range, recurrence pattern and range of recurrence.
2. Click **OK**.



A time profile can contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.

Edit a time profile

1. In the **Overview** pane's **Time Profiles** list, right-click the relevant time profile, and select **Edit Time Profile**. This opens the **Time Profile** window.
2. Edit the time profile as needed. If you have made changes to the time profile, click **OK** in the **Time Profile** window. You return to the **Time Profiles** list.



In the **Time Profile Information** window, you can edit the time profile as needed.

Remember that a time profile may contain more than one time period, and that time periods may be recurring. The small month overview in the top right corner can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold.



In this example, the bold dates indicate that you have specified time periods on several days, and that you have specified a recurring time on Mondays.

Day length time profiles (explained)

When you place cameras outside, you must often lower the camera resolution, enable black/white or change other settings when it gets dark or when it gets light. The further north or south from the equator the cameras are placed, the more the sunrise and sunset time varies during the year. This makes it impossible to use normal fixed time profiles to adjust camera settings according to light conditions.

In such situations, you can create day length time profiles instead to define the sunrise and sunset in a specified geographical area. Via geographic coordinates, the system calculates the sunrise and sunset time, even incorporating daylight saving time on a daily basis. As a result, the time profile automatically follows the yearly changes in sunrise/sunset in the selected area, ensuring the profile to be active only when needed. All times and dates are based on the management server's time and date settings. You can also set a positive or negative offset (in minutes) for the start (sunrise) and end time (sunset). The offset for the start and the end time can be identical or different.

You can use day length profiles both when you create rules and roles.

Create a day length time profile

1. Expand the **Rules and Events** folder > **Time Profiles**.
2. In the **Time Profiles** list, right-click **Time Profiles**, and select **Add Day Length Time Profile**.
3. In the **Day Length Time Profile** window, fill in the needed information. To deal with transition periods between lightness and darkness, you can offset activation and deactivation of the profile. The time and the name of months are shown in the language used your computer's language/regional settings.
4. To see the location of the entered geographic coordinates in a map, click **Show Position in Browser**. This opens a browser where you can see the location.
5. Click **OK**.

Day length time profile properties

Set the following properties for day length time profile:

Name	Description
Name	The name of the profile.
Description	A description of the profile (optional).
Geo coordinates	Geographic coordinates indicating the physical location of the camera(s) assigned to the profile.
Sunrise offset	Number of minutes (+/-) by which activation of the profile is offset by sunrise.
Sunset offset	Number of minutes (+/-) by which deactivation of the profile is offset by sunset.
Time zone	Time zone indicating the physical location of the camera(s).

Notification profiles

Notification profiles (explained)

Notification profiles allow you to set up ready-made email notifications. Notifications can automatically be triggered by a rule, for example when a particular event occurs.

When you create the notification profile, you specify the message text and decides if you want to include still images and AVI video clips in the email notifications.



You may need to disable any email scanners that could prevent the application from sending email notifications.

Requirements for creating notification profiles

Before you can create notification profiles, you must specify mail server settings for email notifications.

You can secure the communication to the mail server, if you install the necessary security certificates on the mail server.

If you want the email notifications to be able to include AVI movie clips, you must first specify the compression settings:

1. Go to **Tools > Options**. This opens the **Options** window.
2. Configure the mail server on the **Mail Server** tab (Mail Server tab (options) on page 112) and the compression settings on the **AVI Generation** tab (AVI Generation tab (options) on page 113).

Add notification profiles

1. Expand **Rules and Events**, right-click **Notification Profiles > Add Notification Profile**. This opens the **Add Notification Profile** wizard.
2. Specify name and description. Click **Next**.

- Specify recipient, subject, message text and time between emails:

Add Notification Profile

E-mail

Recipients:
aa@aa.aa

Subject:
\$DeviceName\$ detection at \$TriggerTime\$

Message text:

Add system information (click links to insert variables into text field)

[Recording server name](#)
[Hardware name](#)
[Device name](#)
[Rule name](#)
[Trigger time](#)

Time btw. e-mails: 0 Seconds **Test E-mail**

Data

☐ Include images ☐ Include AVI

Number of images: 5 Time before event (sec): 2

Time btw. images (ms): 500 Time after event (sec): 4

Frame rate: 5

☒ Embed images in e-mail

Notifications containing H.265 encoded video require a computer that supports hardware acceleration.

Help **< Back** **Finish** **Cancel**

- To send a test email notification to the specified recipients, click **Test E-mail**.
- To include pre-alarm still images, select **Include images**, and specify number of images, time between images and whether to embed images in emails or not.
- To include AVI video clips, select **Include AVI**, and specify the time before and after event and frame rate.



Notifications containing H.265 encoded video require a computer that supports hardware acceleration.

- Click **Finish**.

Use rules to trigger email notifications

You use the **Manage Rule** for creating rules. The wizard takes you through all relevant steps. You specify the use of a notification profile during the step on which you specify the rule's actions.

When you select the action **Send notification to <profile>**, you can select the relevant notification profile and which cameras any recordings to include in the notification profile's email notifications should come from:

Send notification to 'profile'
images from recording device

In **Manage Rule**, you click the links to make your selections.

Remember that you cannot include recordings in the notification profile's email notifications unless something is actually being recorded. If you want still images or AVI video clips in the email notifications, verify that the rule specifies that recording should take place. The following example is from a rule which includes both a **Start recording** action and a **Send notification to** action:

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

Perform an action on Input Activated
from Red Sector Door Sensor
start recording 5 seconds before on Red Sector Entrance Cam
and Send notification to 'Security: Red Sector Entrance'
images from Red Sector Entrance Cam

Perform action 10 seconds after
stop recording immediately

Notification profile (properties)

Specify the following properties for notification profiles:

Component	Requirement
Name	Enter a descriptive name for the notification profile. The name appears later whenever you select the notification profile during the process of creating a rule.
Description (optional)	Enter a description of the notification profile. The description appears when you pause your mouse pointer over the notification profile in the Overview pane's Notification Profiles list.
Recipients	Enter the e-mail addresses to which the notification profile's e-mail notifications should be sent. To enter more than one e-mail address, separate addresses with a semicolon. Example: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc

Component	Requirement
Subject	<p>Enter the text you want to appear as the subject of the e-mail notification.</p> <p>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.</p>
Message text	<p>Enter the text you want to appear in the body of the e-mail notifications. In addition to the message text, the body of each e-mail notification automatically contains this information:</p> <ul style="list-style-type: none"> • What triggered the e-mail notification • The source of any attached still images or AVI video clips
Time between e-mails	<p>Specify required minimum time (in seconds) to pass between the sending of each e-mail notification. Examples:</p> <ul style="list-style-type: none"> • If specifying a value of 120, a minimum of 2 minutes pass between the sending of each e-mail notification, even if the notification profile is triggered again by a rule before the 2 minutes have passed • If specifying a value of 0, e-mail notifications is sent each time the notification profile is triggered by a rule. This can potentially result in a very large number of e-mail notifications being sent. If using the value 0, you should therefore carefully consider whether you want to use the notification profile in rules which are likely to be triggered frequently
Number of images	<p>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.</p>
Time between images (ms)	<p>Specify the number of milliseconds you want between the recordings presented on the included images. Example: With the default value of 500 milliseconds, the included images show recordings with half a second between them.</p>
Time before event (sec.)	<p>This setting is used to specify the start of the AVI file. By default, the AVI file contains recordings from 2 seconds before the notification profile is triggered. You can change this to the number of seconds you require.</p>
Time after event (sec.)	<p>This setting is used to specify the end of the AVI file. By default, the AVI file ends 4 seconds after the notification profile is triggered. You can change this to the number of seconds you require.</p>

Component	Requirement
Frame rate	Specify the number of frames per second you want the AVI file to contain. Default is five frames per second. The higher the frame rate, the higher the image quality and AVI file size.
Embed images in e-mail	If selected (default), images are inserted in the body of e-mail notifications. If not, images are included in e-mail notifications as attached files.

User-defined events

User-defined events (explained)

If the event you require is not on the **Events Overview** list, you can create your own user-defined events. Use such user-defined events to integrate other systems with your surveillance system.

With user-defined events, you can use data received from a third-party access control system as events in the system. The events can later trigger actions. This way, you can, for example, begin recording video from relevant cameras when somebody enters a building.

You can also use user-defined events for manually triggering events while viewing live video in XProtect Smart Client or automatically if you use them in rules. For example, when user-defined event 37 occurs, PTZ camera 224 should stop patrolling and go to preset position 18.

Through roles, you define which of your users are able to trigger the user-defined events. You can use user-defined events in two ways and at the same time if required:

Events	Description
For providing the ability to manually trigger events in XProtect Smart Client	In this case, user-defined events make it possible for end users to manually trigger events while viewing live video in XProtect Smart Client. When a user-defined event occurs because a user of XProtect Smart Client triggers it manually, a rule can trigger that one or more actions should take place on the system.
For providing the ability to trigger events through API	In this case, you can trigger user-defined events outside the surveillance system. Using user-defined events this way requires that a separate API (Application Program Interface. A set of building blocks for creating or customizing software applications)

Events	Description
	<p>is used when triggering the user-defined event. Authentication through Active Directory is required for using user-defined events this way. This ensures that even if the user-defined events can be triggered from outside the surveillance system, only authorized users are to do it.</p> <p>Also, user-defined events can via API be associated with meta-data, defining certain devices or device groups. This is highly usable when using user-defined events to trigger rules: you avoid having a rule for each device, basically doing the same thing. Example: A company uses access control, having 35 entrances, each with an access control device. When an access control device is activated, a user-defined event is triggered in the system. This user-defined event is used in a rule to start recording on a camera associated with the activated access control device. It is defined in the meta-data which camera is associated with what rule. This way the company does not need to have 35 user-defined events and 35 rules triggered by the user-defined events. A single user-defined event and a single rule are enough.</p> <p>When you use user-defined events this way, you may not always want them to be available for manual triggering in XProtect Smart Client. You can use roles to define which user-defined events should be visible in XProtect Smart Client.</p>

No matter how you want to use user-defined events, you must add each user-defined event through the Management Client.



If you rename a user-defined event, already connected XProtect Smart Client users must log out and log in again before the name change is visible.



If you delete a user-defined event, this affects any rules in which the user-defined event is in use. Also, a deleted user-defined event only disappears from XProtect Smart Client when the XProtect Smart Client users log out.

Add a user-defined event

1. Expand **Rules and Events > User-defined Events**.
2. In the **Overview** pane, right-click **Events > Add User-defined Event**.
3. Enter a name for the new user-defined event, and click **OK**. The newly added user-defined event now appears in the list in the **Overview** pane.

The user can now trigger the user-defined event manually in XProtect Smart Client if the user has rights to do so.

Rename a user-defined event

1. Expand **Rules and Events > User-defined Events**.
2. In the **Overview** pane, select the user-defined event.
3. In the **Properties** pane, overwrite the existing name.
4. In the toolbar, click **Save**.

Analytics events

Analytics events (explained)

Analytics events are typically data received from an external third-party video content analysis (VCA) provider.

Using analytics events as basis for alarms is basically a three step process:

- Part one, enabling the analytics events feature and setting up its security. Use a list of allowed addresses to control who can send event data to the system and which port the server listens on
- Part two, creating the analytics event, possibly with a description of the event, and testing it
- Part three, using the analytics event as the source of an alarm definition

You set up analytics events on the **Rules and Events** list in the **Site Navigation** pane.

To use VCA-based events, a third-party VCA tool is required for supplying data to the system. Which VCA tool to use is entirely up to you, as long as the data supplied by the tool adheres to the format. This format is explained in the [MIP SDK Documentation](#) on analytics events.

Contact your system provider for more details. Third-party VCA tools are developed by independent partners delivering solutions based on a Milestone open platform. These solutions can impact performance on the system.

Add and edit an analytics event

Add an analytics event

1. Expand **Rules and Events**, right-click **Analytics Events** and select **Add New**.
2. In the **Properties** window, enter a name for the event in the **Name** field.
3. Enter a description text in the **Description** field if needed.
4. In the toolbar, click **Save**. You can test the validity of the event by clicking **Test Event**. You can continually correct errors indicated in the test and run the test as many times as you want and from anywhere in the process.

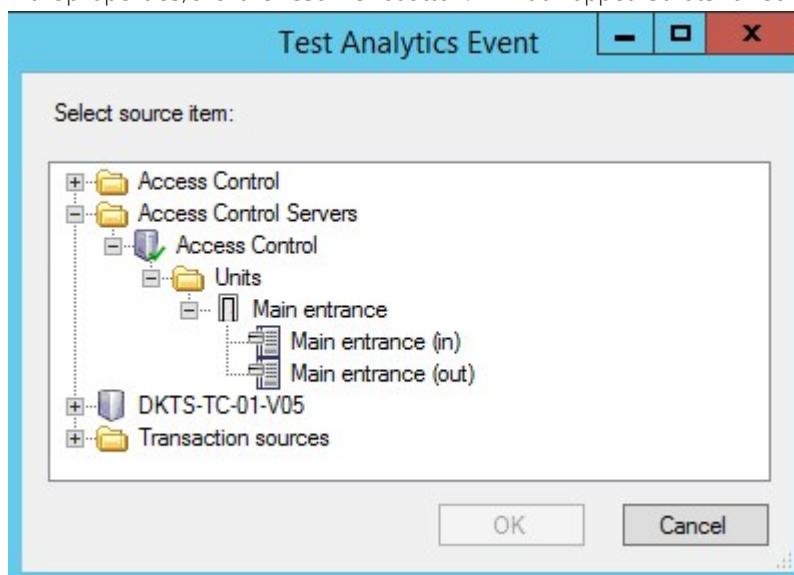
Edit an analytics event

1. Click an existing analytics event to view the **Properties** window, where you can edit relevant fields.
2. You can test the validity of the event by clicking **Test Event**. You can continually correct errors indicated in the test and run the test as many times as you want and from anywhere in the process.

Test an analytics event

After you create an analytics event, you can test the requirements (see Test Analytics Event (properties) on page 319), for example that the analytics events feature has been enabled in Management Client.

1. Select an existing analytics event.
2. In the properties, click the **Test Event** button. A window appears that shows all the possible sources of events.



3. Select the source of your test event, for example a camera. The window is closed and a new window appears that goes through four conditions that must be fulfilled for the analytics event to work.



As an additional test, in XProtect Smart Client you can verify that the analytics event was sent to the event server. To do this, open XProtect Smart Client and view the event in the **Alarm Manager** tab.

See also

Analytics events (explained) on page 317

Test Analytics Event (properties)

When you test the requirements of an analytics event, a window appears that checks four conditions and provides possible error descriptions and solutions.

Condition	Description	Error messages and solutions
Changes saved	If the event is new, is it saved? Or if there are changes to the event name, are these changes saved?	Save changes before testing analytics event. Solution/Explanation: Save changes.
Analytics Events enabled	Is the Analytics Event feature enabled?	Analytics events have not been enabled. Solution/Explanation: Enable the Analytics Events feature. To do this, click Tools > Options > Analytics Events and select the Enabled check box.
Address allowed	Is the IP address/host name of the machine sending the event (s) allowed (listed on the analytics events address list)?	The local host name must be added as allowed address for the Analytics Event service. Solution/Explanation: Add your machine to the analytics events address list of allowed IP addresses or host names. Error resolving the local host name. Solution/Explanation: The IP address or host name of the machine cannot be found or is invalid.
Send analytics event	Did sending a test event to the Event Server succeed?	See table below.

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

Error messages and solutions for the condition **Send analytics event**:

Error message	Solution
Event server not found	Unable to find the event server on the list of registered services.
Error connecting to event server	Unable to connect to the event server on the stated port. The error occurs most likely because of network problems, or the Event Server service has stopped.
Error sending analytics event	The connection to the event server is established, but the event cannot be sent. The error most likely occurs because of network problems, for example a time out.
Error receiving response from event server	The event has been sent to the event server, but no reply received. The error most likely occurs because of network problems or a port that is busy. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
Analytics event unknown by event server	The Event Server service does not know the event. The error most likely occurs because the event or changes to the event have not been saved.
Invalid analytics event received by event server	The event format is incorrect.
Sender unauthorized by event server	Most likely your machine is not on the list of allowed IP addresses or host names.
Internal error in event server	Event server error. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
Invalid response received from Event server	The response is invalid. Possibly the port is busy or there are network problems. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
Unknown response	The response is valid, but not understood. The error occurs possibly because of

Error message	Solution
from event server	network problems, or the port is busy. See the event server log, typically located at <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
Unexpected error	Please contact Milestone support for help.

Edit analytics events settings

In the toolbar, go to the **Tools > Options > Analytics Events** tab to edit relevant settings.

Generic events

Generic events (explained)



This feature does not work if you do not have the XProtect event server installed.

Generic events allow you to trigger actions in the XProtect event server by sending simple strings via the IP network to your system.

You can use any hard- or software, which can send strings via TCP or UDP, to trigger generic events. Your system can analyze received TCP or UDP data packages, and automatically trigger generic events when specific criteria are met. This way, you may integrate your system with external sources, for example access control systems and alarm systems. The aim is to allow as many external sources as possible to interact with the system.

With the concept of data sources, you avoid having to adapt third-party tools to meet the standards of your system. With data sources, you can communicate with a particular piece of hard- or software on a specific IP port and fine-tune how bytes arriving on that port are interpreted. Each generic event type pairs up with a data source and makes up a language used for communication with a specific piece of hard- or software.

Working with data sources requires general knowledge of IP networking and specific knowledge of the individual hard- or software you want to interface from. There are many parameters you can use and no ready-made solution on how to do this. Basically, your system provides the tools, but not the solution. Unlike user-defined events, generic events have no authentication. This makes them easier to trigger but, to avoid jeopardizing security, only events from local host are accepted. You can allow other client IP addresses from the **Generic Events** tab of the **Options** menu.

Add a generic event

You can define generic events to help the VMS recognize specific strings in TCP or UDP packets from an external system. Based on a generic event, you can configure Management Client to trigger actions, for example to start recording, or alarms.

Requirements

You have enabled generic events and specified the source destinations allowed. For more information, see Generic Events tab (options) on page 120.

To add a generic event:

1. Expand **Rules and Events**.
2. Right-click **Generic Events** and select **Add New**.
3. Fill in the needed information and properties. For more information, see Generic event (properties) on page 322.
4. (optional) To validate that the search expression is valid, enter a search string in the **Check if expression matches event string** field that corresponds to the expected packages:
 - **Match** - the string can be validated against the search expression
 - **No match** - the search expression is invalid. Change it and try again



In XProtect Smart Client, you can verify whether your generic events have been received by the event server. You do this in the **Alarm List** on the **Alarm Manager** tab by selecting **Events**.

Generic event (properties)

Component	Requirement
Name	Unique name for the generic event. Name must be unique among all types of events, such as user defined events, analytics events, and so on.
Enabled	Generic events are by default enabled. Clear the check box to disable the event.
Expression	Expression that the system should look out for when analyzing data packages. You can use the following operators:

Component	Requirement
	<ul style="list-style-type: none"> • (): Used to ensure that related terms are processed together as a logical unit. They can be used to force a certain processing order in the analysis <p>Example: The search criteria "User001 OR Door053 AND Sunday" first processes the two terms inside the parenthesis, then combines the result with the last part of the string. So, the system first looks for any packages containing either of the terms User001 or Door053, then takes the results and run through them in order to see which packages also contain the term Sunday.</p> <ul style="list-style-type: none"> • AND: With an AND operator, you specify that the terms on both sides of the AND operator must be present <p>Example: The search criteria "User001 AND Door053 AND Sunday" returns a result only if the terms User001, Door053 and Sunday are all included in your expression. It is not enough for only one or two of the terms to be present. The more terms you combine with AND, the fewer results you retrieve.</p> <ul style="list-style-type: none"> • OR: With an OR operator, you specify that either one or another term must be present <p>Example: The search criteria "User001 OR Door053 OR Sunday" returns any results containing either User001, Door053 or Sunday. The more terms you combine with OR, the more results you retrieve.</p>
Expression type	<p>Indicates how particular the system should be when analyzing received data packages. The options are the following:</p> <ul style="list-style-type: none"> • Search: In order for the event to occur, the received data package must contain the text specified in the Expression field, but may also have more content <p>Example: If you have specified that the received package should contain the terms User001 and Door053, the event is triggered if the received package contains the terms User001 and Door053 and Sunday since your two required terms are contained in the received package</p> <ul style="list-style-type: none"> • Match: In order for the event to occur, the received data package must contain exactly the text specified in the Expression field, and nothing else • Regular expression: In order for the event to occur, the text specified in the Expression field must identify specific patterns in the received data packages <p>If you switch from Search or Match to Regular expression, the text in the Expression field is automatically translated to a regular expression.</p>
Priority	The priority must be specified as a number between 0 (lowest priority) and 999999 (highest)

Component	Requirement
	<p>priority).</p> <p>The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events.</p> <p>When the system receives a TCP and/or UDP package, analysis of the packet starts with analysis for the event with the highest priority. This way, when a package matches the criteria for several events, only the event with the highest priority is triggered. If a package matches the criteria for several events with an identical priority, for example two events with a priority of 999, all events with this priority is triggered.</p>
Check if expression matches event string	An event string to be tested against the expression entered in the Expression field.

Generic event data source (properties)

Component	Requirement
Data source	<p>You can choose between two default data sources and define a custom data source. What to choose depends on your third party program and/or the hard- or software you want to interface from:</p> <p>Compatible: Factory default settings are enabled, echoes all bytes, TCP and UDP, IPv4 only, port 1234, no separator, local host only, current code page encoding (ANSI).</p> <p>International: Factory default settings are enabled, echoes statistics only, TCP only, IPv4+6, port 1235, <CR><LF> as separator, local host only, UTF-8 encoding. (<CR><LF> = 13,10).</p> <p>[Data source A]</p> <p>[Data source B]</p>

Component	Requirement
	and so on.
New	Click to create a new data source.
Name	Name of the data source.
Enabled	Data sources are by default enabled. Clear the check box to disable the data source.
Reset	Click to reset all settings for the selected data source. The entered name in the Name field remains.
Port	The port number of the data source.
Protocol type selector	<p>Protocols which the system should listen for, and analyze, in order to detect generic events:</p> <p>Any: TCP as well as UDP.</p> <p>TCP: TCP only.</p> <p>UDP: UDP only.</p> <p>TCP and UDP packages used for generic events may contain special characters, such as @, #, +, ~, and more.</p>
IP type selector	Selectable IP address types: IPv4, IPv6 or both.
Separator bytes	Select the separator bytes used to separate individual generic event records. Default for data source type International (see Data sources earlier) is 13,10 . (13,10 = <CR><LF>).
Echo type selector	<p>Available echo return formats:</p> <ul style="list-style-type: none"> • Echo statistics: Echoes the following format: [X],[Y],[Z],[Name of generic event] <p>[X] = request number.</p> <p>[Y] = number of characters.</p> <p>[Z] = number of matches with a generic event.</p> <p>[Name of generic event] = name entered in the Name field</p> • Echo all bytes: Echoes all bytes

Component	Requirement
	<ul style="list-style-type: none"> • No echo: Suppresses all echoing
Encoding type selector	By default, the list only shows the most relevant options. Select the Show all check box to display all available encoding options.
Show all	See previous bullet.
Allowed external IPv4 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.
Allowed external IPv6 addresses	Specify the IP addresses, that the management server must be able to communicate with in order to manage external events. You can also use this to exclude IP addresses that you do not want data from.



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**.

Site Navigation: Security

This article describes how to create basic users and how to set up roles, specify user rights for a role and assign users.

Roles (explained)

Roles determine which devices users can access. Roles also determine rights and handle security within the video management system. First, you add roles, then you add users and groups and finally a Smart Client and a Management Client profile as well as other default profiles that belong to each role. Roles you can create in the system have their own view groups in XProtect Smart Client in which their views are created and stored.



It is important that all roles, to have access to the Management Server, enable the **Connect** security right, located in **Role Settings > Management Server > Overall Security** tab (roles) on page 333.

You add users and groups to the **Administrators** role just as with any other role. See Assign and remove users and groups to/from roles (see Assign/remove users and groups to/from roles on page 330).

In addition to the **Administrators** role, you can add as many roles as required to suit your needs. You may, for example, have different roles for users of XProtect Smart Client depending on which cameras you want them to access or similar restrictions. To set up roles in your system, expand the **Security > Roles**.

Rights of a role (explained)

Available functionality depends on the system you are using. See

<https://www.milestonesys.com/solutions/platform/product-index/> for more information.

When you create a role in your system, you can give the role a number of rights to the system components or features that the relevant role can access and use. You may, for example, want to create roles that only have rights to functionality in XProtect Smart Client or other Milestone viewing clients, with the rights to view only certain cameras. If you create such roles, these roles should not have rights to access and use the Management Client, but only have access to some or all functionality found in XProtect Smart Client or other clients. To address this, you may want to set up a role that has some or most typical administrator rights, for example, the rights to add and remove cameras, servers and similar functionality.

You can create roles that have some or most rights of a system administrator. This may, for example, be relevant if your organization wants to separate between people who can administrate a subset of the system and people who can administrate the entire system. The feature allows you to provide differentiated administrator permissions to access, edit or change a large variety of system functions, for example, the right to edit the settings for servers or cameras in your system. You specify these permissions on the Overall Security tab (see Overall Security tab (roles) on page 333). As a minimum, to enable that the differentiated system administrator can launch the Management Client, you must grant read permissions on the management server for the role.



It is important that all roles, to have access to the Management Server, enable the **Connect** security right, located in **Role Settings > Management Server > Overall Security tab (roles)** on page 333.

You can also reflect the same limitations in the user interface of the Management Client for each role by associating the role with a Management Client profile that has removed the corresponding system functions from the user interface. See Management ClientSite Navigation: Clients: Management Client profiles on page 268 for information.

To give a role such differentiated administrator rights, the person with the default full administrator role must set up the role under **Security > Roles > Info tab > Add new**. When you set up the new role, you can then associate the role with your own profiles must similarly to when you set up any other role in the system or use the system's default profiles. For more information, see Add and manage a role on page 329.

Once you have specified what profiles you want to associate the role with, go to the **Overall Security** tab to specify the rights of the role.



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

Users (explained)

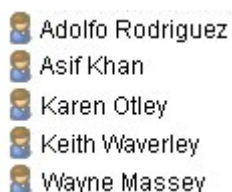
The term **users** primarily refers to users who connect to the surveillance system through the clients. You can configure such users in two ways:

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

Windows Users

You add Windows Users through the use of Active Directory. Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. It identifies resources on a network in order for users or applications to access them. Active Directory uses the concepts of users and groups.

Users are Active Directory objects representing individuals with a user account. Example:



Groups are Active Directory objects with several users. In this example, the Management Group has three users:



Groups can contain any number of users. By adding a group to the system, you add all of its members in one go. Once you have added the group to the system, any changes made to the group in Active Directory, such as new members you add or old members you remove at a later stage, are immediately reflected in the system. A user can be a member of more than one group at a time.

You can use Active Directory to add existing user and group information to the system with some benefits:

- Users and groups are specified centrally in Active Directory so you do not have to create user accounts from scratch
- You do not have to configure any authentication of users on the system as Active Directory handles authentication

Before you can add users and groups through the Active Directory service, you must have a server with Active Directory installed on your network.

Basic users

If your system does not have access to Active Directory, create a basic user (see [Users \(explained\)](#) on page 328). For information about how to set up basic users, see [Create basic user](#) (see [Create basic users](#) on page 372).

Add and manage a role

1. Expand **Security** and right-click **Roles**.
2. Select **Add Role**. This opens the **Add Role** dialog box.
3. Enter a name and description of the new role and click **OK**.
4. The new role is added to the **Roles** list. By default, a new role does not have any users/groups associated with it, but it does have a number of default profiles associated.
5. To choose different Smart Client and Management Client profiles, evidence lock profiles or time profiles, click the drop-down lists.
6. You can now assign users/groups to the role, and specify which of the system's features they can access.

For more information, see [Assign/remove users and groups to/from roles](#) on page 330 and [Roles settings](#) on page 331.

Copy, rename or delete a role

Copy a role

If you have a role with complicated settings and/or rights and need a similar or almost similar role, it might be easier to copy the already existing role and make minor adjustments to the copy than to creating a new role from scratch.

1. Expand **Security**, click **Roles**, right-click the relevant role and select **Copy Role**.
2. In the dialog box that opens, give the copied role a new unique name and description.
3. Click **OK**.

Rename a role

If you rename a role, this does not change the name of the view group based upon the role.

1. Expand **Security**, and right-click **Roles**.
2. Right-click required role and select **Rename Role**.
3. In the dialog box that opens, change the name of the role.
4. Click **OK**.

Delete a role

1. Expand **Security**, and click **Roles**.
2. Right-click the unwanted role and select **Delete Role**.
3. Click **Yes**.



If you delete a role, this does not delete the view group based upon the role.

Assign/remove users and groups to/from roles

To assign or remove Windows users or groups or basic users to/from a role:

1. Expand **Security** and select **Roles**. Then select the required role in the **Overview** pane:
2. In the **Properties** pane, select the **Users and Groups** tab at the bottom.
3. Click **Add**, select between **Windows user** or **Basic user**.

Assign Windows users and groups to a role

1. Select **Windows user**. This opens the **Select Users, Computers and Groups** dialog box:
2. Verify that the required object type is specified. If, for example, you need to add a computer, click **Object Types** and mark **Computer**. Also verify that the required domain is specified in the **From this location** field. If not, click **Locations** to browse for the required domain.
3. In the **Enter the object names to select** box, enter the relevant user names, initials, or other types of identifier which Active Directory can recognize. Use the **Check Names** feature to verify that Active Directory recognizes the names or initials that you have entered. Alternatively, use the **"Advanced..."** function to search for users or groups.
4. Click **OK**. The selected users/groups are now added to the **Users and Groups** tab's list of users who you have assigned the selected role. You can add more users and groups by entering multiple names separated by a semicolon (;).

Assign basic users to a role

1. Select **Basic User**. This opens the **Select Basic Users to add to Role** dialog box:
2. Select the basic user(s) that you want to assign to this role.
3. Optional: Click **New** to create a new basic user.
4. Click **OK**. The selected basic user(s) are now added to the **Users and Groups** tab's list of basic users who you have assigned the selected role.

Remove users and groups from a role

1. On the **Users and Groups** tab, select the user or group you want to remove and click **Remove** in the lower part of the tab. You can select more than one user or group, or a combination of groups and individual users, if you need to.
2. Confirm that you want to remove the selected user(s) or and group(s). Click **Yes**.



A user may also have roles through group memberships. When that is the case, you cannot remove the individual user from the role. Group members may also hold roles as individuals. To find out which roles users, groups, or individual group members have, use the **View Effective Roles** function.

View effective roles

With the Effective Roles feature, you can view all roles of a selected user or group. This is practical if you are using groups and it is the only way of viewing which roles a specific user is a member of.

1. Open the **Effective Roles** window by expanding **Security**, then right-clicking **Roles** and select **Effective Roles**.
2. If you want information about a basic user, enter the name in the **User name** field. Click **Refresh** to display the roles of the user.
3. If you use Windows users or groups in Active Directory, click the "..." browse button. Select object type, enter the name, and click **OK**. The user's roles appear automatically.



Roles settings

Info tab (roles)

Available functionality depends on the system you are using. See

<https://www.milestonesys.com/solutions/platform/product-index/> for more information.

On the **Info** tab of a role, you can set the following:

Name	Description
Name	Enter a name for the role.
Description	Enter a description for the role.
Management Client profile	<p>Select a Management Client profile to associate with the role.</p> <p>You cannot apply this to the default Administrators role.</p> <div>  <p>Requires permissions to manage security on the management server.</p> </div>
Smart Client profile	<p>Select a Smart Client profile to associate with the role.</p> <div>  <p>Requires permissions to manage security on the management server.</p> </div>
Default time profile	<p>Select a default time profile to associate with the role.</p> <p>You cannot apply this to the default Administrators role.</p>
Evidence lock profile	Select an evidence lock profile to associate with the role.
Smart Client login within time profile	<p>Select a time profile for which the XProtect Smart Client user associated with this role is allowed to log in.</p> <p>If the XProtect Smart Client user is logged in when the period expires, he or she is logged off automatically.</p> <p>You cannot apply this to the default Administrators role.</p>
Allow Smart Client login	<p>Select the check box to allow users associated with this role to log in to XProtect Smart Client.</p> <p>Access to Smart Client is allowed by default. Clear the check box to deny access to XProtect Smart Client.</p>
Allow XProtect Mobile client login	<p>Select the check box to allow users associated with this role to log in to XProtect Mobile client.</p> <p>Access to XProtect Mobile client is allowed by default. Clear the check box to deny</p>

Name	Description
	access to XProtect Mobile client.
Allow XProtect Web Client login	<p>Select the check box to allow users associated with this role to log in to XProtect Web Client.</p> <p>Access to XProtect Web Client is allowed by default. Clear the check box to deny access to XProtect Web Client.</p>
Login authorization required	<p>Select the check box to associate login authorization with the role. It means that XProtect Smart Client or the Management Client asks for a second authorization, typically by a superuser or manager, when the user logs in.</p> <p>To enable administrators to authorize users, configure the management server's Authorize Users right on the Overall Security tab.</p> <p>You cannot apply this to the default Administrators role.</p>
Make users anonymous during PTZ sessions	Select the check box to hide the names of users associated with this role when they control PTZ sessions.

User and Groups tab (roles)

On the **User and Groups** tab, you assign users and groups to roles (see Assign/remove users and groups to/from roles on page 330). You can assign Windows users and groups or basic users (see Users (explained) on page 328).

Name	Description
Name	Displays the name of the user or group assigned to this role.
Description	Displays the description that you entered when the basic user was created.

Overall Security tab (roles)

Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

On the **Overall Security** tab, you set up overall rights for roles. For every component available in your system, define access rights for the roles by setting **Allow** or **Deny**. When a role is denied access to a component, that component is not visible in the **Overall Security** tab to a user in that role.



The **Overall Security** tab is not available in the free XProtect Essential+.

You can define more access rights for XProtect Corporate than for XProtect Expert, XProtect Professional+, and XProtect Express+. This is because you can only set up differentiated administrator rights in XProtect Corporate, while you can set up overall rights for a role that uses XProtect Smart Client, XProtect Web Client, or XProtect Mobile client in all products.



The overall security settings only apply to the current site.

If you associate a user with more than one role and select **Deny** on a security setting for one role and **Allow** for another, the **Deny** right permission overrules the **Allow** right permission.

In the following, the descriptions show what happens on each individual right for the different system components if you select **Allow** for the relevant role. If you use XProtect Corporate, you can see which settings are available **only** to your system under each system component.

For every system component or functionality, the full system administrator can use the **Allow** or **Deny** check boxes to set up security permissions for the role. Any security permissions that you set up here are set up for the whole system component or functionality. If, for example, you select the **Deny** check box on **Cameras**, all cameras added to the system are unavailable for the role. In contrast, if you select the **Allow** check box, the role can see all cameras added to the system. The result of selecting **Allow** or **Deny** on your cameras is that the camera settings on the **Device** tab then inherit your selections on the **Overall Security** tab so that either all cameras are either available or unavailable to the particular role.


If you want to set security permissions for **individual** cameras or similar, you can only set these individual permissions on the tab of the relevant system component or functionality if you have **not set any overall permissions** for the system component or functionality on the **Overall Security** tab.



The descriptions below also apply to the rights that you can configure through the MIP SDKs.



If you want to switch your base license from XProtect Corporate to one of the other products, make sure that you remove all security rights that are available to only XProtect Corporate. If you do not remove those rights, you cannot complete the switch.

Management Server


Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Connect	<p>Enables users to connect to the Management Server.</p> <p>This permission is enabled by default.</p> <p>You can temporarily deny connection permission on roles for maintenance purposes, and then reapply access to the system.</p> <div>  <p>This permission must be selected to allow access to the system.</p> </div>	
Read	<p>Enables the right to access a wide range of functionality, including:</p> <ul style="list-style-type: none"> • Logging in with the Management Client • List of current tasks • Server logs <p>It also enables access to:</p> <ul style="list-style-type: none"> • Remote Connect Services • Smart Client Profiles • Management Client Profiles • Matrix • Time Profiles • Registered Servers and Service Registration API 	Only available
Edit	<p>Enables the right to modify data in a wide range of functionality, including:</p> <ul style="list-style-type: none"> • Options • License Management <p>It also enables users to create, delete, and edit the following:</p> <ul style="list-style-type: none"> • Remote Connect Services 	Only available

Security right	Description	XProtect Corporate
	<ul style="list-style-type: none"> • Device groups • Matrix • Time Profiles • Notification Profiles • Registered Servers <div>  <p>Enables the right to configure local IP ranges when configuring the network on the recording server.</p> </div>	
System Monitor	Enables the right to view the data of the System Monitor.	Only available
Status API	Enables the right to perform queries on the Status API located on the recording server. This means that the role with this right enabled has access to read the status of the items located on the recording server.	
Manage Federated site hierarchy	<p>Enables the right to add and detach the current site to other sites in a federated site hierarchy.</p> <div>  <p>If you set this permission to allowed on the child site only, the user can still detach the site from the parent site.</p> </div>	Only available
Backup Configuration	Enables the right to create backups of the system configuration using the system's backup and restore functionality.	Only available
Authorize users	Enables the right to authorize users when they are asked for a second login in XProtect Smart Client or Management Client. You define if a role requires login authorization on the Info tab.	
Manage security	Enables the right to manage permissions for the Management Server.	Only available

Security right	Description	XProtect Corporate
	<p>It also enables users to create, delete, and edit the following features:</p> <ul style="list-style-type: none"> • Roles • Basic users • Smart Client Profiles • Management Client Profiles 	

Recording Servers

The following settings are only available in XProtect Corporate.

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

Security right	Description
Manage security	Enables the right to manage security permissions for recording servers.

Failover Servers

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to see and access failover servers in the Management Client.
Edit	Enables the right to create, update, delete, move, and enable or disable failover servers in the Management Client.
Manage security	Enables the right to manage security permissions for the failover servers.



Mobile Servers

The following settings are only available in XProtect Corporate.

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

Hardware

The following settings are only available in XProtect Corporate.


Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Edit	Enables the right to edit properties on hardware.
Delete	<p>Enables the right to delete hardware.</p> <div>  <p>If any of the hardware devices contains evidence locks, you can only delete the hardware if the recording server is offline.</p> </div>
Driver commands	<p>Enables the right to send special commands to the drivers and thereby control features and configuration on the device itself.</p> <div>  <p>The Driver commands right is for special developed MIP plug-ins in the clients only. It does not control standard configuration tasks.</p> </div>
View passwords	Enables the right to view passwords on hardware devices in the Edit Hardware dialog box.
Manage security	Enables the right to manage security permissions for the hardware.

Cameras

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view camera devices in the clients and the	

Security right	Description	XProtect Corporate
	Management Client.	
Edit	Enables the right to edit properties for cameras in the Management Client. It also enables users to enable or disable a camera.	Only available
View Live	Enables the right to view live video from cameras in the clients and the Management Client.	
Playback	Enables the right to play back recorded video from cameras in all clients.	
Retrieve remote recordings	Enables the right to retrieve recordings in the clients from cameras on remotes sites or from edge storages on cameras.	
Read sequences	Enables the right to read the sequence information related to, for example, playing back recorded video in the clients.	
Smart search	Enables the right to use the Smart search function in the clients.	
Export	Enables the right to export recordings from the clients.	
Create bookmarks	Enables the right to create bookmarks in recorded and live video in the clients.	
Read bookmarks	Enables the right to search for and read bookmark details in the clients.	
Edit bookmarks	Enables the right to edit bookmarks in the clients.	
Delete bookmarks	Enables the right to delete bookmarks in the clients.	
Create and extend evidence locks	Enables the right to create and extend evidence locks in the clients.	Only available
Read evidence	Enables the right to search and read evidence locks in the clients.	Only available

Security right	Description	XProtect Corporate
locks		
Delete and reduce evidence locks	Enables the right to delete or reduce evidence locks in the clients.	Only available
Start manual recording	Enables the right to start manual recording of video in the clients.	
Stop manual recording	Enables the right to stop manual recording of video in the clients.	
AUX commands	<p>Enables the right to use auxiliary (AUX) commands on the camera from the clients.</p> <p>AUX commands offer users the control of, for example, wipers on a camera connected via a video encoder. Camera-associated devices connected via auxiliary connections are controlled from the client.</p>	
Manual PTZ	Enables the right to use PTZ functions on PTZ cameras in the clients and the Management Client.	
Activate PTZ presets or patrolling profile	<p>Enables the right to move PTZ cameras to preset positions, start and stop patrolling profiles, and pause a patrolling in the clients and the Management Client.</p> <p>To allow this role to use other PTZ functions on the camera, enable the Manual PTZ right.</p>	
Manage PTZ presets or patrolling profiles	<p>Enables the right to add, edit, and delete PTZ presets and patrolling profiles on PTZ cameras in the clients and the Management Client.</p> <p>To allow this role to use other PTZ functions on the camera, enable the Manual PTZ right.</p>	
Lock/unlock PTZ presets	Enables the right to lock and unlock PTZ presets in the Management Client. This prevents or allows other users from changing preset positions in the clients and in the Management	Only available

Security right	Description	XProtect Corporate
	Client.	
Reserve PTZ sessions	<p>Enables the right to set PTZ cameras in reserved PTZ session mode in the clients and the Management Client.</p> <p>In a reserved PTZ session, other users with higher PTZ priority are not able to take over the control.</p> <p>To allow this role to use other PTZ functions on the camera, enable the Manual PTZ right.</p>	Only available
Release PTZ sessions	<p>Enables the right to release other users' PTZ sessions from the Management Client.</p> <p>You can always release your own PTZ sessions - without this permission.</p>	Only available
Delete recordings	Enables the right to delete stored video recordings from the system via the Management Client.	Only available
Lift privacy masks	<p>Enables the right to temporarily lift privacy masks in XProtect Smart Client. It also enables the right to authorize other XProtect Smart Client users to lift privacy masks.</p> <div>  <p>Lifting privacy masks only applies to privacy masks configured as liftable privacy masks in the Management Client.</p> </div>	
Manage security	Enables the right to manage security permissions in the Management Client for the camera.	Only available

Microphones

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view microphone devices in the clients and the Management Client.	
Edit	Enables the right to edit microphone properties in the Management Client. It also allows users to enable or disable microphones.	Only available
Listen	Enables the right to listen to live audio from microphones in the clients and the Management Client.	
Playback	Enables the right to play back recorded audio from microphones in the clients.	
Retrieve remote recordings	Enables the right to retrieve recordings in the clients from microphones on remotes sites or from edge storages on cameras.	
Read sequences	Enables the right to read the sequence information related to, for example, the Playback tab in the clients.	
Export	Enables the right to export recordings from the clients.	
Create bookmarks	Enables the right to create bookmarks in the clients.	
Read bookmarks	Enables the right to search for and read bookmark details in the clients.	
Edit bookmarks	Enables the right to edit bookmarks in the clients.	
Delete bookmarks	Enables the right to delete bookmarks in the clients.	
Create and	Enables the right to create or extend evidence locks in the clients.	Only available

Security right	Description	XProtect Corporate
extend evidence locks		
Read evidence locks	Enables the right to search and read evidence lock details in the clients.	Only available
Delete and reduce evidence locks	Enables the right to delete or reduce evidence locks in the clients.	Only available
Start manual recording	Enables the right to start manual recording of audio in the clients.	
Stop manual recording	Enables the right to stop manual recording of audio in the clients.	
Delete recordings	Enables the right to delete stored recordings from the system.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for microphones.	Only available

Speakers

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view speaker devices in the clients and the Management Client.	
Edit	Enables the right to edit properties for speakers in the Management Client. It also allows users to enable or disable speakers.	Only available

Security right	Description	XProtect Corporate
Listen	Enables the right to listen to live audio from speakers in the clients and the Management Client.	
Speak	Enables the right to speak through the speakers in the clients.	
Playback	Enables the right to play back recorded audio from speakers in the clients.	
Retrieve remote recordings	Enables the right to retrieve recordings in the clients from speakers on remotes sites or from edge storages on cameras.	
Read sequences	Enables the right to use the Sequences feature while browsing recorded audio from speakers in the clients.	
Export	Enables the right to export recorded audio from speakers in the clients.	
Create bookmarks	Enables the right to create bookmarks in the clients.	
Read bookmarks	Enables the right to search for and read bookmark details in the clients.	
Edit bookmarks	Enables the right to edit bookmarks in the clients.	
Delete bookmarks	Enables the right to delete bookmarks in the clients.	
Create and extend evidence locks	Enables the right to create or extend evidence locks to protect recorded audio in the clients.	Only available
Read evidence locks	Enables the right to view recorded audio protected by evidence locks in the clients.	Only available
Delete and reduce evidence	Enables the right to delete or reduce evidence locks on protected audio in the clients.	Only available

Security right	Description	XProtect Corporate
locks		
Start manual recording	Enables the right to start manual recording of audio in the clients.	
Stop manual recording	Enables the right to stop manual recording of audio in the clients.	
Delete recordings	Enables the right to delete stored recordings from the system.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for speakers.	Only available

Metadata

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to receive metadata in the clients.	
Edit	Enables the right to edit metadata properties in the Management Client. It also allows users to enable or disable metadata devices.	Only available
Live	Enables the right to receive live metadata from cameras in the clients.	
Playback	Enables the right to play back recorded data from metadata devices in the clients.	
Retrieve remote recordings	Enables the right to retrieve recordings in the clients from metadata devices on remotes sites or from edge storages on	

Security right	Description	XProtect Corporate
	cameras.	
Read sequences	Enables the right to read the sequence information related to, for example, the Playback tab in the clients.	
Export	Enables the right to export recordings in the clients.	
Create and extend evidence locks	Enables the right to create evidence locks in the clients.	Only available
Read evidence locks	Enables the right to view evidence locks in the clients.	Only available
Delete and reduce evidence locks	Enables the right to delete or reduce evidence locks in the clients.	Only available
Start manual recording	Enables the right to start manual recording of metadata in the clients.	
Stop manual recording	Enables the right to stop manual recording of metadata in the clients.	
Delete recordings	Enables the right to delete stored recordings from the system.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for metadata.	Only available

Input

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	Only available
Read	Enables the right to view input devices in the clients and the Management Client.	
Edit	Enables the right to edit properties for input devices in the Management Client. It also enables users to enable or disable an input device.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for input devices.	Only available

Output

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view output devices in the clients.	
Edit	Enables the right to edit properties for output devices in the Management Client. It also enables users to enable or disable an output device.	Only available
Activate	Enables the right to activate outputs in the clients.	
Manage security	Enables the right to manage security permissions in the Management Client for output devices.	Only available

Smart Wall

The following settings are only available in XProtect Expert and XProtect Corporate.

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view Smart Walls in the clients.	
Edit	Enables the right to edit properties for the Smart Wall in the Management Client.	Only available
Delete	Enables the right to delete existing Smart Walls in the Management Client.	Only available
Operate	Enables the right to activate and modify Smart Walls, for example, to change and activate presets or apply cameras on views in the clients and in the Management Client.	
Create Smart Wall	Enables the right to create new Smart Walls in the Management Client.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for the Smart Wall.	Only available
Playback	Enables the right to play back recorded data from within Smart Walls in the clients.	

View Groups

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view View Groups in the clients and in the Management Client. View groups are created in the Management Client.	

Security right	Description	XProtect Corporate
Edit	Enables the right to edit properties on the View Groups in the Management Client.	Only available
Delete	Enables the right to delete View Groups in the Management Client.	
Operate	Enables the right to use View Groups in XProtect Smart Client, that is, to create and delete subgroups and views.	
Create view group	Enables the right to create View Groups in the Management Client.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for View Groups.	Only available

User-defined Events

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view user-defined events in the clients.	
Edit	Enables the right to edit properties on user-defined events in the Management Client.	Only available
Delete	Enables the right to delete user-defined events in the Management Client.	Only available
Trigger	Enables the right to trigger user-defined events in the clients.	
Manage security	Enables the right to manage security permissions in the Management Client for user-defined events.	Only available
Create user-defined event	Enables the right to create new user-defined events in the Management Client.	Only available

Analytics Events

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view analytics events in the Management Client.
Edit	Enables the right to edit properties on analytics events in the Management Client.
Manage security	Enables the right to manage security permissions in the Management Client for analytics events.

Generic Events

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view generic events in the clients and the Management Client.
Edit	Enables the right to edit properties on generic events in the Management Client.
Manage security	Enables the right to manage security permissions in the Management Client for generic events.

Matrix

Security right	Description	XProtect Corporate
Full control	Enables the right to manage all security entries on this part of the system.	Only available

Security right	Description	XProtect Corporate
Read	Enables the right to select and send video to the Matrix recipient from the clients.	
Edit	Enables the right to edit properties for a Matrix in the Management Client.	Only available
Delete	Enables the right to delete a Matrix in the Management Client.	Only available
Create Matrix	Enables the right to create a new Matrix in the Management Client.	Only available
Manage security	Enables the right to manage security permissions in the Management Client for all Matrix's.	Only available

Rules

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view existing rules in the Management Client.
Edit	Enables the right to edit properties for rules and to define rule behavior in the Management Client. It also requires that the user has read permissions on all the devices that are impacted by the rule.
Delete	Enables the right to delete rules from the Management Client. It also requires that the user has read permissions on all devices that are impacted by the rule.
Create rule	Enables the right to create new rules in the Management Client.

Security right	Description
	It also requires that the user has read permissions on all devices that are impacted by the rule.
Manage security	Enables the right to manage security permissions in the Management Client for all rules.

Sites

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view other sites in the Management Client. Connected sites are connected via Milestone Federated Architecture. To edit properties, you need Edit permissions on the Management Server on each site.
Manage security	Enables the right to manage security permissions on all sites.

System Monitors

The following settings are only available in XProtect Expert and XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view system monitors in XProtect Smart Client.

Security right	Description
Edit	Enables the right to edit properties for system monitors in the Management Client.
Manage security	Enables the right to manage security permissions in the Management Client for all system monitors.


Search

The following settings are only available in XProtect Expert and XProtect Corporate.

Security right	Description
Read public searches	Enables the right to view and open saved public searches in XProtect Smart Client.
Create public searches	Enables the right to save newly configured searches as public searches in XProtect Smart Client.
Edit public searches	Enables the right to edit the details or the configuration of saved public searches in XProtect Smart Client, for example the name, description, cameras, and search categories.
Delete public searches	Enables the right to delete saved public searches.
Manage security	Enables the right to manage security permissions in the Management Client for search.

Alarms

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Manage	<p>Enables the right to manage alarms in the Management Client. For example, change priorities of alarms and re-delegate alarms to other users, acknowledge alarms and change the state, for example, from New to Assigned, of several alarms at the same time view alarm definitions, alarm sounds, and alarm data settings.</p> <div>  Only when you set this to allowed does the Alarms and Events tab in the Options dialog appear. </div>
Edit	Enables the right to view alarms and print alarm reports.
Disable alarms	Enables the right to disable alarms.
Receive notifications	Enables the right to receive notifications about alarms in XProtect Mobile clients and XProtect Web Client.
Manage security	Enables the right to manage security permissions for alarms.
Create	Enables the right to create new alarm definitions in the Management Client.

Server Logs

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read system log entries	Enables the right to see system

Security right	Description
	log entries.
Read audit log entries	Enables the right to see audit log entries.
Read rule-triggered log entries	Enables the right to see rule-triggered log entries.
Read log configuration	Enables the right to read log settings in Tools > Options > Server Logs .
Update log configuration	Enables the right to change log settings in Tools > Options > Server Logs .
Manage security	Enables the right to manage security permissions for alarms.

Access Control

The following settings are only available in XProtect Corporate.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Edit	Enables the right to edit properties for the Access Control systems in the Management Client.
Use access control	Allows the user to use any access control-related features in the clients.
View cardholders list	Allows the user to view the cardholders list on the Access Control tab in the clients.
Receive	Allows the user to receive notifications about access requests in the clients.

Security right	Description
notifications	
Manage security	Enables the right to manage security permissions for all Access Control systems.

LPR

If your system runs with XProtect LPR, specify the following rights for the user:

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Use LPR	Enables the right to use any LPR-related features in the clients
Manage license plate match lists	Enables the right to add, import, modify, export, and delete license plate match lists in the Management Client.
Read license plate match lists	Enables the right to view license plate match lists.
Manage security	Enables the right to manage security permissions in the Management Client for all Transaction definitions.

Transaction sources

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view properties for the Transaction sources in the Management Client.
Edit	Enables the right to edit properties for the Transaction sources in the Management Client.

Security right	Description
Delete	Enables the right to delete Transaction sources in the Management Client.
Create	Enables the right to create new Transaction sources in the Management Client.
Manage security	Enables the right to manage security permissions in the Management Client for all Transaction sources.

Transaction definition

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view properties for the Transaction definitions in the Management Client.
Edit	Enables the right to edit properties for the Transaction definitions in the Management Client.
Delete	Enables the right to delete Transaction definitions in the Management Client.
Create	Enables the right to create new Transaction definitions in the Management Client.
Manage security	Enables the right to manage security permissions in the Management Client for all Transaction definitions.

MIP plug-ins

Through the MIP SDK, a third-party vendor can develop custom plug-ins for your system, for example, integration to external access control systems or similar functionality.

Device tab (roles)

Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

The **Device** tab lets you specify which features users/groups with the selected role can use for each device (for example, a camera) or device group in XProtect Smart Client.



Remember to repeat for each device. You can also select a device group, and specify role rights for all the devices in the group in one go.

You can still select or clear such square-filled check boxes, but note that your choice in that case applies for **all** devices within the device group. Alternatively, select the individual devices in the device group to verify exactly which devices the relevant right applies for.

Camera-related rights

Specify the following rights for camera devices:



Name	Description
Read	The selected camera(s) will be visible in the clients.
View live	Allows live viewing of video from the selected camera(s) in the clients. For XProtect Smart Client, it requires that the role has been granted the right to view the clients' Live tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Within time profile	Allows playback of recorded video from the selected camera(s) in the clients. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded video from the selected camera(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Smart search	Allows the user to use the Smart search function in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of video from the selected camera(s) in the clients.
Stop manual	Allows stopping manual recording of video from the selected camera(s) in the clients.

Name	Description
recording	
Read bookmarks	Allows search for and read bookmark details in the clients.
Edit bookmarks	Allows editing bookmarks in the clients.
Create bookmarks	Allows adding bookmarks in the clients.
Delete bookmarks	Allows deleting bookmarks in the clients.
AUX commands	Allows the use of auxiliary commands from the clients.
Create and extend evidence locks	<p>Allows the client user to:</p> <ul style="list-style-type: none"> • Add the camera to new or existing evidence locks • Extend the expiry time for existing evidence locks • Extend the protected interval for existing evidence locks <div>  Requires user rights to all devices included in the evidence lock. </div>
Delete and reduce evidence locks	<p>Allows the client user to:</p> <ul style="list-style-type: none"> • Remove the camera from existing evidence locks • Delete existing evidence locks • Shorten the expiry time for existing evidence locks • Shorten the protected interval for existing evidence locks <div>  Requires user rights to all devices included in the evidence lock. </div>
Read evidence locks	Allows the client user to search for and read evidence lock details.

Microphone-related rights

Specify the following rights for microphone devices:


Name	Description
Read	The selected microphone(s) will be visible in the clients.
Live > Listen	Allows listening to live audio from the selected microphones(s) in the clients. For XProtect Smart Client, it requires that the role has been granted the right to view the clients' Live tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Within time profile	Allows playback of recorded audio from the selected microphone(s) in the clients. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded audio from the selected microphone(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of audio from the selected microphone(s) in the clients.
Stop manual recording	Allows stopping manual recording of audio from the selected microphone(s) in the clients.
Read bookmarks	Allows search for and read bookmark details in the clients.
Edit bookmarks	Allows editing bookmarks in the clients.
Create bookmarks	Allows adding bookmarks in the clients.
Delete bookmarks	Allows deleting bookmarks in the clients.
Create and extend evidence locks	Allows the client user to: <ul style="list-style-type: none"> • Add the microphone to new or existing evidence locks • Extend the expiry time for existing evidence locks


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

Speaker-related rights

Specify the following rights for speaker devices:

Name	Description
Read	The selected speaker(s) is visible in the clients.
Live > Listen	<p>Allows listening to live audio from the selected speaker(s) in the clients.</p> <p>For XProtect Smart Client, it requires that the role has been granted the right to view the clients' Live tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.</p>
Playback > Within time profile	Allows playback of recorded audio from the selected speaker(s) in the clients. Specify the time profile or leave the default value.
Playback > Limit	Allows playback of recorded audio from the selected speaker(s) in the clients. Specify a

Name	Description
playback to	playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of audio from the selected speaker(s) in the clients.
Stop manual recording	Allows stopping manual recording of audio from the selected speaker(s) in the clients.
Read bookmarks	Allows search for and read bookmark details in the clients.
Edit bookmarks	Allows editing bookmarks in the clients.
Create bookmarks	Allows adding bookmarks in the clients.
Delete bookmarks	Allows deleting bookmarks in the clients.
Create and extend evidence locks	<p>Allows the client user to:</p> <ul style="list-style-type: none"> • Add the speaker to new or existing evidence locks • Extend the expiry time for existing evidence locks • Extend the protected interval for existing evidence locks <div>  Requires user rights to all devices included in the evidence lock. </div>
Delete and reduce evidence locks	<p>Allows the client user to:</p> <ul style="list-style-type: none"> • Remove the speaker from existing evidence locks • Delete existing evidence locks • Shorten the expiry time for existing evidence locks

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

Metadata-related rights

Specify the following rights for metadata devices:

Name	Description
Read	Enables the right to see metadata devices and retrieve data from them in the clients.
Edit	Enables the right to edit metadata properties. It also allows users to enable or disable metadata devices in the Management Client and via the MIP SDK.
View Live	Enables the right to view metadata from cameras in the clients. For XProtect Smart Client, it requires that the role has been granted the right to view the clients' Live tab. This right is granted as part of the application rights.
Playback	Enables the right to play back recorded data from metadata devices in the clients.
Read sequences	Enables the right to use the Sequences feature while browsing recorded data from metadata devices in the clients.
Export	Enables the right to export recorded audio from metadata devices in the clients.
Create and extend evidence locks	Enables the right to create and extend the evidence locks on metadata in the clients.
Read evidence locks	Enables the right to view evidence locks on metadata in the clients.

Name	Description
Delete and reduce evidence locks	Enables the right to delete or reduce evidence locks on metadata in the clients.
Start manual recording	Enables the right to start manual recording of metadata in the clients.
Stop manual recording	Enables the right to stop manual recording of metadata in the clients.

Input-related rights

Specify the following rights for input devices:

Name	Description
Read	The selected input(s) will be visible in the clients.

Output-related rights

Specify the following rights for output devices:

Name	Description
Read	The selected output(s) will be visible in the clients. If visible, the output will be selectable on a list in the clients.
Activate	The selected output(s) can be activated from the Management Client and the clients. Specify the time profile or leave the default value.

PTZ tab (roles)

You set up rights for pan-tilt-zoom (PTZ) cameras on the **PTZ** tab. You can specify the features users/groups can use in the clients. You can select individual PTZ cameras or device groups containing PTZ cameras.

Specify the following rights for PTZ:

Name	Description
Manual PTZ	<p>Determines if the selected role can use PTZ functions and pause a patrolling on the selected camera.</p> <p>Specify a time profile, select Always, or leave the default value that follows the default time profile defined on the Info tab for that role.</p>
Activate PTZ presets or patrolling profiles	<p>Determines if the selected role can move the selected camera to preset positions, start and stop patrolling profiles, and pause a patrolling.</p> <p>Specify a time profile, select Always, or leave the default value that follows the default time profile defined on the Info tab for that role.</p> <p>To allow this role to use other PTZ functions on the camera, enable the Manual PTZ right.</p>
PTZ Priority	<p>Determines the priority of PTZ cameras. When several users on a surveillance system want to control the same PTZ camera at the same time, conflicts may occur.</p> <p>You can avoid such a situation by specifying a priority for use of the selected PTZ camera(s) by users/groups with the selected role. Specify a priority from 1 to 32,000, where 1 is the lowest priority. The default priority is 3,000. The role with the highest priority number is the one who can control the PTZ camera(s).</p>
Manage PTZ presets or patrolling profiles	<p>Determines the right to add, edit and delete PTZ presets and patrolling profiles on the selected camera in both the Management Client and XProtect Smart Client.</p> <p>To allow this role to use other PTZ functions on the camera, enable the Manual PTZ right.</p>
Lock/unlock PTZ presets	<p>Determines if the role can lock and unlock preset positions for the selected camera.</p>
Reserve PTZ sessions	<p>Determines the right to set the selected camera in reserved PTZ session mode.</p> <p>In a reserved PTZ session other users or patrolling sessions with higher PTZ priority are not able to take over the control.</p>

Name	Description
	To allow this role to use other PTZ functions on the camera, enable the Manual PTZ right.
Release PTZ sessions	<p>Determines if the selected role can release other users' PTZ sessions from the Management Client.</p> <p>You can always release your own PTZ sessions - without this permission.</p>

Speech tab (roles)

Relevant only if you use speakers on your system. Specify the following rights for speakers:

Name	Description
Speak	Determine if users should be allowed to talk through the selected speaker(s). Specify the time profile or leave the default value.
Speak priority	<p>When several client users want to talk through the same speaker at the same time, conflicts may occur.</p> <p>Solve the problem by specifying a priority for use of the selected speaker(s) by users/groups with the selected role. Specify a priority from Very low to Very high. The role with the highest priority is allowed use the speaker before other roles.</p> <p>Should two users with the same role want to speak at the same time, the first come, first served-principle applies.</p>

Remote Recordings tab (roles)

Specify the following rights for remote recordings:

Name	Description
Retrieve remote recordings	Enables the right to retrieve recordings in the clients from cameras, microphones, speakers, and metadata devices on remotes sites or from edge storages on cameras.

Smart Wall tab (roles)

Through roles, you can grant your client users Smart Wall-related user rights for the Smart Wall feature:

Name	Description
Read	Allows users to view the selected Smart Wall in the clients.
Edit	Allows users to edit the selected Smart Wall in the Management Client.
Delete	Allows users to delete the selected Smart Wall in the Management Client.
Operate	Allows users to apply layouts on the selected Smart Wall in the client and to activate the selected preset.
Playback	Allows users to play back recorded data from the selected Smart Wall in the clients.

External Event tab (roles)

Specify the following external event rights:

Name	Description
Read	Allows users to search for and view the selected external system event in the clients and the Management Client.

Name	Description
Edit	Allows users to edit the selected external system event in the Management Client.
Delete	Allows users to delete the selected external system event in the Management Client.
Trigger	Allows users to trigger the selected external system event in the clients.

View Group tab (roles)

On the **View Group** tab, you specify which view groups the users and user groups with the selected role can use in the clients.

Specify the following rights for view groups:

Name	Description
Read	Enables the right to view the View Groups in the clients and in the Management Client. View groups are created in the Management Client.
Edit	Enables the right to edit properties on View Groups in the Management Client.
Delete	Enables the right to delete View Groups in the Management Client.
Operate	Enables the right to use View Groups in XProtect Smart Client, that is to create and delete subgroups and views.

Servers tab (roles)

Specifying role rights on the **Servers** tab is only relevant if your system works in a Milestone Federated Architecture setup.

Name	Description
Sites	<p>Enables the right to view the selected site in the Management Client. Connected sites are connected via Milestone Federated Architecture.</p> <p>To edit properties, you need Edit permissions on the Management Server on each site.</p>

See Configuring Milestone Federated Architecture on page 403 for more information.

Matrix tab (roles)

If you have configured Matrix recipients on your system, you may configure Matrix role rights. From a client, you can send video to selected Matrix recipients. Select the users who can receive this on the Matrix tab.

The following rights are available:

Name	Description
Read	Determine if users and groups with the selected role can select and send video to the Matrix recipient from the clients.

Alarms tab (roles)

If you use alarms in your system setup to provide central overview and control of your installation (including any other XProtect servers), you can use the **Alarms** tab to specify the alarm rights users/groups with the selected role should have, for example, how to handle alarms in the clients.

Specify the following rights for alarms:

Name	Description
Manage	<p>Enables the right to manage alarms, for example changing priorities of alarms and re-delegate alarms to other users, acknowledge alarms and change the state, for example from New to Assigned, of several alarms at the same time.</p>

Name	Description
View	Enables the right to view alarms and print alarm reports.
Disable alarms	Enables the right to disable alarms.
Receive notifications	Enables the right to receive notifications about alarms in XProtect Mobile clients and XProtect Web Client.

Access Control tab (roles)

When you add or edit basic users, Windows users or groups, specify access control settings:

Name	Description
Use access control	Allows the user to use any access control-related features in the clients.
View cardholders list	Allows the user to view the cardholders list on the Access Control tab in the clients.
Receive notifications	Allows the user to receive notifications about access requests in the clients.

LPR tab (roles)

If your system runs with XProtect LPR, specify the following rights for the users:

Name	Description
Use LPR	Enables the right to use any LPR-related features in the clients.
Manage license plate match lists	Enables the right to add, import, modify, export, and delete license plate match lists in the Management Client.
Read license plate match lists	Enables the right to view license plate match lists.

MIP tab (roles)



Through the MIP SDK, a third-party vendor can develop custom plug-ins for your system, for example, integration to external access control systems or similar functionality.

The settings you change depend on the actual plug-in. Find the custom settings for the plug-ins on the **MIP** tab.

Basic users (explained)

When you add a basic user to your system, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. This is in contrast to the Windows user, added through Active Directory.

When working with basic users, it is important to understand the difference between basic user and Windows user.

-  Basic users are authenticated by a user name/password combination and are specific to a system. Even if basic users have the same name and password, a basic user created at one federated site does not have access to another federated site
-  Windows users are authenticated based on their Windows login and are specific to a machine

Create basic users

To create a basic user on your system:

1. Expand **Security > Basic Users**.
2. In the **Basic Users** pane, right-click and select **Create Basic User**.
3. Specify a user name and a password, and repeat it to be sure you have specified it correctly.



The password must meet the complexity requirements for the Windows operating system on the computer with the Management Server service installed.

4. Click **OK** to create the basic user.

Site Navigation: System dashboard

This article describes how to monitor your system including how to create reports and protect data.

System dashboard (explained)

System dashboard provides you with the functionality to monitor your system and its components.

Access the following functionality:

Name	Description
System Monitor	Monitor the status of your servers and cameras by parameters you define.
System Monitor Thresholds	Set threshold values for monitored parameters on server and monitor tiles used in System Monitor.
Evidence Lock	Get an overview of all protected data in the system.
Current Task	Get an overview of ongoing tasks on a selected recording server.
Configuration Reports	Decide what to include in your system configuration reports before printing.

System monitor (explained)

System monitor provides you with a quick, visual overview of the current state of your system's servers and cameras through colored tiles that represent the system hardware. By default, the system displays tiles that represent all **Recording servers**, **All servers** and **All cameras**.

The color of the tiles:

Tile color	Description
Green	Normal state. Everything is running normally.
Yellow	Warning state. One or more monitoring parameters is above the threshold value (see System monitor thresholds (explained) on page 376) for the Normal state.
Red	Critical state. One or more monitoring parameters is above the threshold value for the Normal and Warning state.

You can customize the server and camera tiles if you want to display more or less tiles on the dashboard. For example, you can set up tiles to represent a single server, a single camera, a group of cameras, or a server group. You can also delete a tile if you do not want to use it or edit its monitoring parameters. Monitoring parameters are,

for example, CPU usage or memory available for a server. If you remove these parameters from the server tile, the tile does not monitor these parameters on the relevant tile. Click **Customize** in the upper right corner of the tab to open the Customize dashboard window. See [Customize dashboard](#) for more information.

Tiles change their state and thereby color based on threshold values set in System monitor thresholds. While the system does set some default threshold values for you, you can decide for yourself what the threshold value should be for each of the three states. To set up or change threshold values, you can use **System monitor thresholds**. See System monitor thresholds (explained) on page 376.

If a tile changes color and you want to know which server/parameter that makes the tile change color, click the tile. This opens an overview in the bottom of the screen which shows the colors red, yellow or green for each monitoring parameter you have enabled for your tile. Click the **Details** button to get more detailed information about why the state has changed.



If you see a warning sign and place your mouse above it, the system shows you an error message.



The system monitor functionality requires that the Data Collector service is running.

Customize dashboard

Add a new camera or server tile:

1. In the System monitor window, click **Customize**.
2. In the **Customize dashboard** window that opens, click **New** under **Server tiles** or **Camera tiles**.
3. In the **New server tile/New camera tile** window, select the cameras or servers to monitor.
4. Under **Monitoring parameters**, select or clear check boxes for any parameters to add or remove from the relevant tile.
5. Click **OK**. The new server or camera tile is now added to the tiles displayed on your dashboard.

Edit monitoring parameters:

1. In the System monitor dashboard window, click **Customize**.
2. In the **Customize dashboard** window that opens, click **Edit** under **Server tiles** or **Camera tiles**.
3. In the **Edit server tile** or **Edit camera tile** window, select the server component or cameras you want to edit.

4. In the **Monitoring parameters** box, select or clear the check boxes for the monitoring parameters you want to add or remove from the relevant tile.
5. Click **OK**. The changed monitoring parameters are now a part of or removed from the relevant tile.



You can enable and disable historical data on the system if you want to. If you disable this data, you cannot see graphs of previous system behavior. If you want to reduce the load on the SQL Server and database or on your bandwidth, you can reduce the sampling interval of historical data. If you reduce the sampling interval of historical data, less details are available in graphs.

System monitor details (explained)

If you click a server or camera tile, you can see the status of each selected monitoring parameter below the dashboard.

State	Name	Live FPS	Recording FPS	Used space	
	Panasonic SPxxx/SFxxx/SWxxx no I/O Camera Series	<div></div>	<div></div>	<div></div>	Details

Example: A camera's LIVE FPS monitoring parameters has reached the Warning state.

The **State** field shows the camera's state. For example, a red warning is shown if the connection to the device is broken. The icon includes a tooltip with a short description of the issue that is causing the warning.

The **Used space** field shows data from other recording servers where this device has recordings if, for example, the device has been located on other recording servers previously.

If you click the **Details** button for the relevant camera/server, you can view system information and create reports regarding:

Component	Description
Management server	Shows data from the selected management server
Recording server(s)	Shows data from the selected recording server. You can view these per: <ul style="list-style-type: none"> • Disk • Storage • Network • Camera

Component	Description
Failover recording servers	Shows data from the selected failover recording server.
Additional servers	Shows data on log server, event servers and more.
Cameras	Shows data from any camera in any camera group in your setup.

Each of these elements is an area you can click and expand. When you click this area, it provides relevant dynamic data on this server or camera.

The **Cameras** bar contains a list of camera groups to select from. Once you select a group, select a specific camera and see dynamic data for it. All servers display CPU usage and available memory information. Recording servers also display connection status information. Within each view, find a **History** link. Click it to view historic data and reports (to view reports on a camera, click the name of the camera). For each historic report, you can view data for the last 24 hours, 7 days or 30 days. To save and/or print reports, click the **Send to PDF** icon. Use the < and home icons to navigate System Monitor.



You can only create historical reports with data from the recording server where the device is currently located.



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

System monitor thresholds (explained)

System monitor thresholds allow you to set up and adjust the global thresholds for when tiles on System monitor should visually indicate that your system hardware changes state, for example when the CPU usage of a server changes from a normal state (green) state to a warning state (yellow).

The system is set up with default threshold values so that you can start monitoring your system hardware from the moment your system is set up. To change threshold values, see Set system monitor thresholds on page 379

As a default, the system is set up to show threshold values for all units of a particular hardware, for example all cameras or servers. You can also set up threshold values for individual servers or cameras or a subset of these. Setting threshold values for individual servers or cameras may be a good idea if, for example, some cameras should be allowed to use a higher **Live FPS** or **Recording FPS** than other cameras.

You can set the threshold values for servers, cameras, disks and storage. If you want to change threshold values, you can use the threshold control slider. The threshold control slider allows you to increase or decrease threshold values by dragging the handles separating states either up or down. The threshold control slider is divided into colors similar to those shown in your server or camera tiles present in System monitor (see System monitor thresholds (explained) on page 376).

To ensure that you do not see a **Critical** or **Warning** state in cases where the usage of or the load on your system hardware reaches a high threshold value only for a second or similar, use **Calculation interval**. The calculation interval feature averages out the effect of brief or frequent changes to a system hardware state. In practice, this means that the calculation interval feature evens out the effect of hardware changes over time so that you do not get alerts every time a threshold is exceeded.

For example, you can set **Calculation interval** to one (1) minute which ensures that you only get alerts if the average value for the whole minute exceeds the threshold. The benefit of this is that you avoid alerts about frequent and maybe possibly irrelevant changes in hardware states and only receive alerts that reflect sustained issues with, for example, CPU usage or memory consumption. To change the values of calculation intervals, see Set system monitor thresholds on page 379

Server thresholds

Threshold	Description	Unit
CPU usage	Thresholds for the CPU usage on the servers you monitor.	%
Memory available	Thresholds for RAM memory in use on the servers you monitor.	MB
NVIDIA decoding	Thresholds for the NVIDIA decoding usage on the servers you monitor.	%
NVIDIA memory	Thresholds for NVIDIA RAM memory in use on the servers you monitor.	%
NVIDIA rendering	Thresholds for the NVIDIA rendering usage on the servers you monitor.	%

Camera thresholds

Threshold	Description	Unit
Live FPS	Thresholds for cameras' FPS in use when live video is shown on cameras you	%

Threshold	Description	Unit
	monitor.	
Recording FPS	Thresholds for cameras' FPS in use when the system is recording video on cameras you monitor.	%
Used space	Thresholds for the space used by cameras you monitor.	GB

Disk thresholds

Threshold	Description	Unit
Free space	Thresholds for available space on disks you monitor.	GB

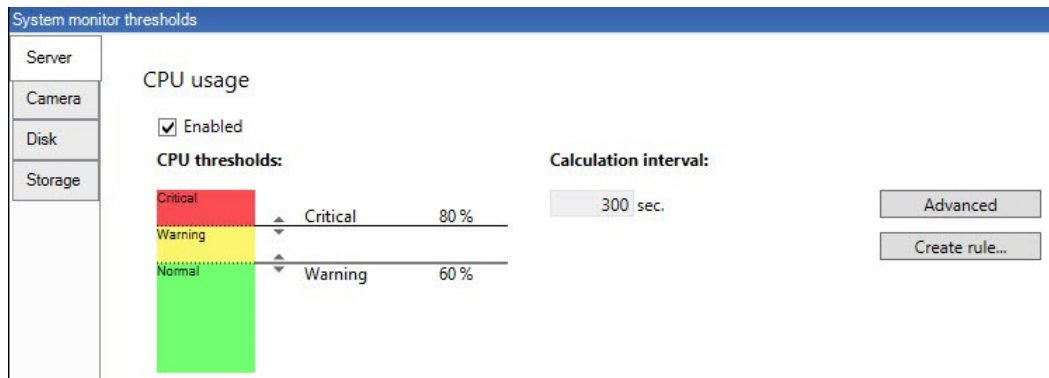
Storage thresholds

Threshold	Description	Unit
Retention time	Threshold showing a prediction for when you run out of space on your storage. The state shown is based on your system setup and is updated twice a day.	Days

You can also set up rules (see Rules on page 298) to perform specific actions or activate alarms (see System dashboard (explained) on page 372) when a threshold changes from one state to another.

Set system monitor thresholds

1. In the **Site Navigation** pane, select **System Monitor Thresholds**.
2. Select the **Enable** check box for the relevant hardware if you have not already enabled it. The figure below shows an example.



3. Drag the threshold control slider up or down to increase or decrease the threshold value. There are two sliders available for each piece of hardware shown in the threshold control, separating the **Normal**, **Warning** and **Critical** levels.
4. Enter a value for the calculation interval or keep the default value.
5. If you want to set values on individual pieces of hardware, click **Advanced**.
6. If you want to specify rules for certain events or within specific time intervals, click **Create rule**.
7. Once you have set the relevant thresholds levels and calculation intervals, select **File > Save** from the menu.

Example of a threshold setting:



- Red indicates you have reached a Critical state
- Yellow is a Warning state indicating that you are close to reaching the Critical state
- Green indicates that things are at a normal state and within your selected threshold values

Evidence lock (explained)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.



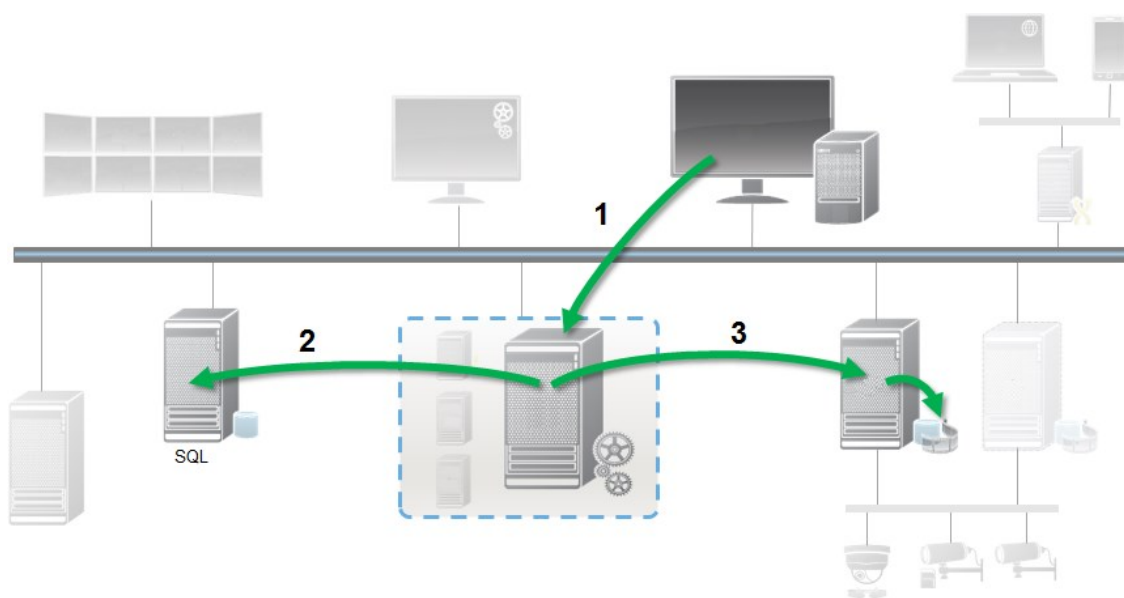
As of XProtect VMS version 2020 R2, when you upgrade the management server from an earlier version, it will not be possible to create or modify evidence locks on recording servers that are version 2020 R1 or earlier, until these recording servers have been upgraded.

This also means that if hardware has been moved from one recording server (from 2020 R1 or earlier) to another recording server, and it still has recordings on it, then evidence locks cannot be created or modified.

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

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

Flow diagram for Evidence Lock:



1. User creates an evidence lock in XProtect Smart Client. Information sent to Management Server.
2. Management Server stores information about the evidence lock in the SQL database.
3. Management Server informs Recording Server to store and protect the protected recordings in the database.

When the operator creates an evidence lock, the protected data remains in the recording storage that it was recorded to, and is moved to archiving disks together with non-protected data, but the protected data:

- Follows the retention time configured for the evidence lock. Potentially infinitely
- Keeps the original quality of the recordings, even if grooming has been configured for non-protected data

When an operator creates locks, the minimum size of a sequence is the period that the database divides recorded files into, this is by default one-hour sequences. You can change this, but it requires that you customize the RecorderConfig.xml file on the recording server. If a small sequence spans two one-hour periods, the system locks the recordings in both periods.

In the audit log in the Management Client, you can see when a user creates, edits or deletes evidence locks.

When a disk runs out of disk space, it does not impact the protected data. Instead the oldest non-protected data will be deleted. If there are no more non-protected data to delete, the system stops recording. You can create rules and alarms triggered by disk full events, so you are automatically notified.

Except for more data being stored for a longer period and potentially affecting disk storage, the evidence lock feature as such does not influence system performance.

If you move hardware (see Move hardware on page 439) to another recording server:

- Recordings protected with evidence locks, remains on the old recording server following the retention time set for the evidence lock, when it was created
- The XProtect Smart Client user can still protect data with evidence locks on the recordings that were made on a camera before it was moved to another recording server. Even if you move the camera multiple times and the recordings are stored on multiple recording servers

By default, all operators have the default evidence lock profile assigned to them but no user access rights to the feature. To specify the evidence lock access rights of a role, see the Device tab (see Device tab (roles) on page 358) for role settings. To specify the evidence lock profile of a role, see the Info tab (see Info tab (roles) on page 331) for role settings.

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

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

- Start and end date for the protected data
- The user who locked the evidence
- When the evidence is no longer locked

- Where the data is stored
- The size of each evidence lock

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

Current tasks (explained)

The **Current Tasks** node shows an overview of tasks under a selected recording server, their begin time, estimated end time and progress. All information shown in **Current Tasks** are snapshots. You can refresh these by clicking on the **Refresh** button in the lower right corner of the **Properties** pane.

Configuration reports (explained)

When you create PDF configuration reports, you can include any possible elements of your system in the report. You can, for example, include licenses, device configuration, alarm configuration, and much more. You can also customize your font and page setup and include a customized front page.

Add a configuration report

1. Expand **System Dashboard** and click **Configuration Reports**. This brings up the report configuration page.
2. Select the elements that you want to include in your report.
3. **Optional:** Click **Front Page** to customize your front page. In the window that appears, fill in the needed info. Select **Front page** as an element to include in you report, otherwise the front page you customize is not included in your report.
4. Click **Formatting** to customize your font, page size and margins. In the window that appears, select the wanted settings.
5. When you are ready to export, click **Export** and select a name and save location for you report.

Configure report details

The following is available when setting up reports:

Name	Description
Select All	Selects all elements in the list.
Clear All	Clears all elements in the list.

Name	Description
Front Page	Customize the front page of the report.
Formatting	Format the report.
Export	Select a save location for the report and create a PDF.

Site Navigation: Server logs

This article describes how to change log settings, filter logs, and create exports.

Logs (explained)

Logs are a detailed record of user activity, events, actions, and errors in the system.

To see logs, in the **Site Navigation** pane, select **Server Logs**.

Log type	What is logged?
System logs	System-related information
Audit logs	User activity
Rule-triggered logs	Rules in which users have specified the Make new <log entry> action. For more information about the <log entry> action, see Actions and stop actions (explained) on page 276.

To see logs in a different language, see General tab (options) on page 109 under **Options**.

To export logs as comma-separated values (.csv) files, see Export logs on page 384.

To change log settings, see Server Logs tab (options) on page 111.

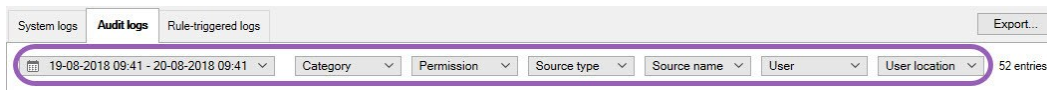
Filter logs

In each log window, you can apply filters to see log entries from, for example, a specific time span, device, or user.

1. In the **Site Navigation** pane, select **Server Logs**. By default, the **System logs** tab appears.

To navigate between log types, select a different tab.

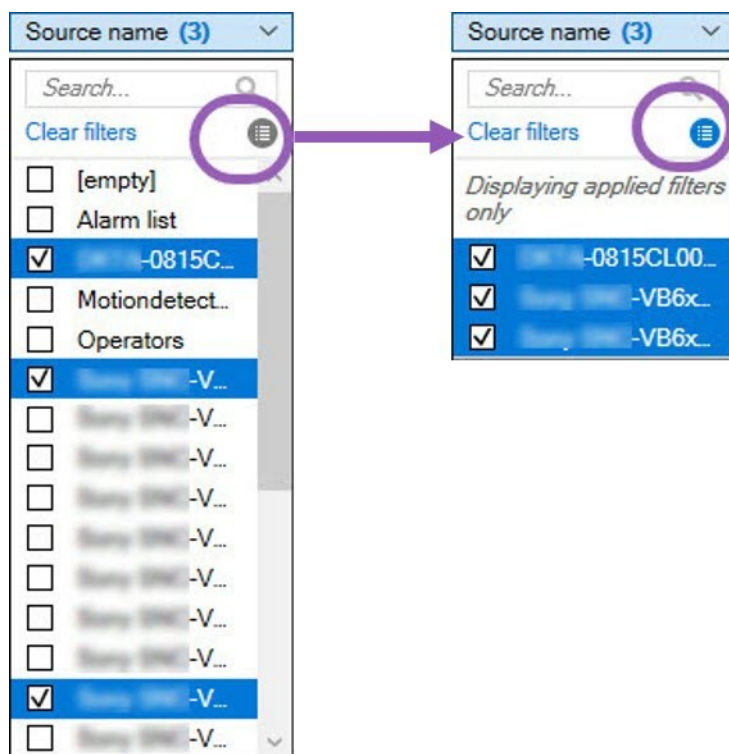
2. Under the tabs, select a filter group, for example, **Category**, **Source type**, or **User**.



A list of filters appears.

3. Select a filter to apply it. Select the filter again to remove it.

Optional: In a list of filters, select **Display applied filters only** to see only the filters that you applied.



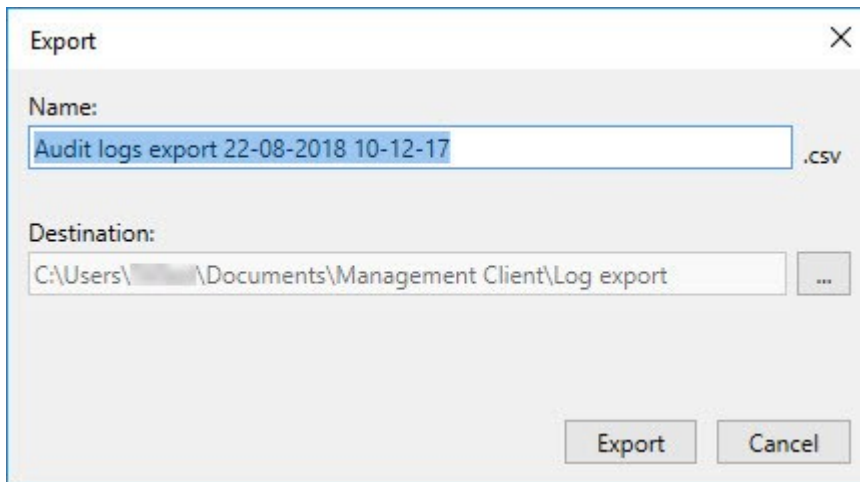
The contents of your export change depending on the filters that you apply. For information about your export, see [Export logs](#) on page 384.


Export logs

Exporting logs helps you to, for example, save log entries beyond the log retention period. You can export logs as comma-separated values (.csv) files.

To export a log:

1. Select **Export** in the upper-right corner. The **Export** window appears.



2. In the **Export** window, in the **Name** field, specify a name for the log file.
3. By default, exported log files are saved in your **Log export** folder. To specify a different location, select  to the right of the **Destination** field.
4. Select **Export** to export the log.



The contents of your export change depending on the filters that you apply. For information about your export, see [Filter logs](#) on page 383.

Allow 2018 R2 and earlier components to write logs

The 2018 R3 version of the log server introduces authentication for added security. This prevents 2018 R2 and earlier components from writing logs to the new log server.

Affected components:

- XProtect Smart Client
- XProtect LPR Plug-in
- LPR Server
- Access Control Plug-in
- Event Server
- Alarm Plug-in

If you're using the 2018 R2 or earlier version of any of the components listed above, you must decide whether or not to allow the component to write logs to the new log server:

1. Select **Tools > Options**.
2. In the **Options** dialog box, at the bottom of the **Server Logs** tab, find **the Allow 2018 R2 and earlier components to write logs** check box.
 - Select the check box to allow 2018 R2 and earlier components to write logs
 - Clear the check box to not allow 2018 R2 and earlier components to write logs

System logs (properties)

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Log level	Info, warning, or error.
Local time	Timestamped in the local time of your system's server.
Message text	The identification number for the logged incident.
Category	The type of logged incident.
Source type	The type of equipment on which the logged incident occurred, for example, server or device.
Source name	The name of the equipment on which the logged incident occurred.
Event type	The type of event represented by the logged incident.

Audit logs (properties)

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Local time	Timestamped in the local time of your system's server.
Message text	Shows a description of the logged incident.
Permission	The information about whether the remote user action was allowed (granted) or not.
Category	The type of logged incident.
Source type	The type of equipment on which the logged incident occurred, for example, server or device.
Source name	The name of the equipment on which the logged incident occurred.
User	The user name of the remote user causing the logged incident.
User location	The IP address or host name of the computer from which the remote user caused the logged incident.

Rule-triggered logs (properties)

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Local time	Timestamped in the local time of your system's server.
Message text	Shows a description of the logged incident.
Category	The type of logged incident.
Source type	The type of equipment on which the logged incident occurred, for example, server or device.

Name	Description
Source name	The name of the equipment on which the logged incident occurred.
Event type	The type of event represented by the logged incident.
Rule name	The name of the rule triggering the log entry.
Service name	The name of the service on which the logged incident occurred.

Site Navigation: Metadata use

In this article, you will learn to configure how your video surveillance system uses metadata.



To manage and configure metadata devices, see [Metadata devices \(explained\)](#) on page 193.

What is metadata?

Metadata is data about data, for example, data that describes the video image, the content or objects in the image, or the location of where the image was recorded.

Metadata can be generated by:

- The device itself delivering the data, for example a camera that is delivering video
- A third-party system or integration via a generic metadata driver

Metadata search (explained)

Metadata search is any search for video recordings in XProtect Smart Client that uses search categories and search filters related to metadata.

The default Milestone metadata search categories are:

- Location
- People
- Vehicles

Metadata search requirements

To get search results, you need one of the following:

- At least one device in your video surveillance system that can perform video analytics and is configured correctly
- A video processing service in your video surveillance system that generates metadata

In either case, metadata must be in the required metadata format. For more information about the required metadata format and where metadata is stored, see the *Metadata Search integration* documentation on the [Milestone Documentation](#) website.

Show or hide metadata search categories and search filters in XProtect Smart Client

Users of XProtect Management Client with administrator rights can show or hide the default Milestone metadata search categories and search filters in XProtect Smart Client. By default, these search categories and search filters are hidden. Showing them is useful if your video surveillance system meets the [metadata search requirements](#).

This setting affects all XProtect Smart Client users.

This setting does not affect the visibility of:



- Other, non-metadata Milestone search categories and search filters, for example **Motion, Bookmarks, Alarms, and Events**
- Third-party search categories and search filters

1. In XProtect Management Client, in the **Site Navigation** pane, select **Metadata Use > Metadata Search**.
2. In the **Metadata Search** pane, select the search category that you want to change visibility settings for.
3. To enable the visibility of a search category or search filter, select the corresponding check box. To disable the visibility of a search category or search filter, clear the check box.

Site Navigation: Alarms

This article describes how to set up alarms to appear in the system, triggered by events.

Alarms (explained)



This feature only works if you have XProtect Event Server installed.

Based on functionality handled in the event server, the alarms feature provides central overview, control and scalability of alarms in any number of installations (including any other XProtect systems) throughout your organization. You can configure it to generate alarms based on either:

- **Internal system related events**

For example, motion, server responding/not responding, archiving problems, lack of disk space and more.

- **External integrated events**

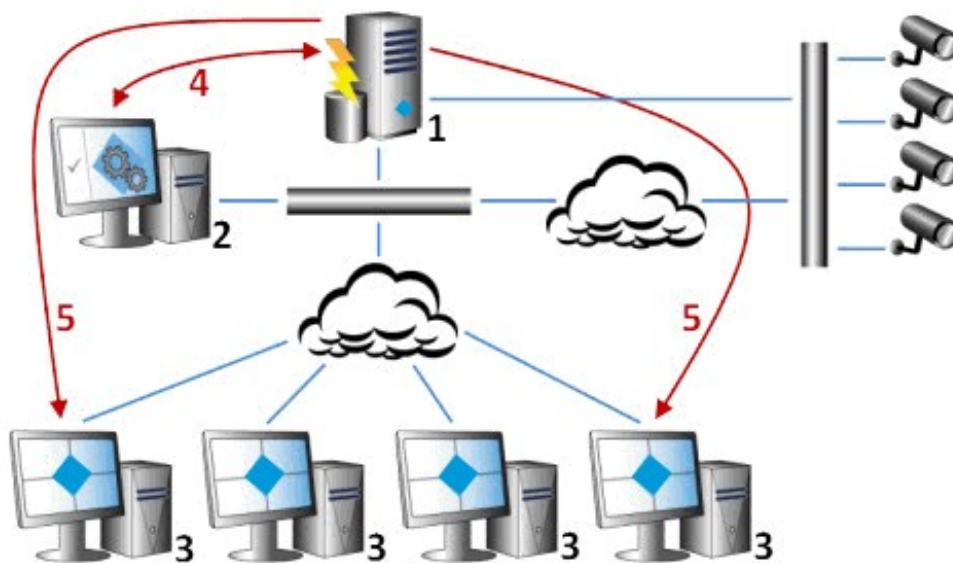
This group can consist of several types of external events:

- **Analytics events**

Typically data received from an external third-party video content analysis (VCA) providers.

- **MIP plug-in events**

Through the MIP SDK a third-party vendor can develop custom plug-ins (for example, integration to external access control systems or similar) to your system.



Legend:

1. Surveillance system
2. Management Client
3. XProtect Smart Client
4. Alarm configuration
5. Alarm data flow

You handle and delegate alarms in the alarm list in XProtect Smart Client. You can also integrate alarms with the XProtect Smart Client's smart map and map functionality.

Alarm configuration (explained)

Alarm configuration includes:

- Dynamic role-based setup of alarm handling
- Central technical overview of all components: servers, cameras, and external units
- Setup of central logging of all incoming alarms and system information
- Handling of plug-ins, allowing customized integration of other systems, for example external access control or VCA-based systems

In general, alarms are controlled by the visibility of the object causing the alarm. This means that four possible aspects can play a role with regards to alarms and who can control/manage them and to what degree:

Name	Description
Source/device visibility	If the device causing the alarm is not set to be visible to the user's role, the user cannot see the alarm in the alarm list in XProtect Smart Client.
The right to trigger user-defined events	This right determines if the user's role can trigger selected user-defined events in XProtect Smart Client.
External plug-ins	If any external plug-ins are set up in your system, these might control users' rights to handle alarms.
General role rights	Determine whether the user is allowed to only view or also to manage alarms. What a user of Alarms can do with alarms depends on the user's role and on settings configured for that particular role.

On the **Alarms and Events** tab in **Options**, you can specify settings for alarms, events and logs.

Alarm Definitions

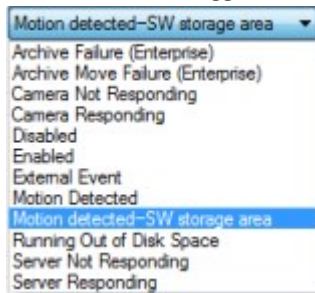
When your system registers an event on your system, you can configure the system to generate an alarm in XProtect Smart Client. You must define alarms before you can use them, and alarms are defined based on events registered in your system servers. You can also use user-defined events for triggering alarms and use the same event to trigger several different alarms.

Add an alarm

To define an alarm, you need to create an alarm definition, where you specify, for example, what triggers the alarm, instructions on what the operator needs to do, and what or when the alarm stops. For detailed information about the settings, see [Alarm Definitions \(properties\)](#).

1. In the **Site Navigation** pane, expand **Alarms**, and right-click **Alarm Definitions**.
2. Select **Add New**.
3. Fill in these properties:

- **Name:** Enter a name for the alarm definition. The name of the alarm definition appears whenever the alarm definition is listed.
- **Instructions:** You can write instructions for the operator who receives the alarm.
- **Triggering event:** Use the drop-down menu to select an event type and an event message to be used when the alarm is triggered.



A list of selectable triggering events. The one highlighted is created and customized using analytics events.

- **Sources:** Select the cameras or other devices that the event should originate from to trigger the alarm. Your options depend on the type of event you have selected.
 - **Time profile:** If you want the alarm to be activated during a specific time interval, select the radio button and then a time profile in the drop-down menu.
 - **Event based:** If you want the alarm to be activated by an event, select the radio button and specify which event will start the alarm. You also need to specify the event that will stop the alarm.
4. In the **Time limit** drop-down menu, specify a time limit for when action is required by the operator.
 5. In the **Events triggered** drop-down menu, specify which event to trigger when the time limit has passed.
 6. Specify additional settings, for example related cameras and initial alarm owner.

Alarm Definitions (properties)

Alarm definition settings:

Name	Description
Enable	By default, the alarm definition is enabled. To disable it, clear the check box.
Name	Alarm names do not have to be unique, but using unique and descriptive alarm names are advantageous in many situations.
Instructions	Enter a descriptive text about the alarm and how to resolve the issue that caused the alarm. The text appears in XProtect Smart Client when the user handles the alarm.
Triggering event	Select the event message to use when the alarm is triggered. Choose from two drop-downs: <ul style="list-style-type: none"> The first drop-down: Select the type of event, for example analytics event and system events The second drop-down: Select the specific event message to use. The messages available are determined by the event type you selected in the first drop-down menu
Sources	Specify the sources that the events originate from. Aside from cameras or other devices, sources may also be plug-in defined sources, for example VCA and MIP. The options depend on the type of event you have selected.


Alarm trigger:

Name	Description
Time profile	Select the Time profile radio button to specify the time interval during which the alarm definition is active. Only the time profile you have defined under the Rules and Events node are displayed in the list. If none are defined, only the Always option is available.
Event based	If you want the alarm to be based on an event, select this radio button. Once selected, specify the start and stop event. You can select hardware events defined on cameras, video servers and input (see Events overview on page 288). Also global/manual event definitions can be used (see User-defined events on page 315)

Operator action required:

Name	Description
Time limit	Select a time limit for when operator action is required. The default value is 1 minute. The time limit is not active before you have attached an event in the Events triggered drop-down menu.
Events triggered	Select which event to trigger when the time limit has passed.

Maps:

Name	Description
Alarm Manager view	<p>Assign either a smart map or a map to the alarm when the alarm is listed in XProtect Smart Client > Alarm Manager.</p> <div>  Smart map displays alarms if they are triggered by a camera. </div>

Other:

Name	Description
Related cameras	Select up to 15 cameras to include in the alarm definition, even if these cameras themselves do not trigger the alarm. This can be relevant, for example, if you have selected an external event message (such as a door being opened) as the source of your alarm. By defining one or more cameras near the door, you can attach the cameras' recordings of the incident to the alarm.
Initial alarm owner	Select a default user responsible for the alarm.

Name	Description
Initial alarm priority	Select a priority for the alarm. Use these priorities in XProtect Smart Client to determine the importance of an alarm.
Alarm category	Select an alarm category for the alarm, for example False alarm or Need investigation .
Events triggered by alarm	Define an event that the alarm can trigger in XProtect Smart Client.
Auto-close alarm	If you want a particular event to automatically stop the alarm, select this check box. Not all events can trigger alarms. Clear the check box to disable the new alarm from the beginning.
Alarm assignable to Administrators	<p>Select the check box to include users with an administrator role in the Assigned to list.</p> <p>The Assigned to list is in the alarm details on the Alarm Manager tab in XProtect Smart Client.</p> <p>Clear the check box to filter out users with an administrator role from the Assigned to list to shorten the list.</p>

Alarm Data Settings

When you configure alarm data settings, specify the following:

Alarm Data Levels tab Priorities

Name	Description
Level	Add new priorities with level numbers of your choosing or use/edit the default priority levels (numbers 1, 2 or 3). These priority levels are used to configure the Initial alarm priority setting.
Name	Enter a name for the entity. You can create as many as you like.

Name	Description
Sound	Select the sound to be associated with the alarm. Use one of the default sounds or add more in Sound Settings .
Repeat sound	Decide whether the sound should play only once or repeatedly until in XProtect Smart Client, the operator clicks the alarm in the alarm list.
Enable desktop notifications	For each alarm priority, you can enable or disable desktop notifications. If you are using an XProtect VMS that supports Smart Client profiles, you must also enable notifications on the required Smart Client profiles. See Alarm Manager tab (Smart Client profiles) on page 267.

States

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

Categories

Name	Description
Level	Add new categories with level numbers of your choosing. These category levels are used to configure the Initial alarm category setting.
Name	Enter a name for the entity. You can create as many as you like.

Alarm List Configuration tab

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

Reasons for Closing tab

Name	Description
Enable	Select to enable that all alarms must be assigned a reason for closing before they can be closed.
Reason	Add reasons for closing that the user can choose between when closing alarms. Examples could be <i>Solved-Trespasser</i> or <i>False Alarm</i> . You can create as many as you like.

Sound Settings

When you configure sound settings, specify the following:

Name	Description
Sounds	Select the sound to be associated with the alarm. The list of sounds contains a number of default Windows sounds. You can also add new sounds (.wav or .mp3).
Add	Add sounds. Browse the sound file and upload one or several .wav or .mp3 files.
Remove	Remove a selected sound from the list of manually added sounds. Default sounds cannot be removed.
Test	Test the sound. In the list, select the sound. The sound plays once.

Enable encryption

Enable encryption to and from the management server

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see *Management server encryption (explained)* on page 65.

Prerequisites:

- A server authentication certificate is trusted on the computer that hosts the management server

First, enable encryption on the management server.

Steps:

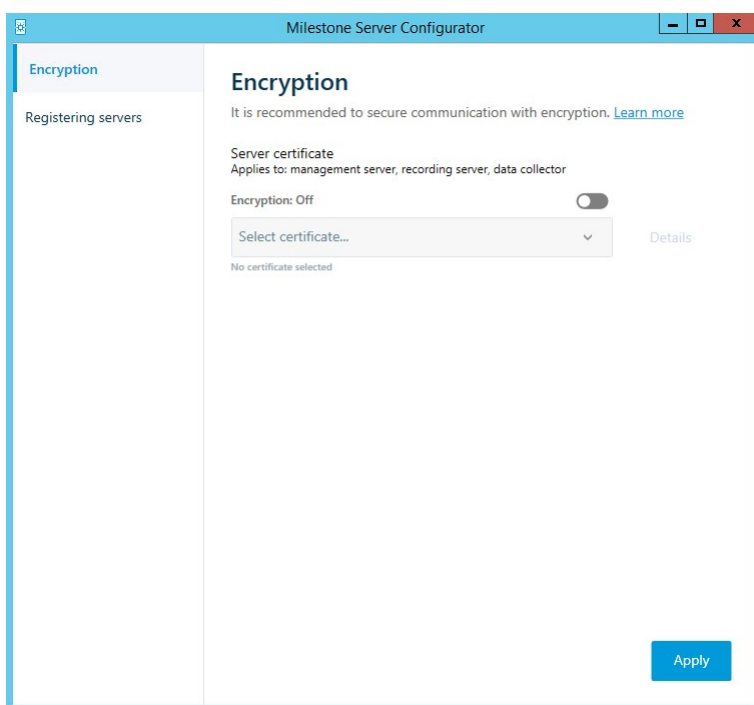
1. On the computer that runs the management server, right-click the Management Server Manager icon in the notification area and select **Server Configurator**.

The **Server Configurator** window appears. The options in this window depend on what servers are installed on the computer.

2. Under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each recording server and each server with a data collector (Event Server, Log Server, LPR Server, and Mobile Server). For more information, see [Enable server encryption for recording servers or remote servers](#) on page 398.

Enable server encryption for recording servers or remote servers

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see Encryption from the management server to the recording server (explained) on page 66 and Encryption between the management server and the Data Collector Server (explained) on page 68.

Prerequisites:

- You have enabled encryption on the management server, see Enable encryption on page 397

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

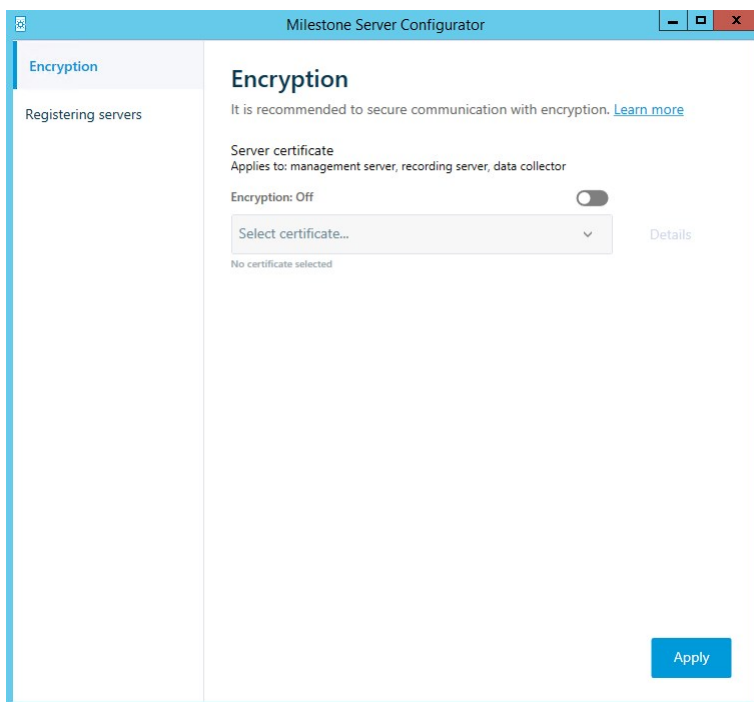
The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.



When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

Enable encryption to clients and servers

You can encrypt connections from the recording server to clients and servers that stream data from the recording server. For more information, see *Encryption to clients and servers that retrieve data from the recording server (explained)* on page 69.

Prerequisites:

- The server authentication certificate to be used is trusted on all computers running services that retrieve data streams from the recording server
- XProtect Smart Client and all services that retrieve data streams from the recording server must be version 2019 R1 or later
- Some third-party solutions created using MIP SDK versions earlier than 2019 R1 may need to be updated

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

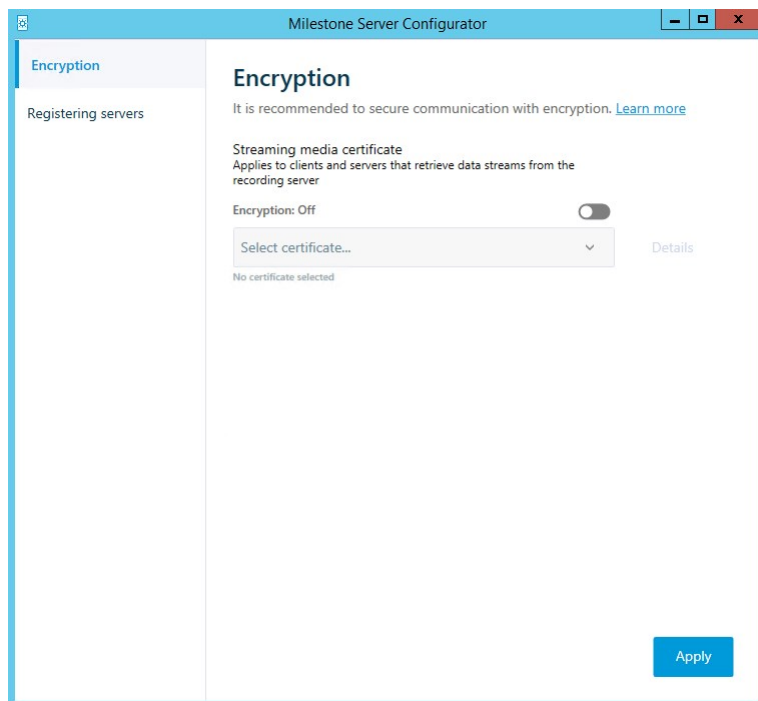
The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Streaming media certificate**, turn on encryption and select the certificate to encrypt communication between the clients and servers that retrieve data streams from the recording server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.



When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

To verify if the recording server uses encryption, see View encryption status to clients on page 402.


Enable encryption on the mobile server

To use an HTTPS protocol for establishing secure connection between the mobile server and clients and services, you must apply a valid certificate on the server. The certificate confirms that the certificate holder is authorized to establish secure connections. For more information, see Mobile server data encryption (explained) on page 71 and Mobile server encryption requirements for clients on page 72.



Certificates issued by CA (Certificate Authority) have a chain of certificates and on the root of that chain is the CA root certificate. When a device or browser sees this certificate, it compares its root certificate with pre-installed ones on the OS (Android, iOS, Windows, etc.). If the root certificate is listed in the pre-installed certificates list, then the OS ensures the user that the connection to the server is secure enough. These certificates are issued for a domain name and are not free of charge.


To enable encryption, after the mobile server has been installed:

1. On a computer with a mobile server installed, right-click the Mobile Server Manager tray icon in the taskbar of the operating system and select **Edit certificate**.
2. Select the **Encrypt the connections for clients and services that retrieve data streams from the mobile server** check box.
3. To select a valid certificate, click . A Windows Security dialog box opens.
4. Select the certificate that you want to apply.
5. Click **OK**.

Edit certificate

If the certificate that you use for secure connection has expired, you can select another certificate that is installed on the computer on which the mobile server is running.

To change a certificate:

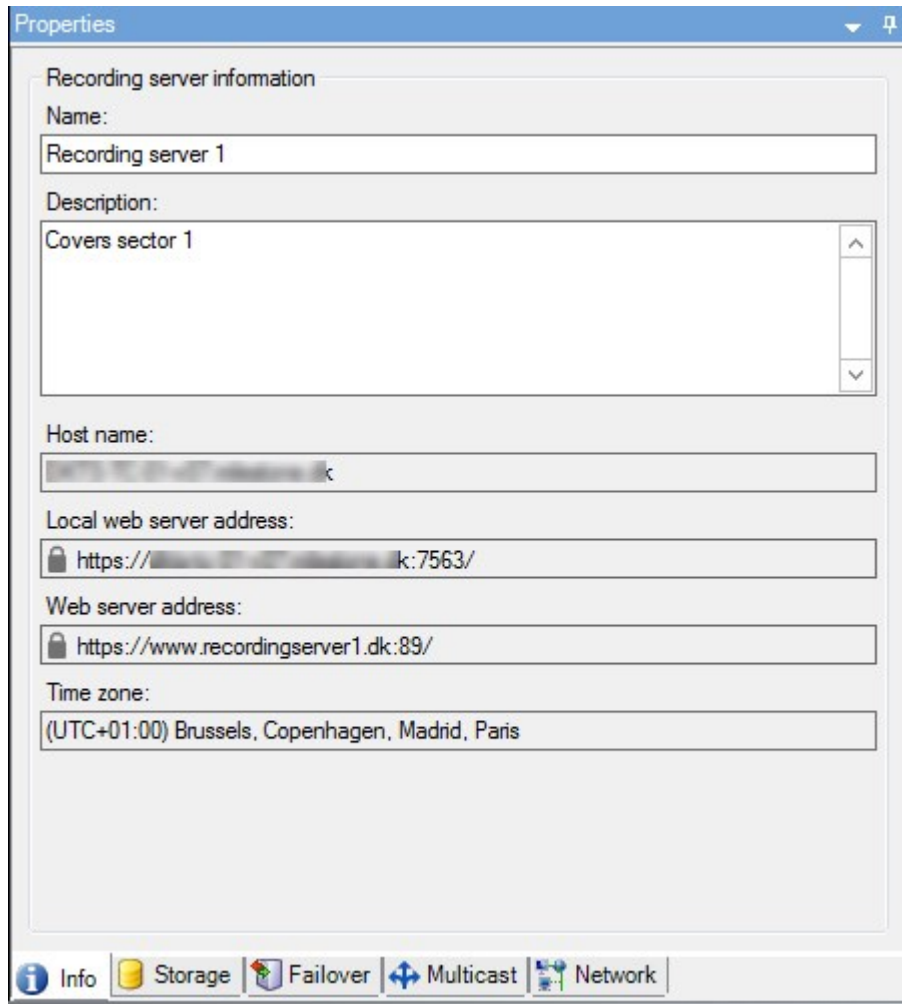
1. On a computer with a mobile server installed, right-click the Mobile Server Manager tray icon in the taskbar of the operating system and select **Edit certificate**.
2. To select a valid certificate, click . A Windows Security dialog box opens.
3. Select the certificate that you want to apply.
4. Click **OK**.

A message informs you that the certificate has been installed and that the Mobile Server service has been restarted to apply the change.

View encryption status to clients

To verify if your recording server encrypt connections:

1. Open the Management Client.
2. In the **Site Navigation** pane, select **Servers > Recording Servers**. This opens a list of recording servers.
3. In the **Overview** pane, select the relevant recording server and go to the **Info** tab.
If encryption is enabled to clients and servers that retrieve data streams from the recording server, a padlock icon appears in front of the local web server address and the optional web server address.



The screenshot shows the 'Properties' dialog box for a recording server. The 'Recording server information' section contains the following fields:

- Name:** Recording server 1
- Description:** Covers sector 1
- Host name:** [Redacted]
- Local web server address:** https://[Redacted]:7563/ (with a padlock icon)
- Web server address:** https://www.recordingserver1.dk:89/ (with a padlock icon)
- Time zone:** (UTC+01:00) Brussels, Copenhagen, Madrid, Paris

The bottom of the dialog box features a tabbed interface with the following tabs: Info, Storage, Failover, Multicast, and Network.

Configuring Milestone Federated Architecture

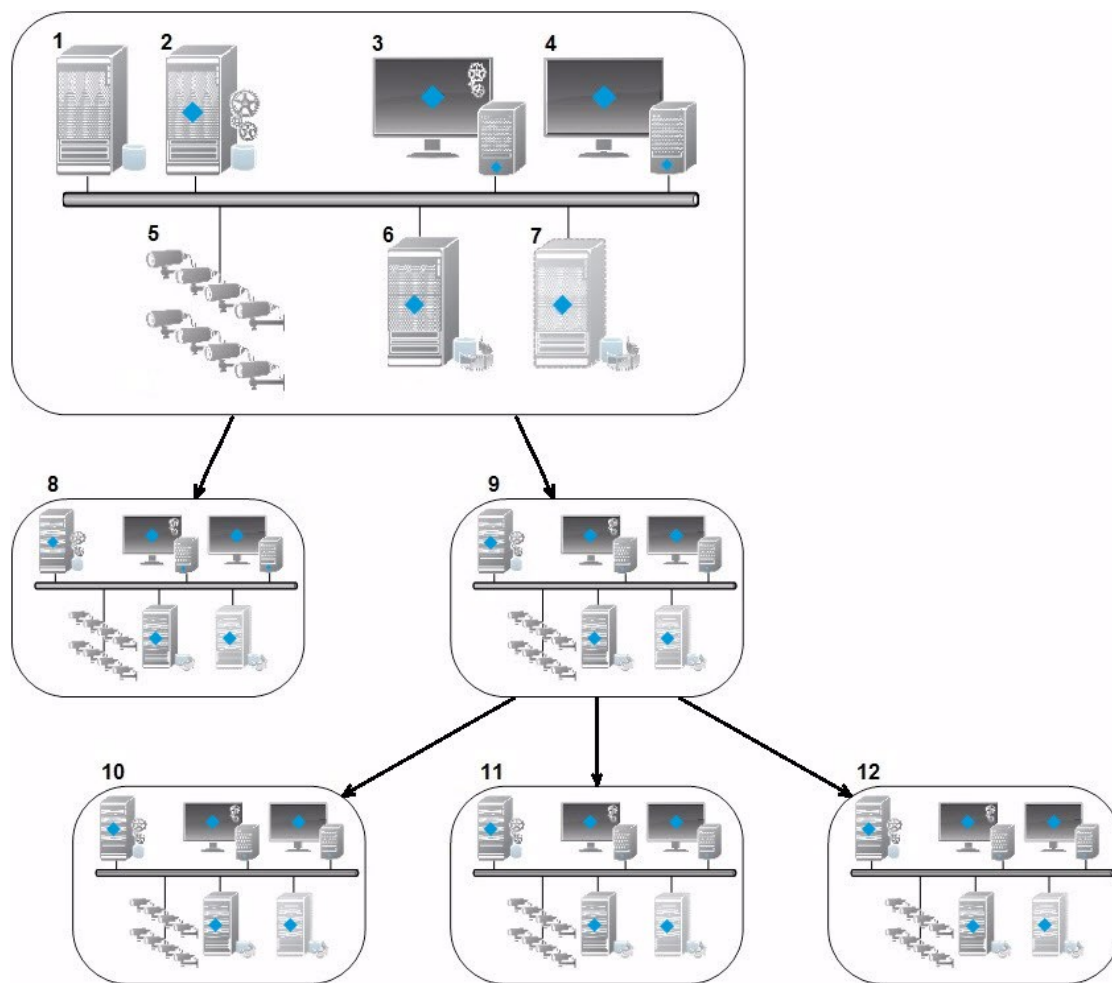


XProtect Expert can only be federated as child sites.

Milestone Federated Architecture links multiple individual standard systems into a federated site hierarchy of parent/child sites. Client users with sufficient rights have seamless access to video, audio and other resources across individual sites. Administrators can centrally manage all sites from version 2018 R1 and newer within the federated hierarchy, based on administrator rights for the individual sites.

Basic users are not supported in Milestone Federated Architecture systems, so you must add users as Windows users through the Active Directory service.

Milestone Federated Architecture is set up with one central site (top site) and an unlimited number of federated sites (see Set up your system to run federated sites on page 407). When you are logged into a site, you can access information about all of its child sites and the child sites' child sites. The link between two sites is established, when you request the link from the parent site (see Add site to hierarchy on page 408). A child site can only be linked to one parent site. If you are not the administrator of the child site when you add it to the federated site hierarchy, the request must be accepted by the child site administrator.



The components of a Milestone Federated Architecture setup:

1. Server with SQL Server
2. Management server
3. Management Client
4. XProtect Smart Client
5. Cameras

6. Recording server
7. Failover recording server
8. to 12. Federated sites

Hierarchy synchronization

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

Data traffic

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

Milestone Federated Architecture with other products

- If the central site uses XProtect Smart Wall, you can also use the XProtect Smart Wall features in the federated site hierarchy. See [Configure Smart Walls](#) on page 252 on how set up XProtect Smart Wall
- If the central site uses XProtect Access and XProtect Smart Client user logs into a site in a federated site hierarchy, access request notifications from the federated sites also appear in XProtect Smart Client
- You can add XProtect Expert 2013 systems or newer to the federated site hierarchy as child sites, not as parent sites
- Milestone Federated Architecture does not require additional licenses
- For more information about use cases and benefits, see the white paper about the Milestone Federated Architecture technology on the Milestone website

Establishing a federated site hierarchy

Before you start building up the hierarchy in the Management Client, Milestone recommends that you map how you want your sites to link together.

You install and configure each site in a federated hierarchy as a normal standalone system with standard system components, settings, rules, schedules, administrators, users, and user rights. If you already have the sites installed and configured and only need to combine them in a federated site hierarchy, your systems are ready to be set up.

Once the individual sites are installed, you must set them up to run as federated sites (see Set up your system to run federated sites on page 407).

To start the hierarchy, you can log into the site that you want to work as the central site and add (see Add site to hierarchy on page 408) the first federated site. When the link is established, the two sites automatically create a federated site hierarchy in the **Federated Site Hierarchy** pane in the Management Client to which you can add more sites to grow the federated hierarchy.

When you have created a federated site hierarchy, users and administrators can log into a site to access that site and any federated sites it may have. Access to federated sites depend on the user rights.

There is no limit to the number of sites you can add to the federated hierarchy. Also, you can have a site on an older product version linked to a newer version and vice versa. The version numbers appear automatically and cannot be deleted. The site that you are logged into is always at the top of the **Federated Site Hierarchy** pane and is called home site.

Below is an example of federated sited in the Management Client. To the left, the user has logged into the top site. To the right, the user has logged into one of the child sites, the Paris Server, which is then the home site.



Status icons in Milestone Federated Architecture

The icons represent the possible states of a site:

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

Set up your system to run federated sites

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

Alternative 1: Connect sites from the same domain (with a common domain user)

Before you install the management server, you must create a common domain user and configure this user as the administrator on all servers involved in the federated site hierarchy. How you connect the sites depends on the created user account.

With a Windows user account

1. Start the installation of the product on the server to be used as the management server and select **Custom**.
2. Select to install the Management Server service using a user account. The selected user account must be the administrator account used on all management servers. You must use the same user account when you install the other management servers in the federated site hierarchy.
3. Finish the installation. Repeat steps 1-3 to install any other systems you want to add to the federated site hierarchy.
4. Add site to hierarchy (see Add site to hierarchy on page 408).

With a Windows built-in user account (network service)

1. Start the installation of the product on the first server to be used as the management server and select **Single Computer** or **Custom**. This installs the management server using a network service account. Repeat this step for all the sites in your federated site hierarchy.
2. Log into the site that you want as your central site in the federated site hierarchy.
3. In the Management Client, expand **Security > Roles > Administrators**.
4. On the **Users and Groups** tab, click **Add** and select **Windows User**.
5. In the dialog box, select **Computers** as object type, enter the server name of the federated site and click **OK** to add the server to the **Administrator** role of the central site. Repeat this step until you have added all the federated sites in this way and exit the application.
6. Log into each federated site, and add the following servers to the **Administrator** role, in the same way as above:
 - The parent site server.
 - The child site servers that you want to connect directly to this federated site.
7. Add site to hierarchy (see Add site to hierarchy on page 408).

Alternative 2: Connecting sites from different domains

To connect to sites across domains, make sure that the domains trust each other. You set up domains to trust each other in the Microsoft Windows Domain configuration. When you have established trust between the different domains on each site in the federated site hierarchy are placed, follow the same description as described in Alternative 1. For more information about how to set up trusted domains, see the Microsoft website ([https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481\(v=technet.10\)/](https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/)).



Milestone recommends Milestone Interconnect for creating connected multi-site systems with multiple domains.

Alternative 3: Connect sites in workgroup(s)

When you connect sites inside workgroups, the same administrator account must be present on all servers you want connected in the federated site hierarchy. You must define the administrator account before you install the system.

1. Log into **Windows** using a common administrator account.
2. Start the installation of the product and click **Custom**.
3. Select to install the Management Server service using the common administrator account.
4. Finish the installation. Repeat steps 1-4 to install any other systems you want to connect. You must install all of these systems using the common administrator account.
5. Add site to hierarchy (see Add site to hierarchy on page 408).



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




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


Add site to hierarchy

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


1. Select the **Federated Site Hierarchy** pane.
2. Select the site to which you want to add a child site, right-click, and click **Add Site to Hierarchy**.
3. Enter the URL of the requested site in the **Add Site to Hierarchy** window and click **OK**.
4. The parent site sends a link request to the child site and after a while, a link between the two sites is added to the **Federated Site Hierarchy** pane.

5. If you can establish the link to the child site without requesting acceptance from the child site administrator, go to step 7.


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

6. Make sure that the administrator of the child site authorizes the link request from the parent site (see Accept inclusion in the hierarchy on page 409).
7. The new parent/child link is established and the **Federated Site Hierarchy** pane is updated with the  icon for the new child site.

Accept inclusion in the hierarchy

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

To accept a link request:

1. Log into the site.
2. In the **Federated Site Hierarchy** pane, right-click the site and click **Accept Inclusion in Hierarchy**.
If the site runs the XProtect Expert version, you right-click the site in the **Site Navigation** pane.
3. Click **Yes**.
4. The new parent/child link is established and the **Federated Site Hierarchy** pane is updated with the normal site  icon for the selected site.

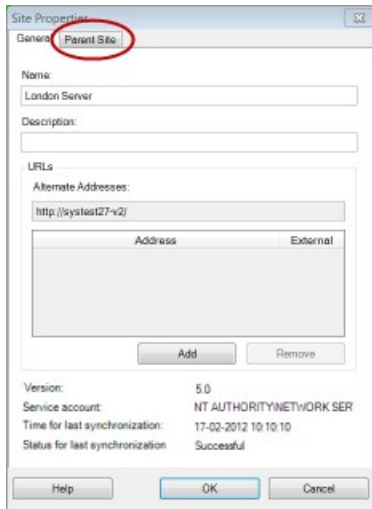


Changes that you make to child sites located far from the parent site can take some time to be reflected in the **Federated Site Hierarchy** pane.

Set site properties

You can view and, possibly, edit properties on your home site and its child sites.

1. In the Management Client, in the **Federated Site Hierarchy** pane, select the relevant site, right-click, and select **Properties**.



2. If needed, change the following:

General tab (see General tab on page 411)

Parent Site tab (see Parent Site tab on page 412) (**available on child sites only**)



Due to synchronization issues, any changes made to remote children might take some time to be reflected in the **Site Navigation** pane.

Refresh site hierarchy

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

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

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

This will take a few seconds.



Log into other sites in the hierarchy

You can log into other sites and administrate these. The site you are logged into is your home site.

1. In the **Federated Site Hierarchy** pane, right-click the site that you want to log into.
2. Click **Log into Site**.
The Management Client for that site opens.
3. Enter login information and click **OK**.
4. After login is complete, you are ready to do your administrative tasks for that site.

Detach a site from the hierarchy

When you detach a site from its parent site, the link between the sites are broken. You can detach sites from the central site, from the site itself or its parent site.

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

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

Federated site properties

This section describes the **General** tab and the **Parent Site** tab.

General tab

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

Name	Description
Name	Enter the name of the site.
Description	Enter a site description.
URLs	Use the list to add and remove URL(s) for this site and indicate if they are external or not. External addresses can be reached from outside the local network.
Version	The version number of the site's management server.

Name	Description
Service account	The service account under which the management server is running.
Time for last synchronization	Time and date of the last synchronization of the hierarchy.
Status for last synchronization	The status of the last synchronization of the hierarchy. It can be either Successful or Failed .

Parent Site tab

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

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

Configuring Milestone Interconnect

This section describes Milestone Interconnect and how to configure the feature.

Selecting Milestone Interconnect or Milestone Federated Architecture (explained)

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

Milestone recommends Milestone Federated Architecture when:

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

Milestone recommends Milestone Interconnect when:

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

Milestone Interconnect and licensing

To run Milestone Interconnect, you need Milestone Interconnect camera licenses on your central site to view video from hardware devices on remote sites. Only XProtect Corporate can act as a central site.

The status of your Milestone Interconnect camera licenses are listed on the **License Information** page of the central site.

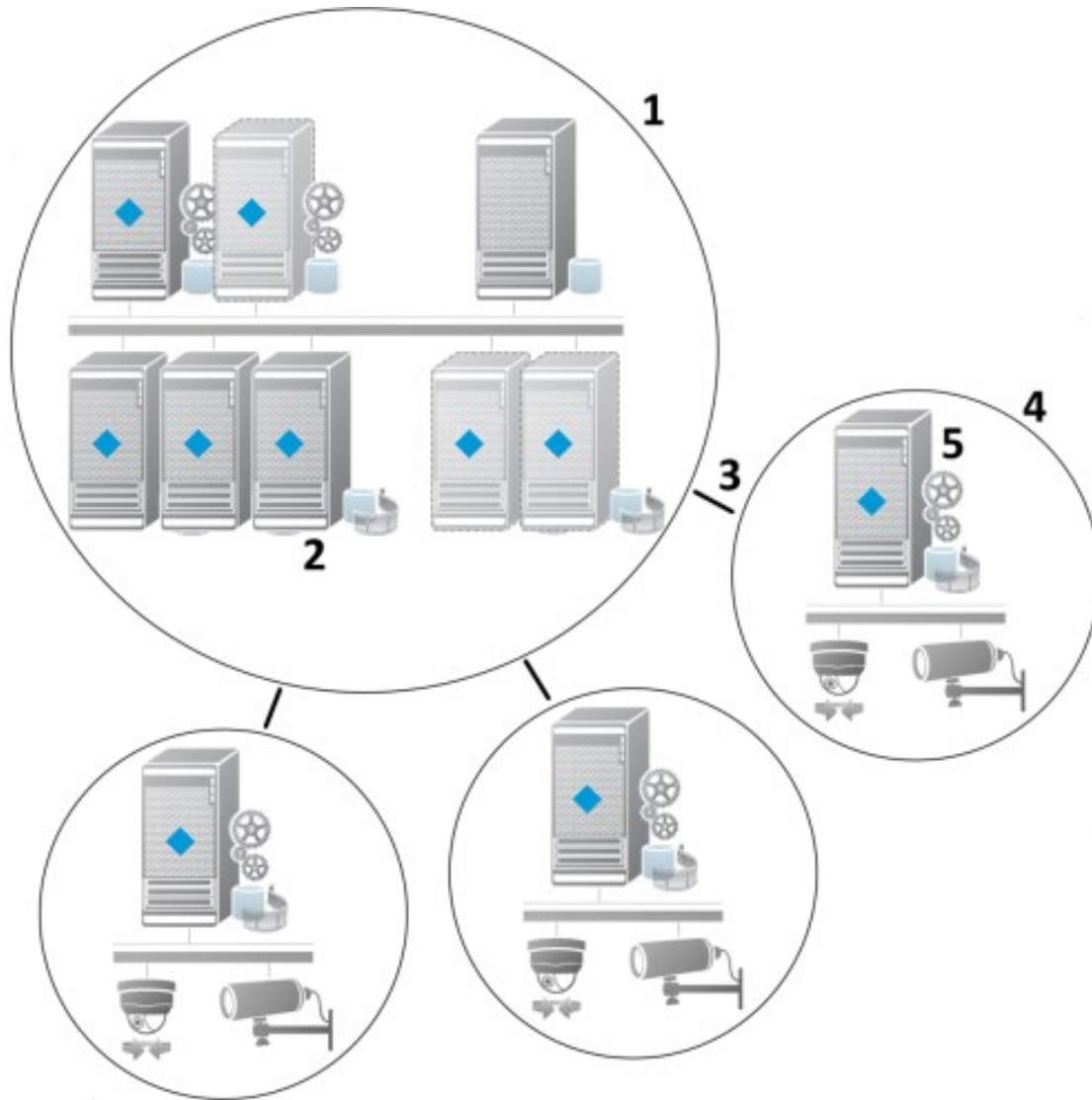
Milestone Interconnect (explained)



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

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



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

You add remote sites to your central site with the **Add Hardware** wizard from the central site (see Add a remote site to your central Milestone Interconnect site on page 416).

Each remote site runs independently and can perform any normal surveillance tasks. Depending on the network connections and appropriate user rights (see Assign user rights on page 417), Milestone Interconnect offers you direct live viewing of remote site cameras and play back of remote site recordings on the central site.

The central site can only see and access devices that the specified user account (when adding the remote site) has access to. This allows local system administrators to control which devices should be made available to the central site and its users.

On the central site, you can view the system's own status for the interconnected cameras, but not directly the state of the remote site. Instead, to monitor the remote site, you can use the remote site events to trigger alarms or other notifications on the central site (see Configure your central site to respond to events from remote sites on page 419).

It also offers you the possibility to transfer remote site recordings to the central site based on either events, rules/schedules, or manual requests by XProtect Smart Client users.

Only XProtect Corporate systems can work as central sites. All other products can act as remote sites including XProtect Corporate. It differs from setup to setup which versions, how many cameras, and how devices and events originating from the remote site are handled - if at all - by the central site. For further details on how specific XProtect products interact in a Milestone Interconnect setup, go to the Milestone Interconnect website (<https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/>).

Milestone Interconnect setups (explained)

There are three ways to run Milestone Interconnect. How to run your setup depends on your network connection, how to play back recordings, and whether you retrieve remote recordings and to what degree.

In the following, the three most likely setups are described:

Direct playback from remote sites (good network connections)

The most straightforward setup. The central site is continuously online with its remote sites and the central site users play back remote recordings directly from the remote sites. This requires use of the **Play back recordings from remote system** option (see Enable playback directly from remote site camera on page 418).

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

Used when selected recording sequences (originating from remote sites) should be stored centrally to ensure independence from remote sites. Independence is crucial in case of network failure or network restrictions. You configure remote recordings retrieval settings on the **Remote Retrieval** tab (see Remote Retrieval tab on page 189).

Remote recordings retrieval can be started from the XProtect Smart Client when needed or a rule can be set up. In some scenarios, remote sites are online and in others, offline most of the time. This is often industry specific. For some industries it is common for the central site to be permanently online with its remote sites (for example a retail HQ (central site) and a number of shops (remote sites)). For other industries, like transportation, the remote

sites are mobile (for example, busses, trains, ships, and so on) and can only establish network connection randomly. Should the network connection fail during a commenced remote recording retrieval, the job continues at next given opportunity.

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

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

Uses remote sites like a recording server uses the edge storage on a camera. Typically, remote sites are online with their central site, feeding it a live stream that the central site records. Should the network fail for some reason, the central site misses out on recording sequences. However, once the network is reestablished, the central site automatically retrieves remote recordings covering the down-period. This requires use of the **Automatically retrieve remote recordings when connection is restored** option (see Retrieve remote recordings from remote site camera on page 418) on the **Record** tab for the camera.

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

Add a remote site to your central Milestone Interconnect site

You add remote sites to the central site with the **Add Hardware** wizard.

Requirements

- Sufficient number of Milestone Interconnect camera licenses (see Milestone Interconnect and licensing on page 413)
- Another configured and working XProtect system including a user account (basic users, local Windows user or Windows Active Directory user) with rights for the devices that the central XProtect Corporate system should be able to access
- Network connection between the central XProtect Corporate site and the remote sites with access or port forwarding to the ports used on the remote sites

To add a remote site:

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the relevant recording server and right-click.
3. Select **Add Hardware** to start the wizard.
4. On the first page select **Address range scanning** or **Manual** and click **Next**.
5. Specify user names and passwords. The user account must be predefined on the remote system. You can add user names and passwords as needed by clicking **Add**. When ready, click **Next**.
6. Select the drivers to use when you scan. In this case choose between the Milestone drivers. Click **Next**.

- Specify the IP addresses and port numbers you want to scan. Default is port 80. Click **Next**.

Wait while your system detects the remote sites. A status indicator shows the detection process. In case of a successful detection, a **Success** message appears in the **Status** column. If you fail to add, you can click the **Failed** error message to see why.

- Choose to enable or disable successfully detected systems. Click **Next**.
- Wait while your system detects hardware and collects device specific information. Click **Next**.
- Choose to enable or disable successfully detected hardware and devices. Click **Next**.
- Select a default group. Click **Finish**.
- After installation, you can see the system and its devices in the **Overview** pane.

Depending on the user rights for the selected user on the remote site, the central site gets access to all cameras and functions or a sub-set of them.

Assign user rights

You configure user rights for an interconnected camera as you do with other cameras, by creating a role and assigning access to functions.

- On the central site, in the **Site Navigation** pane, expand **Security** and select **Roles**.
- In the Overview pane, right-click the built-in administrator role and select **Add Role** (see Add and manage a role on page 329).
- Name the role and configure the settings on the **Device** tab (see Roles settings on page 331) and the **Remote Recordings** tab (see Roles settings on page 331).

Update remote site hardware

If the configuration has been changed on a remote site, for example, added or removed cameras and events, you must update the configuration on the central site to reflect the new configuration on the remote site.

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

Establish remote desktop connection to remote system

You can connect remotely to systems in your Milestone Interconnect setup.

Requirements

The remote desktop connections to the computer you want to remote to must be up and running.

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

Enable playback directly from remote site camera

If your central site is continuously connected with its remote sites, you can configure your system so that the users playback the recordings directly from the remote sites. See also possible Milestone Interconnect setups (see Milestone Interconnect setups (explained) on page 415).

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

In a Milestone Interconnect setup, the central site disregards privacy masks defined in a remote site. If you want to apply the same privacy masks, you must redefine it on the central site.

Retrieve remote recordings from remote site camera

If your central site is **not** continuously connected with its remote sites, you can configure your system to store remote recordings centrally and you can configure retrieval of remote recordings when the network connection is optimal. See also possible Milestone Interconnect setups (see Milestone Interconnect setups (explained) on page 415).

To allow users to actually retrieve recordings, you must enable this permission for the relevant role (see Roles settings on page 331).

To configure your system:

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant remote server.
3. In the Properties pane, select the **Remote Retrieval** tab and update the settings (see Remote Retrieval tab on page 189).

If the network fails for some reason, the central site misses out on recording sequences. You can configure your system to let the central site automatically retrieve remote recordings to cover the down-period, once the network is reestablished.

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.
3. In the Properties pane, select the **Record** tab, and select the **Automatically retrieve remote recordings when connection is restored** option (see Devices that support pre-buffering on page 211).
4. In the toolbar, click **Save**.

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

In a Milestone Interconnect setup, the central site disregards privacy masks defined in a remote site. If you want to apply the same privacy masks, you must redefine it on the central site.

Configure your central site to respond to events from remote sites

You can use events defined on the remote sites to trigger rules and alarms on your central site and thereby respond immediately to events from the remote sites. This requires that the remote sites are connected and online. The number and type of events depend on the events configured and predefined in the remote sites.

The list of supported events is available on the Milestone website (<https://www.milestonesys.com/>).

You cannot delete predefined events.

Requirements:

- If you want to use user-defined/manual events from the remote sites as triggering events, you must first create these on the remote sites
- Make sure that you have an updated list of events from the remote sites (see Update remote site hardware on page 417)

Add a user-defined/manual event from a remote site:

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, select the relevant remote server and the **Events** tab.
3. The list contains the predefined events. Click **Add** to include user-defined or manual events from the remote site in the list.

Use an event on a remote site to trigger an alarm on the central site:

1. On the central site, expand **Alarms** and select **Alarm Definitions**.
2. In the Overview pane, right-click **Alarm Definitions** and click **Add New**.
3. Enter values as needed.
4. In the **Triggering Event** field, you can select between the supported predefined and user-defined events.
5. In the **Sources** field, select the remote server representing the remote site that you want alarms from.
6. Save the configuration when done.

Use an event on a remote site to trigger a rule-based action on the central site:

1. On the central site, expand **Rules and Events** and select **Rules**.
2. In the Overview pane, right-click **Rules** and click **Add Rule**.
3. In the wizard that appears, select **Perform an action on <event>**.
4. In the **Edit the rule description** area, click **event** and select between the supported predefined and user-defined events. Click **OK**.
5. Click **devices/recording server/management server** and select the remote server representing the remote site that you want the central site to start an action for. Click **OK**.
6. Click **Next** to get to the next wizard page.
7. Select the conditions that you want to apply for this rule. If you do not select any conditions, the rule always applies. Click **Next**.
8. Select an action and specify the details in the **Edit the rule description** area. Click **Next**.
9. Select a stop criterion if required. Click **Next**.
10. Select a stop action if required. Click **Finish**.

Configuring remote connect services



Available functionality depends on the system you are using. See <https://www.milestonesys.com/solutions/platform/product-index/> for more information.

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

Remote connect services allows you to

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

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

Install STS environment for One-Click camera connection

Requirements

- Contact your system provider to obtain the needed user name and password for Axis Dispatch Services
 - Make sure your camera(s) support Axis Video Hosting System. Go to the Axis website to see supported devices (<https://www.axis.com/products/axis-guardian>)
 - If needed, update your Axis cameras with the newest firmware. Go to the Axis website to download firmware (<https://www.axis.com/techsup/firmware.php/>)
1. On each camera's homepage, go to **Basic Setup, TCP/IP**, and select **Enable AVHS** and **Always**.
 2. From your management server, go to the Milestone download page (<https://www.milestonesys.com/downloads/>) and download the **AXIS One-Click** software. Run the program to setup a suitable Axis secure tunnel framework.

Add/edit STSs

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

Register new Axis One-Click camera

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

4. The camera now appears under the relevant ST server.

The camera can have the following color coding:

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

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

Axis One-Click Camera connection properties

Name	Description
Camera password	Enter/edit. Provided with your camera at purchase. For further details, see your camera's manual or go to the Axis website (https://www.axis.com/).
Camera user	See details for Camera password .
Description	Enter/edit a description for the camera.
External address	Enter/edit the web address of the ST server to which the camera(s) connect.
Internal address	Enter/edit the web address of the ST server to which the recording server connects.
Name	If needed, edit the name of the item.
Owner authentication	See Camera password .

Name	Description
key	
Passwords (for Dispatch Server)	Enter password. Must be identical to the one received from your system provider.
Passwords (for ST server)	Enter password. Must be identical to the one entered d when the Axis One-Click Connection Component was installed.
Register/Unregister at the Axis Dispatch Service	Indicate whether you wish to register your Axis camera with the Axis dispatch service. Can be done at time of setup or later.
Serial number	Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
Use credentials	Select the check box if you decided to use credentials during the installation of the ST server.
User name (for Dispatch Server)	Enter a user name. The user name must be identical to the one received from your system provider.
User name (for ST server)	Enter user name. Must be identical to the one entered when the Axis One-Click Connection Component was installed.

Configuring smart map

This section describes how to:

- Configure the geographic backgrounds that you can choose for your smart map
- Enable editing of smart maps, including cameras, in XProtect Smart Client
- Set up your smart map with Milestone Federated Architecture

Geographic backgrounds (explained)

Before you can select a geographic background in XProtect Smart Client, first you must configure the geographic backgrounds in XProtect Management Client.

- **Basic world map** - use the standard geographic background provided in XProtect Smart Client. It requires no configuration. This map is intended for use as a general reference, and does not contain features such as country boundaries, cities, or other details. However, like the other geographic backgrounds, it does contain geo-reference data
- **Bing Maps** - connect to Bing Maps
- **Google Maps** - connect to Google Maps
- **OpenStreetMap** gives you three options:
 - Connect to the OpenStreetMap open source mapping project. For information about the organization's open database license or tile usage policy, see <https://www.openstreetmap.org/>
 - Connect to an alternative tile server of your own choice. See Specify OpenStreetMap tile server on page 424
 - Connect to your own local tile server



The Bing Maps and Google Maps options require access to the Internet, and you must purchase a key from Microsoft or Google.

Unless you are using your own, local tile server, OpenStreetMap also requires Internet access.

By default, Bing Maps and Google Maps display satellite imagery (Satellite). You can change the imagery, for example to aerial or terrain, to see different details. For more information, see [Change geographic backgrounds on smart maps](#).

Specify OpenStreetMap tile server

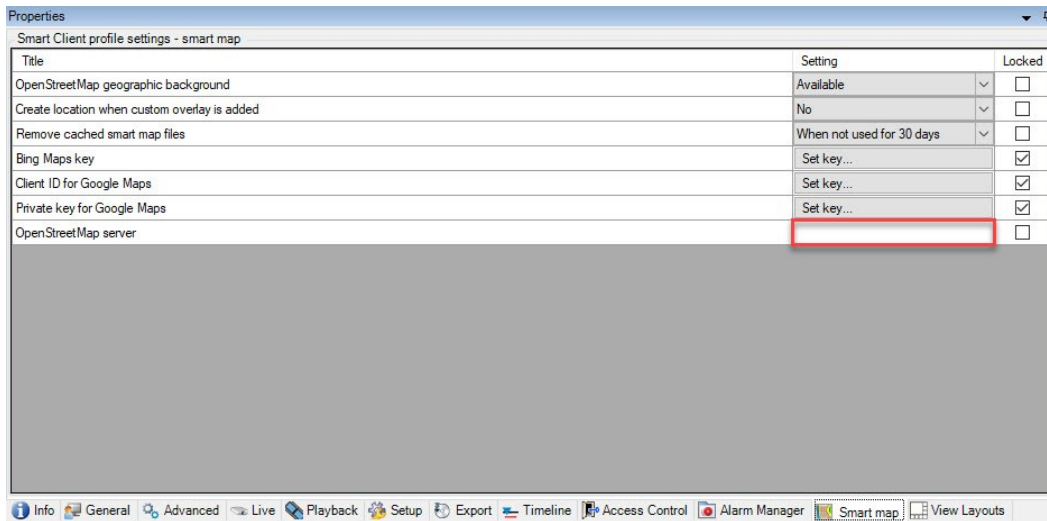
If you use the **OpenStreetMap** option as the geographic background for your smart map, you can change the location where the tiled images are retrieved from. You do this by changing the tile server address. This allows you to use a commercial tile server or a local tile server, for example if your organization has its own maps for areas such as airports or harbors.



The steps in the current topic describe how to specify the tile server address in XProtect Management Client. However, you can also specify the tile server address in the **Settings** window in XProtect Smart Client.

Steps:

1. In the **Site Navigation** pane, expand the **Client** node and click **Smart Client Profiles**.
2. In the overview pane, select the relevant Smart Client profile.
3. In the **Properties** pane, click the **Smart map** tab.



4. In the **OpenStreetMap server** field, enter the address of the tile server.
5. To prevent XProtect Smart Client users from changing the setting, select the **Locked** check box.
6. Save the changes.

Acquire API key for Google Maps or Bing Maps

Google Maps

To embed Google Maps into your smart map, you need a Maps Static API key from Google. To get the API key, first you must create a Google Cloud billing account. You are billed in accordance with the volume of map loads per month.

Once you have the API key, you must enter it in XProtect Management Client. See **Enable Bing Maps or Google Maps** in Management Client on page 426.

For more information, see:

- Google Maps Platform - get started: <https://cloud.google.com/maps-platform/>
- Guide to Google Maps Platform billing: <https://developers.google.com/maps/billing/gmp-billing>
- Developer guide for Maps Static API: <https://developers.google.com/maps/documentation/maps-static/dev-guide>

Bing Maps

To embed Bing Maps into your smart map, you need a Basic Key or an Enterprise Key. The difference is that basic keys are free, but allow a limited number of transactions before the transactions become billable or access to the map service is denied. The enterprise key is not free, but allow unlimited transactions.

For more information about Bing Maps, see (<https://www.microsoft.com/en-us/maps/licensing/>).

Once you have the API key, you must enter it in XProtect Management Client. See Enable Bing Maps or Google Maps in Management Client on page 426.

Enable Bing Maps or Google Maps in Management Client

You can make a key available to multiple users by entering it for a Smart Client profile in Management Client. All users who are assigned to the profile will use this key.

Steps:

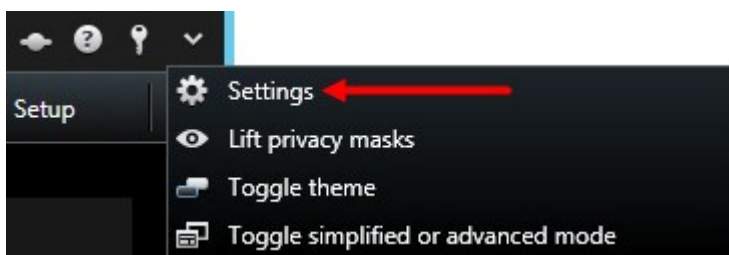
1. In Management Client, on the **Site Navigation** pane, click **Smart Client Profiles**.
2. In the **Smart Client Profiles** pane, select the relevant Smart Client profile.
3. In the **Properties** pane, click the **Smart map** tab:
 - For Bing Maps, enter your Basic Key or Enterprise Key in the **Bing Maps key** field
 - For Google Maps, enter your Maps Static API key in the **Private key for Google Maps** field
4. To prevent XProtect Smart Client operators from using a different key, select the **Locked** check box.

Enable Bing Maps or Google Maps in XProtect Smart Client

To allow XProtect Smart Client operators to use a different key than the key from the Smart Client profile, you must enter the key in the settings in XProtect Smart Client.

Steps:

1. In XProtect Smart Client, open the **Settings** window.



2. Click **Smart map**.
3. Depending on the map service you want to use, do one of the following:
 - For Bing Maps, enter your key in the **Bing Maps key** field
 - For Google Maps, enter your key in the **Private key for Google Maps** field

Cached smart map files (explained)

The files that you use for your geographic background are retrieved from a tile server. The time that the files are stored in the cache folder depends on the value selected in the **Removed cached smart map files** list in the **Settings** dialog in XProtect Smart Client. The files are stored either:

- Indefinitely (**Never**)
- For 30 days if the file is not used (**When not used for 30 days**)
- When the operator exits XProtect Smart Client (**On exit**)

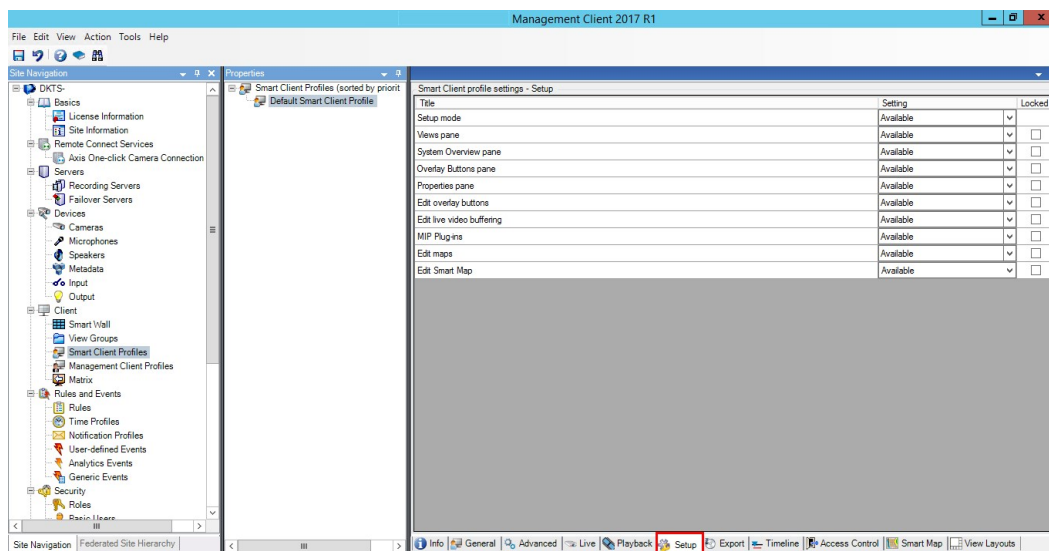
When you change the tile server address, automatically a new cache folder is created. The previous map files are retained in the associated cache folder on your local computer.

Enable smart map editing

Operators can edit smart maps in XProtect Smart Client in setup mode only if editing is enabled in Management Client. If not already enabled, you need to enable editing for each relevant Smart Client profile.

Steps:

1. In the **Site Navigation** pane, expand the **Client** node.
2. Click **Smart Client Profiles**.



3. In the overview pane, select the relevant Smart Client profile.
4. In the **Properties** pane, click the **Setup** tab.
5. In the **Edit smart map** list, select **Available**.

6. Repeat these steps for each relevant Smart Client profile.
7. Save your changes. Next time users assigned to the Smart Client profile you selected log into XProtect Smart Client, they will be able to edit smart maps.



To disable editing, in **Edit smart map** list, select **Unavailable**.

Enable editing of cameras on smart map

To allow operators to position a camera on the smart map, adjust the field of view, and direction, you must enable editing of cameras per role.

Requirements

Before you start, make sure that Smart map editing has been enabled (see Enable smart map editing on page 427). You do this on the Smart Client profile that the role of the operator is associated with.

Steps:

1. Expand the **Security** node > **Roles**.
2. In the **Roles** pane, select the role that your operator is associated with.
3. To give the role editing rights:
 - Click the **Overall Security** tab, and select **Cameras** in the **Role Settings** pane
 - In the **Allow** column, select the **Full control** or **Edit** check box
4. Save the changes.



The steps above gives the role the right to edit all cameras. To enable editing for individual cameras, go to the **Device** tab and select the relevant camera.

Set camera position, direction, field of view, and depth (smart map)

To ensure that a camera is positioned correctly on the smart map, you can set the geographic coordinates, the direction of the camera, the field of view, and the viewing depth. In doing so, automatically the camera is added to the smart map next time an operator loads it in XProtect Smart Client.

Steps:

1. In Management Client, expand the **Devices** node and select **Cameras**.
2. In the **Devices** pane, select the relevant camera group and camera.
3. On the **Info** tab, scroll down to **Positioning information**.

Properties

Device information

Name:
10.100.x.xxx_camera1

Short name:
Back entry

Description:

Hardware name:
Back entry →

Port number:
2

Positioning information

Geo coordinates:
55.6553634527205, 12.43028007233498
(Example: -33.856900, 151.215100)

Direction (a):
87,75 Degrees

Field of view (b):
150 Degrees

Depth (c):
112,36 Meter

Illustration:

Preview position in browser...

Info Settings Streams Record Motion Fisheye Lens Client Privacy Mask

4. Specify the latitude and the longitude in the **Geo coordinates** field, in that order. Use a period as decimal separator and a comma to separate the values.
5. In the **Direction** field, enter a value in the range of 0 and 360 degrees.
6. In the **Field of view** field, enter a value in the range of 0 and 360 degrees.
7. In the **Depth** field, enter the viewing depth, either in meters or feet.
8. Save the changes.



You can also set the properties on the recording servers.

Setting up smart map with Milestone Federated Architecture

When you use smart map in a Milestone Federated Architecture, all the cameras from the connected sites appear on the smart map. The overall steps in this topic describes how to set up smart map in a federated architecture.



For general information about Milestone Federated Architecture, see [Configuring Milestone Federated Architecture](#) on page 403.

1. Before connecting the top site with child sites, make sure that geographic coordinates have been specified on all cameras on all sites. Geographic coordinates are added automatically when a camera is positioned on the smart map through XProtect Smart Client, but you can also add them manually in Management Client in the camera properties. For more information, see [Set camera position, direction, field of view, and depth](#) (see [Set camera position, direction, field of view, and depth \(smart map\)](#) on page 428).
2. You must add the Smart Client operators as Windows users on the parent site and all the federated sites. At least on the top site, the Windows users must have smart map editing rights. This allows them to edit the smart map for the top site and all child sites. Next, you need to determine whether the Windows users on the child sites need smart map editing rights. In Management Client, first you create the Windows users under **Roles**, and then you enable smart map editing. For more information, see [Enable smart map editing](#) on page 427.
3. On the top site, add the child sites as Windows users to a role with administrator rights. When you specify the object type, select the **Computers** check box.
4. On each child site, add the top site as a Windows user to the same administrator role that is used on the top site. When you specify the object type, select the **Computers** check box.
5. On the top site, make sure that you can view the **Federated Site Hierarchy** window. In Management Client, go to **View** and select **Federated Site Hierarchy**. Add each of the child sites to the top site. For more information, see [Add site to hierarchy](#) on page 408.
6. Now you can test that it works in XProtect Smart Client. Log into the top site as administrator or as an operator, and open a view that contains the smart map. If the setup has been done correctly, all cameras from the top site and the child sites appear on the smart map. If you log into one of the child sites, you will see only the cameras from that site and its child sites.



To edit cameras on a smart map, for example the camera position and angle, users need camera editing rights.

Troubleshooting (smart map)

Error when adding camera to smart map

Error

If an operator tries to add cameras to a smart map manually, because the cameras were not added automatically when loading the smart map, the following error may be displayed: *Cannot save the map. Cannot perform the operation.*

What may cause the error is that the operator is running version 2017 R1 of XProtect Smart Client against an XProtect Corporate 2017 R2 installation. XProtect Smart Client looks for the GPS position of the camera on the event server, but in version 2017 R2 or newer of XProtect Corporate, the GPS position is stored on the management server.

Solution

Upgrade XProtect Smart Client to version 2017 R2 or newer.

Maintenance

Backing up and restoring system configuration

Milestone recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. It is important that you protect your backups, either through technical or organizational measures.

Backing up and restoring your system configuration (explained)

The system offers a built-in feature that backs up all the system configuration you can define in the Management Client. The log server database and the log files, including audit log files, are not included in this backup.

If your system is large, Milestone recommends that you define scheduled backups. This is done with the third-party tool: Microsoft® SQL Server Management Studio. This backup includes the same data as a manual backup.

During a backup, your system stays online.

Backing up your system configuration can take some time. Backup duration depends on:

- Your system configuration
- Your hardware
- Whether you have installed the SQL Server, Event Server component and the Management Server component on a single server or several servers

Each time you make a backup both manual and scheduled, the SQL database's transaction log file is flushed. For additional information about how to flush the transaction log file see SQL database transaction log (explained) on page 55.

Back up log server's SQL database

Handle the log server's SQL database by using the method that you use when handling system configuration as described earlier. The log server's SQL database contains all your system logs, including errors reported by recording servers and cameras. The default name of the log server's SQL database is **SurveillanceLogServerV2**.

The SQL database is located on the log server's SQL Server. Typically, the log server and the management server have their SQL databases on the same SQL Server. Backing up the log server SQL database is not vital since it does not contain any system configuration, but you may appreciate having access to system logs from before the management server backup/restore.

Manually backing up your system configuration (explained)

When you want to perform a manual backup of the management server's SQL database that contains your system configuration, make sure that your system stays online. The default name of the management server's SQL database is **Surveillance**.

Here are a few things to consider before you start the backup:

- You cannot use a backup of the SQL database to copy system configurations to other systems
- It can take some time to back up the SQL database. It depends on your system configuration, your hardware, and on whether your SQL Server, management server and Management Client are installed on the same computer
- Logs, including audit logs, are stored in the log server's SQL database and are therefore **not** part of a backup of the management server's SQL database. The default name of the log server's SQL database is **SurveillanceLogServerV2**. You back up both SQL databases the same way.

Backing up and restoring the event server configuration (explained)

The content of your event server configuration is included when you back up and restore system configuration.

The first time you run the event server, all its configuration files are automatically moved to the SQL database. You can apply the restored configuration to the event server without needing to restart the event server, and the event server can start and stop all external communication while the restoration of the configuration is being loaded.

Backup and restore fail and problem scenarios (explained)

If, after your last system configuration backup, you have moved the event server or other registered services such as the log server, you must select which registered service configuration you want for the new system. You can decide to keep the new configuration after the system is restored to the old version. You decide by looking at the host names of the services.

If your restore of the system configuration fails because the event server is not located at the specified destination (for example, if you have chosen the old registered service setup), do another restore.

Back up system configuration manually

1. From the menu bar, select **File > Backup Configuration**.
2. Read the note in the dialog box and click **Backup**.
3. Enter a file name for the .cnf file.
4. Enter a folder destination and click **Save**.
5. Wait until the backup is finished and click **Close**.



All relevant system configuration files are combined into one single .cnf file that is saved at a specified location. During the backup, all backup files are first exported to a temporary system backup folder on the management server. You can select another temporary folder by right-clicking the notification area's Management Server service icon and by selecting Select shared backup folder.

Restore system configuration from a manual backup

Important information

- Both the user who installs and the user who restores must be local administrator of the system configuration SQL database on the management server **and** on the SQL Server
- Except for your recording servers, your system is completely shut down for the duration of the restore, which can take some time
- A backup can only be restored on the system installation where it was created. Make sure that the setup is as similar as possible to when the backup was made. Otherwise, the restore might fail
- If you do a backup of the SQL database and restore it on a clean SQL Server, then the raise errors from the SQL database will not work and you will only receive one generic error message from the SQL Server. To avoid that, first reinstall your XProtect system using the clean SQL Server and then restore the backup on top of that
- If restoring fails during the validation phase, you can start the old configuration again because you have made no changes
If restoring fails elsewhere in the process, you cannot roll back to the old configuration
As long as the backup file is not corrupted, you can do another restore
- Restoring replaces the current configuration. This means that any changes to the configuration since last backup are lost
- No logs, including audit logs, are restored
- Once restoring has started, you cannot cancel it

Restoring

1. Right-click the notification area's Management Server service icon and select **Restore Configuration**.
2. Read the important note and click **Restore**.
3. In the file open dialog box, browse to the location of the system configuration backup file, select it, and click **Open**.



The backup file is located on the Management Client computer. If the Management Client is installed on a different server, copy the backup file to this server before you select the destination.

4. The **Restore Configuration** window opens. Wait for the restore to finish and click **Close**.

Select shared backup folder

Before backing up and restoring any system configuration, you must set a backup folder for this purpose.

1. Right-click the notification area's Management Server service icon and select **Select shared backup folder**.
2. In the window that appears, browse to the wanted file location.
3. Click **OK** twice.
4. If asked if you want to delete files in the current backup folder, click **Yes** or **No** depending on your needs

Scheduled backup and restore of system configuration (explained)

The management server stores your system's configuration in an SQL database. Milestone recommends that you regularly make scheduled backups of this SQL database as a disaster recovery measure. While it is rare to lose your system configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute, and backups also have the added benefit that they flush your SQL database's transaction log.

If you have a smaller setup and do not need scheduled backups, you can back up your system configuration manually. For instructions, see [Manually backing up your system configuration \(explained\)](#) on page 432.

When you back up/restore your management server, make sure that the SQL database with the system configuration is included in the backup/restore.

Requirements for using scheduled backup and restore

Microsoft® SQL Server Management Studio, a tool download-able for free from their website (<https://www.microsoft.com/downloads/>).

Apart from managing SQL Servers and their databases, the tool includes some easy-to-use backup and restoration features. Download and install the tool on your management server.

Back up system configuration with scheduled backup

1. From Windows' Start menu, launch Microsoft® SQL Server Management Studio.
2. When connecting, specify the name of the required SQL Server. Use the account under which you created the SQL database.
 1. Find the SQL database that contains your entire system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, and more. The default name of this SQL database is **Surveillance**.
 2. Make a backup of the SQL database and make sure to:
 - Verify that the selected SQL database is the correct one
 - Verify that the backup type is **full**
 - Set the schedule for the recurrent backup. You can read more about scheduled and automated backups on the Microsoft website (<https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017>)
 - Verify that the suggested path is satisfactory or select alternative path
 - Select to **verify backup when finished** and to **perform checksum before writing to media**
 3. Follow the instructions in the tool to the end.

Also consider backing up the log server's SQL database with your logs by using the same method. The default name for the log server's SQL database is **SurveillanceLogServerV2**.

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 database. You can apply the restored configuration to the event server without needing to restart the event server, and the event server can start and stop all external communication while the restoration of the configuration is being loaded.

Restore system configuration from a scheduled backup

Requirements

To prevent system configuration changes being made while you restore the system configuration SQL database, stop the:

- Management Server service (see Managing server services on page 448)
- 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 ([https://technet.microsoft.com/library/cc732317\(W5.10\).aspx/](https://technet.microsoft.com/library/cc732317(W5.10).aspx/))

Open Microsoft® SQL Server Management Studio from Windows' **Start** menu.

In the tool do the following:

1. When connecting, specify the name of the required SQL Server. Use the user account under which the SQL database was created.
2. Find the SQL database (the default name is **Surveillance**) that contains your entire system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.
3. Make a restore of the SQL database and make sure to:
 - Select to back up **from** device
 - Select backup media type **file**
 - Find and select your backup file (**.bak**)
 - Select to **overwrite the existing database**
4. Follow the instructions in the tool to the end.

Use the same method to restore the log server's SQL database with your logs. The default name of the log server's SQL database is **SurveillanceLogServerV2**.



The system does not work while the Management Server service is stopped. It is important to remember to start all the services again once you have finished restoring the database.

Moving the management server

The management server stores your system configuration in an SQL 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 SQL database. The system configuration SQL database can be stored in two different ways:

- **Network SQL Server:** If you are storing your system configuration in an SQL database on a SQL Server on your network, you can point to the SQL 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 host name and IP address applies and you should ignore the rest of this topic:

Management server host name 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 because the recording server automatically connects to the hostname and IP address of the old management server. If you give the new management server a new hostname and/or IP address, the recording server cannot find the management server and you must manually stop each Recording Server service in your system, change their management server URL, register the recording server again and when done, start the Recording Server service.

- **Local SQL Server:** If you are storing your system configuration in an SQL database on a SQL Server on the management server itself, it is important that you back up the existing management server's system configuration SQL database before the move. By backing up the SQL database, and subsequently restoring it on a SQL Server on the new management server, you avoid having to reconfigure your cameras, rules, time profiles, etc. after the move

Requirements

- **Your software installation file for installation on the new management server**
- **Your software license file (.lic)**, that you received when you purchased your system and initially installed it. You should not use the activated software license file which you have received after a manual offline license activation. An activated software license file contains information about the specific server on which the system is installed. Therefore, an activated software license file cannot be reused when moving to a new server

If you are also upgrading your system software in connection with the move, you have received a new software license file. Simply use this.

- **Local SQL Server users only: Microsoft® SQL Server Management Studio**
- What happens while the management server is unavailable? Unavailable management servers (explained) on page 438)
- Copy log server database (see Back up log server's SQL database on page 432)

Unavailable management servers (explained)

- **Recording servers can still record:** Any currently working recording servers received a copy of their configuration from the management server, so they can work and store recordings on their own while the management server is down. Scheduled and motion-triggered recording therefore works, and event-triggered recording works unless based on events related to the management server or any other recording server because these go through the management server
- **Recording servers temporarily store log data locally:** They automatically send log data to the management server when it becomes available again:
 - **Clients cannot log in:** Client access is authorized through the management server. Without the management server, clients cannot log in
 - **Clients that are already logged in can remain logged in for up to one hour:** When clients log in, they are authorized by the management server and can communicate with recording servers for up to one hour. If you can get the new management server up and running within an hour, many of your users are not affected
 - **No ability to configure the system:** Without the management server, you cannot change the system configuration

Milestone recommends that you inform your users about the risk of losing contact with the surveillance system while the management server is down.

Move the system configuration

Moving your system configuration is a three step process:

1. Make a backup of your system configuration. This is identical to making a scheduled backup (see Back up system configuration with scheduled backup on page 435).
2. Install the new management server on the new server. See scheduled backup, step 2.
3. Restore your system configuration to the new system. See Restore system configuration from scheduled backup (see Restore system configuration from a scheduled backup on page 436).

Replace a recording server

If a recording server is malfunctioning and you want to replace it with a new server that inherits the settings of the old recording server:

1. Retrieve the recording server ID from the old recording server:
 1. Select **Recording Servers**, then in the **Overview** pane select the old recording server.
 2. Select the **Storage** tab.
 3. Press and hold down the CTRL key on your keyboard while selecting the **Info** tab.

4. Copy the recording server ID-number in the lower part of the **Info** tab. Do not copy the term *ID*, only the number itself.



2. Replace the recording server ID on the new recording server:

1. Stop the Recording Server service on the old recording server, then in Windows' **Services** set the service's **Startup type** to **Disabled**.



It is very important that you do not start two recording servers with identical IDs at the same time.

2. On the new recording server, open an explorer and go to *C:\ProgramData\Milestone\XProtect Recording Server* or the path where your recording server is located.
3. Open the file *RecorderConfig.xml*.
4. Delete the ID stated in between the tags *<id>* and *</id>*.

```
- <recorderconfig>
- <recorder>
  <id>ff0b3d62-4b1b-4e9e-93ac-40073f4374b2</id>
```

5. Paste the copied recording server ID in between the tags *<id>* and *</id>*. Save the *RecorderConfig.xml* file.
6. Go to the registry: *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation*.
7. Open **RecorderIDOnMachine** and change the old recording server ID with the new ID.
3. Register the new recording server on the management server. To do that, right- click the Recording Server Manager tray icon and click **Register**. For more information, see Register a recording server on page 133.
4. Restart the Recording Server service. When the new Recording Server service starts up, it has inherited all settings from the old recording server.

Move hardware

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

The recordings on the old recording server remain there until:

- The system deletes them when the retention time expires. Recordings that someone has protected with Evidence Lock (see Evidence lock (explained) on page 380) is not deleted until the evidence lock's retention time expires. You define the retention time for evidence locks when you create them. Potentially the retention time never expires
- You delete them from each device's new recording server on the **Record** tab

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



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

You can use the move hardware feature to:

- **Load balance:** If, for example, the disk on a recording server is overloaded, you can add a new recording server and move some of your hardware
- **Upgrade:** If you, for example, have to replace the server that hosts the recording server with a newer model, you can install a new recording server and move the hardware from the old server to the new server
- **Replace a defective recording server:** If, for example, the server is offline and will never come online again, you can move the hardware to other recording servers and thereby keep the system running. You cannot access the old recordings. For more information, see Replace a recording server on page 438.

Remote recordings

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

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

Move hardware (wizard)

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

Requirements

Before you start the wizard:

- Make sure that the new recording server can access the physical camera via the network
- Install a recording server that you want to move hardware to (see [Install new XProtect components on page 84](#) or [Install new XProtect components on page 84](#))
- Install the same device pack versions on the new recording server that you run on the existing server (see [Device drivers \(explained\) on page 64](#))

To run the wizard:

1. In the **Site Navigation** pane, select **Recording Servers**.
2. In the **Overview** pane, right-click the recording server you want to move hardware from or right-click a specific hardware device.
3. Select **Move Hardware**.



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

4. If you started the wizard from the recording server level, the **Select the hardware you want to move** page appears. Select the hardware devices you want to move.
5. On the **Select the recording server you want to move the hardware to** page, select from the list of recording servers installed on this site.
6. On the **Select the storage you want to use for future recordings** page, the storage usage bar indicates the free space in the recording database for live recordings only, not the archives. The total retention time is the retention period for both the recording database and the archives.
7. The system processes your request.
8. If the move was successful, click **Close**. If you select the new recording server in the Management Client, you can see the moved hardware and now recordings are stored on this server.

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



In an interconnected system, you must manually synchronize the central site after moving hardware on a remote site to reflect the changes you, or another system administrator, made at the remote site.

Move hardware troubleshooting

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

Error type	Troubleshooting
The recording server is not connected or in failover mode.	Make sure that the recording server is online. You may need to register it. If the server is in failover mode, wait and try again.
The recording server is not the latest version.	Update the recording server so it runs the same version as the management server.
The recording server could not be found in the configuration.	Make sure that the recording server has not been removed.
Updating the configuration or communication with the configuration database failed.	Make sure that your SQL Server and database are connected and running.
Stopping the hardware on the current recording server failed	Maybe another process has locked the recording server, or the recording server is in error mode. Make sure that the recording server is running and try again.
The hardware does not exist.	Make sure that the hardware you try to move has not simultaneously been removed from the system by another user. The scenario is quite unlikely.
The recording server that hardware was moved from is back online, but you chose to ignore it when it was offline.	Most likely, you have accepted that the old recording server will never get online again when you started the Move Hardware wizard, but during the move, the server came online. Start the wizard again and select No when you are asked to confirm if the server comes online again.
The source recording storage is unavailable.	You are trying to move hardware with devices configured with a recording storage which is currently offline. A recording storage is offline if the disk is offline or otherwise

Error type	Troubleshooting
	<p>unavailable.</p> <p>Make sure that the recording storage is online and try again.</p>
All recording storages on the target recording server must be available.	<p>You are trying to move hardware to a recording server where one or more recording storages are currently offline.</p> <p>Make sure that all recording storages on the target recording server are online.</p> <p>A recording storage is offline of the disk is offline or otherwise unavailable.</p>

Replace hardware

When you replace a hardware device on your network with another hardware device, you must know the IP address, port, user name and password of the new hardware device.



If you have not enabled License information on page 124 and have used all device changes without activation (see License information on page 124), you must manually activate your licenses **after** replacing hardware devices. If the new number of hardware devices exceeds your total number of hardware device licenses, you have to purchase new hardware device licenses.

1. Expand the required recording server, right-click the hardware you want to replace.
2. Select **Replace Hardware**.
3. The **Replace Hardware** wizard appears. Click **Next**.

4. In the wizard, in the **Address** field (marked by red arrow in the image), enter the IP address of the new hardware. If known, select the relevant driver from the **Hardware Driver** drop-down list. Otherwise select **Auto Detect**. If port, user name or password data is different for the new hardware, correct this **before** starting the auto detect process (if needed).

Address	Port	User Name	Password	Hardware Driver
10.100.10.10	80	root	****	Axis 216MFD Camera

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

5. Do one of the following:

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

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

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



Make sure to map **all** cameras, microphones, inputs, outputs, etc. Contents mapped to **None**, are **lost**.

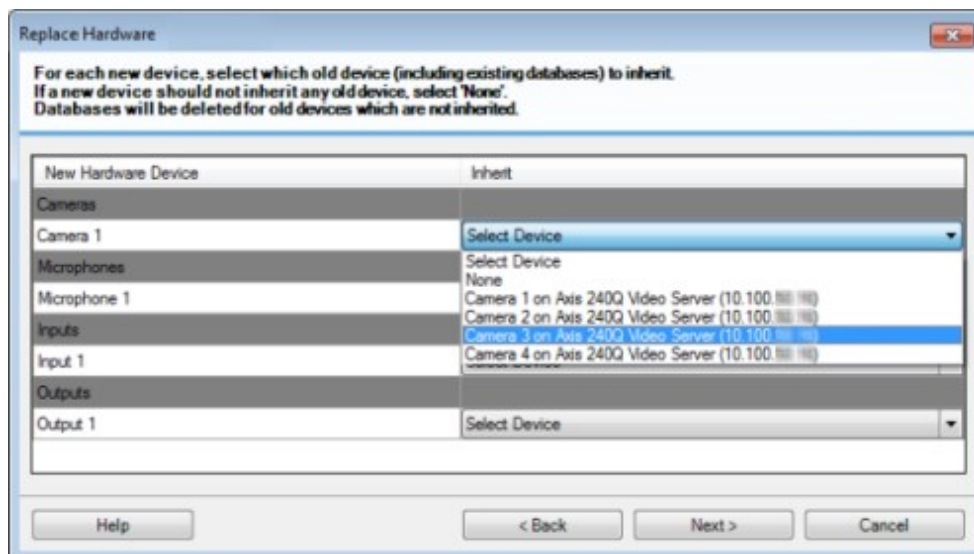
Replace Hardware

For each new device, select which old device (including existing databases) to inherit.
If a new device should not inherit any old device, select 'None'.
Databases will be deleted for old devices which are not inherited.

New Hardware Device	Inherit
Cameras	
Camera 1	Select Device
Camera 2	Select Device
Camera 3	Select Device
Camera 4	None Camera 1 on Axis 240Q Video Server (10.100.100.100)
Inputs	
Input 1	Select Device
Input 2	Select Device
Input 3	Select Device

Help < Back Next > Cancel

Example of the old hardware device having more individual devices than the new one:



Click **Next**.

6. You are presented with a list of hardware to be added, replaced or removed. Click **Confirm**.
7. Final step is a summary of added, replaced and inherited devices and their settings. Click **Copy to Clipboard** to copy contents to the Windows clipboard or/and **Close** to end the wizard.

Managing the SQL Server and databases

Changing the SQL Server and database addresses (explained)

When you install a system as a trial, or if you restructure a large installation, you may need to use a different SQL Server and database. You can do this with the **Update SQL Server Address** tool.

With the tool, you can change the address of the SQL Server and database used by the management server and by the event server, and the address of the SQL Server and database used by the log server. The only limitation is that you cannot change the management server and the event server's SQL addresses at the same time as the log server's SQL addresses. You can do it one after another.

You must change the SQL Server and database addresses locally on the computers where you have installed the management server, the event server and the log server. If your management server and event server are installed on separate computers, you must run the **Update SQL Server Address** tool on both computers.



You must copy the SQL databases before you proceed.

Change the log server's SQL Server and database

1. Go to the computer where your management server is installed and copy the folder *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (with content) to a temporary folder on the event server.
2. Paste the folder that you copied to a temporary place on the computer where the log server is installed and run the included file: *VideoOS.Server.ChangeSqlAddress.exe*. The **Update SQL Server Address** dialog box appears.
3. Select **Log Server** and click **Next**.
4. Enter or select the new SQL Server and click **Next**.
5. Select the new SQL database and click **Select**.
6. Wait while the address change takes place. Click **OK** to confirm.

Change the management server and event server's SQL addresses

The management server and event server uses the same SQL database.










1. If your management server and event server are located:
 1. together on the same computer and you want to update the SQL addresses, go to the computer where your management server is installed.
 2. on different computers and you want to update the management server's SQL address (and later the event server SQL address), go to the computer where your management server is installed.
 3. on different computers and you want to update the event server SQL address only (or you have already updated it on the management server), go to the computer where your management server is installed and copy the directory *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (with content) to temporary directory on the event server.
2. If you choose:
 1. steps **1.1** and **1.2**, go to the notification area of the taskbar. Right-click the **Management Server** icon, select **Update SQL address**. Repeat the process to update the event server SQL address.
 2. step **1.3**, paste the directory you copied to a temporary place on the computer where the event server is installed and run the included file: *VideoOS.Server.ChangeSqlAddress.exe*.
3. The **Update SQL Server Address** dialog box appears. Select **Management Server services** and click **Next**.
4. Enter or select the new SQL Server and click **Next**.
5. Select the new SQL database and click **Select**.
6. Wait while the address change takes place. When a confirmation message is presented, click **OK**.













Managing server services

On the computer that runs server services, you find server manager tray icons in the notification area. Through these icons, you can get information about the services and perform certain tasks. This includes, for example, checking the state of the services, viewing logs or status messages, and starting and stopping the services.

Server manager tray icons (explained)

The tray icons in the table show the different states of the services running on the management server, recording server, failover recording server, and event server. They are visible on the computers with the servers installed, in the notification area:

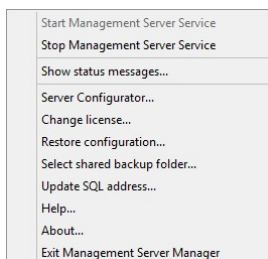
Management Server Manager tray icon	Recording Server Managertray icon	Event Server Manager tray icon	Failover Recording Server Manager tray icon	Description
				Running Appears when a server service is enabled and started. <div>  If the Failover Recording Server service is running, it can take over if the standard recording servers fails. </div>
				Stopped Appears when a server service has stopped.

Management Server Manager tray icon	Recording Server Managertray icon	Event Server Manager tray icon	Failover Recording Server Manager tray icon	Description
				<div>  <p>If the Failover Recording Server service stops, it cannot take over if the standard recording server fails.</p> </div>
				Starting Appears when a server service is in the process of starting. Under normal circumstances, the tray icon changes after a short while to Running .
				Stopping Appears when a server service is in the process of stopping. Under normal circumstances, the tray icon changes after a short while to Stopped .
				In indeterminate state Appears when the server service is initially loaded and until the first information is received, upon which the tray icon, under normal circumstances, changes to Starting and afterwards to Running .
				Running offline Typically appears when the Recording Server or Failover recording service is running but the Management Server service is not.

Start or stop the Management Server service

The Management Server Manager tray icon indicates the state of the Management Server service, for example **Running**. Through this icon, you can start or stop the Management Server service. If you stop the Management Server service, you cannot use the Management Client.

1. In the notification area, right-click the Management Server Manager tray icon. A context-menu appears.



2. If the service has stopped, click **Start Management Server service** to start it. The tray icon changes to reflect the new state.
3. To stop the service, click **Stop Management Server service**.

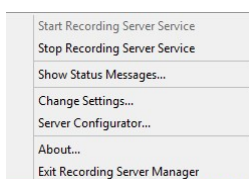


For more information about the tray icons, see Server manager tray icons (explained) on page 448.

Start or stop the Recording Server service

The Recording Server Manager tray icon indicates the state of the Recording Server service, for example **Running**. Through this icon, you can start or stop the Recording Server service. If you stop the Recording Server service, your system cannot interact with devices connected to the server. This means you cannot view live video or record video.

1. In the notification area, right-click the Recording Server Manager tray icon. A context-menu appears.



2. If the service has stopped, click **Start Recording Server service** to start it. The tray icon changes to reflect the new state.
3. To stop the service, click **Stop Recording Server service**.



For more information about the tray icons, see [Server manager tray icons \(explained\)](#) on page 448.

View status messages for Management Server or Recording Server

1. In the notification area, right-click the relevant tray icon. A context-menu appears.
2. Select **Show Status Messages**. Depending on the server type, either the **Management Server Status Messages** or **Recording Server Status Messages** window appears, listing time-stamped status messages:



Manage encryption with the Server Configurator

Use the Server Configurator to select certificates on local servers for encrypted communication and register server services to make them qualified to communicate with the servers.

Open the Server Configurator from either the Windows startup menu or from the management server tray icon.

Before you enable encryption, you must install security certificates on the computer that has the management server and on all computers with recording servers. For more information, see the *XProtect VMS Certificates guide*.

In the **Encryption** section of the Server Configurator, set encryption of the following types:

- **Server certificate**

Select the certificate to be used to encrypt the two-way connection between the management server, data collectors, and recording servers.



Encryption for the Mobile Server is enabled from the Mobile Server tray icon.

- **Streaming media certificate**

Select the certificate to be used to encrypt communication between the recording servers and all clients, servers, and integrations that retrieve data streams from the recording servers.

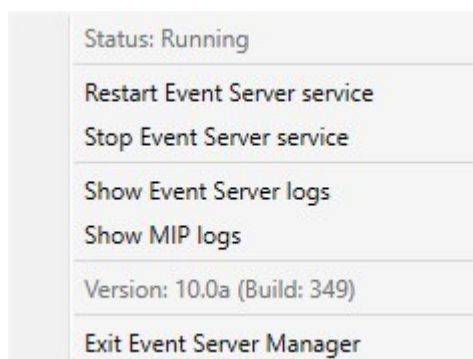
In the **Registering servers** section of the Server Configurator, register the servers that are running on the computer with the designated management server.

To register the servers, verify the address of the management server and select **Register**.

Start, stop, or restart the Event Server service

The Event Server Manager tray icon indicates the state of the Event Server service, for example **Running**. Through this icon, you can start, stop, or restart the Event Server service. If you stop the service, parts of the system will not work, including events and alarms. However, you can still view and record video. For more information, see Stopping the Event Server service on page 452.

1. In the notification area, right-click the Event Server Manager tray icon. A context-menu appears.



2. If the service has stopped, click **Start Event Server service** to start it. The tray icon changes to reflect the new state.
3. To restart or stop the service, click **Restart Event Server service** or **Stop Event Server service**.



For more information about the tray icons, see Server manager tray icons (explained) on page 448.

Stopping the Event Server service

When installing MIP plug-ins in the Event Server, first you must stop the Event Server service and then, afterward, restart it. However, while the service is stopped, many areas of the VMS system will not function:

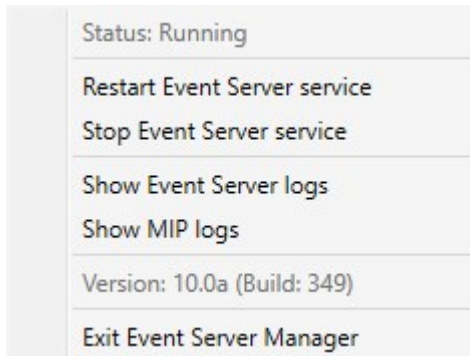
- No events or alarms are stored in the Event Server. However, system and device events still trigger actions, for example start recording
- Add-on products do not work in XProtect Smart Client and cannot be configured from the Management Client.
- Analytic events do not work
- Generic events do not work

- No alarms are triggered
- In XProtect Smart Client, map view items, alarm list view items, and the Alarm Manager workspace do not work
- MIP plug-ins in the Event Server cannot run
- MIP plug-ins in Management Client and XProtect Smart Client do not work correctly

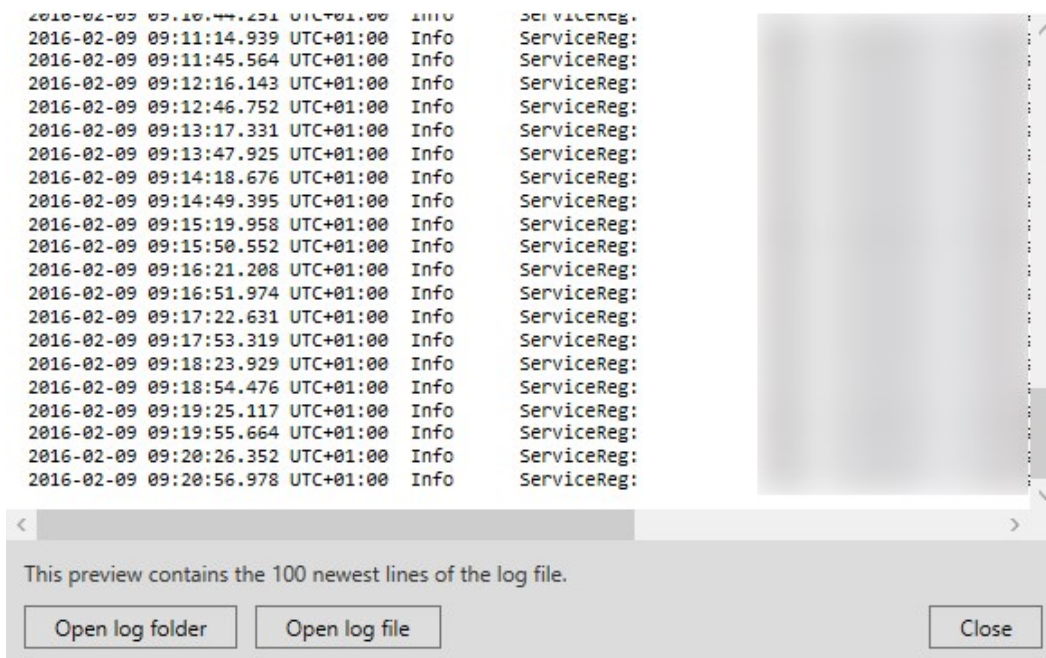
View Event Server or MIP logs

You can view time-stamped information about Event Server activities in the Event Server log. Information about third party integrations is logged in the MIP log in a sub-folder in the **Event Server** folder.

1. In the notification area, right-click the Event Server Manager tray icon. A context-menu appears.



2. To view the 100 most recent lines in the Event Server log, click **Show Event Server Logs**. A log viewer appears.



1. To view the log file, click **Open log file**.
2. To open the log folder, click **Open log folder**.
3. To view the 100 most recent lines in the MIP log, go back to the context-menu and click **Show MIP logs**. A log viewer is displayed.



If someone removes the log files from the log directory, the menu items are grayed out. To open the log viewer, first you need to copy the log files back into one of these folders:
C:\ProgramData\Milestone\XProtect Event Server\logs or *C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs*.

Managing registered services

Occasionally, you have servers and/or services which should be able to communicate with the system even if they are not directly part of the system. Some services, but not all, can register themselves automatically in the system. Services that can automatically be registered are:

- Event Server service
- Log Server service

Automatically registered services are displayed in the list of registered services.

You can manually specify servers/services as registered services in the Management Client.

Add and edit registered services

1. In the **Add/Remove Registered Services** window, click **Add** or **Edit**, depending on your needs.
2. In the **Add Registered Service** or **Edit Registered Service** window (depending on your earlier selection), specify or edit settings.
3. Click **OK**.

Manage network configuration

With the network configuration settings, you can specify the management server's server LAN and WAN addresses so the management server and the trusted servers can communicate.

1. In the **Add/Remove Registered Services** window, click **Network**.
2. Specify the LAN and/or WAN IP address of the management server.

If all involved servers (both the management server and the trusted servers) are on your local network, you can simply specify the LAN address. If one or more involved servers access the system through an internet connection, you must also specify the WAN address.



3. Click **OK**.

Registered services properties

In the **Add Registered Service** or **Edit Registered Service** window, specify the following:

Component	Requirement
Type	Prefilled field.
Name	Name of the registered service. The name is only used for display purposes in the Management Client.
URLs	<p>Click Add to add the IP address or hostname of the registered service. If specifying a hostname as part of a URL, the host must exist and be available on the network. URLs must begin with <i>http://</i> or <i>https://</i> and must not contain any of the following characters: <code>< > & ' " * ? []</code>.</p> <p>Example of a typical URL format: <i>http://ipaddress:port/directory</i> (where port and directory are optional). You can add more than one URL if required.</p>
Trusted	<p>Select if the registered service should be trusted immediately (this is often the case, but the option gives you the flexibility to add the registered service and then mark it as trusted by editing the registered service later).</p> <p>Changing the trusted state also changes the state of other registered services sharing one or more of the URLs defined for the relevant registered service.</p>
Description	Description of the registered service. The description is only used for display purposes in the Management Client.
Advanced	When a service is advanced, it has specific URI schemes (for example, HTTP, HTTPS, TCP, or UDP) that need to be set up for each host address you define. A host address therefore has multiple endpoints, each with its own scheme, host address and IP port for that scheme.

Removing device drivers (explained)

If you no longer require device drivers on your computer, you can delete the device packs from your system. To do so, follow the standard Windows procedure for removing programs.

If you have multiple device packs installed and have problems deleting the files, you can use the script in the device pack installation folder to delete them completely.

If you remove device drivers, the recording server and the camera devices cannot communicate any longer. Do not remove device packs when you upgrade because you can install a new version on top of an old one. Only if you uninstall the entire system, you may remove the device pack.

Remove a recording server



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

1. Right-click the recording server you want to remove in the **Overview** pane.
2. Select **Remove Recording Server**.
3. If you are sure, click **Yes**.
4. The recording server and all of its associated hardware are removed.

Delete all hardware on a recording server



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

1. Right-click the recording server on which you want to delete all hardware.
2. Select **Delete All Hardware**.
3. Confirm the deletion.

Troubleshooting

Issue: Change of SQL Server and database addresses prevents database access

If the addresses to the SQL Server and database are changed, for example by changing the host name of the computer running the SQL Server, the recording server's access to the database is lost.

Solution: Use the update SQL address tool found from the Recording Server Manager tray icon.

Issue: Recording server startup fails due to port conflict

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

SMTP Service: Verification and solutions

To verify whether SMTP Service is installed:

1. From Windows' **Start** menu, select **Control Panel**.
2. In the **Control Panel**, double-click **Add or Remove Programs**.
3. In the left side of the **Add or Remove Programs** window, click **Add/Remove Windows Components**.
4. In the **Windows Components** wizard, select **Internet Information Services (IIS)**, and click **Details**.
5. In the **Internet Information Services (IIS)** window, verify whether the **SMTP Service** check box is selected. If so, SMTP Service is installed.

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

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

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

1. From Windows' **Start** menu, select **Control Panel**.
2. In the **Control Panel**, double-click **Administrative Tools**.
3. In the **Administrative Tools** window, double-click **Services**.
4. In the **Services** window, double-click **Simple Mail Transfer Protocol (SMTP)**.
5. In the **SMTP Properties** window, click **Stop**, then set **Startup type** to either **Manual** or **Disabled**.

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

6. Click **OK**.

Solution 2: Remove SMTP service

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

1. From Windows' **Start** menu, select **Control Panel**.
2. In the **Control Panel** window, double-click **Add or Remove Programs**.
3. In the left side of the **Add or Remove Programs** window, click **Add/Remove Windows Components**.
4. In the **Windows Components** wizard, select the **Internet Information Services (IIS)** item, and click **Details**.
5. In the **Internet Information Services (IIS)** window, clear the **SMTP Service** check box.
6. Click **OK**, **Next**, and **Finish**.

Issue: Recording Server goes offline when switching Management Server cluster node

If you set up a Microsoft cluster for Management Server redundancy, the Recording Server or Recording Servers may go offline when switching Management Server between the cluster nodes.

To correct this, modify the following configuration settings:

On the Management Server nodes:

- In C:\ProgramData\Milestone\XProtectManagement Server\ServerConfig.xml:

```
<AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
```

- In C:\Program Files\Milestone\XProtectManagement Server\IIS\IDP\appsettings.json:

```
"Authority": "http://ClusterRoleAddress/IDP"
```

On the Recording Servers, verify that the authorizationserveraddress is also set to the cluster role address:

In C:\ProgramData\Milestone\XProtectRecording Server\RecorderConfig.xml:

```
<authorizationserveraddress>http://ClusterRoleAddress/IDP</authorizationserveraddress>
```

Upgrade

Upgrade (explained)

When you upgrade, all components currently installed on the computer are upgraded. It is not possible to remove installed components during an upgrade. If you want to remove installed components, use Windows' **Add and remove programs** functionality before or after an upgrade. During the upgrade, all components, except the management server database, are automatically removed and replaced. This includes the drivers of your device pack.

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



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

When you upgrade including your recording servers, you are asked if you want to update or keep your video device drivers. If you choose to update, it might take a few minutes for your hardware devices to make connect to the new video device drivers after restart of your system. This is due to several internal checks on the newly installed drivers.



If you upgrade from version 2017 R3 or earlier to version 2018 R1 or later, and if your system has older cameras, you must manually download the device pack with legacy drivers from the download page on our website (<https://www.milestonesys.com/downloads/>). To see if you have cameras that use drivers in the legacy device pack, visit this page on our website (<https://www.milestonesys.com/community/business-partner-tools/device-packs/>).



If you upgrade from version 2018 R1 or earlier to version 2018 R2 or later, it is important that you update all recording servers in your system with a security patch before you upgrade. Upgrading without the security patch, will cause the recording servers to fail.



The instructions for installing the security patch on your recording servers are available on our website <https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/>.



When all recording servers in your system are upgraded to version 2019 R2 or later, Milestone recommends that you set UseRemoting to False in the management server configuration file. For more information, see the *Hardening guide*.



If you want to encrypt the connection between the management server and the recording servers, all recording servers must be upgraded to 2019 R2 or newer.

Upgrade requirements

- Have your software license file (see Licenses (explained) on page 47) (.lic) ready:
 - **Service pack upgrade:** During the installation of the management server, the wizard may ask you to specify the location of the software license file. You can use both the software license file you got after your purchase of your system (or latest upgrade) and the activated software license file you got after your last license activation
 - **Version upgrade:** After you purchased the new version, you receive a new software license file. During the installation of the management server, the wizard asks you to specify the location of the new software license file

The system verifies the software license file before you can continue. Already added hardware devices and other devices that require licenses will enter a grace period. If you have not enabled automatic license activation (see Enable automatic license activation on page 129), remember to activate your licenses manually before the grace period expires. If you do not have your software license file, contact your XProtect reseller.

- Have your **new product version** software ready. You can download it from the download page on the Milestone website.

- Make sure that you have backed up the system configuration (see Backing up and restoring your system configuration (explained) on page 432)

The management server stores the system configuration in an SQL database. The SQL database can be located in a SQL Server on the management server machine itself or in a SQL Server on the network.

If you use an SQL database in a SQL Server on your network, the management server must have administrator rights on the SQL Server whenever you want to create, move or upgrade the SQL database. For regular use and maintenance of the SQL database, the management server only needs to be SQL database owner.

- If you plan to enable encryption during installation, you need to have the proper certificates installed and trusted on relevant computers. For more information, see Secure communication (explained) on page 64

When you are ready to start the upgrade, follow the procedures in Upgrade best practices on page 462.

Upgrade best practices

Read about upgrade requirements (see Upgrade requirements on page 461) including SQL database backup before you start the actual upgrade.



Device drivers are now split into two device packs: the regular device pack with newer drivers and a legacy device pack with older drivers. The regular device pack is always automatically installed with an update or upgrade. If you have older cameras that use device drivers from the legacy device pack, and you do not have a legacy device pack installed already, the system does not automatically install the legacy device pack.



If your system has older cameras, Milestone recommends that you check if the cameras use drivers from the legacy device pack on this page (<https://www.milestonesys.com/community/business-partner-tools/device-packs/>). To check if you have the legacy pack installed already, look in the XProtect system folders. If you need to download the legacy device pack, go to download page (<https://www.milestonesys.com/downloads/>).

If your system is a **Single Computer** system, you can install the new software on top of the existing installation.

In a Milestone Interconnect or Milestone Federated Architecture system, you must start upgrading the central site and afterward the remote sites.

In a distributed system, perform the upgrade in this order:

1. Upgrade the management server with the **Custom** option in the installer (see Install your system - Custom option on page 80).
 1. On the wizard page where you choose components, all management server components are preselected.
 2. Specify the SQL Server and database. Decide whether to keep the SQL database that you are already using and to keep the existing data in the database.



When you start the installation, you lose the failover recording server functionality (see Failover recording servers (explained) on page 165).



If you enable encryption on the management server, the recording servers are offline until they are upgraded, and you have enabled encryption to the management server (see Before you start installation on page 55).

2. Upgrade failover recording servers. From your management server's download web page (controlled by the Download Manager), install Recording Server.



If you plan to enable encryption on the failover recording servers and you want to retain the failover functionality, upgrade the failover recording server without encryption and enable it after you have upgraded the recording servers.

At this point the failover server functionality works again.

3. If you plan to enable encryption from the recording servers or failover recording servers to the clients and it is important that the clients can retrieve data during the upgrade, upgrade all clients and services that retrieve data streams from the recording servers before you upgrade the recording servers. These clients and services are:
 - XProtect Smart Client
 - Management Client
 - Management Server
 - XProtect Mobile server
 - XProtect Event Server
 - DLNA Server Manager

- ONVIF Bridge
 - Sites that retrieve data streams from the recording server through Milestone Interconnect
 - Some MIP SDK third-party integrations
4. Upgrade the recording servers. You can install recording servers using the installation wizard (see Install new XProtect components on page 84) or silently (see Install new XProtect components on page 84). The advantage of a silent install is that you can do it remotely.



If you enable encryption and the selected server authentication certificate is not trusted on all relevant computers running, they lose connection. For more information, see Before you start installation on page 55.

Continue these steps for the other sites in your system.

Upgrade in a workgroup setup

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

1. On the recording server, create a local Windows user.
2. From the Windows **Control Panel**, find the **Data Collector service**. Right-click it, select **Properties**, and select the **Log on** tab. Set the Data Collector service to run as the local windows user you just created on the recording server.
3. On the management server, create the same local Windows user (with the same user name and password).
4. In the Management Client, add this local Windows user to the **Administrator's** group.

For installing with workgroups, see Installation for workgroups on page 91.

Upgrade in a cluster

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

1. Stop the Management Server service on all management servers in the cluster.
2. Uninstall the management server on all servers in the cluster.
3. Use the procedure for installing multiple management servers in a cluster as described for install in a cluster. Refer to Install a new XProtect system on page 73.



When installing, make sure to reuse the existing SQL Server and the existing SQL database that currently stores the system configuration. The system configuration is automatically upgraded.



helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit <https://www.milestonesys.com/>.

