MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2024 R1

System architecture document

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

milestone

Contents

Copyright, trademarks, and disclaimer

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.

Introduction

This document contains illustrations and descriptions of communication and dataflow between the most common system components in a distributed system.

The document shows a range of scenarios with a supporting illustration and a description of actions supplemented by information about port numbers, protocols and bandwidth usage.

The illustrations are simplified and primarily focus on the general dataflow between system components. This means that less important flows may have been omitted in order to reduce the level of complexity.

Target audience and purpose

This document is primarily aimed at system integrators and IT administrators. It gives insight on the benefits and simplicity of using Milestone XProtect as a VMS and you can use it for assistance in the process of selecting, deploying, administrating, maintaining, and expanding a Milestone XProtect VMS.

Read the document for guidance on the following subjects:

- Overall system architecture
- Primary system components and their functions
- Data flow and communication through the system
- Basic system design

To benefit from the information in this document, you should have a general experience with administrating an IT installation.

Overall system architecture

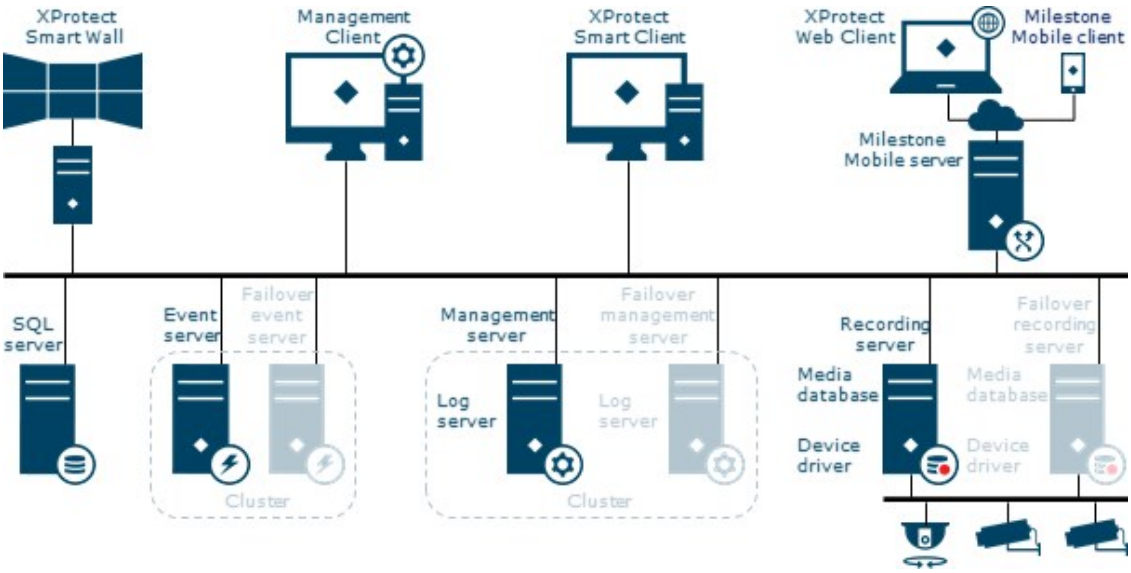
To enable scaling of thousands of cameras across multiple sites, the system consists of several components that handle specific tasks. You can install all components on a single server if the server can handle the load, or you can install the components on separate, dedicated servers to scale and distribute the load.

Depending on hardware and configuration, smaller systems with 50 to100 cameras can run on a single server.

For systems with more than 100 cameras, Milestone recommends that you use dedicated servers for all or some of the components.

As a starting point, all components need not be available in all installations. Components such as failover recording servers or mobile servers can be added if the functionality they offer is needed at a later time for hosting and providing access to both XProtect Web Client and XProtect Mobile.

The components of the XProtect VMS:



Server components

Management server

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

Failover management server

You can get failover support on the management server by installing the management server in a Microsoft Windows cluster. The cluster ensures that another server takes over the management server function in case the first server fails.

Recording server

Recording servers are computers where you have installed the Recording Server software, and configured it to communicate with the management server. A surveillance system typically consists of several recording servers.

The recording server is responsible for all communication, recording, and event handling related to devices such as cameras, video and audio encoders, I/O modules, and metadata sources. Examples of actions the recording server handles:

- Retrieve video, audio, metadata and I/O event streams from the devices
- Record video, audio and metadata from devices
- Provide operators with access to live and recorded video, audio and metadata
- Provide operators with access to device status
- Trigger system and video events on device failures or events
- Perform motion detection and generate smart search metadata

The recording server is also responsible for communicating with other Milestone products when using the Milestone Interconnect™ technology. For more information, see Milestone Interconnect.

The recording server supports encryption of data streams to the clients and services as well as encryption of the connection with the management server.For more information, see the certificates guide about how to secure your XProtect VMS installations.

Failover recording server

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

The failover recording server operates in two modes:

Cold standby, for monitoring multiple 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 also specify a secondary failover server group that takes over from the primary group if all the recording servers in the primary group are busy

Hot standby, for monitoring a single recording server

In a hot standby failover recording server setup, you dedicate a failover recording server to take over from one recording server only. With this approach, the failover recording server is continuously synchronized with the correct/current configuration of the recording server it is dedicated to and it can take over much faster than a cold standby failover recording server.

Media database

The system stores the retrieved video, audio and metadata in the customized high performance Milestone media database which is optimized for recording and storing audio and video data.

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

Event server

The event server handles the tasks related to events, alarms, and maps and also third-party integrations via the Milestone Integration Platform.

Events:

- All system events are consolidated in the event server so there is a single place and interface for partners to make integrations that use system events
- The event server offers third-party access for 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 and handling of the alarm database. The alarm database is stored in the same SQL Server database as the management server uses

Maps:

- The event server also hosts maps. You configure and use maps in the XProtect Smart Client

Milestone Integration Platform:

- You can install third-party developed plug-ins on the event server and utilize access to system events

You can get failover support on the event server by installing the event server in a Microsoft Windows cluster. The cluster ensures that another server takes over the event server function in case the first server fails.

Log server

The log server stores all log messages for the entire system. The log server typically uses the same SQL Server as the management server but has its own SQL Server database. The log server is also typically installed on the same server as the management server. If you need to increase the performance of the management server or log server, you can install the log server on a separate server and use separate SQL Server.

The system can through the log server write three types of log messages:

- System logs: the system administrator can choose to log errors, warnings, and information, or a combination of these. The default is to log errors only
- Audit logs: the system administrator can choose to log user activity in clients in addition to login and administration logs
- Rule-triggered logs: the system administrator can use the rule log to create logs on specific events

SQL Server

The management server, the event server, and the log server use SQL Server databases on one or two SQL Server installations to store, for example, configuration, alarms, events and log messages.

The installation wizard installs Microsoft SQL Server Express 2022 unless SQL Server is already installed on the computer. When you install XProtect VMS as an upgrade, the wizard keeps the previous SQL Server installation.

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

Mobile server

XProtect Mobile server handles logins to the system from XProtect Mobile client or XProtect Web Client.

A XProtect Mobile server distributes video streams from recording servers to XProtect Mobile client or XProtect Web Client. This offers a secure setup where recording servers are never connected to the Internet. When a XProtect Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

API Gateway

The MIP VMS API provides a unified RESTful API, based on industry standard protocols such as OpenAPI, for accessing XProtect VMS functionality, simplifying integration projects and serving as a basis for cloud connected communication.

The XProtect VMS API Gateway supports these integration options through the Milestone Integration Platform VMS API (MIP VMS API).

The API Gateway is installed on-premise and is intended to serve as a front-end and common entry point for RESTful API and WebSocket Messaging API services on all the current VMS server components (management server, event server, recording servers, log server, etc). An API Gateway service can be installed on the same host as the management server or separately, and more than one can be installed (each on their own host).

The RESTful API is implemented in part by each specific VMS server component, and the API Gateway can simply pass-through these requests and responses, while for other requests, the API Gateway will convert requests and responses as appropriate.

Currently, the configuration API, hosted by the management server, is available as a RESTful API. The RESTful Events API, Websockets messaging API, and the RESTful Alarms API, hosted by the event server, are also available.

For more information, see the API Gateway administrator manual and the Milestone Integration Platform VMS API reference documentation.

Client components

XProtect Management Client

The Management Client is the administration interface for all parts of the system.

The VMS is designed for large-scale operation so the Management Client is designed to run remotely from, for example, the administrator's computer.

You can access the settings in the Management Client from a tree structure where you can open items and sub items.

XProtect Smart Client

XProtect Smart Client is the main client for the VMS. It is designed to run remotely from the operators' computer for day-to-day use in order to manage IP surveillance cameras. It provides instant control of cameras and connected security devices and quick access to live and recorded video and metadata.

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.

For more information, see the user manual for XProtect Smart Client.

XProtect Web Client

XProtect Web Client is a client designed for the occasional or remote user that needs easy access to live monitoring, playback and export. XProtect Web Client also provides access to activating system events and outputs.

For more information, see the user manual for XProtect Web Client.

On the System Requirements web page, you can find information about compatible browsers under XProtect Web Client.

XProtect Mobile client

The XProtect Mobile client is a mobile surveillance solution and it offers easy access to cameras, views and other functionality that is set up in the management clients.

It runs on an Android tablet or smartphone or on an Apple® tablet, smartphone or portable music player.

You can use the XProtect Mobile client as a remote recording device by using the device's built-in camera and the Milestone Video Push feature. With Video Push activated, video from the device's camera is streamed back to the VMS and recorded as if it was from a standard camera.

For more information, see the user manual for XProtect Mobile.

On the System Requirements web page, you can find information about which operating systems are compatible with XProtect Mobile.

Encryption

This section gives you an introduction to encryption and certificates.

XProtect systems support secure communication:

From	To
Recording Server	Management Server
Management Server	Recording Server
Clients, servers, and integrations that retrieve data streams from the recording server	Recording Server
Mobile devices	Mobile Server
Management Server	Data Collector servers affiliated with remote servers
Data Collector servers affiliated with remote servers	Management Server

When do you need to install certificates?

First, decide whether your system actually needs encrypted communication.

Don't use certificates with recording server encryption if you are using one or more integrations that don't support HTTPS communication. This is, for example, third-part MIP SDK integrations that don't support HTTPS.

Unless your installation is made in a physically isolated network, it's recommended that you secure the communication by using certificates.

This document describes when to use certificates:

- If your XProtect VMS system is set up in a Windows Workgroup environment
- Before you install or upgrade to XProtect VMS 2019 R1 or newer, if you want to enable encryption during the installation
- Before you enable encryption, if you installed XProtect VMS 2019 R1 or newer without encryption
- When you renew or replace certificates due to expiry

Introduction to certificates

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

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

A certificate authority (CA) is anyone who can issue root certificates. This can be an internet service that issues root certificates, or anyone who manually generates and distributes a certificate. A CA can issue certificates to web services, that is to any software using https communication. This certificate contains two keys, a private key and a 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 certificates to exchange a secret key and thereby establish a secure TLS/SSL connection.

For manually distributed certificates, certificates must be installed before the client can make such a verification.

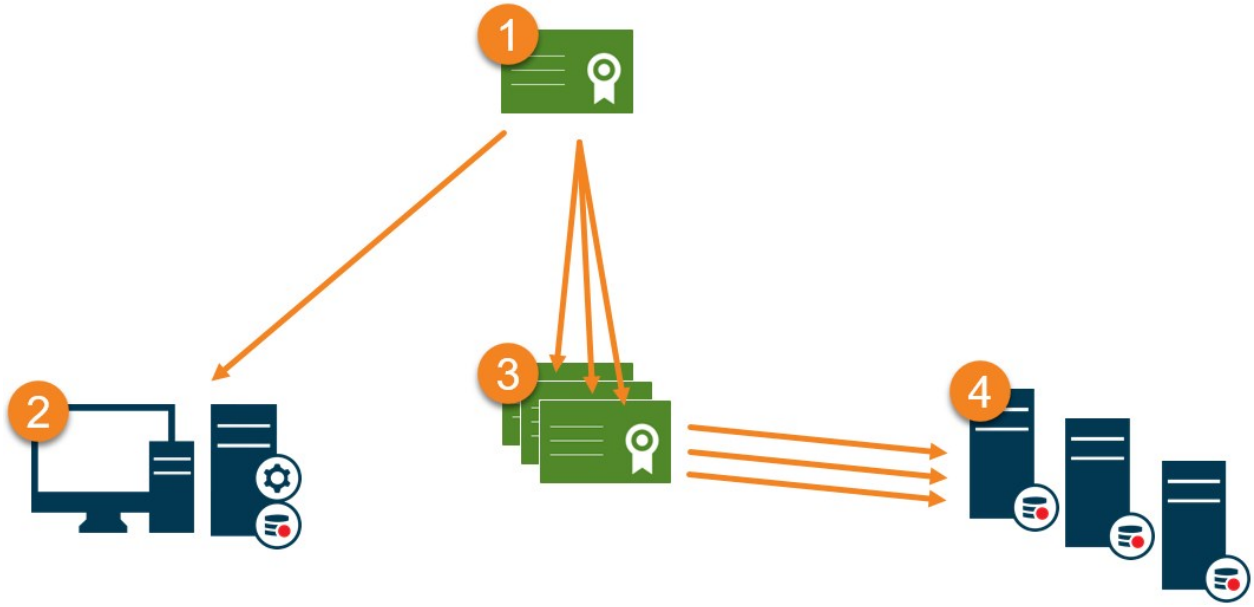
See Transport Layer Security for more information about TLS.

In XProtect VMS, the following locations are where you can enable TLS/SSL encryption:

- In the communication between the management server and the recording servers, event servers, and mobile servers
- On the recording server in the communication with clients, servers, and integrations that retrieve data streams from the recording server
- In the communication between clients and the mobile server

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS.



❶ A CA certificate acts as a trusted third-party, trusted by both the Subject/owner (server) and by the party that verifies the certificate (clients).

❷ The public CA certificate must be trusted on all client computers. In this way the clients can verify the validity of the certificates issued by the CA.

❸ The CA certificate is used to issue private server authentication certificates to the servers.

❹ The created private SSL certificates must be imported to the Windows Certificate Store on all servers.

Requirements for the private SSL certificate:

- Issued to the server so that the 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 or applications that communicate with the service on the servers, by trusting the CA certificate that was used to issue the SSL certificate
- The service account that runs the server must have access to the private key of the certificate on the server.

> ⚠ 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 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.

For more information, see the certificates guide about how to secure your XProtect VMS installations.

Identity Provider (explained)

Identity Provider app pool (IDP) is a system entity that creates, maintains, and manages identity information for basic users.

Identity Provider also provides authentication and registration services to relying applications or services, in this case: Recording Server, Management Server, Data Collector, and Report Server.

When you log in to XProtect clients and services as a basic user, your request goes to the Identity Provider. When authenticated the user can call the management server.

Identity Provider runs in the IIS as a part of the management server using the same SQL Server with a separate database and is responsible for creating and handling OAuth communication tokens that services use when communicating (Surveillance_IDP).

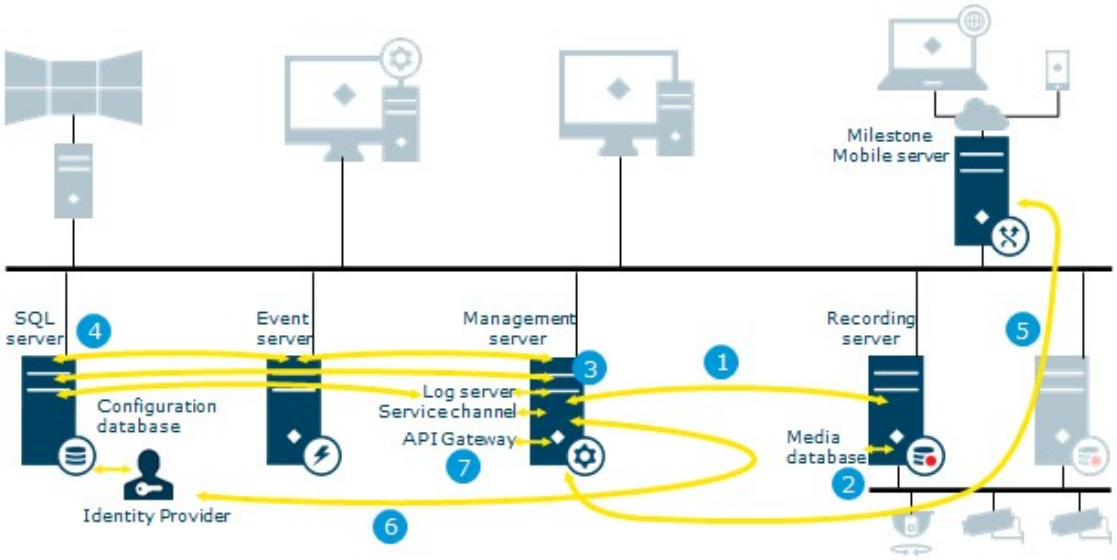
Identity Provider logs can be found at: `\\ProgramData\Milestone\IDP\Logs`.

System communication and data flow

The following illustrations provide an overview of the flow of data between XProtect components.

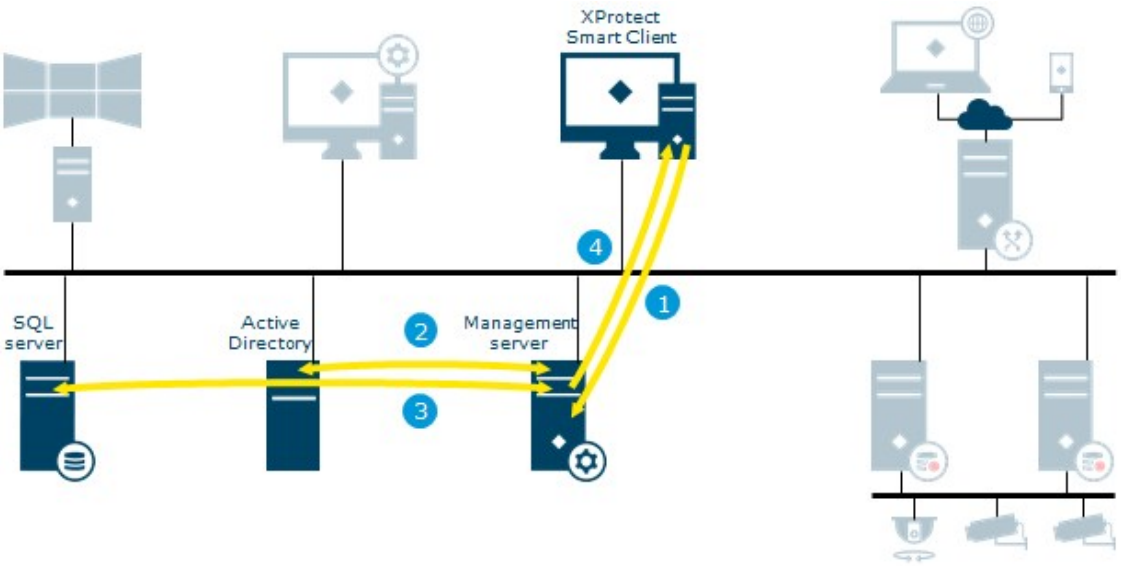
For a complete list of the ports that must be enabled for communication between components, see Ports used by the system.

Server communication



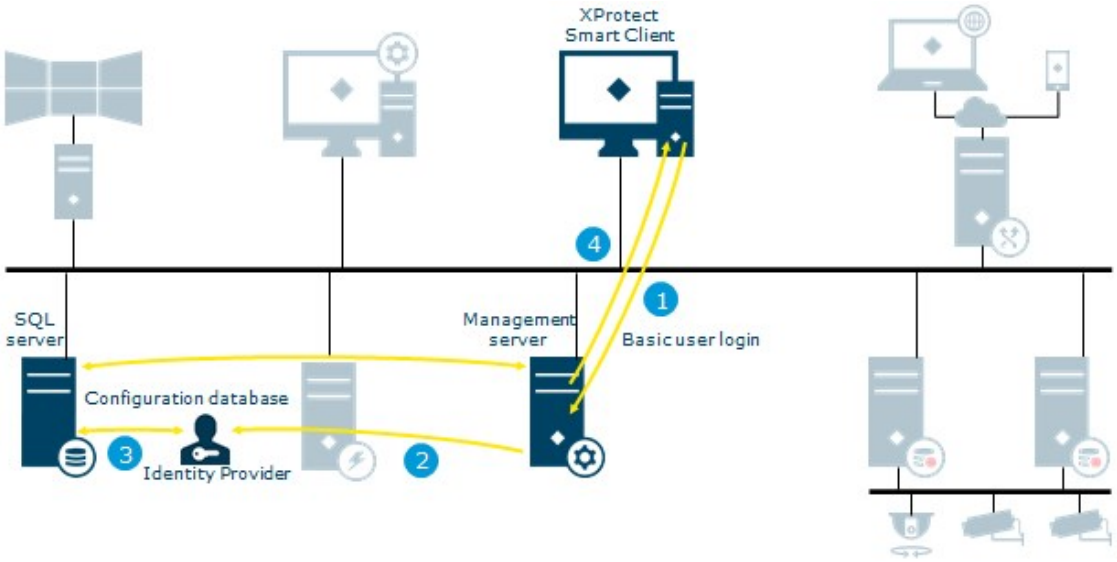
1. Management server - Recording server
2. Recording server - Media database
3. Management server - Internal
4. SQL Server database communication
5. Management server - Mobile server
6. Authentication of basic users by the Identity Provider
7. API Gateway - Management server

Login from XProtect Smart Client as an AD user



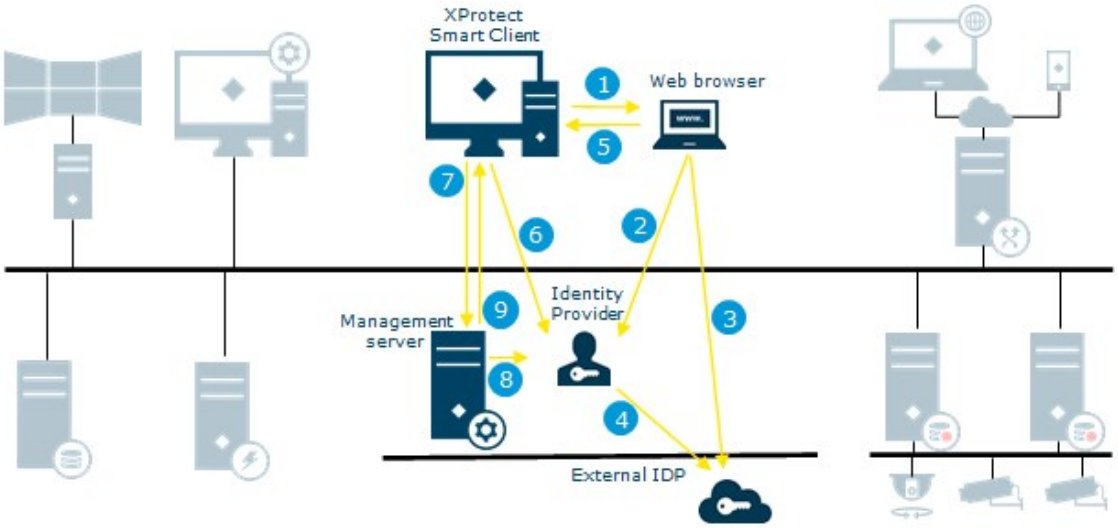
1. XProtect Smart Client connects to the management server and attempts to log in
2. The management server contacts Active Directory to authenticate the user
3. User-specific configuration is retrieved from the SQL Server database
4. Login is granted and the configuration is sent to XProtect Smart Client

Login from XProtect Smart Client as a basic user



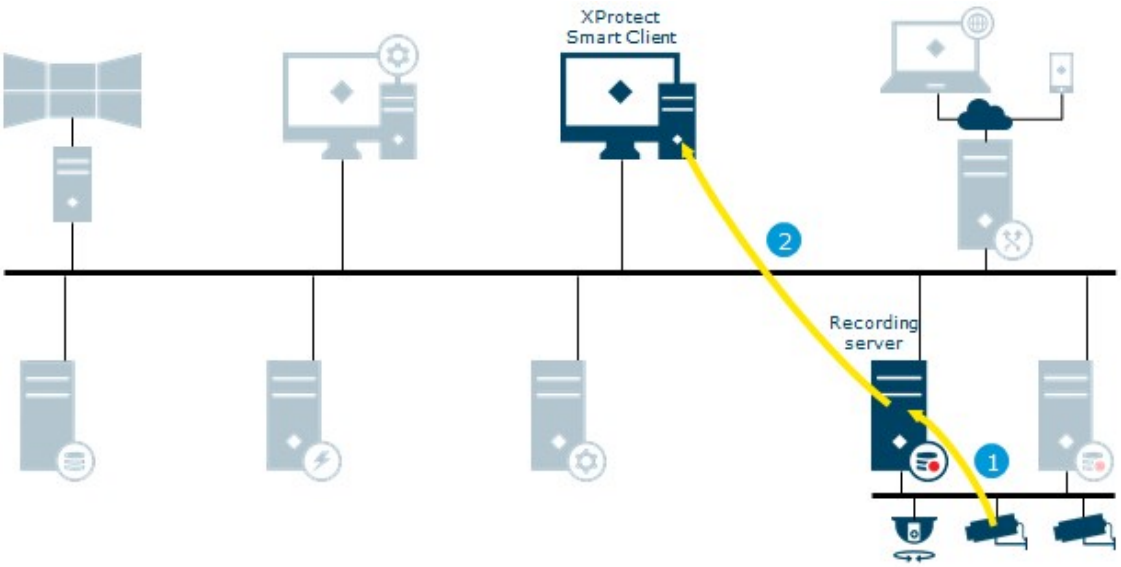
1. XProtect Smart Client attempts to connect to the management server as a basic user
2. The login request goes to the Identity Provider for authentication
3. User-specific configuration is retrieved from the SQL Server database
4. Login is granted and the configuration is sent to XProtect Smart Client

Login from XProtect Smart Client with an external IDP



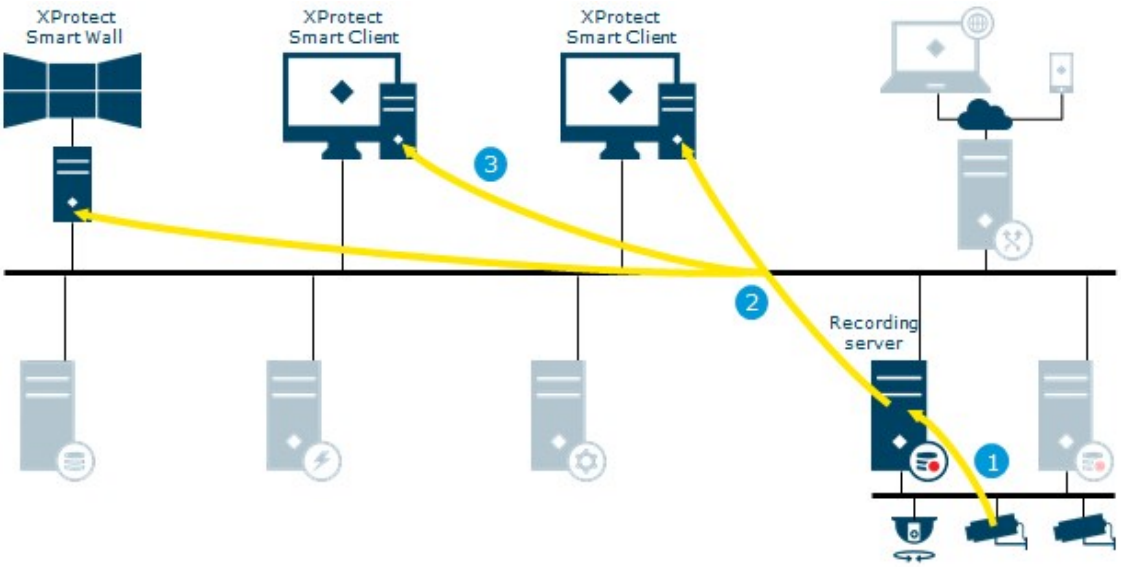
1. Login from XProtect Smart Client launches a web browser on the client computer.
2. The login request goes from the web browser to the Identity Provider for authentication.
3. The web browser is redirected to the external IDP login page where the user enters credentials and the browser receives an authorization code.
4. The Identity Provider requests information about the user from the external IDP and receives a list of claims. If a new user logs in to the VMS, the user is created in the VMS.
5. The web browser is redirected to XProtect Smart Client with the authorization code from the Identity Provider.
6. XProtect Smart Client gets an access token from the Identity Provider.
7. XProtect Smart Client login to the management server using the access token.
8. Verification of user permissions according to claims to role mapping.
9. The user logs in to XProtect Smart Client upon successful authorization.

Live video and audio



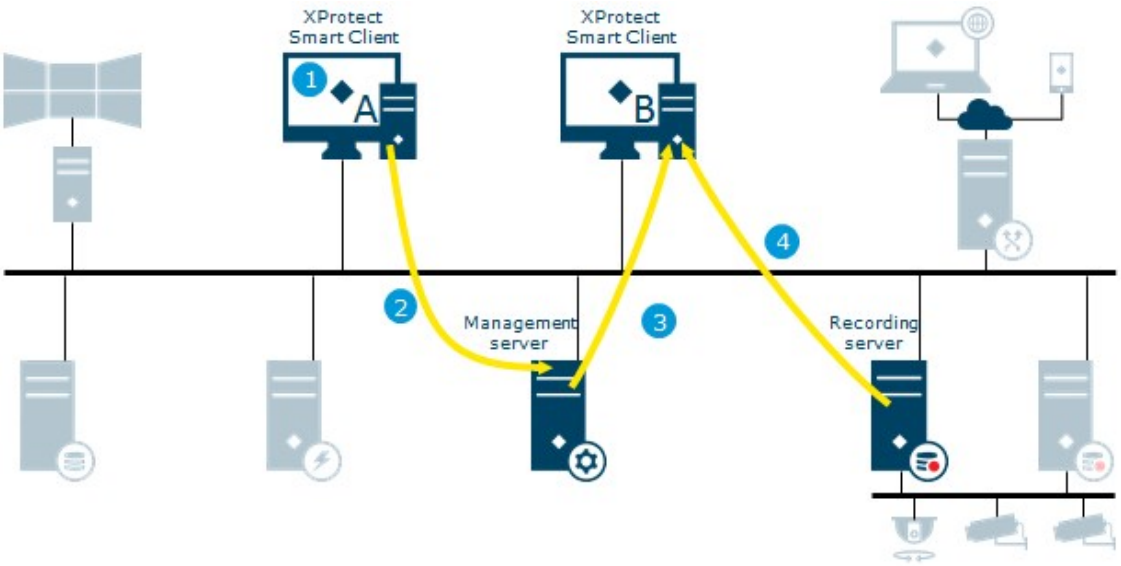
1. Live streams from cameras retrieved by the recording server
2. Streams are sent to XProtect Smart Client on request

Live video multicasting



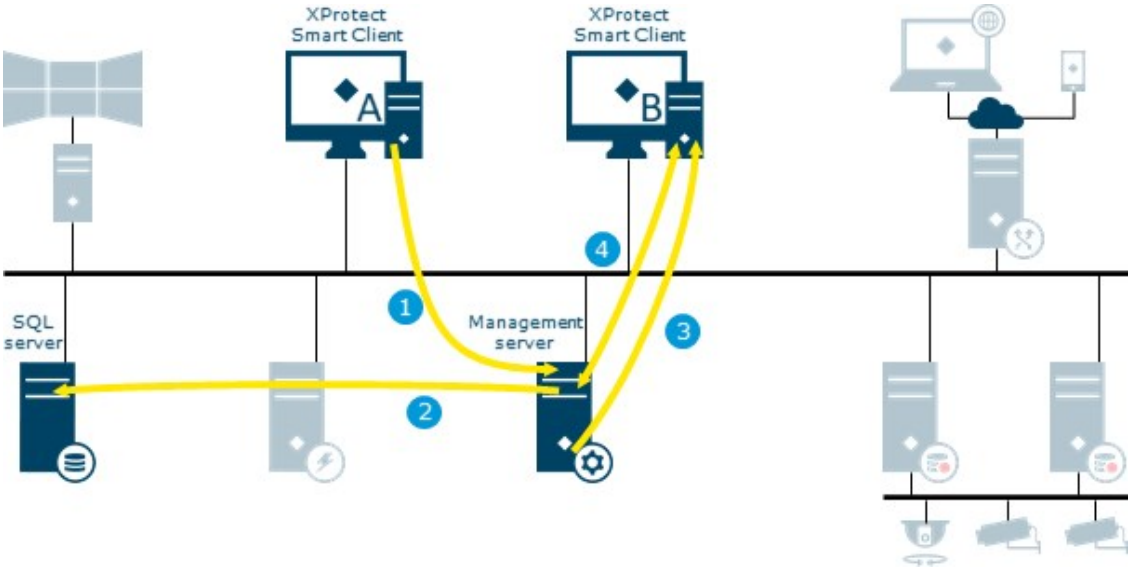
1. Live streams from cameras retrieved by the recording server
2. Recording server sends multicast stream to the multicast enabled network. This requires that all switches handling the data traffic between the XProtect Smart Client and the recording server must be configured for multicast
3. The multicast stream is received by all XProtect Smart Clients on request

Matrix



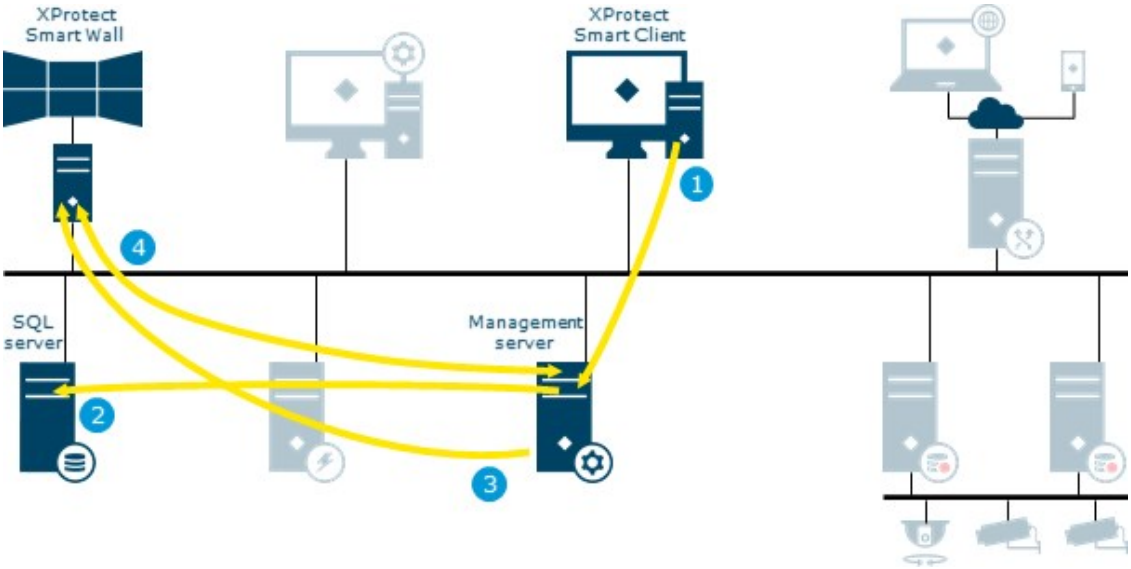
1. XProtect Smart Client user selects to send a camera to a Matrix-recipient
2. Information is sent to management server
3. Management server sends request to Matrix-recipient on specified IP address and port (XProtect Smart Client B)
4. Streams are sent to XProtect Smart Client from recording server on request

Management server – view update



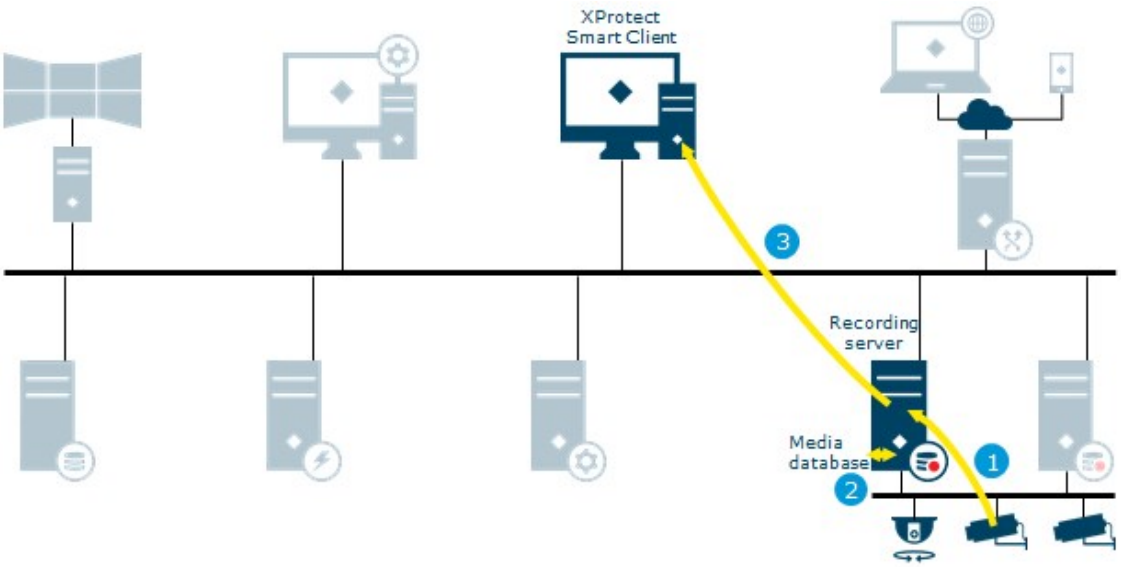
1. View updated on XProtect Smart Client
2. The system configuration is stored in the SQL Server database
3. The management server sends notification about view update to XProtect Smart Clients
4. XProtect Smart Clients retrieves and applies the new view

XProtect Smart Wall



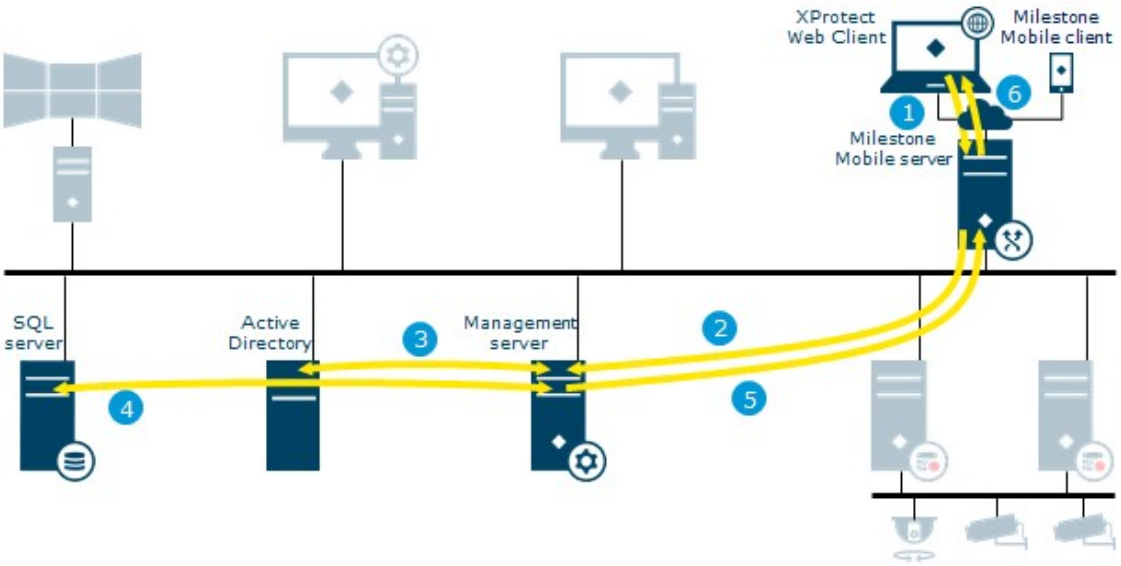
1. An XProtect Smart Client user updates the XProtect Smart Wall view
2. The XProtect Smart Wall view configuration is updated and stored in the SQL Server database
3. The management server sends a notification to the XProtect Smart Client running the XProtect Smart Wall
4. The XProtect Smart Client running the XProtect Smart Wall retrieves and applies new layout

Play back video and audio



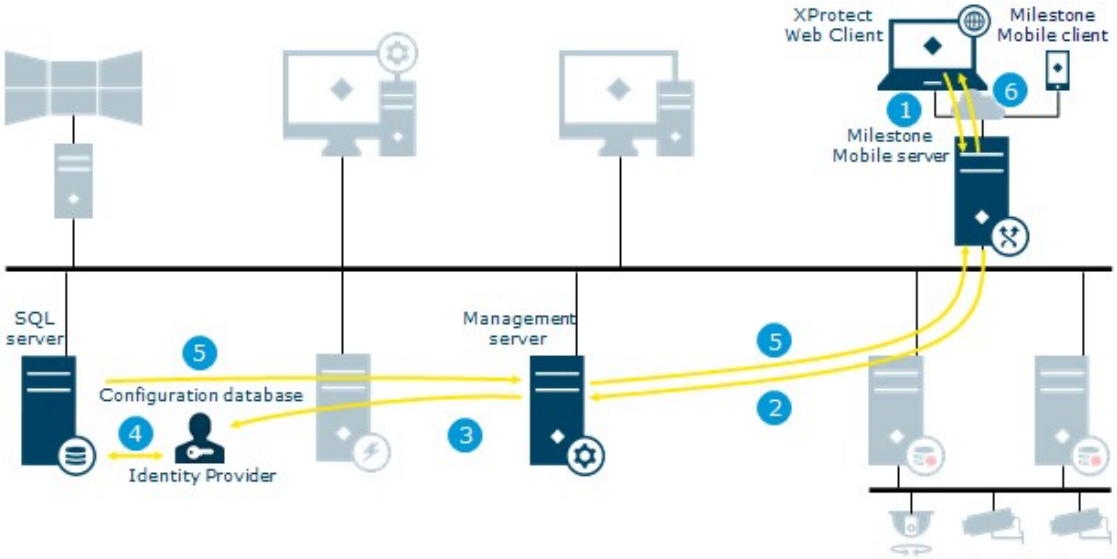
1. Recording stream from cameras retrieved by the recording server
2. The stream is recorded in the recording server database based on rules
3. The recorded stream is retrieved by XProtect Smart Client on playback request

Login from XProtect Web Client and XProtect Mobile as an AD user



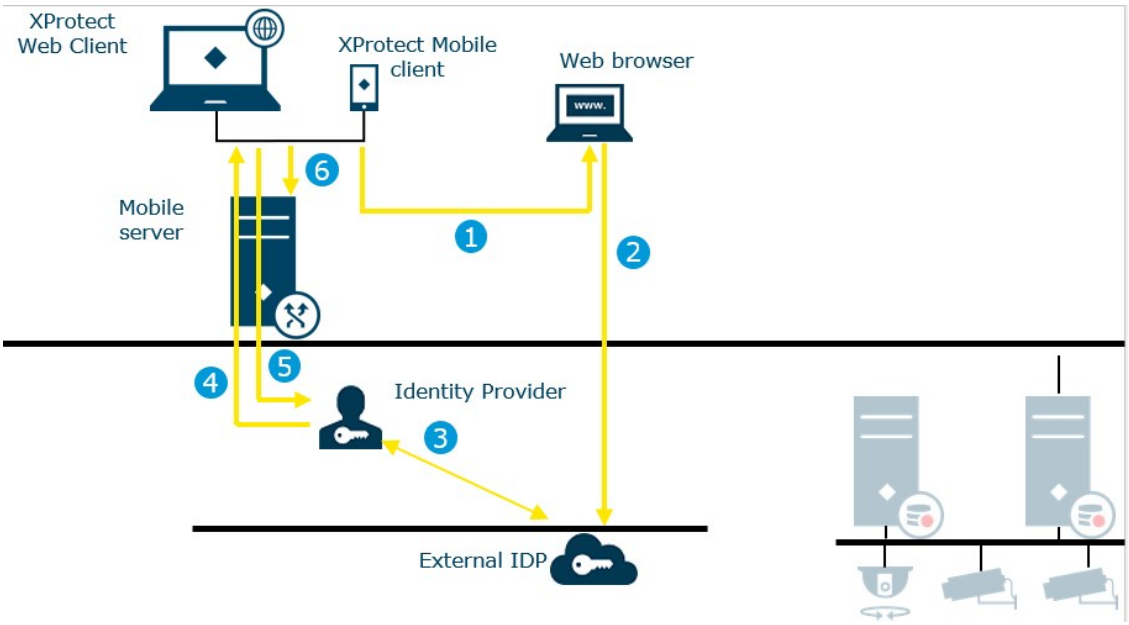
1. Login request from XProtect Web Client or XProtect Mobile received on the mobile server
2. The mobile server forwards request to the management server
3. The management server contacts Active Directory to authenticate the user
4. User-specific configuration is retrieved from the SQL Server database
5. Information returned to the mobile server
6. The login is granted and configuration is sent to XProtect Web Client or XProtect Mobile

Login from XProtect Web Client and XProtect Mobile as a basic user



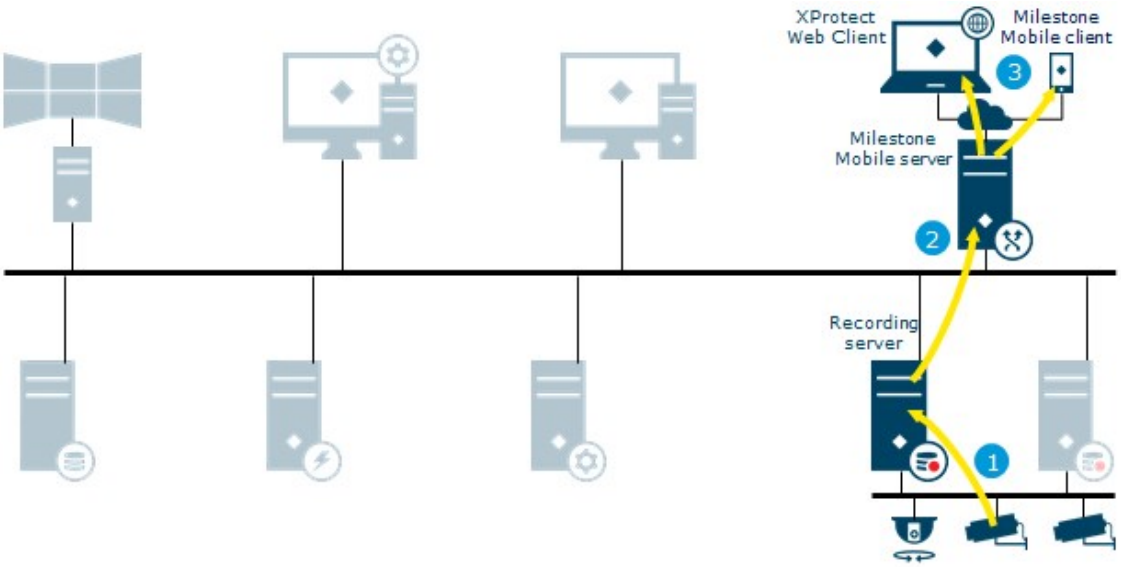
1. Login request from XProtect Web Client or XProtect Mobile received on the mobile server
2. The mobile server forwards a request to the management server
3. The login request goes to the Identity Provider for authentication
4. User-specific configuration is retrieved from the SQL Server database
5. Information returned to the mobile server
6. The login is granted and configuration is sent to XProtect Web Client or XProtect Mobile

Login from XProtect Web Client and the XProtect Mobile client with an external IDP



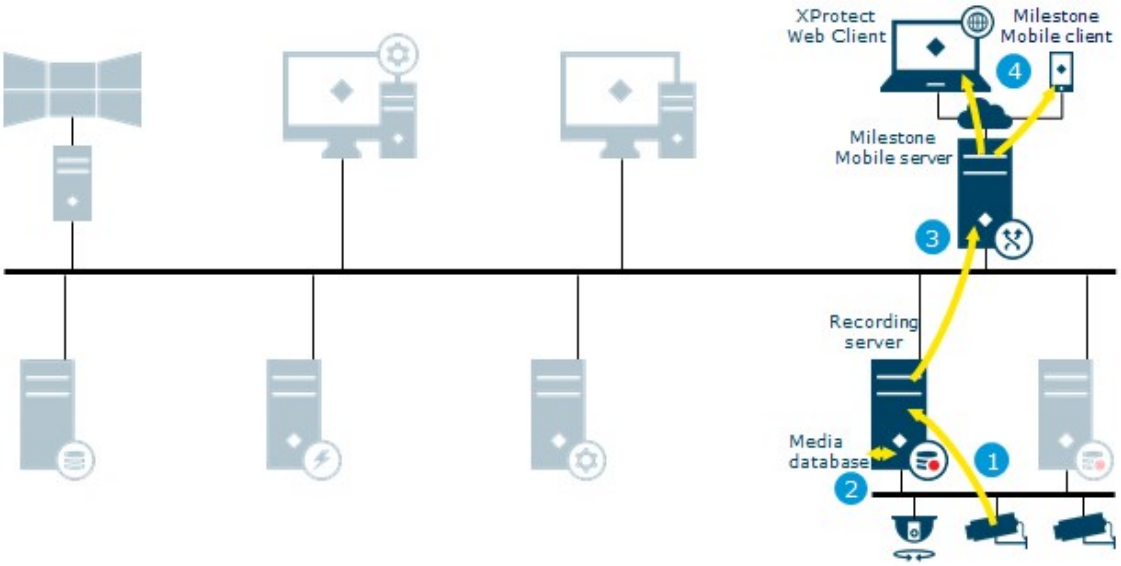
1. In XProtect Web Client or in the XProtect Mobile client, the user selects to log in via an external IDP. The login request launches a web browser.
2. The web browser is redirected to the external IDP login page where the user enters credentials.
3. The Identity Provider receives an authorization code from the external IDP to be exchanged for an access token. Then the Identity Provider requests information about the user from the external IDP and gets a list of claims. If a new user logs in to the VMS, the user is created in the VMS.
4. The Identity Provider returns an authorization code to XProtect Web Client or the XProtect Mobile client.
5. XProtect Web Client or the XProtect Mobile client requests an access token from the Identity Provider.
6. XProtect Web Client or the XProtect Mobile client logs in to the mobile server using the access token.

Live video for XProtect Web Client and XProtect Mobile



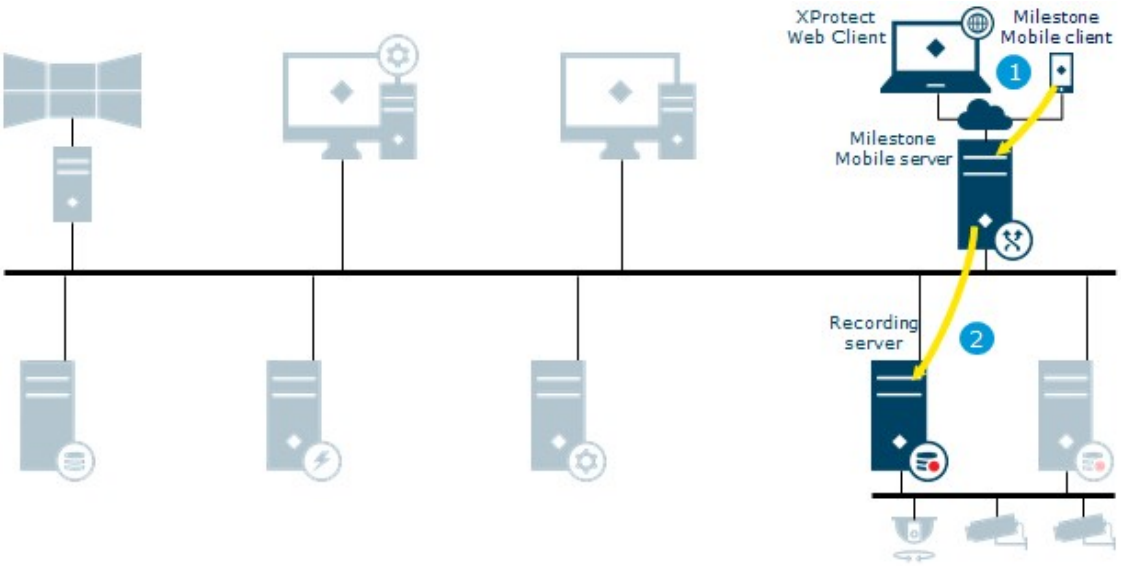
1. Live stream(s) from cameras retrieved on the recording server
2. Streams are sent to the mobile server for transcoding or as direct streaming
3. Video is streamed to the clients

Recording and playback video for XProtect Web Client and XProtect Mobile



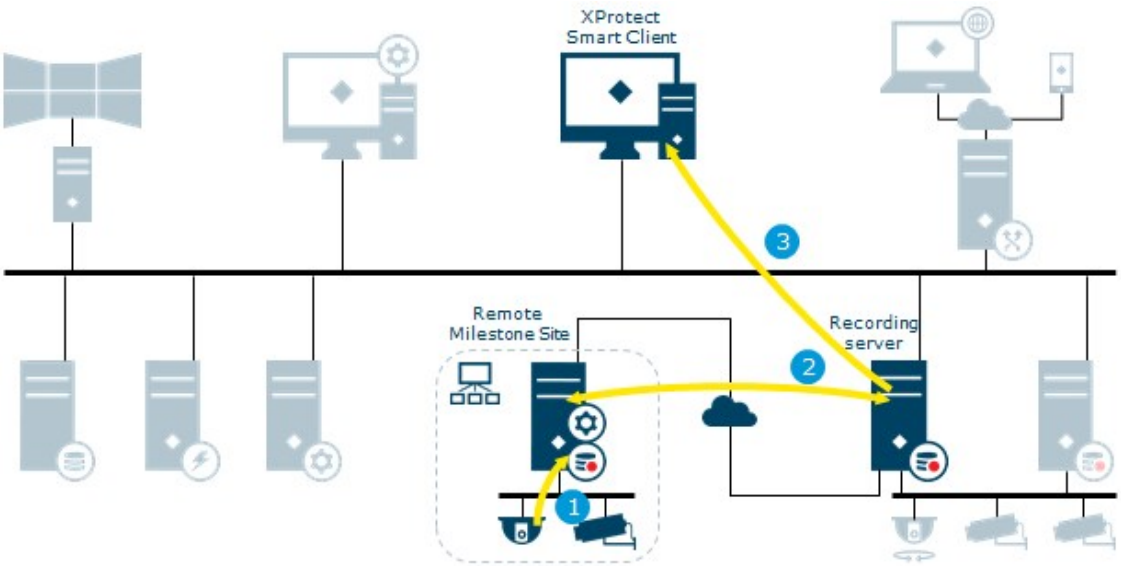
1. Recording stream from cameras retrieved on the recording server
2. The stream is recorded in the recording server database based on rules
3. Recordings are sent to the mobile server for transcoding or as direct streaming
4. Video is streamed to clients

Video push



1. Video push stream from a device running XProtect Mobile is sent instantly to the mobile server
2. The video push stream is retrieved by recording server using the specific video push device driver

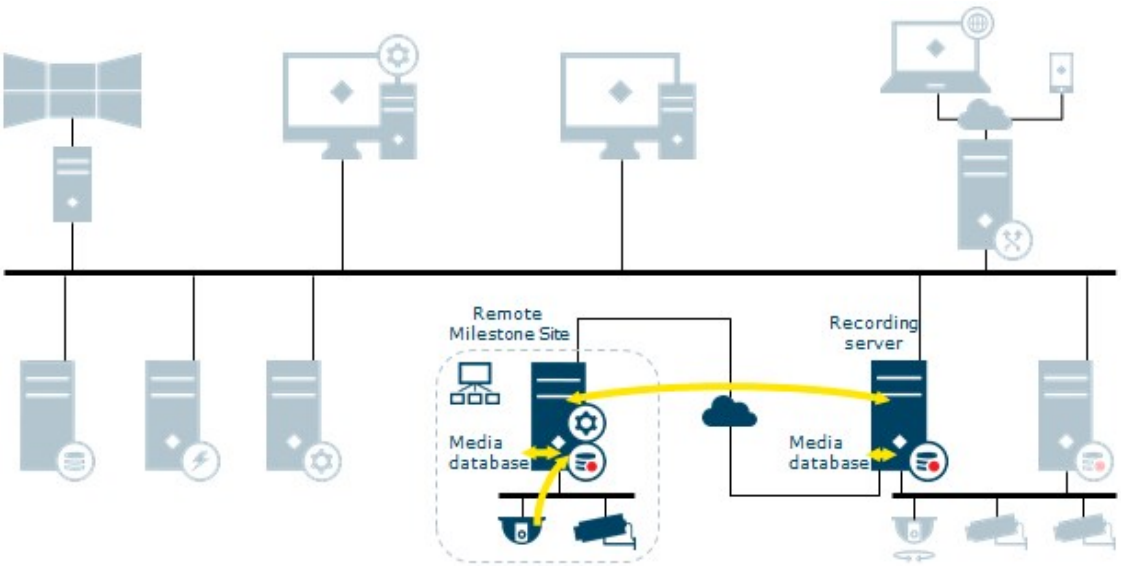
Milestone Interconnect live



Illustrates how XProtect Smart Client users, specified for the interconnected system, only need to log into the management server on the central site to view video.

1. Live stream(s) from the remote site cameras retrieved by the remote site recording server
2. Live streams from the remote site recording server retrieved by the central site recording server
3. Stream(s) are sent to XProtect Smart Client on request

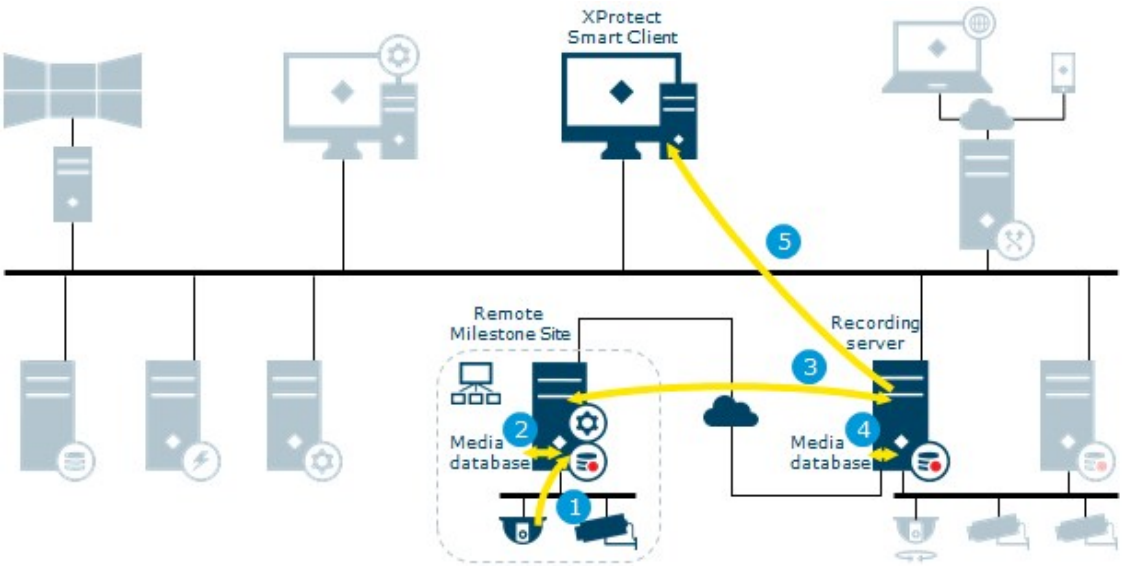
Milestone Interconnect recording options



Some of the different options when configuring your system recording settings:

- No recording
- Record at remote site only
- Retrieve recordings from remote site on request
- Retrieve recordings from remote site based on rule (time profile)
- Record at central site only
- Retrieve recordings from remote site after site link down
- Record at both sites
- Combinations of above and other options

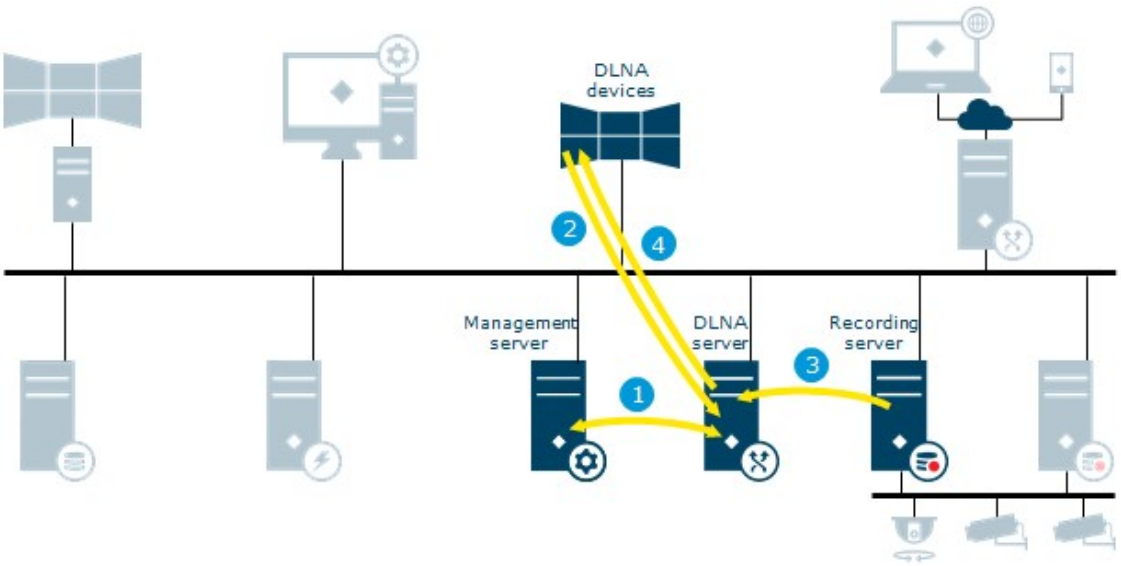
Milestone Interconnect play back



Illustrates when recording is done on both sites. Recordings can be retrieved to the central site based on schedule, event or request. XProtect Smart Client users, specified for the interconnected system, only need to log into the management server on the central site to view video.

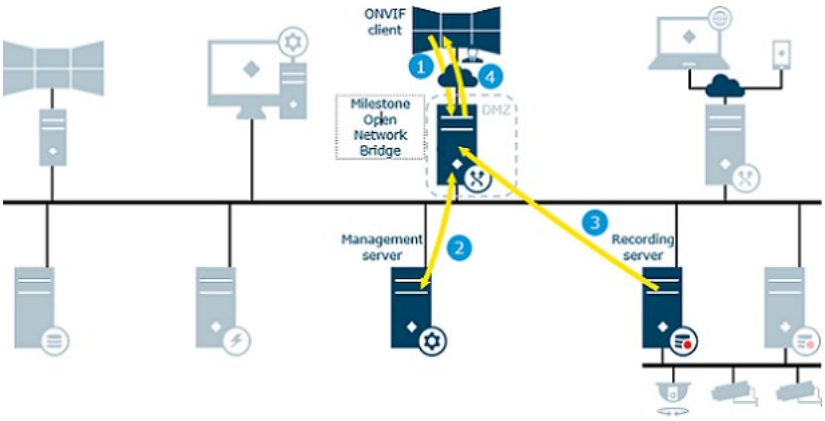
1. Recording stream from the remote site cameras retrieved by the remote site recording server
2. The stream is recorded in the remote site recording server database based on rules
3. Recording stream from the remote site recording server retrieved by the central site recording server
4. The stream is recorded in the central site recording server database based on rules. Recordings not available due to remote site link downtime can be retrieved automatically or based on schedule, event or request
5. The recorded stream(s) are retrieved by XProtect Smart Client on playback request

XProtect DLNA Server



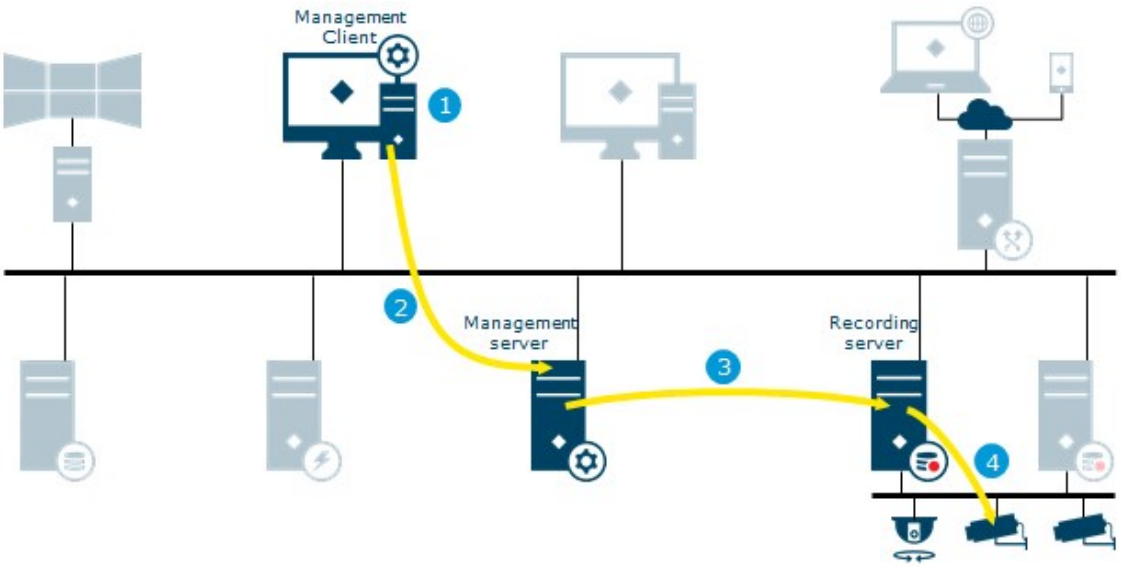
1. The XProtect DLNA Server connects to the management server to authorize itself with the provided credentials
2. A DLNA device scans the network and connects to the XProtect system via the XProtect DLNA Server and requests a live camera video stream
3. XProtect DLNA Server retrieves the requested camera video stream from the recording server
4. XProtect DLNA Server sends the live video stream from the requested camera to the DLNA device

Milestone Open Network Bridge



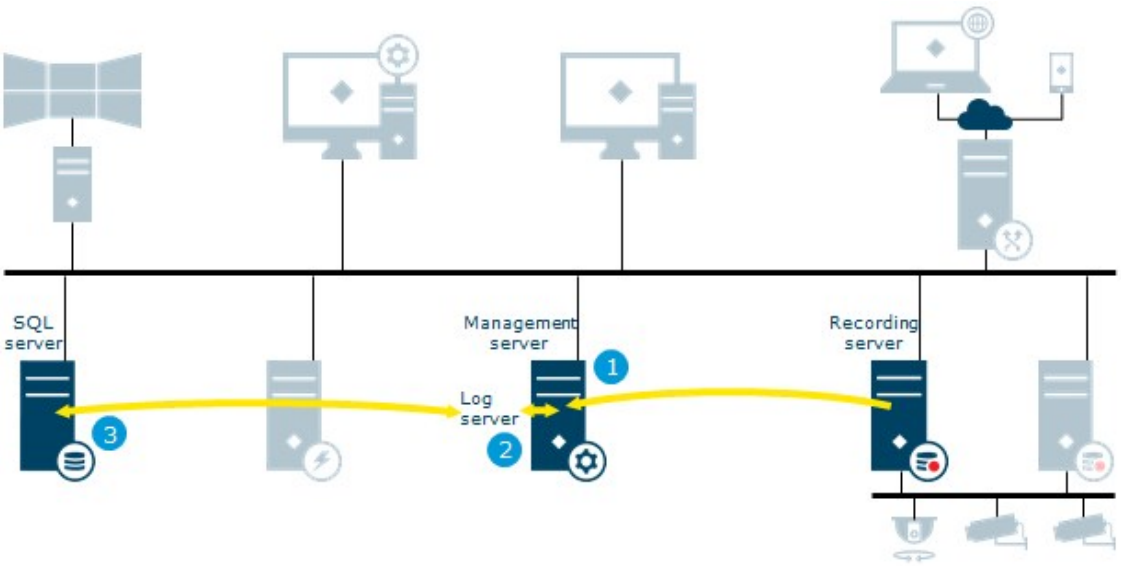
1. Login, stream or PTZ request from ONVIF client received on the Milestone Open Network Bridge server. The Milestone Open Network Bridge is a gateway for non-Milestone clients to the Milestone VMS
2. The Milestone Open Network Bridge forwards the login request to the management server to authenticate the user.
   Access to the Milestone VMS is granted and sent to the Milestone Open Network Bridge server
3. Requested live or playback stream from the recording server is retrieved by the Milestone Open Network Bridge server
4. Video is streamed to the ONVIF client

Management Client configuration update



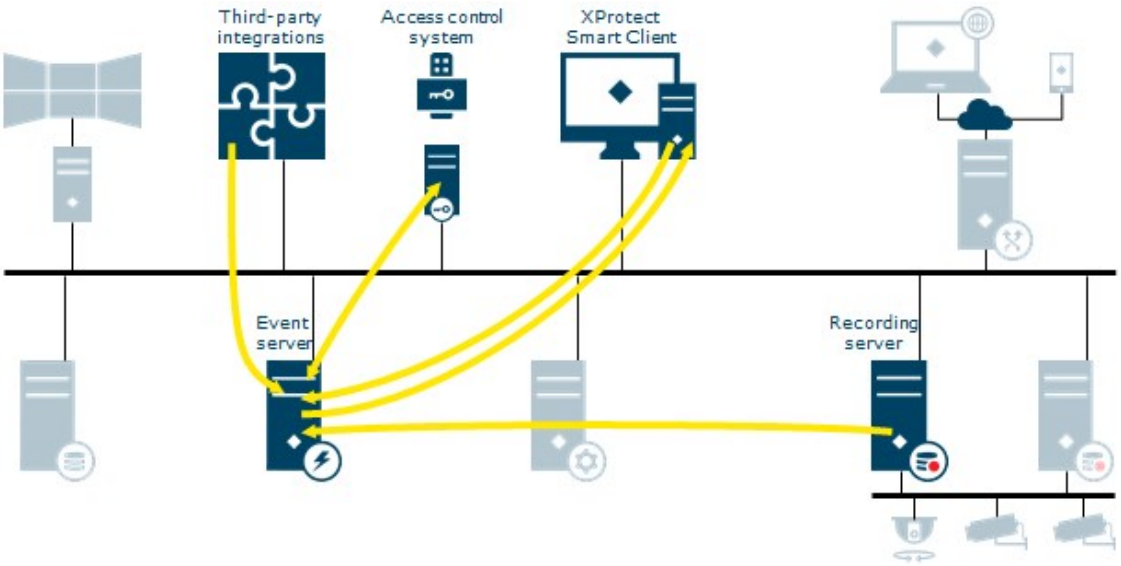
1. Configuration updated on the Management Client
2. Changes are stored on the management server
3. Configuration update sent to relevant components. In this case, the recording server
4. If updates concern cameras, the recording server applies new settings

Log server



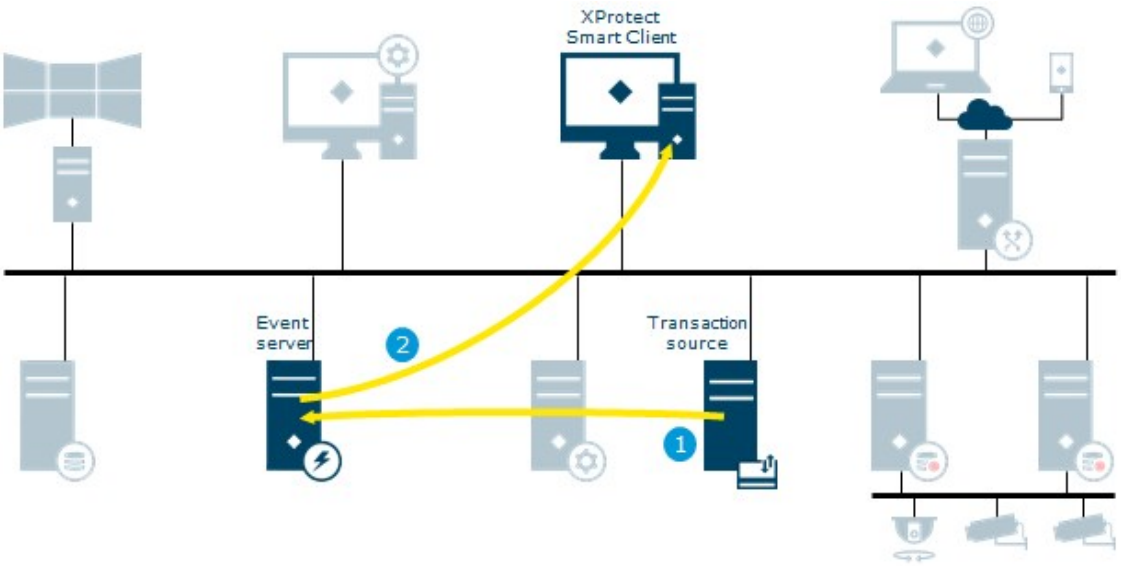
1. The Management server or recording server creates a log message
2. The log message is forwarded to the log server
3. The log message is stored in the log server's SQL Server database

Event server



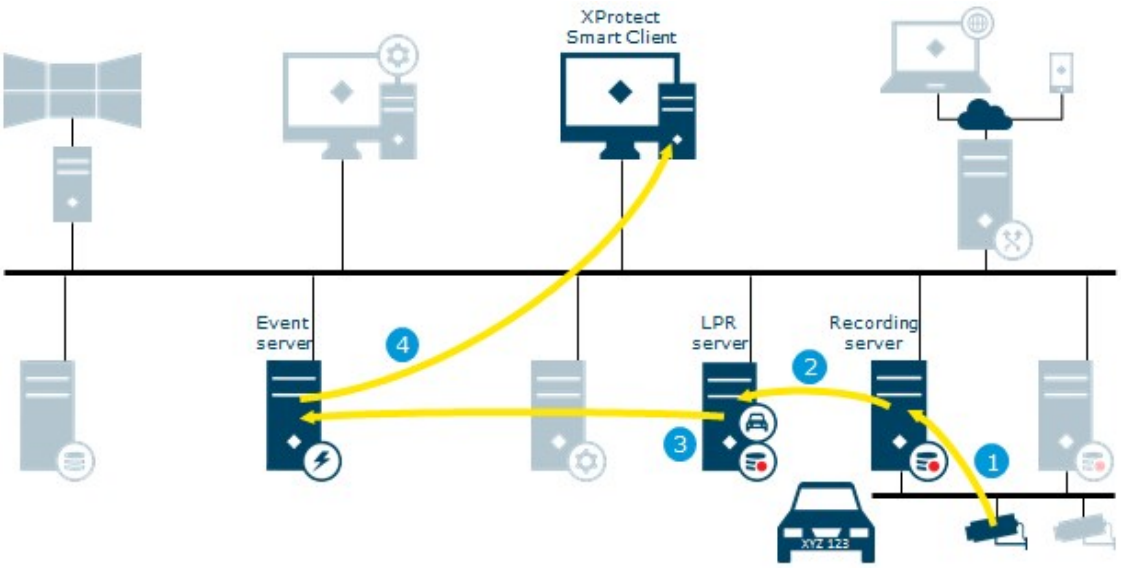
The event server sends data to XProtect Smart Client to show in alarm list, XProtect Access or the map overview.
The event server Plug-in is a client to the access control system.
The XProtect Smart Client user responds to the notification and returns data to event server.

XProtect Transact



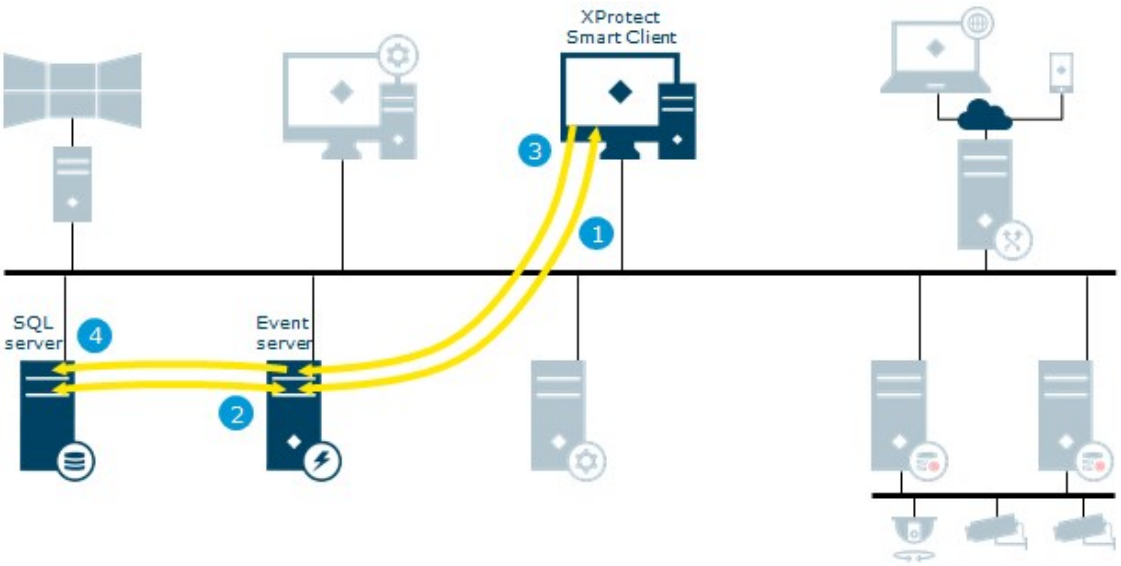
1. Transaction data generated by the transaction source is sent to the event server and stored
2. The event server sends transaction data to XProtect Smart Client. View items containing transaction data and the associated video is updated

XProtect LPR



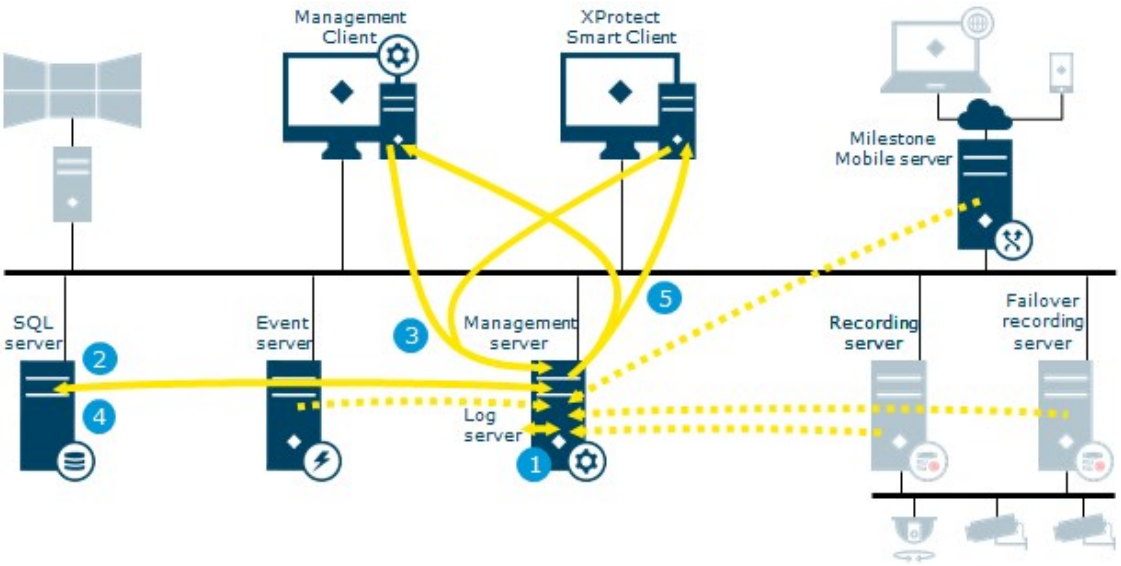
1. Live streams from cameras configured for LPR (License Plate Recognition) retrieved by the recording server
2. Streams from the recording server retrieved by the LPR server
3. The LPR server recognizes license plates by comparing them with the license plate styles of the installed country modules. Found license plates are compared with the match list requests from the event server LPR plug-in
4. The event server sends events and alarms to XProtect Smart Client when there is a match

View and manage alarms



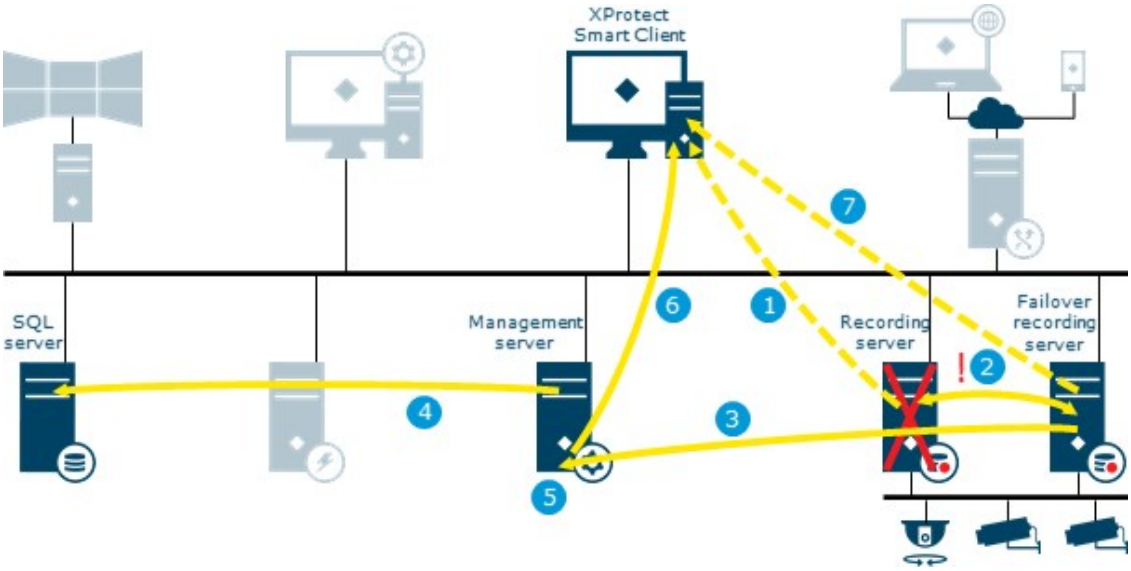
1. XProtect Smart Client requests an alarm list from event server
2. The alarm list is retrieved from the SQL Server database and returned to XProtect Smart Client
3. The alarm is handled and its state/details is updated by the user
4. New state/details stored in the SQL Server database

Data collector



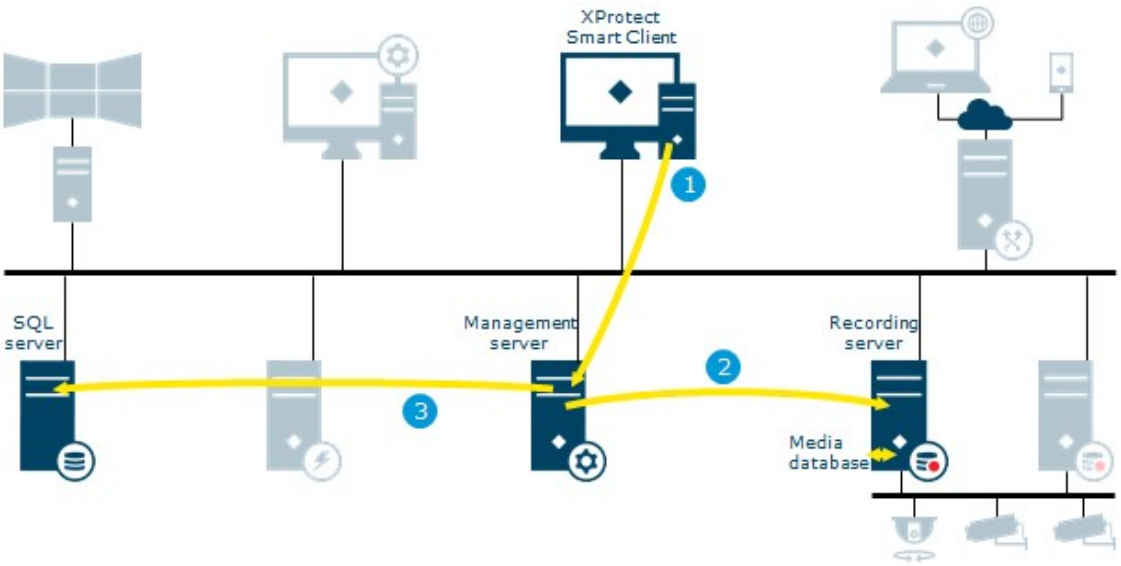
1. System status received on management server delivered by: log server, event server, recording server, failover recording server and mobile server
2. The collected data is stored in a SQL Server database on SQL Server
3. XProtect Smart Client or the Management Client requests status via System Monitor
4. Requested data is collected from a SQL Server database on SQL Server
5. Data returned to clients

Recording server failover



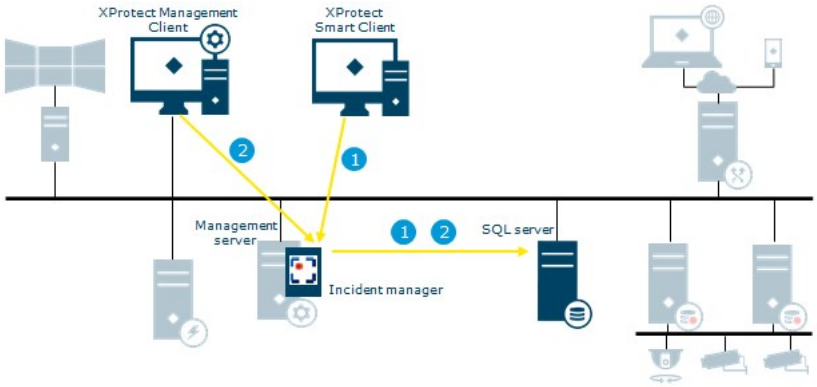
1. Video streamed from the recording server
2. Alive messages exchanged between recording and failover recording server
3. Cold standby: failover message sent, configuration retrieved, start failover
   Hot standby: failover message sent, start failover
4. Configuration updated with active failover recording server
5. Update configuration message sent to the management server
6. Update message distributed to all clients
7. Video streamed from failover recording server

Evidence lock



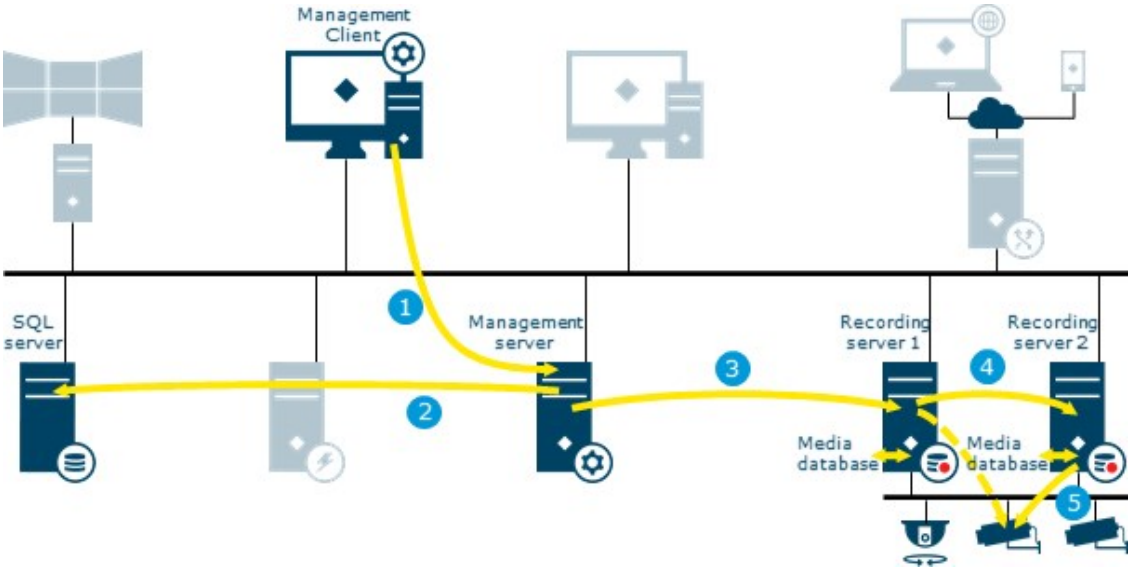
1. The user creates an evidence lock in XProtect Smart Client. XProtect Smart Client sends the information to the management server
2. The management server informs the recording server to store and protect the locked recordings in the Media database
3. The management server stores information about the evidence lock in the SQL Server database

XProtect Incident Manager



Flow	Actions and components
1	An operator of XProtect Smart Client starts, saves, edits, or deletes an incident project. Information about the incident project and its data is saved in the extension's own SQL Server database Surveillance_IM. The activities related to incident projects are - depending on the activity - logged in the extension's own SQL Server database Surveillance_IM, in the Log Server service's SQL Server database SurveillanceLogServerV2, or in both.
2	A Management Client administrator creates, edits, or deletes an incident property. The incident property definition is saved in the extension's own SQL Server database Surveillance_IM. The user activity is logged in the Log Server service's SQL Server database SurveillanceLogServerV2.

Move hardware



1. The user moves hardware from recording server 1 to recording server 2 in Management Client
2. The management server receives the update in the system configuration and stores it in the SQL Server database
3. The management server sends update to recording server 1
4. The management server sends update to recording server 2
5. Recording server 2 connects to Hardware. All new recordings are stored in the recording server 2 database

Old recordings are still available on recording server 1. The system deletes them when the retention time expires. Recordings marked with evidence lock are not deleted until the evidence lock's retention time expires.

Clients connect to recording server 2

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. These are not explicitly listed in this doc.

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 servers and the XProtect Smart Client and the Management Client	The purpose of port 80 and port 443 is the same. However, which port the VMS uses depends on whether you have used certificates to secure the communication. • When you have not secured the communication with certificates, the VMS uses port 80. • When you have secured the communication with certificates, the VMS uses port 443 except for communication from the event server to the management server. The communication from the event server to the management server uses Windows Secured Framework (WCF) and Windows authentication on port 80.
443	HTTPS	IIS		
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.
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.

Port number	Protocol	Process	Connections from...	Purpose
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 via the Identity Provider.
1433	TCP	SQL Server	Event Server service	Storing and retrieving events via the Identity Provider.
1433	TCP	SQL Server	Log Server service	Storing and retrieving log entries via the Identity Provider.

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.
22332	WS/WSS HTTP/HTTPS*	Event Server service	API Gateway and the Management Client	Event/State Subscription, Events REST API, Websockets Messaging API, and Alarms REST API.
22333	TCP	Event Server service	MIP Plug-ins and applications.	MIP messaging.

*A 403 error will be returned when accessing HTTP to access an HTTPS-only endpoint.

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. (Deprecated) Enabling this will open a port for non-encrypted connections and is not recommended.
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.

Port number	Protocol	Process	Connections from...	Purpose
11000	TCP	Recording Server Service	Failover recording servers	Polling the state of recording servers.
12975	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. In XProtect 2014 systems or older, the port number was 6474. In XProtect 2019 R2 systems and older, the port number was 7474.
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:

- Cameras
- NVRs
- Remote interconnected sites (Milestone Interconnect ICP)

Failover Server service and Failover Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Failover	Cameras, encoders, and	Listening for event messages from

Port number	Protocol	Process	Connections from...	Purpose
		Recording Server Service	I/O devices.	devices. The port is disabled by default. (Deprecated) Enabling this will open a port for non-encrypted connections and is not recommended.
5210	TCP	Failover Recording Server Service	Failover recording servers	Merging of databases after a failover recording server had been running.
5432	TCP	Failover Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled by default.
7474	TCP	Failover 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	Failover Recording Server Service	XProtect Smart Client	Retrieving video and audio streams, PTZ commands.
8844	UDP	Failover Recording Server Service	Communication between failover recording server services.	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.

Port number	Protocol	Process	Connections from...	Purpose
8967	TCP	Failover Server Service	Failover Server Manager tray icon, local connection only.	Showing status and managing the service.
8990	HTTP	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.

In addition to the inbound connections to the Failover Server / Failover Recording Server service listed above, the Failover Server / Failover Recording Server service establishes outbound connections to the regular recorders, cameras, and for Video Push.

Log Server service

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

This port uses HTTP, but the communication is encrypted with message security which uses the WS-Security specification to secure messages. For more information, see Message Security in WCF.

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.
40001 - 40099	HTTP	Mobile Server service	Recording server service	Mobile Server Video Push. This port range is disabled by default.

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 must have the LPR plug-in installed.
22334	TCP	LPR Server Service	LPR Server Manager tray icon, local connection only.	SysTray application

Milestone Open Network Bridge service

Port number	Protocol	Process	Connections from...	Purpose
580	TCP	Milestone Open Network 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.

XProtect Incident Manager service

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	XProtect Smart Client and the Management Client	The purpose of port 80 and port 443 is the same. However, which port the VMS uses depends on whether you have used certificates to secure the communication. • When you have not secured the communication with certificates, the VMS uses port 80. • When you have secured the communication with certificates, the VMS uses port 443.
443	HTTPS	IIS		

Server components (outbound connections)

Management Server service

Port number	Protocol	Connections to...	Purpose
443	HTTPS	The License server that hosts the License Management service. Communication is via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Activating licenses.

Recording Server service

Port number	Protocol	Connections to...	Purpose
80	HTTP	Cameras, NVRs, encoders	Authentication, configuration, data streams, video, and audio.

Port number	Protocol	Connections to...	Purpose
		Interconnected sites	Login
443	HTTPS	Cameras, NVRs, encoders	Authentication, configuration, data streams, video, and audio.
554	RTSP	Cameras, NVRs, encoders	Data streams, video, and audio.
7563	TCP	Interconnected sites	Data streams and events.
11000	TCP	Failover recording servers	Polling the state of recording servers.
40001 – 40099	HTTP	Mobile Server service	Mobile Server Video Push. This port range is disabled by default.

Failover Server service and Failover Recording Server service

Port number	Protocol	Connections to...	Purpose
11000	TCP	Failover recording servers	Polling the state of recording servers.

Event Server service

Port number	Protocol	Connections to...	Purpose
80	HTTP	API Gateway and the Management Server	Access the Configuration API from the API Gateway

Port number	Protocol	Connections to...	Purpose
443	HTTPS	API Gateway and the Management Server	Access the Configuration API from the API Gateway
443	HTTPS	Milestone Customer Dashboard via https://service.milestonesys.com/	Send status, events and error messages from the XProtect system to Milestone Customer Dashboard.

Log Server service

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

API Gateway

Port number	Protocol	Connections to...	Purpose
443	HTTPS	Management Server	RESTful API
22332	WS/WSS HTTP/HTTPS*	Management Client	Event/State Subscription, Events REST API, Websockets Messaging API, and Alarms REST API.

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	API Gateway and Management Server service	Authentication and other APIs in the API Gateway.
443	HTTPS	API Gateway and Management Server service	Authentication of basic users when encryption is enabled and other APIs in the API Gateway.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com at 52.178.114.226)	Management Client and Smart Client occasionally check if the online help is available by accessing the help URL.
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.

API Gateway

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

Application pools

The VMS contains standard application pools such as.NET v4.5, .NET v4.5 Classic and the DefaultAppPool. The application pools that are available on your system appear in the Internet Information Services (IIS) Manager. In addition to the standard application pools mentioned above, a set of VideoOS application pools are delivered with the Milestone XProtect VMS.

Application pools in Milestone XProtect

In the table below you can get an overview of the VideoOS application pools that are delivered with Milestone XProtect.

Name	Identity	Purpose
.NET v4.5	ApplicationPoolId	Standard IIS feature
.NET v4.5 Classic	ApplicationPoolId	Standard IIS feature
DefaultAppPool	ApplicationPoolId	Standard IIS feature
VideoOS ApiGateway	NetworkService	Hosts the XProtect API Gateway which is the future public API and gateway to the VMS.
VideoOS Classic	NetworkService	Hosts legacy components such as the local help mainly to comply with backwards compatibility.
VideoOS IDP	NetworkService	Hosts the Identity Provider API. The Identity Provider creates, maintains, and manages identity information for basic users and provides authentication and registration services to relying applications or services.
VideoOS IM	NetworkService	Hosts the XProtect Incident Manager API. The XProtect Incident Manager documents incidents and combine them with sequence evidence (video and, potentially, audio) from their

Name	Identity	Purpose
		XProtect VMS.
VideoOS Management Server	NetworkService	Hosts the Configuration API, server component APIs and other Management Server services, and manages user authorization.
VideoOS ReportServer	NetworkService	Hosts the web application that is responsible for collecting and creating reports for alarms and events.
VideoOS ShareService	NetworkService	Hosts the service that facilitates bookmarks and live video sharing between the users of XProtect Mobile client.

Working with application pools

From the **Application Pools** page in the **Internet Information Services (IIS)** window you can add application pools or set appplication pool defaults and you can view the applications hosted by each application pool.

Open the Application Pools page

1. From the Windows **Start** menu, open **Internet Information Servces (IIS) Manager**.
2. In the **Connections** pane, click the name of your environment, and then click **Application Pools**.
3. Under **Actions**, click **Add Application Pool** or **Set Application Pool Defaults** to perform any of these tasks.
4. Select an application pool on the **Application Pools** page to display further options under **Actions** for each application pool.

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/.