Milestone Systems

XProtect® Advanced VMS 2014

System Architecture

milestone

The Open Platform Company

Content

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 reserve the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance

to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply.

When that is the case, you can find more information in the file

3rd_party_software_terms_and_conditions.txt located in your Milestone surveillance system

installation folder.

Introduction

The Milestone XProtect® Advanced VMS 2014 System Architecture document contains illustrations and descriptions of communication and dataflow between the most common system components in a distributed installation of XProtect® Corporate or XProtect® Expert.

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

In general, the illustrations are simplified and primarily focus on general dataflow between system components. This means that less important flows might be left out in order to reduce the complexity level.

Target audience and purpose

The primary audience for this document is system integrators and IT administrators with limited experience with Milestone XProtect Advanced VMS solutions that are in the process of selecting, deploying, administrating, maintaining and expanding a VMS.

The purpose is to provide insight to the benefits and ease of using Milestone XProtect Expert and Corporate as the VMS, including introducing the system components and the system architecture.

This document should enable the reader to understand the:

- Overall system architecture
- Primary system components and their functions

as well as give some guidelines to basic system design.

The reader is assumed to have a general experience in administrating an IT installation.

Overall system architecture

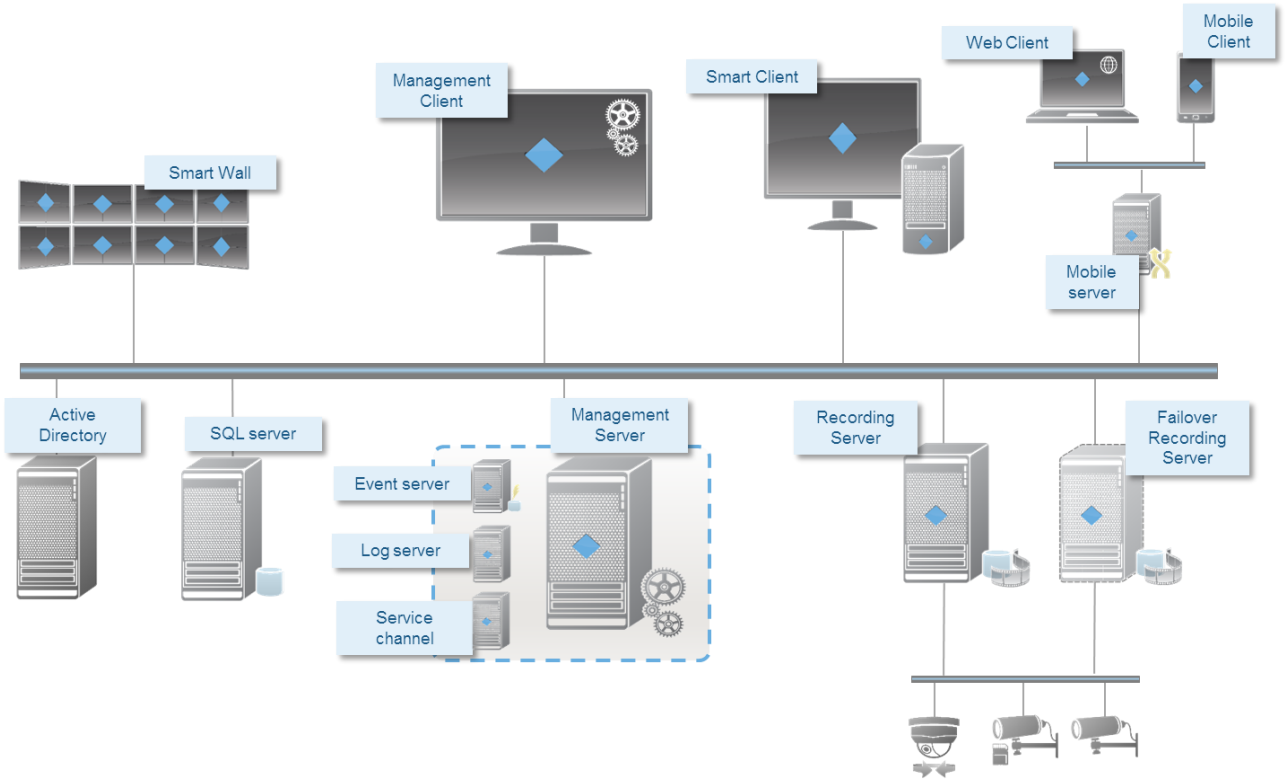
To enable scaling of up to thousands of cameras across multiple sites, the system consists of several components that handle specific tasks. All components can be installed on a single server if the server is able to handle the load, or the components can be installed on separate dedicated servers to scale and distribute the load.

Depending on hardware and configuration, smaller systems with up to 50~100 cameras can run on a single server

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

Not all components are needed in all installations, but can be added if the functionality they offer is needed, for example, failover recording servers or mobile servers for hosting and providing access to both the web and mobile client.

The diagram below shows an overview of the system components.



Note:

- Failover recording servers are not supported in XProtect Expert.
- Smart Wall is an add-on product to XProtect Expert

Server components

Management Server
The management server is the central component of the VMS. It handles the system configuration, distributes the configuration to other system components like the recording servers and facilitates user authentication.

The configuration is stored on a standard Microsoft SQL server installed either on the management server itself or on a separate dedicated server.

Failover Management Server
Failover support on the management server is achieved 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.

For more information on configuring Failover Clusters in Windows Server 2008 R2:
http://technet.microsoft.com/en-us/library/ff182338(v=ws.10).aspx

For more information on configuring Failover Clusters in Windows Server 2012:
http://technet.microsoft.com/library/hh831579

Recording Server
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. For example:

- Retrieve video, audio, metadata and I/O event streams from the devices.
- Record video, audio and metadata.
- Provide access to live and recorded video, audio and metadata.
- Provide 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 on Milestone Interconnect:

www.milestonesys.com/SharePoint/White%20papers/Milestone_Interconnect.pdf

Media Database
The system stores the retrieved video, audio and metadata in the tailor-made high performance Milestone media database that is 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.

For more information on the media database and the storage architecture:
http://www.milestonesys.com/Company/Additional-Resources/resourcelibrary/

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:

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

Event server
The event server handles the 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 is one place and interface for partners to make integrations that utilize system events.
- 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 of the alarm database. The alarm database is stored in the same SQL server that the management server uses.

Maps:

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

MIP SDK:

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

Failover event server
Failover support on the event server is achieved 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.

For more information on configuring Failover Clusters in Windows Server 2008 R2:
http://technet.microsoft.com/en-us/library/ff182338(v=ws.10).aspx

For more information on configuring Failover Clusters in Windows Server 2012:
http://technet.microsoft.com/library/hh831579

Log server
The log server is responsible for storing all log messages for the entire system. The log server uses the same SQL server as the management server and is typically installed on the same server as the management server, but can be installed on a separate server if the management or log server performance needs to be increased.

The system can log three types of logs:

- **System log:** the system administrator can choose to log errors, warnings and information or combinations of these. Default is logging errors only.
- **Audit log:** the system administrator can choose to log user activity in the clients in addition to login and administration logs
- **Rule log:** the rule log can be used by the system administrator to create logs on specific events

Service channel
The service channel is responsible for communicating service and configuration messages to XProtect Smart Client, the mobile server, and third-party components listening to the service channel. This could for example be communicating updates to an XProtect Smart Wall monitor layout or communicating that a failover server is now active plus the address of it.

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

In addition to acting as a system gateway for mobile and web clients, the mobile server also offers video transcoding capabilities as the original camera video stream in many cases are too large to fit the bandwidth available for the mobile and web users.

Milestone recommends that you install the mobile server on a dedicated server.

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

The XProtect Expert and XProtect Corporate installer include Microsoft SQL Server 2012 Express that can be used freely for systems up to 300 cameras.

For larger systems over 300 cameras, Milestone recommends that you use the SQL Server 2008 R2 Standard or Enterprise edition on a dedicated server as these editions can handle larger databases and offer backup functionality.

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.

When you select a function in the node tree, the settings for this node appear, typically in a second tree structure where you can manage sub items. Once you have selected the correct item, the actual settings appear in the properties dialog box in the upper right hand corner. The settings are grouped on different tabs if an item has many settings.

XProtect Smart Client®
XProtect Smart Client is the main client for the VMS offering a full set of advanced features and designed for a day-to-day use by dedicated operators.

XProtect Smart Client is designed to run remotely from the operators' computer and supports multiscreen usage in full screen mode as shown below or in floating windows mode where the user can resize the windows and move them around freely.

For more information about the XProtect Smart Client:
http://www.milestonesys.com/Software/XProtect-Clients/XProtect-Smart-Client/

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

For more information about the XProtect Web Client:
http://www.milestonesys.com/Software/XProtect-Clients/XProtect-Web-Client/

Compatible browsers can be found here: (click on XProtect Web Client)
http://www.milestonesys.com/Support/Technical-Support/Product-System-Requirements/

Milestone Mobile
The Milestone Mobile client is the client designed for the user on the go. It offers easy access to live monitoring, playback and export of video, as well as access to activate system events and outputs.

The Milestone Mobile client can be used as a remote recording device by using the device's built-in camera and the Milestone Video Push feature. With Video Push activated, the video from the device's camera is streamed back to the VMS and recorded like a standard camera.

For more information about the Milestone Mobile client:
http://www.milestonesys.com/Software/XProtect-Clients/XProtect-Mobile/

Compatible smart phone operating systems can be found here: (click on Milestone Mobile)
http://www.milestonesys.com/Support/Technical-Support/Product-System-Requirements/

Additional products and components

XProtect Smart Wall 2014
XProtect Smart Wall is designed for control centers to display live video from selected cameras on one or more video wall displays.

The cameras can be selected either manually by the operators using the XProtect Smart Client, via the VMS' rule system on events and/or time schedule, or via MIP SDK integrations.

The Smart Wall does not require a dedicated XProtect software component itself, nor does it use a dedicated XProtect client - all the required components are included in the standard XProtect Corporate management server and XProtect Smart Client. It just needs a PC to run XProtect Smart Client to show the Smart Wall views.

XProtect Smart Wall 2014 is included in XProtect Corporate 2014 and can be purchased as an add-on for XProtect Expert 2014.

For more information on XProtect Smart Wall:
http://www.milestonesys.com/Software/Add-ons-for-XProtect/xprotectsmartwall/

MIP SDK
The Milestone Integration Platform Software Development Kit (MIP SDK) is a comprehensive tool that makes it easy to create applications, plug-ins or integrations for Milestone's XProtect products.

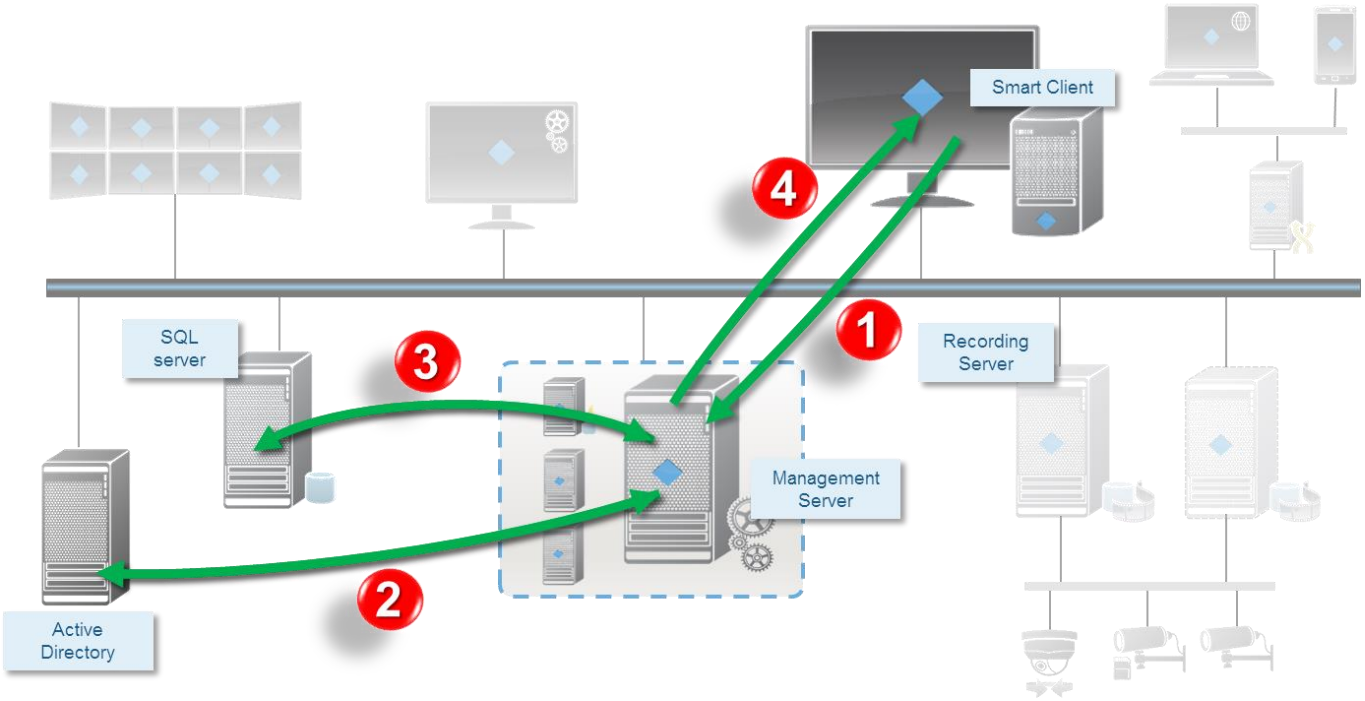
Software manager

The software manager is a tool that, from a central point, can be used to remotely install and upgrade recording servers, recording server device packs and XProtect Smart Clients on servers or PCs in the network.

For larger installations the tool makes it easy and fast to upgrade the components that are installed remotely and in many places; namely the recording servers and their device packs as well as all the client PCs.

http://www.milestonesys.com/Software/Add-ons-for-XProtect/utilities/

Login



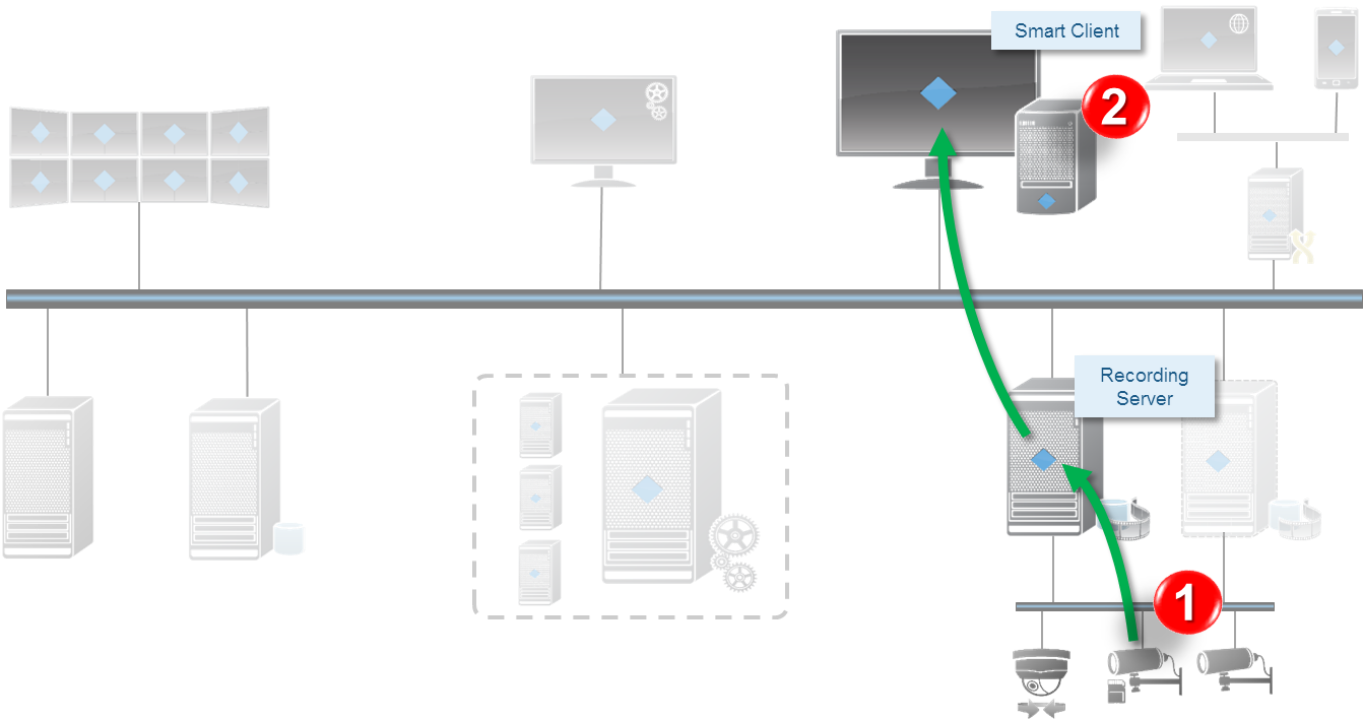
1) XProtect Smart Client attempts to log in and sends command to Management Server
Port: device dependent and configurable - typically port 80 for Active Directory user and 443 for basic user.
Protocol: HTTP for Active Directory (AD) user and HTTPS for basic user.
Bandwidth: low, 1 Kbit/call

2) User authentication towards Active Directory
Port: OS and AD dependent
Protocol: OS and AD dependent
Bandwidth: low, 5 Kbit / Call

3) User specific configuration is retrieved from the database on the SQL server
Port: 1433
Protocol: TCP/IP
Bandwidth: depends on configuration, cameras, views etc.

4) Login granted and configuration sent to XProtect Smart Client
Port: Configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: depends on configuration, cameras, views etc. - typically 1-10 MB

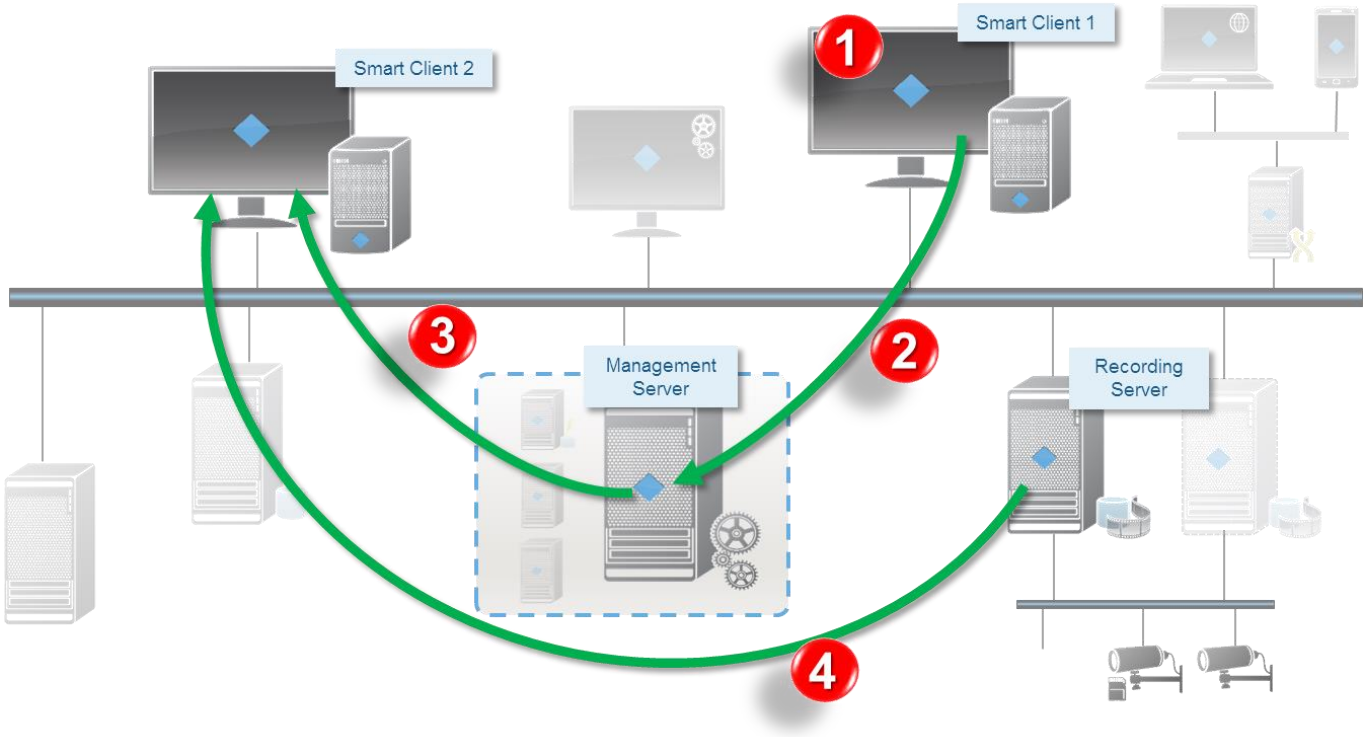
Live video and audio



1) Live streams from cameras retrieved by Recording Server
Port: device dependent and configurable - typically port 80.
Protocol: device dependent and configurable – typically RTSP, UDP, TCP/IP
Bandwidth: device configurable – typically 1-10 Mbit/s

2) Streams are sent to XProtect Smart Clients (and XProtect Smart Wall) on request
Port: configurable - default port 7563
Protocol: configurable, TCP/IP, UDP Multicast – default TCP/IP
Bandwidth: usage dependable. Calculation: add bandwidth per camera viewed to get the sum

Matrix



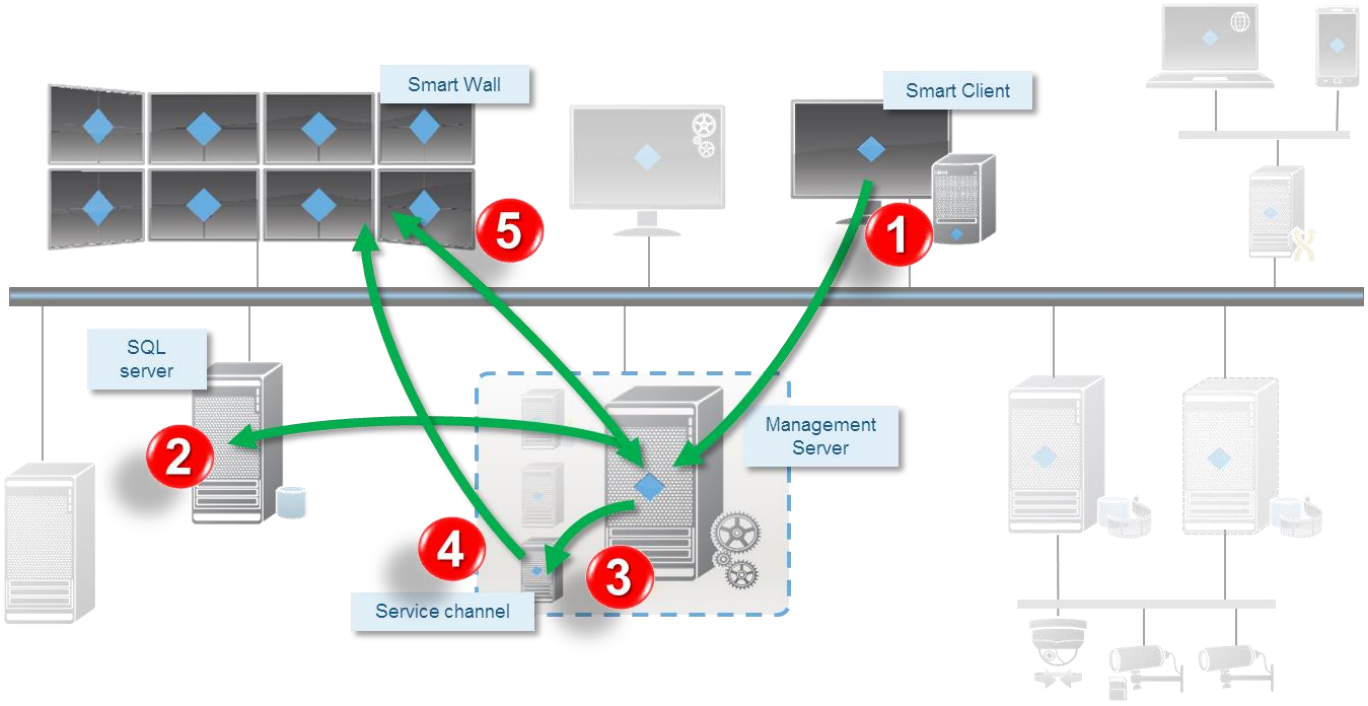
1) XProtect Smart Client user selects to send a camera to a Matrix recipient
Port: N/A
Protocol: N/A
Bandwidth: N/A

2) Information sent to Management Server
Port: device dependent and configurable - typically port 80 for AD user and 443 for basic user.
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call

3) Management Server sends request to Matrix recipient on specified IP address and port (XProtect Smart Client 2)
Port: configurable – default is 12345
Protocol: TCP/IP
Bandwidth: Low, 1 Kbit/call

4) Streams are sent to XProtect Smart Client from Recording Server on request
Port: configurable - default port 7563
Protocol: configurable, TCP/IP, UDP Multicast – default TCP/IP
Bandwidth: usage dependable – calculation: add bandwidth per camera viewed to get the sum

Smart Wall



1) Smart Client user updates view on Smart Wall
Port: configurable – default is 5432
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

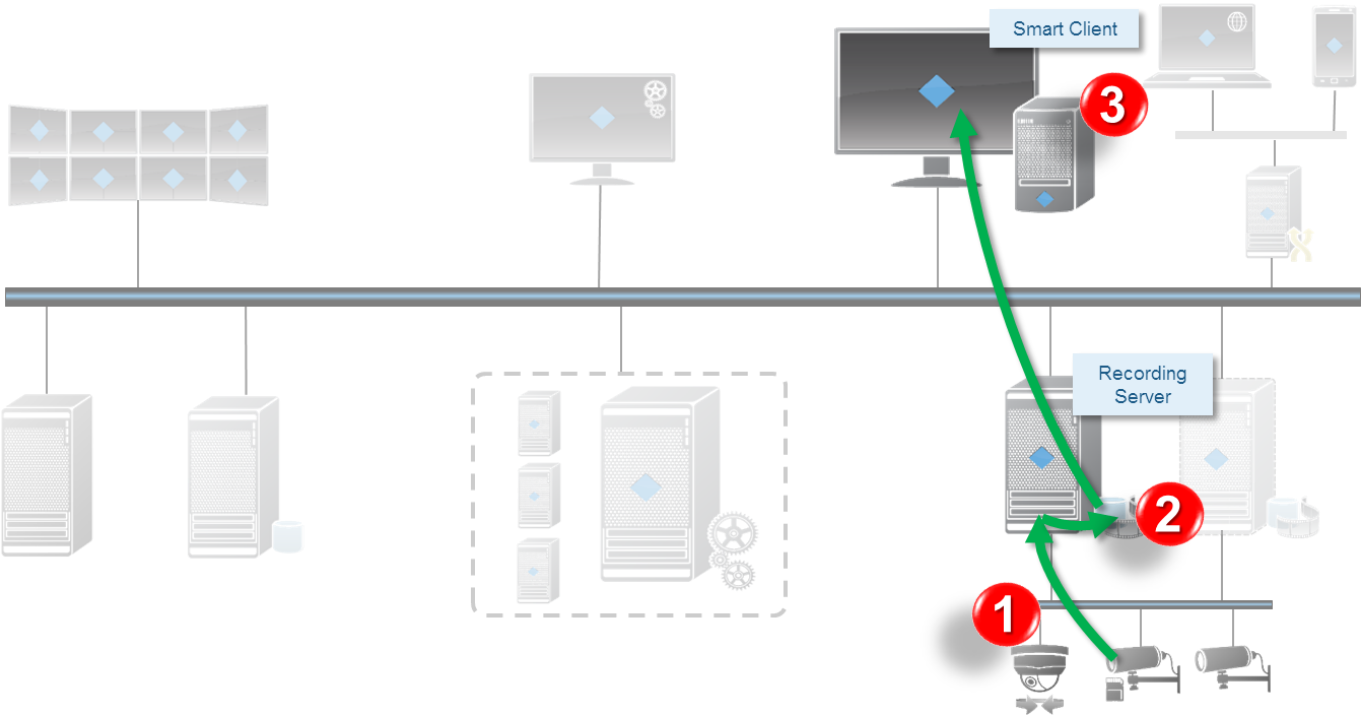
2) Smart Wall view configuration updated and stored on the SQL server
Port: 1433
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

3) Management Server contacts Service channel
Port: 80
Protocol: HTTP
Bandwidth: low, 1 Kbit/call

4) Service channel sends notification to XProtect Smart Clients running Smart Wall
Port: configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call

5) XProtect Smart Client running Smart Wall retrieves and applies new layout
Port: configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call

Play back video and audio

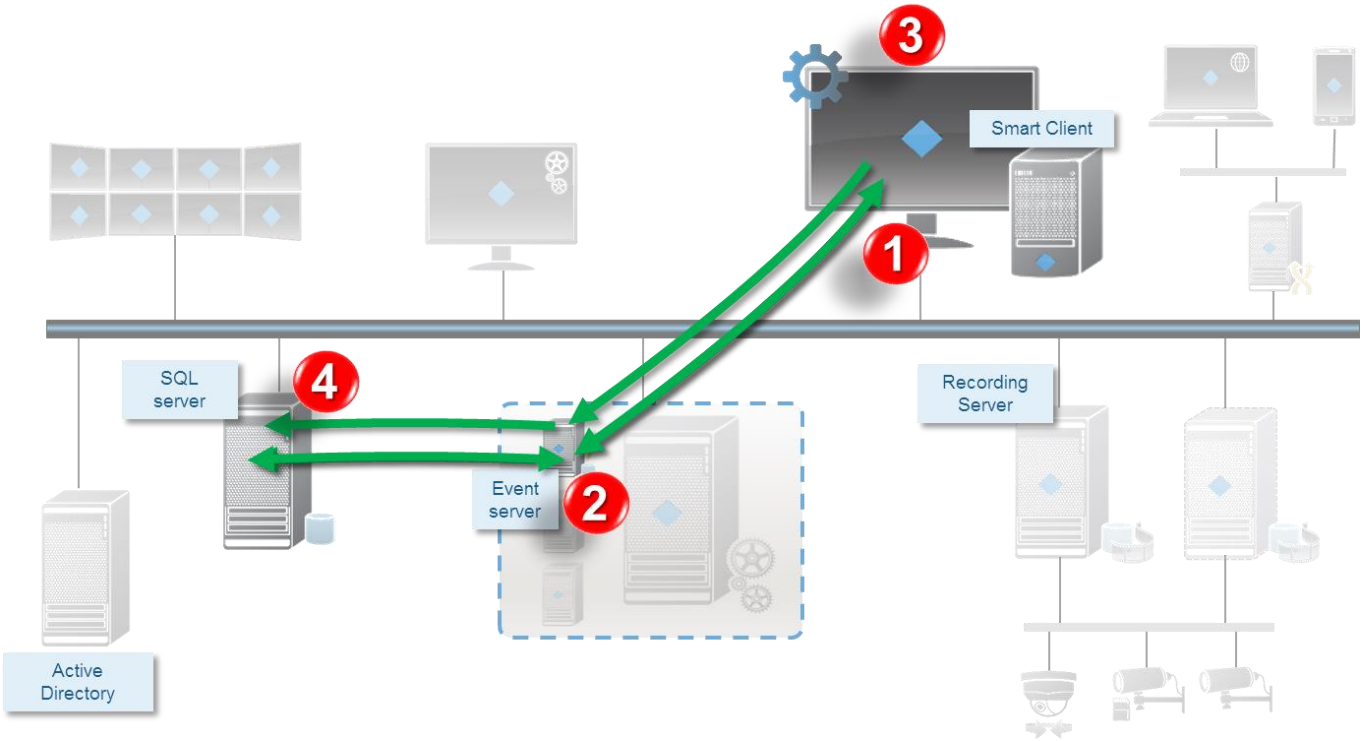


1) Recording stream from cameras retrieved by Recording Server
Port: device dependent and configurable - typically port 80.
Protocol: device dependent and configurable – typically RTSP, UDP, TCP/IP
Bandwidth: device configurable – typically 1-10 Mbit/s

2) Stream is recorded in the Recording Server database based on rules
Port: N/A
Protocol: N/A
Bandwidth: device configurable – typically 1-10 Mbit/s

3) Recorded stream is retrieved by XProtect Smart Client on playback request
Port: configurable - default port 7563
Protocol: TCP/IP
Bandwidth: usage dependable. Calculation: add bandwidth per camera viewed to get the sum

View and manage alarms



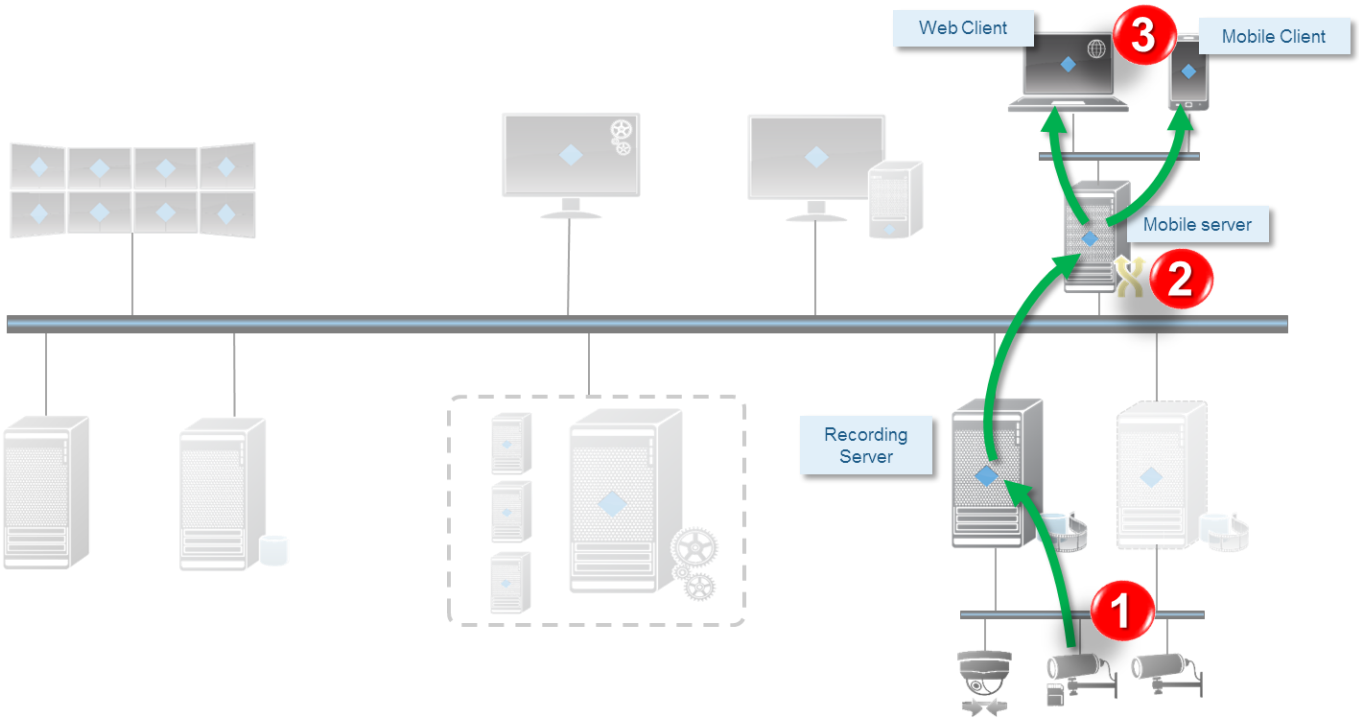
1) XProtect Smart Client requests alarm list from Event server
Port: configurable – default is 22331
Protocol: TCP/IP
Bandwidth: Low, 1 Kbit/call

2) Alarm list retrieved from SQL server and returned to XProtect Smart Client
Port: 1433
Protocol: TCP/IP
Bandwidth: Low. 100 Kbit/call

3) Alarm handled and state and details updated by the user

4) New state and details stored on SQL server
Port: 1433
Protocol: TCP/IP
Bandwidth: Low. 1 Kbit/call

Live video for web and mobile

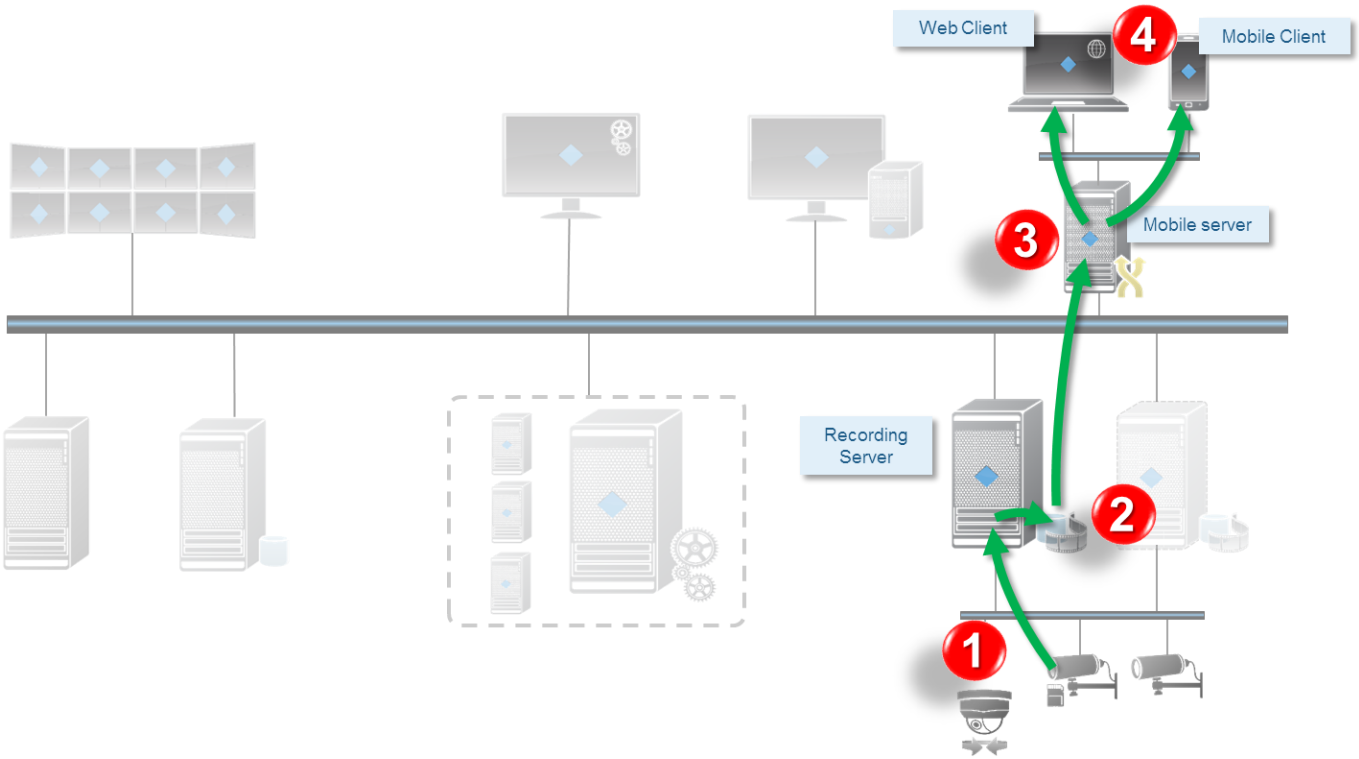


1) Live stream(s) retrieved from cameras
Port: device dependent and configurable - typically port 80
Protocol: device dependent and configurable – typically RTSP, UDP, TCP/IP
Bandwidth: device configurable – typically 1-10 Mbit/s

2) Streams are sent to Milestone Mobile server for transcoding or as direct stream
Port: configurable - default port 7563
Protocol: configurable, TCP/IP, UDP Multicast – default TCP/IP
Bandwidth: usage dependable. Calculation: add bandwidth per camera viewed to get the sum

3) Streams are sent to Mobile Client or Web clients
Port: device dependent and configurable - typically port 8081 for HTTP and 8082 for HTTPS
Protocol: HTTP or HTTPS
Bandwidth: Transcoding: typically 50–200 Kbit/s
Native: device configurable – typically 0.05-1 Mbit/s

Recording and playback video for web and mobile

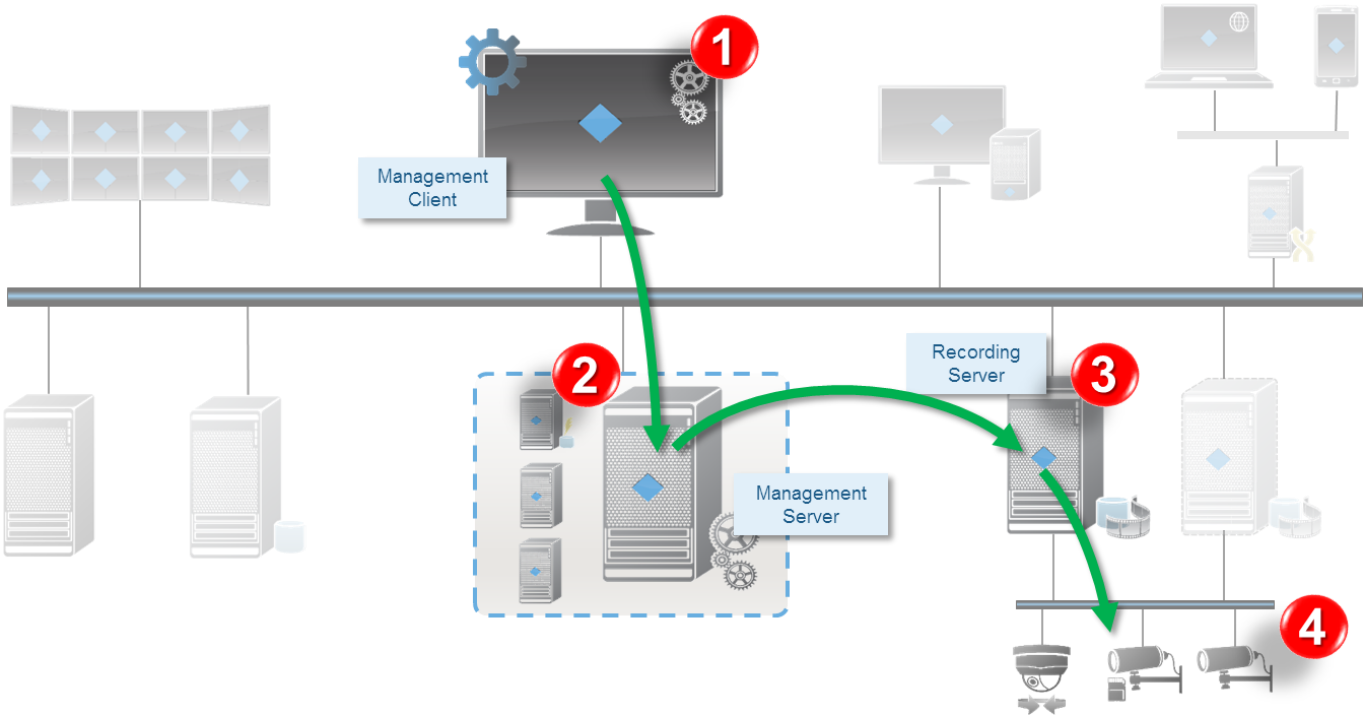


1) Live stream(s) retrieved from cameras
Port: device dependent and configurable - typically port 80
Protocol: device dependent and configurable – typically RTSP, UDP, TCP/IP
Bandwidth: device configurable – typically 1-10 Mbit/s

2) Streams are sent to Mobile Server for transcoding or as direct stream
Port: configurable - default port 7563
Protocol: configurable, TCP/IP, UDP Multicast – default TCP/IP
Bandwidth: usage dependable. Calculation: add bandwidth per camera viewed to get the sum

3) Streams are sent to Mobile or Web clients
Port: device dependent and configurable - typically port 8081 for HTTP and 8082 for HTTPS
Protocol: HTTP or HTTPS
Bandwidth: Transcoding: typically 50–200 Kbit/s
Native: device configurable – typically 1-10 Mbit/s

Management Client – configuration update



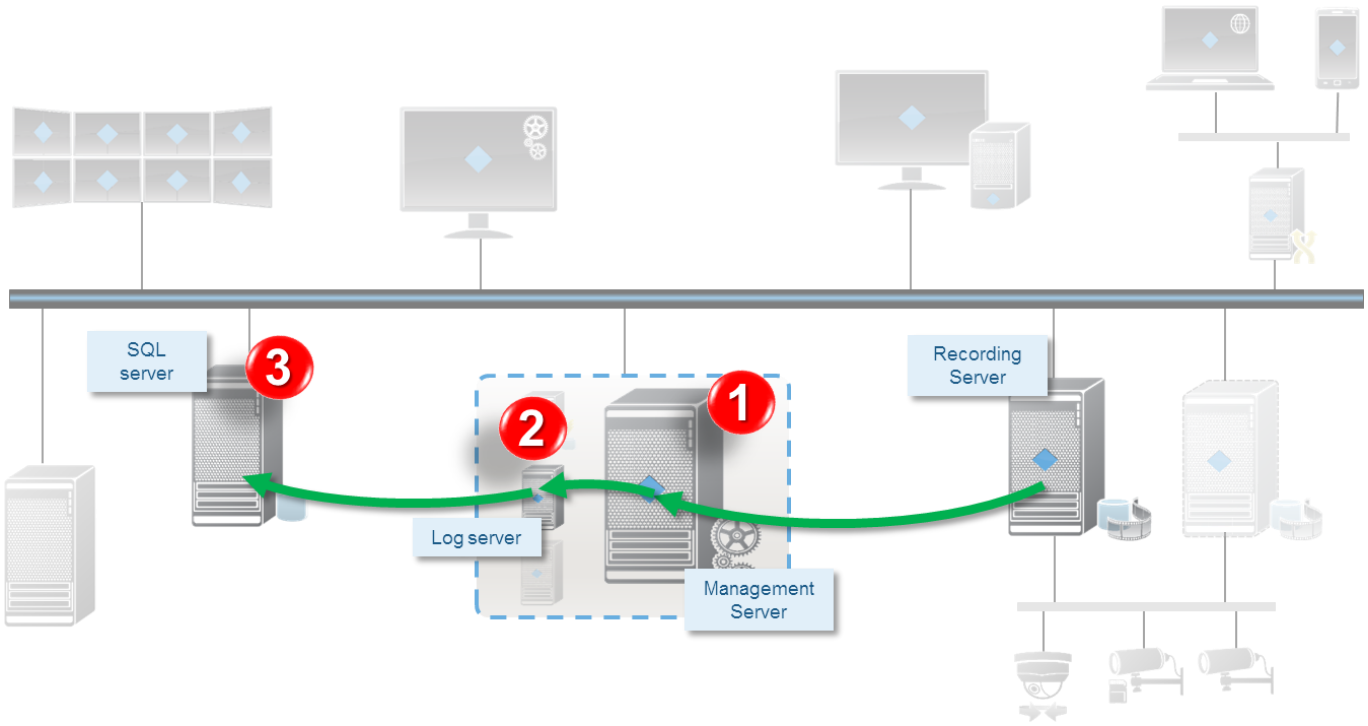
1) Configuration updated on Management Client

2) Changes are sent to Management Server
Port: configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic User
Bandwidth: low, 10 Kbit/call

3) Configuration update sent to relevant components – in this case Recording Server
Port: configurable - default port 7563
Protocol: configurable, TCP/IP
Bandwidth: low, 10-100 Kbit/call

4) If updates concern the cameras, Recording Server applies new settings
Port: device dependent and configurable - typically port 80 for HTTP and 443 for HTTPS
Protocol: HTTP or HTTPS
Bandwidth: low, 1 Kbit/call

Log server

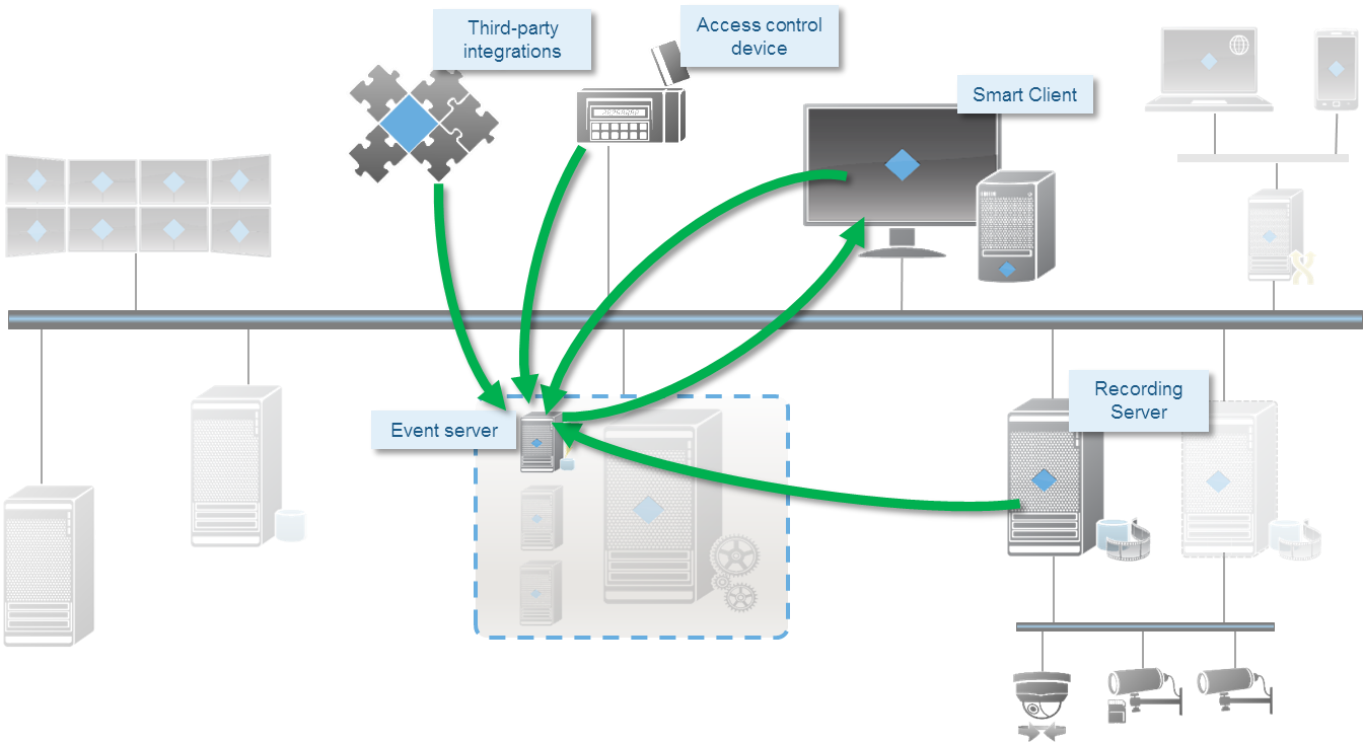


1) Management Server or Recording Server creates log message
Port: 9993
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

2) Log message is forwarded to Log server
Port: Configurable – default is 80
Protocol: HTTP
Bandwidth: low, 1 Kbit/call

3) Log message is stored in the SQL server database
Port: 1433
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

Event server



Event Server receives events in the following ways:

Recording Server
Port: 7563 (on Recording Server)
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

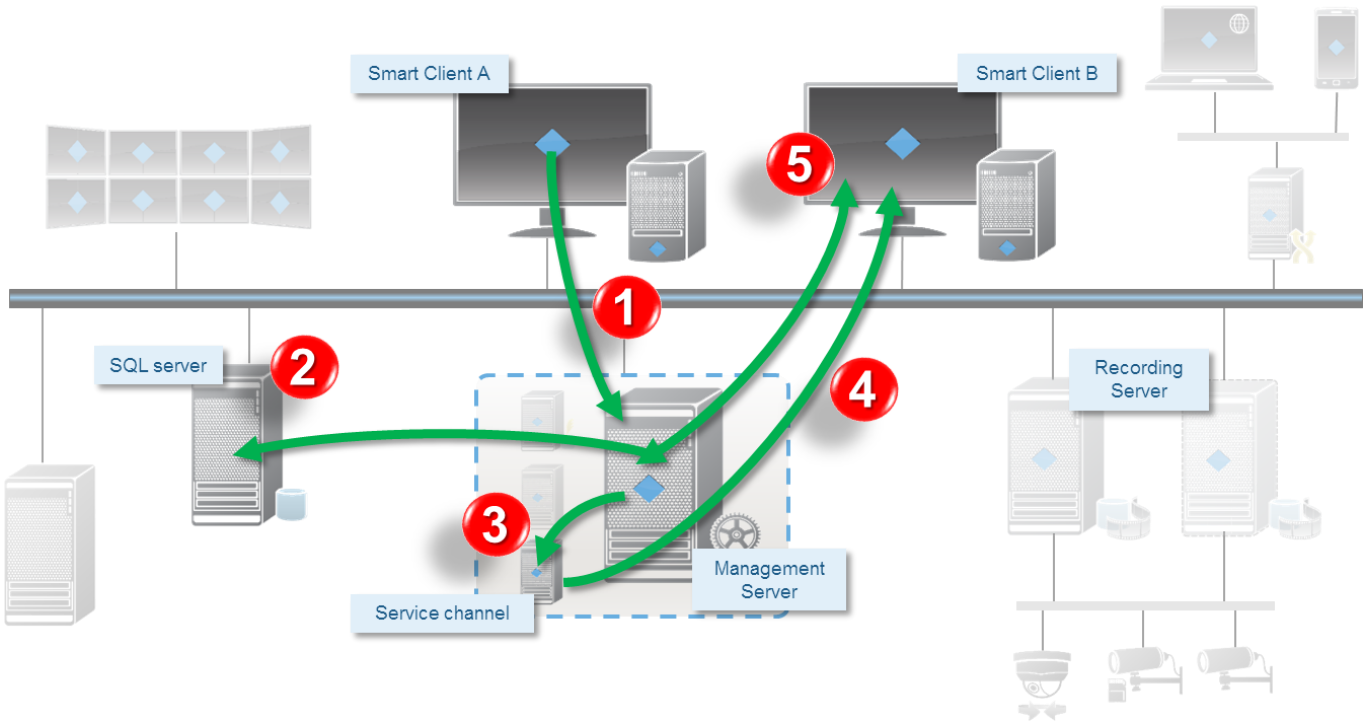
MIP Message Communication
Port: 22333
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

Analytics Events
Port: configurable – default is 9090
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

Generic Events
Port: configurable – defaults are 1234 and 1235
Protocol: TCP/IP / UDP
Bandwidth: low, 1 Kbit/call

Access Control integrations
Port: Depends on the integration
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

Service Channel – view update



1) View updated on XProtect Smart Client A
Port: configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call

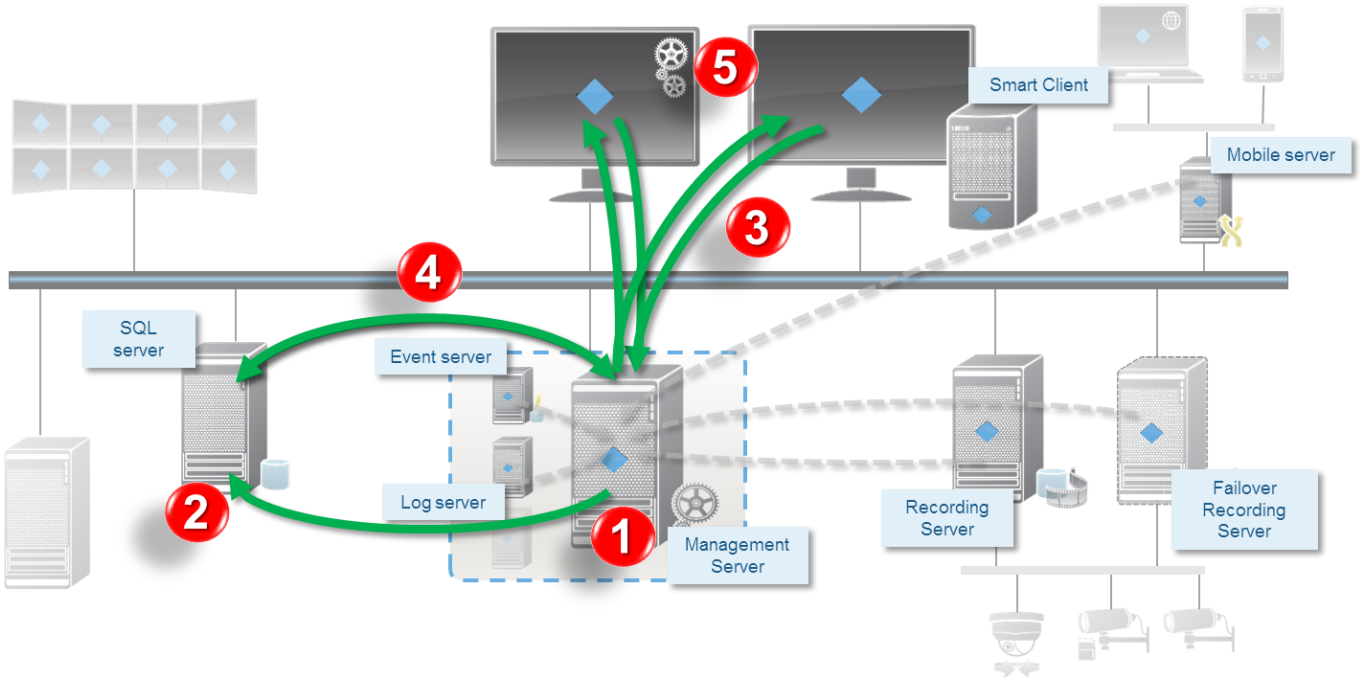
2) Configuration stored in SQL server
Port: 1433
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

3) Management Server contacts Service channel
Port: 80
Protocol: HTTP
Bandwidth: low, 1 Kbit/call

4) Service channel sends notification about view update to XProtect Smart Clients
Port: configurable - typically port 80 for AD user and 443 for basic user.
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call + constant low utilization

5) Smart Clients retrieve and apply the new view
Port: configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call

Data collector



1) System status received on Management Server
(Delivered by Log server, Event server, Recording Server, Failover Recording Server and Mobile server)
Port: 7609
Protocol: HTTP
Bandwidth: low, 10 Kbit/call

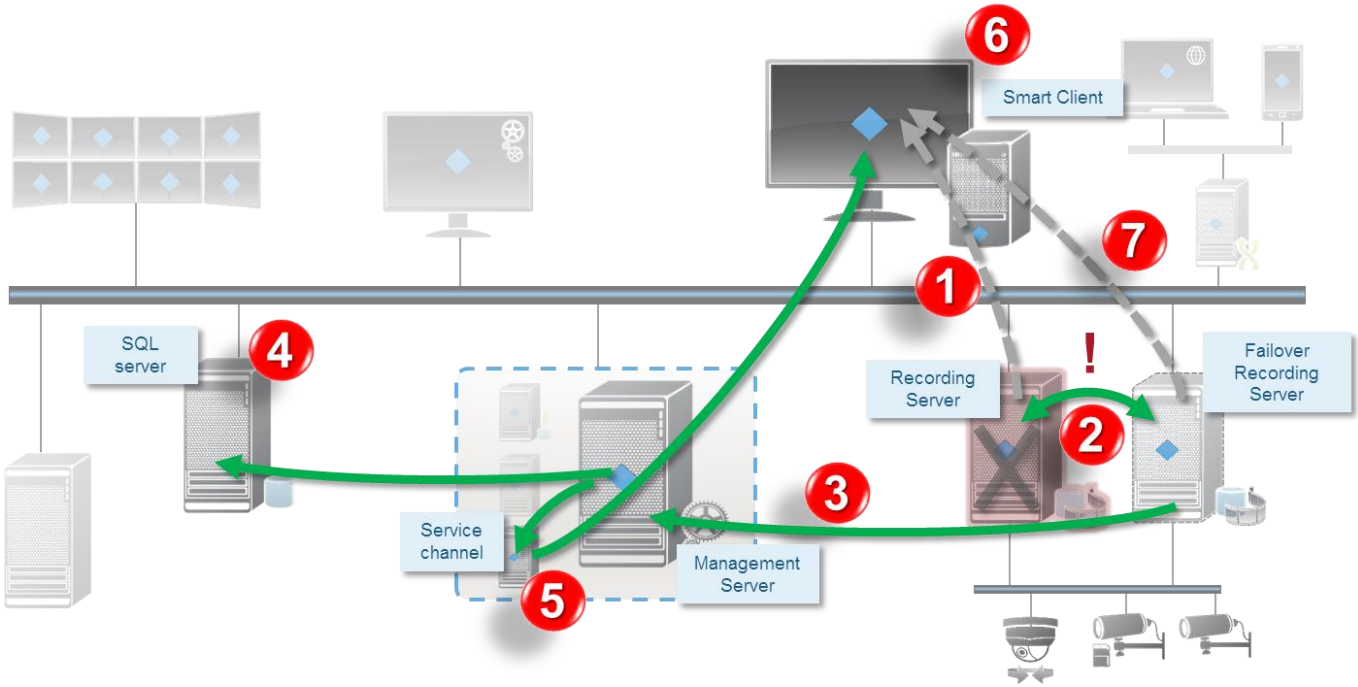
2) Collected data stored in SQL server
Port: 1433
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

3) System monitor in XProtect Smart Client or Management Client requests data
Port: 80
Protocol: HTTP
Bandwidth: low, 1 Kbit/call

4) Requested data collected from SQL server
Port: 1433
Protocol: TCP/IP
Bandwidth: Low, 100 Kbit/call

5) Data returned to clients
Port: 80
Protocol: HTTP
Bandwidth: Low, 100 Kbit/call

Recording Server failover



1) Video streamed from Recording Server (before failure)
Port: configurable - default port 7563
Protocol: configurable, TCP/IP, UDP Multicast – default TCP/IP
Bandwidth: usage dependable – calculation: add bandwidth per camera viewed to get the sum

2) 'Alive' messages exchanged between recording and failover recording server
Port: configurable - default port 11000
Protocol: configurable, TCP/IP
Bandwidth: low, 1 Kbit/call

3) Cold standby mode
Port: 80
Protocol: HTTP
Bandwidth: depends on size of configuration

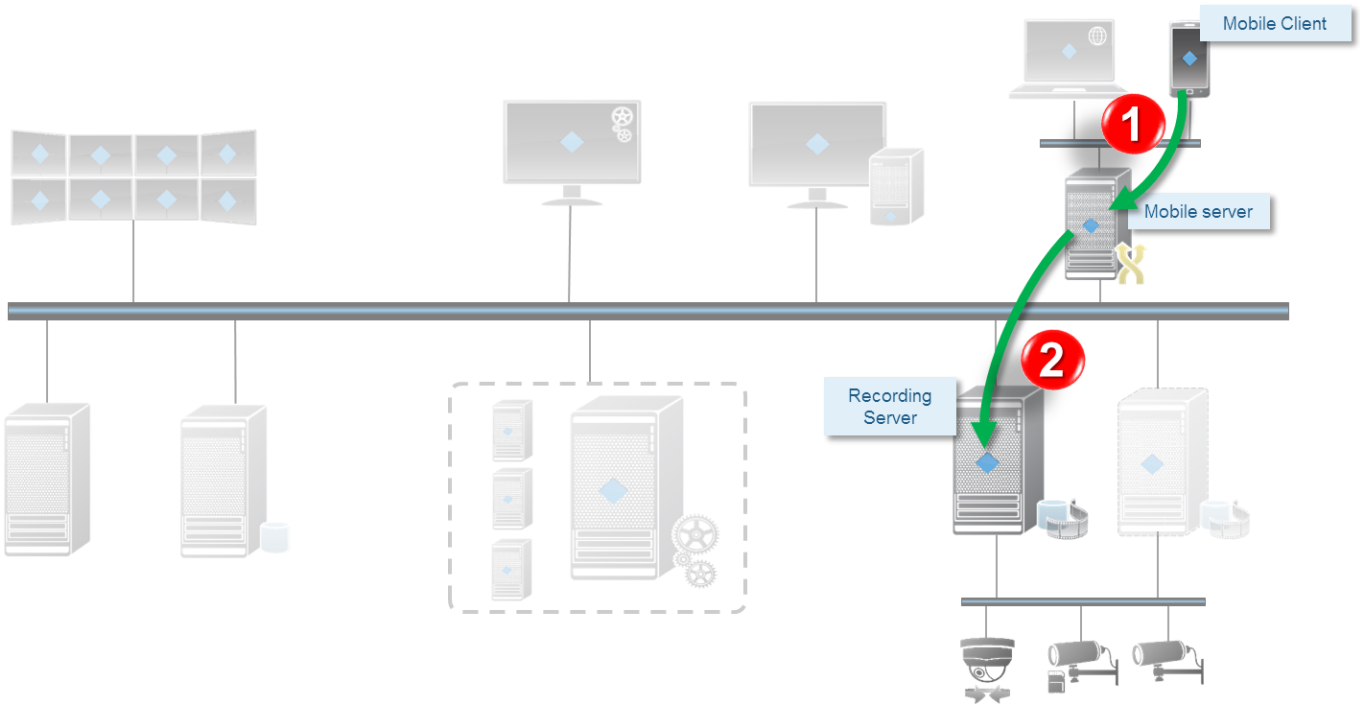
4) Configuration updated with active Failover Recording Server
Port: 1433
Protocol: TCP/IP
Bandwidth: low, 1 Kbit/call

5) Update configuration message sent to Service channel
Port: 80
Protocol: HTTP
Bandwidth: low, 1 Kbit/call

6) Update message distributed to all clients
Port: Configurable - typically port 80 for AD user and 443 for basic user
Protocol: HTTP for AD user and HTTPS for basic user
Bandwidth: low, 1 Kbit/call

7) Video streamed from Failover Recording Server
Port: configurable - default port 7563
Protocol: configurable, TCP/IP, UDP Multicast – default TCP/IP
Bandwidth: usage dependable – calculation: add bandwidth per camera viewed to get the sum

Video Push



1) Video Push stream sent instantly to Mobile server
Port: configurable - typically port 8081 for HTTP and 8082 for HTTPS
Protocol: HTTP or HTTPS
Bandwidth: usage dependable – depends on the resolution and frame-rate set up in the Mobile device. Typically 0.05 – 1 Mbit/s

2) Video Push stream is retrieved by Recording Server (Video Push driver)
Port: configurable – typically 40001 (40002, 40003, etc., if many devices are present)
Protocol: TCP/IP
Bandwidth: usage dependable – depends on the resolution and frame-rate set up in the Mobile device. Typically 0.05 – 1 Mbit/s