Milestone Systems

XProtect® VMS 2017 R3

System Architecture Document

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

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

The Milestone XProtect® VMS System Architecture Document contains illustrations and descriptions of communication and dataflow between the most common system components in a distributed installation of XProtect.

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's primary audience is system integrators and IT administrators with limited experience and knowledge about Milestone XProtect VMS solutions and who are in the process of selecting, deploying, administrating, maintaining and expanding a VMS.

The purpose of the document is to provide insight to the benefits and simplicity of using Milestone XProtect as a VMS, including an introduction of the system components and the system architecture.

This document should enable the reader to understand:

- The overall system architecture
- The primary system components and their functions
- Provide guidelines to basic system design

The reader of the document should have general experience with administrating an IT installation.

Overall system architecture

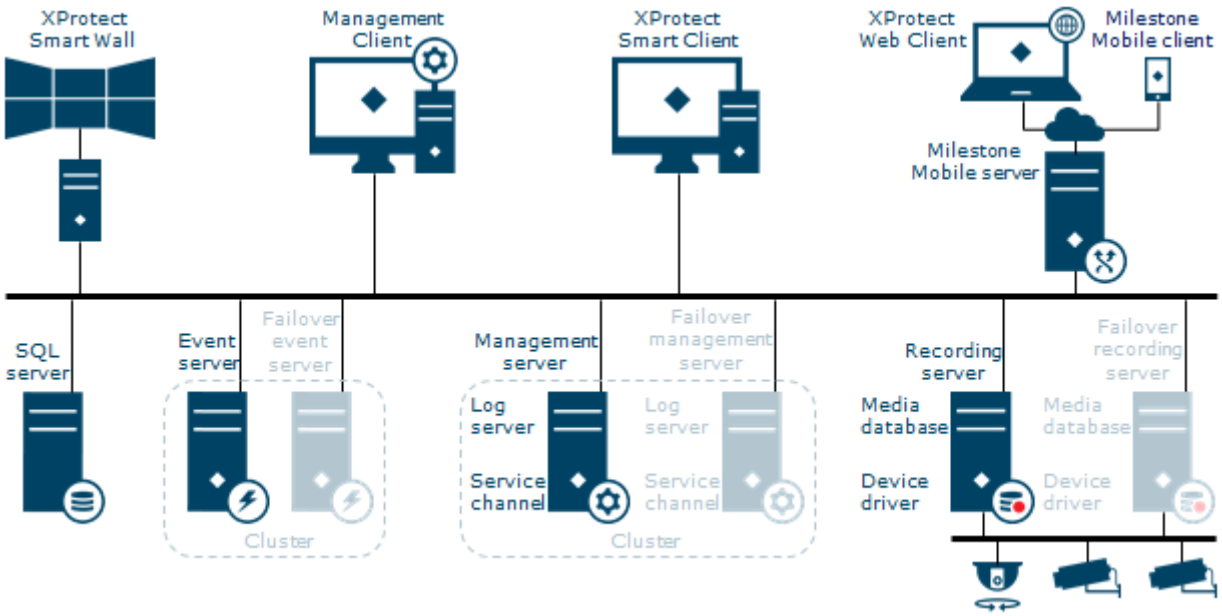
To enable scaling of thousands of cameras across multiple sites, the system consists of several components that handle specific tasks. You can install all components on a single server if the server can handle the load, or you can install the components on separate, dedicated servers to scale and distribute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

Depending on hardware and configuration, smaller systems with between 50~100 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.

You do not need all components in all installations. However, you can add them if the functionality they offer is needed at a later time, for example, failover recording servers or Mobile servers for hosting and providing access to both XProtect Web Client and Milestone Mobile.

The diagram below shows an overview of the system components.



Note:

- XProtect Smart Wall is an add-on product for XProtect Expert.

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 various 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, see (http://www.milestonesys.com/Software/XProtect-Clients/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 (http://www.milestonesys.com/Software/XProtect-Clients/XProtect-Web-Client/)

Find compatible browsers under XProtect Web Client here: (http://www.milestonesys.com/SystemRequirements)

Milestone Mobile client

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

You can use the Milestone 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 is a standard camera.

For more information, see (http://www.milestonesys.com/Software/XProtect-Clients/XProtect-Mobile/)

Find the operating systems compatible with Milestone Mobile here: (http://www.milestonesys.com/SystemRequirements)

Additional products and components

Note: Available functionality depends on the system you are using. See the Product comparison chart (https://www.milestonesys.com/solutions/platform/product-index/) for more information.

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.

MIP

The open platform is integrated in the following Milestone XProtect system components and applications:

- XProtect Smart Client
- XProtect Management Client
- XProtect Management Application
- Management Server
- Event Server

MIP SDK

To have a truly open platform and a community around it Milestone provides the SDK that contains:

- The tools for developing integrations.
- Documentation of a set of interfaces.
- A set of wrapper .NET DLLs providing an easy interface to a variety of functionality.
- A large collection of samples demonstrating different ways of using the MIP SDK.
- Short descriptions and how-to guides.
- A small application to display links to this information.
- Libraries.

The MIP SDK is also used internally by Milestone software development teams.

For more information, see (http://www.milestonesys.com/mipsdk/)

Software Manager

The Software Manager is a tool that you, from a central point, can use 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 remotely upgrade the components that are installed on servers and client PCs.

For more information, see (https://www.milestonesys.com/xprotectutilities)

XProtect Smart Wall

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

There are several ways you can select the cameras:

- Manually using the XProtect Smart Client.
- Via the VMS' rule system on events and/or time schedule.
- Via MIP SDK integrations.

XProtect 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 running XProtect Smart Client to show the Smart Wall views.

Note: XProtect Smart Wall 2017 is included in XProtect Corporate 2017. You can be purchase it as an add-on for XProtect Expert 2017.

For more information, see (https://www.milestonesys.com/our-products/xprotect-addons/xprotect-smart-wall/)

XProtect Access

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.

Note: 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. You must install this plug-in on the event server before you can start an integration.

For more information, see (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/access/)

XProtect Transact

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

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).

For more information, see (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/transact/)

XProtect LPR

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

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

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

Examples of events in XProtect LPR:

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

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

For more information, see (https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/lpr/)

Milestone Interconnect

Milestone Interconnect allows you to integrate several XProtect or Milestone Husky™ installations with one XProtect Corporate central site. You can also install these 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 central site considers the remote site as an advanced camera or multi-channel encoder with edge storage capabilities.

Each remote site runs independently and can perform surveillance tasks as configured. Depending on the network connections and appropriate user rights, Milestone Interconnect offers you direct live viewing of remote site cameras and play back of remote site recordings on the central site.

It also offers you the possibility to transfer remote site recordings to the central site based on either system-defined events, rules, schedules or by manual requests from XProtect Smart Client users.

The central site can only see and access devices that the user account specified on the remote site has access to. This allows local system administrators on the remote sites to control which devices should be made available to the central site and its users.

On the central site, you can view the status for the interconnected cameras, but not the entire status of the remote site. Instead, to monitor the remote site, you can use remote site events to trigger alarms or other notifications on the central site.

Only XProtect Corporate systems can work as central sites. All other products can act as remote sites including XProtect Corporate. How specific the products interact in a Milestone Interconnect setup depends on the version of the XProtect or Milestone Husky installations, the number of cameras and how devices and events are configured on the remote site. For further details, go to the Milestone Interconnect website (http://www.milestonesys.com/our-products/milestone-interconnect/).

Note: It is not possible to add systems with free XProtect installation as remote sites.

Milestone DLNA Server

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. Milestone 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.

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

Milestone 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 Milestone DLNA Server.

Milestone ONVIF Bridge

The ONVIF standard facilitates full video interoperability in multivendor installations and ensures information exchange by defining a common protocol. The protocol contains ONVIF profiles, which are collections of specifications for interoperability between ONVIF compliant devices.

Milestone ONVIF Bridge is compliant with the parts of ONVIF Profile G and Profile S that provide access to live and recorded video, and the ability to control pan-tilt-zoom cameras:

- Profile G - Provides support for video recording, storage, search, and retrieval. For more information, see ONVIF Profile G Specification (https://www.onvif.org/profiles/profile-g/).
- Profile S - Provides support for streaming live video using the H.264 codec, audio streaming, and pan-tilt-zoom (PTZ) controls. For more information, see ONVIF Profile S Specification (https://www.onvif.org/profiles/profile-s/).

For more information about the ONVIF standard, see the ONVIF® website (http://www.onvif.org/).

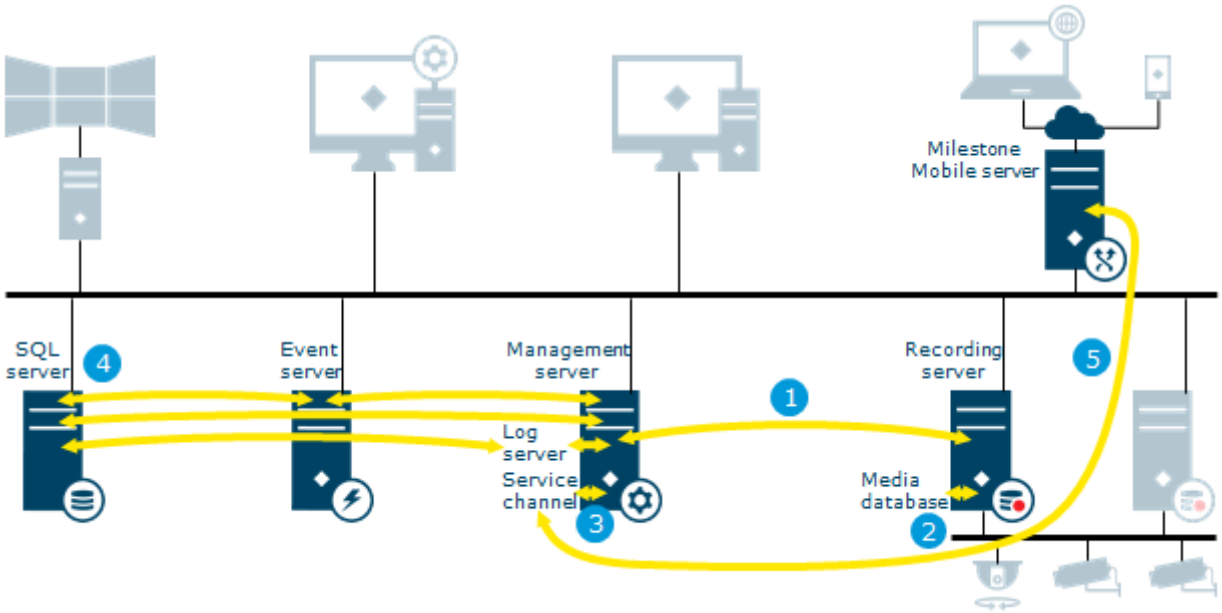
ONVIF Profiles support "get" functions that retrieve data, and "set" functions that configure settings. Each function is either mandatory, conditional, or optional. For security reasons, Milestone ONVIF Bridge supports only the mandatory, conditional, and optional "get" functions that do the following:

- Request video
- Authenticate users
- Stream video
- Play recorded video

For more information, see (https://www.milestonesys.com/community/developer-tools/milestone-ecosystem/)

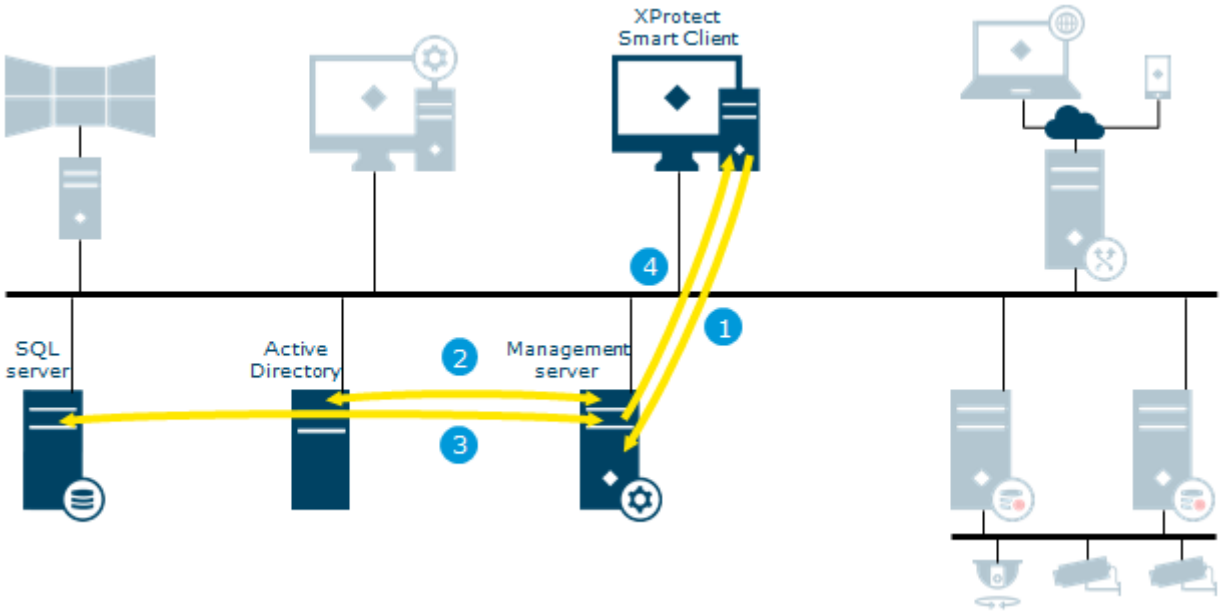
System communication and data flow

Server communication



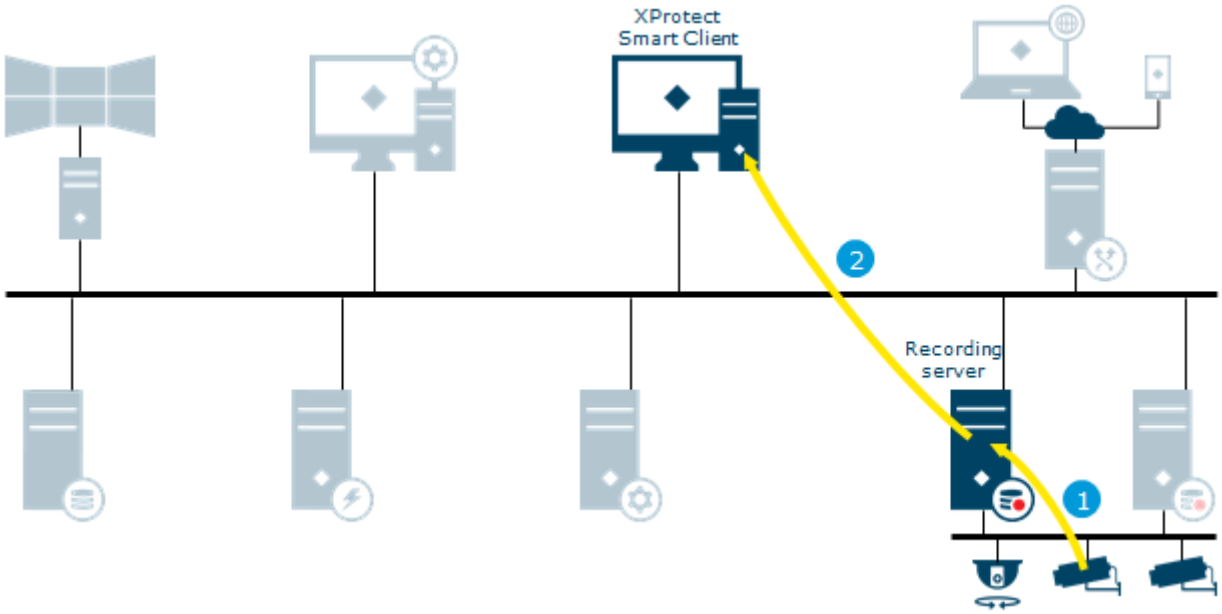
	Component	Port	Protocol	Bandwidth
1	Management server - Recording server	9993	TCP	1 kbit/call
2	Recording server - Media database	-	-	-
3	Management server - Internal	8080	UDP	1 kbit/call
4	SQL database communication	1433	TCP	1 kbit/call
5	Service channel - Mobile server	80	HTTP	1 kbit/call

Login from XProtect Smart Client



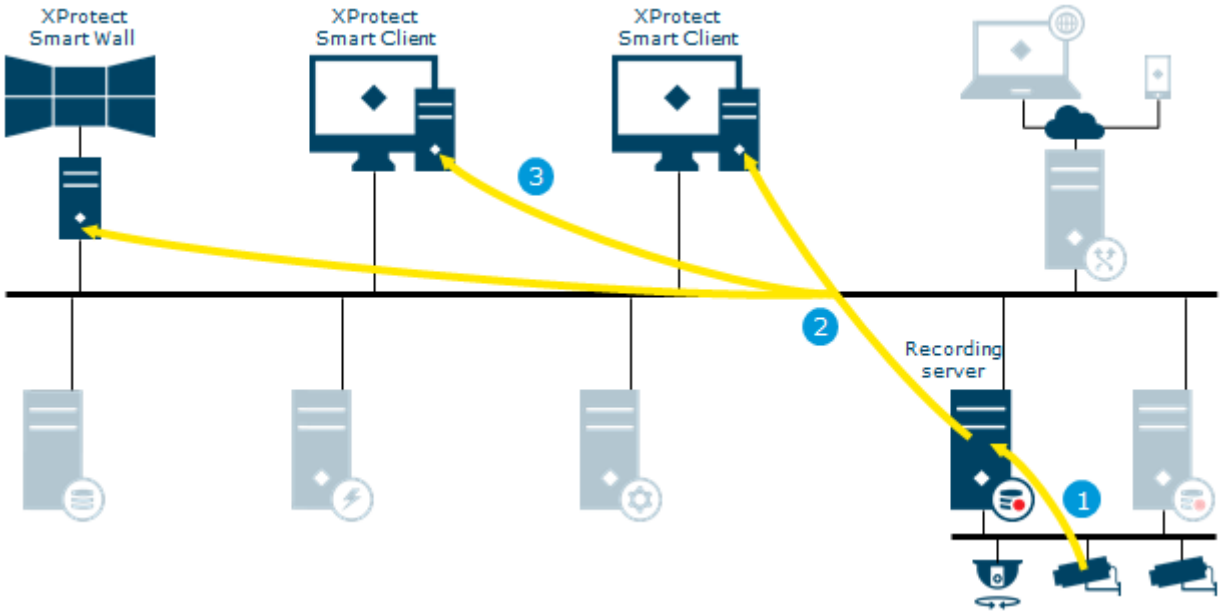
	Process	Port	Protocol	Bandwidth
1	XProtect Smart Client connects to the Management Server and attempts to log in	Configurable. Typically port 80 for an AD user and port 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
2	The management server contacts Active Directory to authenticate the user	OS- and AD-dependent	OS- and AD-dependent	Low 5 kbit/call
3	User-specific configuration is retrieved from the SQL database	1433	TCP	Depends on configuration
4	Login is granted and the configuration is sent to XProtect Smart Client	Configurable. Typically port 80 for an AD user and port 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Depends on configuration, Typically 1-10 MByte

Live video and audio



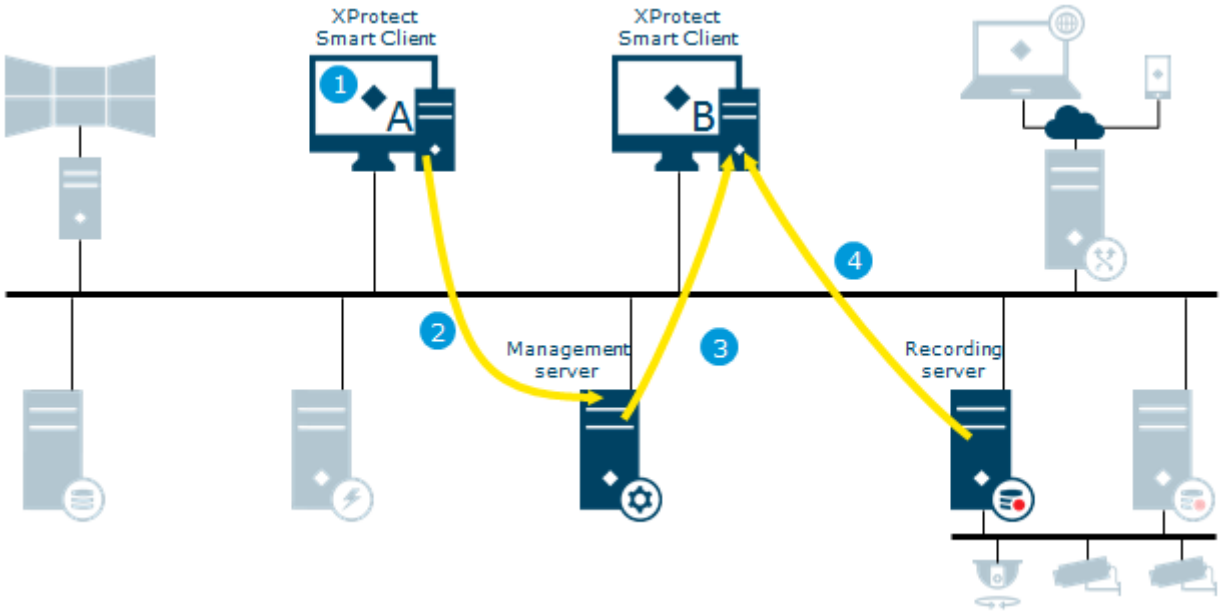
	Process	Port	Protocol	Bandwidth
1	Live streams from cameras retrieved by the recording server	Configurable. Typically port 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	Streams are sent to XProtect Smart Client on request	Configurable. The default port is 7563	Configurable, TCP/IP, UDP Multicast. The default is TCP/IP	Usage dependable, sum of camera streams viewed

Live video multicasting



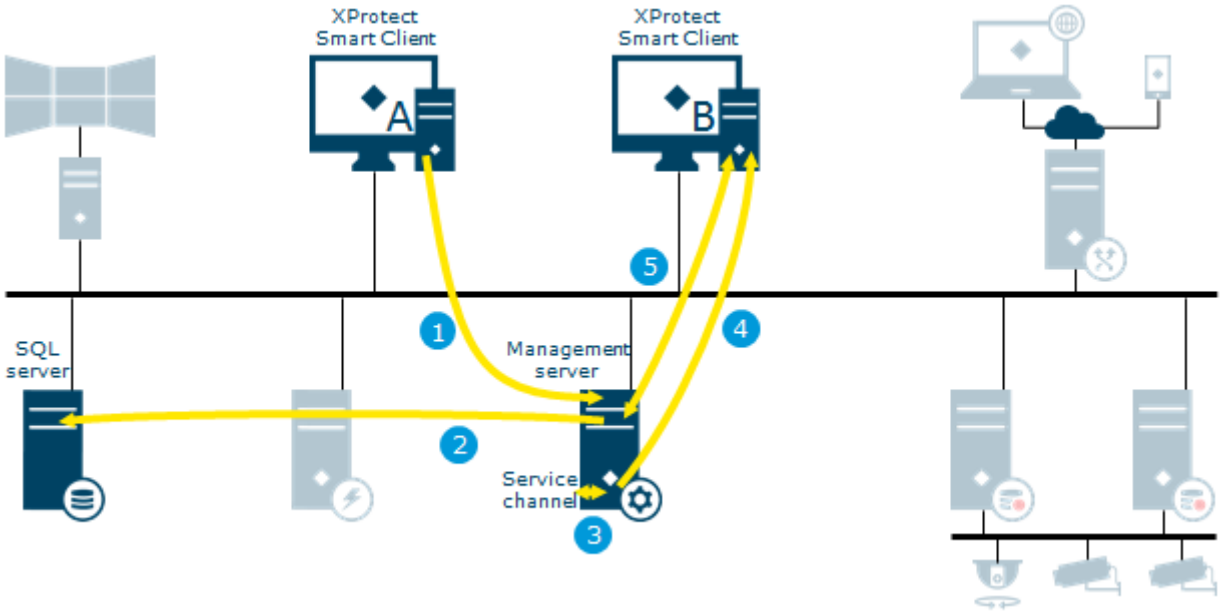
	Process	Port	Protocol	Bandwidth
1	Live streams from cameras retrieved by the recording server	Configurable. Typically port 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	Recording server sends multicast stream to the multicast enabled network. This requires that all switches handling the data traffic between the Smart Client and the recording server must be configured for multicast	Configurable. The default port range is 6000-7000	UDP IGMP Multicast	Usage dependable, sum of camera streams viewed
3	The multicast stream is received by all XProtect Smart Clients on request	Configurable. The default port range is 6000-7000	UDP IGMP Multicast	Usage dependable, sum of camera streams viewed

Matrix



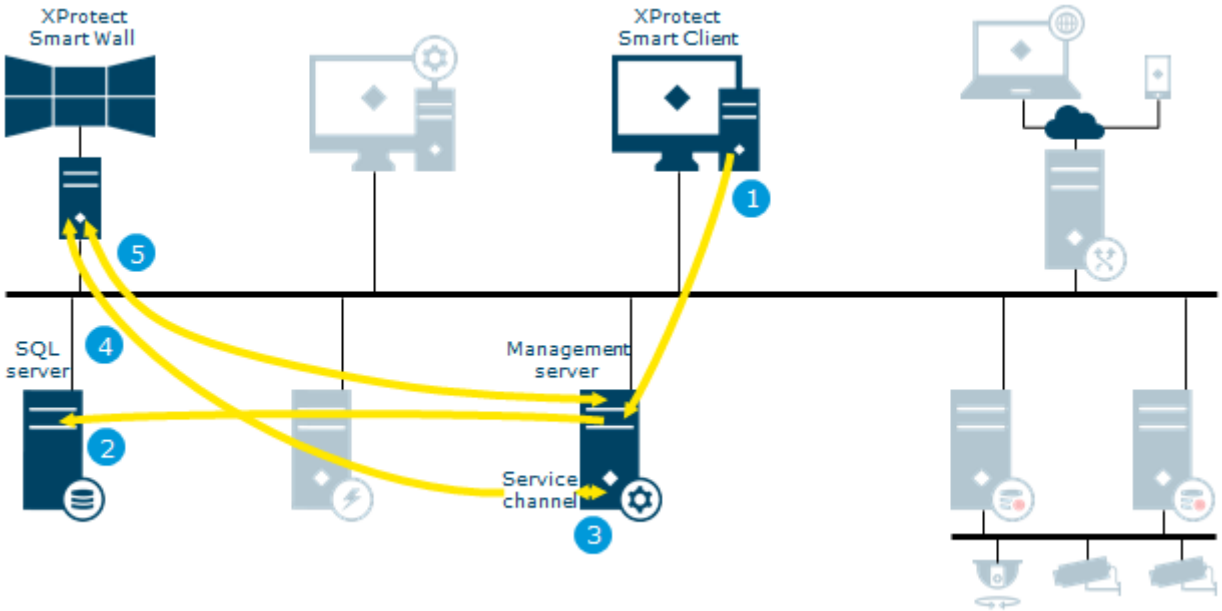
	Process	Port	Protocol	Bandwidth
1	XProtect Smart Client user selects to send a camera to a Matrix-recipient	N/A	N/A	N/A
2	Information sent to Management server	Configurable. Typically port 80 for an AD user and port 443 a for basic user	HTTP for AD user and HTTPS for basic user	Low 1 kbit/call
3	Management server sends request to Matrix-recipient on specified IP address and port (Smart Client B)	Configurable. The default port is 12345	TCP/IP	Low 1 kbit/call
4	Streams are sent to XProtect Smart Client from recording server on request	Configurable. The default port is 7563	Configurable, TCP/IP, UDP Multicast. The default is TCP/IP	Usage dependable, sum of camera streams viewed

Service channel – view update



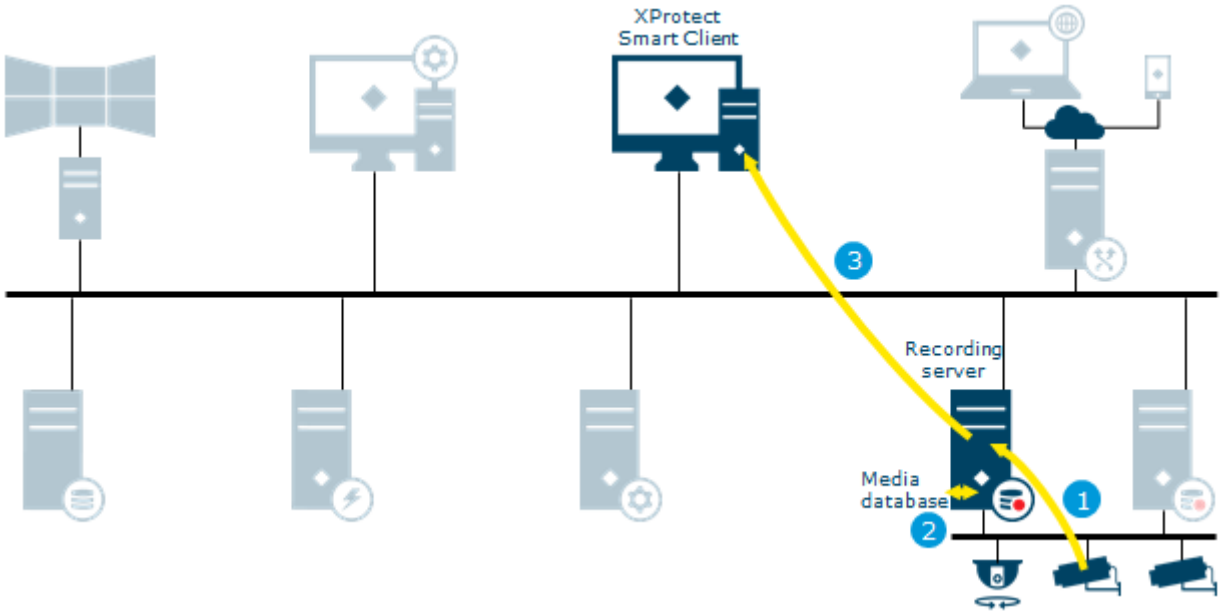
	Process	Port	Protocol	Bandwidth
1	View updated on XProtect Smart Client A	Configurable. Typically port 80 for an AD user and port 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
2	The configuration is stored in the SQL server	1433	TCP	Low 1 kbit/call
3	The management server contacts the service channel with update information	80	HTTP	Low 1 kbit/call
4	The service channel sends notification about view update to XProtect Smart Clients	Configurable. Typically port 80 for an AD user and port 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call + constant low use
5	XProtect Smart Clients retrieves and applies the new view	Configurable. Typically port 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call

XProtect Smart Wall



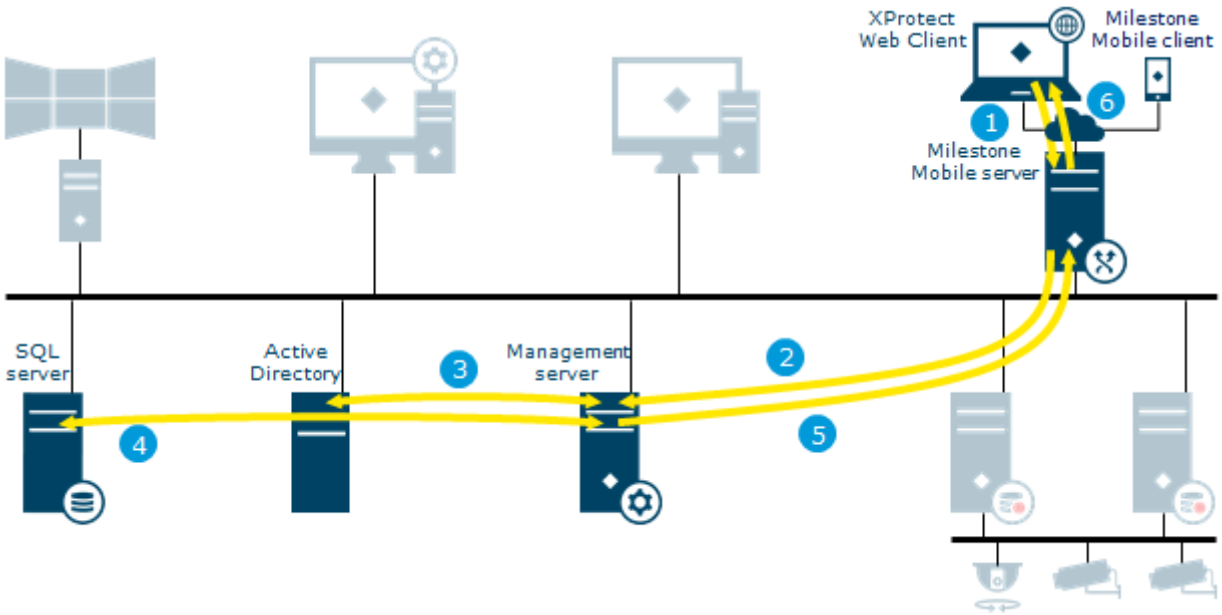
	Process	Port	Protocol	Bandwidth
1	An XProtect Smart Client user updates the XProtect Smart Wall view	Configurable. The default is 5432	TCP/IP	Low 1 kbit/call
2	The XProtect Smart Wall view configuration is updated and stored in the SQL server	1433	TCP	Low 1 kbit/call
3	Management server contacts the service channel	80	HTTP	Low 1 kbit/call
4	The service channel sends a notification to the XProtect Smart Client running the XProtect Smart Wall	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
5	The XProtect Smart Client running the XProtect Smart Wall retrieves and applies new layout	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call

Play back video and audio



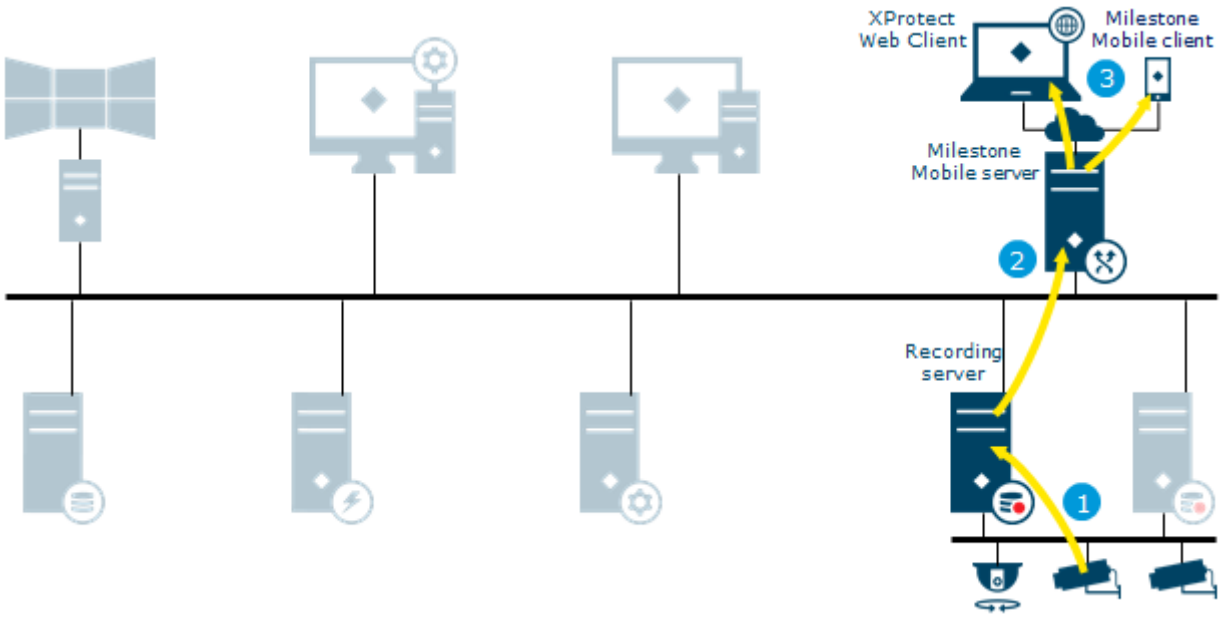
	Process	Port	Protocol	Bandwidth
1	Recording stream from cameras retrieved by the recording server	Configurable. Typically port 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	The stream is recorded in the recording server database based on rules	N/A	N/A	Device configurable. Typically 1-10 Mbit/s
3	The recorded stream is retrieved by XProtect Smart Client on playback request	Configurable. The default port is 7563	TCP/IP	Usage dependable, sum of camera streams viewed

Login from XProtect Web Client and Milestone Mobile



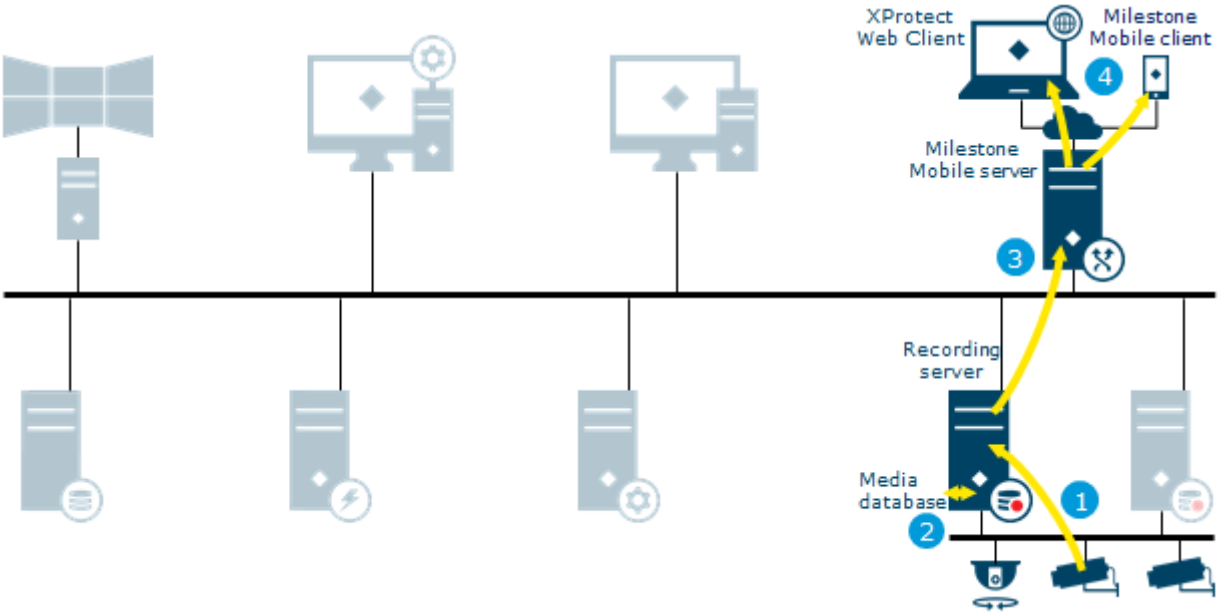
	Process	Port	Protocol	Bandwidth
1	Login request from XProtect Web Client or Milestone Mobile received on the mobile server	Configurable. Typically 8081 for HTTP and 8082 for HTTPS	HTTP or HTTPS	Low 1kbit/call
2	The mobile server forwards request to the management server	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1kbit/call
3	The management server contacts Active Directory to authenticate the user	OS- and AD-dependent	OS- and AD-dependent	Low 1kbit/call
4	User-specific configuration is retrieved from the SQL database	1433	TCP	Configuration dependent
5	Information returned to the mobile server	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD User and HTTPS for a basic user	Configuration dependent, typically 1-10 MByte
6	The login is granted and configuration is sent to XProtect Web Client or Milestone Mobile	Configurable. Typically 8081 for HTTP and 8082 for HTTPS	HTTP or HTTPS	Configuration dependent, typically < 100 kByte

Live video for XProtect Web Client and Milestone Mobile



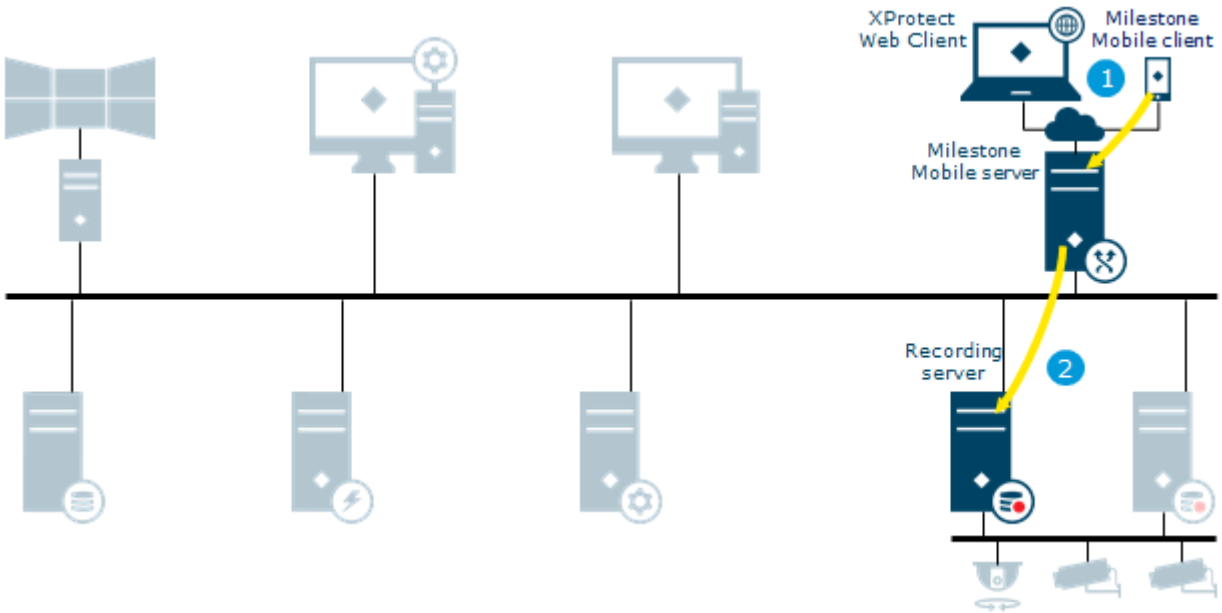
	Process	Port	Protocol	Bandwidth
1	Live stream(s) from cameras retrieved on the recording server	Configurable. Typically port 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	Streams are sent to the mobile server for transcoding or as direct streaming	Configurable. The default is 7563	Configurable, TCP/IP, UDP Multicast. The default is TCP/IP	Usage dependable, sum of camera streams viewed
3	Video is streamed to the clients	Configurable. Typically 8081 for HTTP and 8082 for HTTPS	HTTP or HTTPS	Transcoding: typically 50–200 kbit/s Native: device configurable. Typically 0.05-1 Mbit/s

Recording and playback video for XProtect Web Client and Milestone Mobile



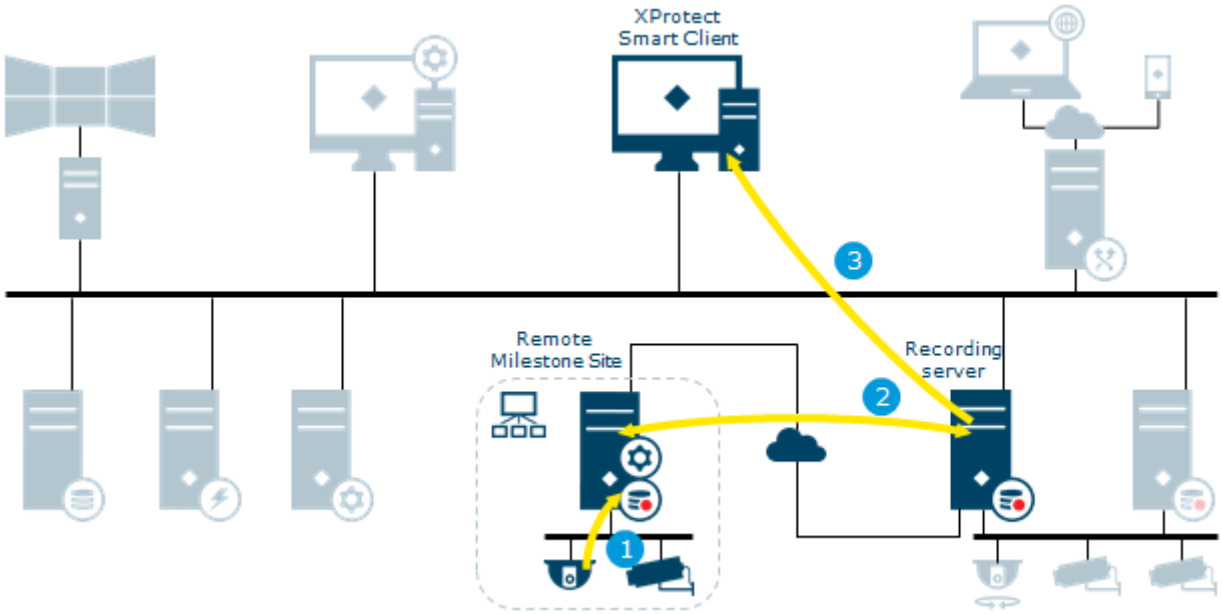
	Process	Port	Protocol	Bandwidth
1	Recording stream from cameras retrieved on the recording server	Configurable. Typically port 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	The stream is recorded in the recording server database based on rules	Configurable. The default is 7563	Configurable. TCP/IP, UDP Multicast. The default is TCP/IP.	Usage dependable, sum of camera streams viewed
3	Recordings are sent to the mobile server for transcoding or as direct streaming	Configurable. Typically 8081 for HTTP and 8082 for HTTPS	HTTP or HTTPS	Transcoding: typically 50–200 kbit/s Native: device configurable Typically 1-10 Mbit/s
4	Video is streamed to clients	-	-	-

Video push



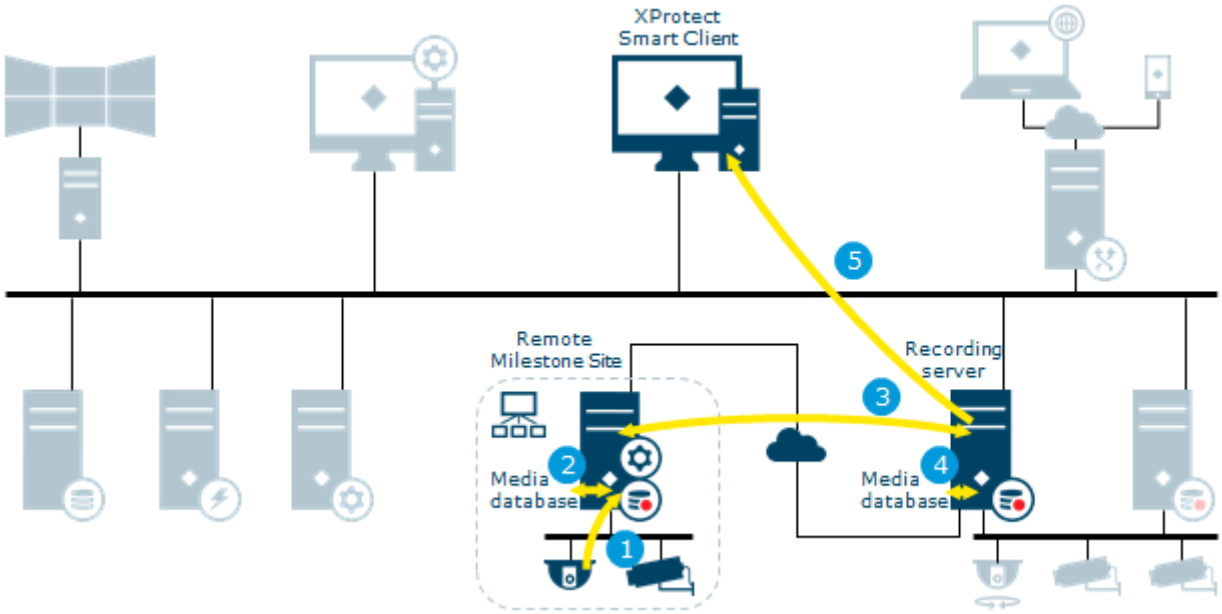
	Process	Port	Protocol	Bandwidth
1	Video push stream from a device running Milestone Mobile is sent instantly to the mobile server	Configurable. Typically port 8081 for HTTP and port 8082 for HTTPS	HTTP or HTTPS	Usage dependable, resolution and frame-rate set up in the mobile device. Typically 0.05 – 1 Mbit/s
2	The video push stream is retrieved by recording server using the specific video push device driver	Configurable. Typically port 40001 (40002, 40003, if many devices are present)	TCP/IP	Usage dependable, resolution and frame-rate set up in the mobile device. Typically 0.05 – 1 Mbit/s

Milestone Interconnect live



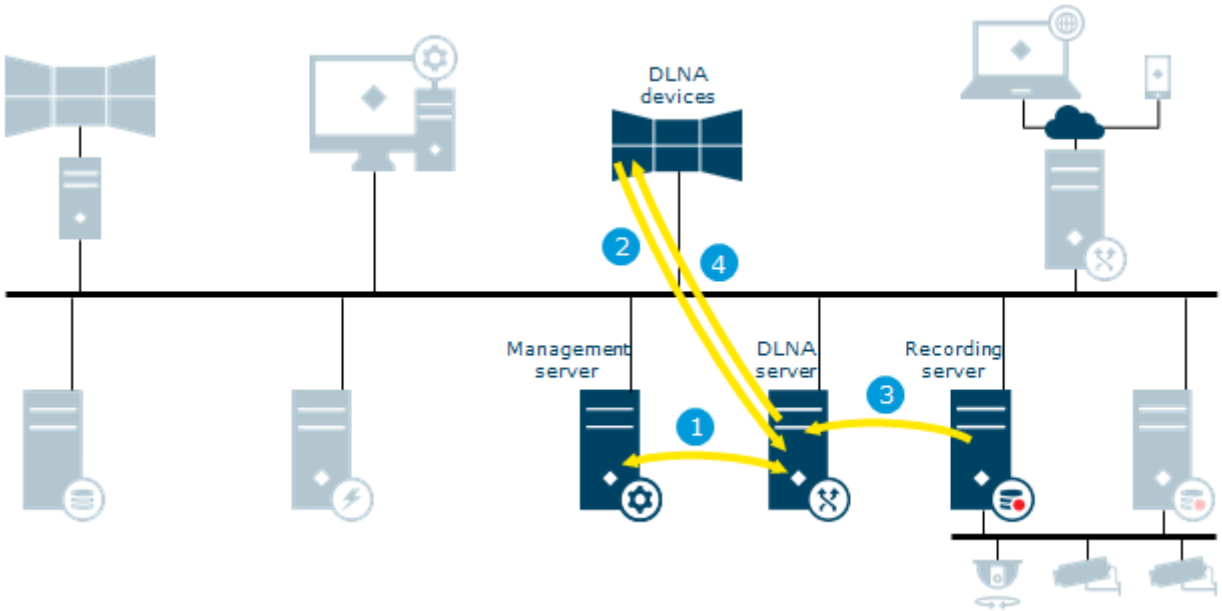
	Process	Port	Protocol	Bandwidth
	This illustrates how XProtect Smart Client users, specified for the interconnected system, only need to log into the management server on the central site to view video			
1	Live stream(s) from the remote site cameras retrieved by the remote site recording server	Configurable. Typically 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	Live streams from the remote site recording server retrieved by the central site recording server	Configurable. The default is 7563*	TCP/IP	Usage dependable, sum of camera streams viewed
	* In XProtect Professional VMS the default port is 80, events 2233, central 1237 must be open. The recording server on the central site connects to the remote site in the same way as a XProtect Smart Client			
3	Stream(s) are sent to XProtect Smart Client on request. XProtect Smart Client	Configurable. The default is 7563	Configurable, TCP/IP, UDP Multicast. The default is TCP/IP	Usage dependable, sum of camera streams viewed

Milestone Interconnect play back



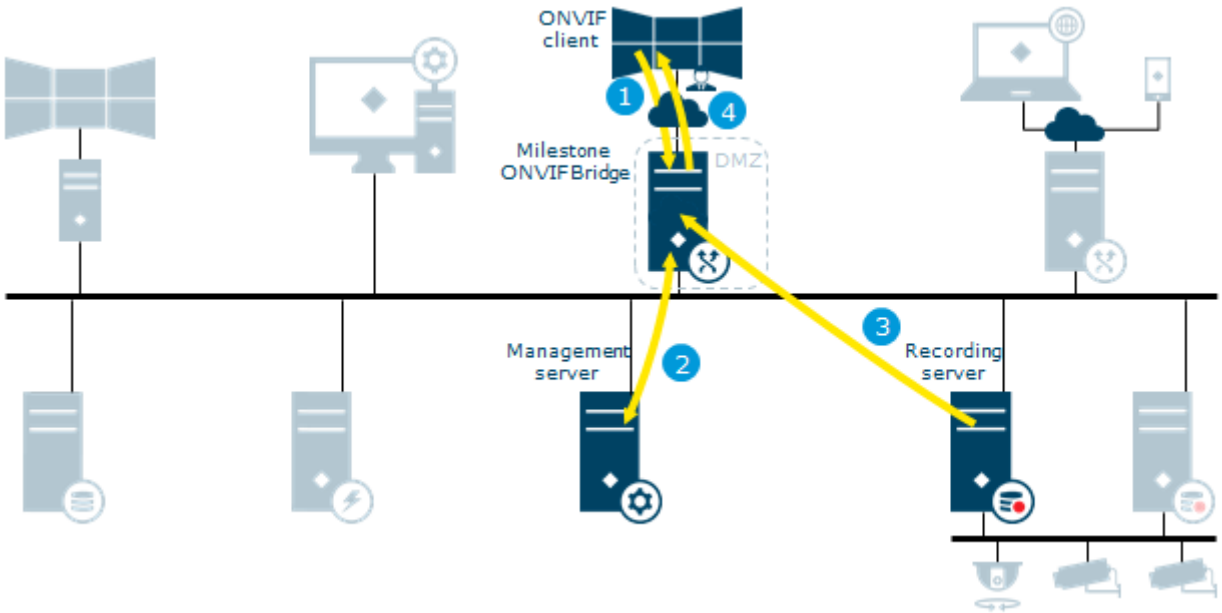
	Process	Port	Protocol	Bandwidth
	This illustrates when recording is done on both sites Recordings can be retrieved to the central site based on schedule, event or request XProtect Smart Client users, specified for the interconnected system, only need to log into the management server on the central site to view video			
1	Recording stream from the remote site cameras retrieved by the remote site recording server	Configurable. Typically 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	The stream is recorded in the remote site recording server database based on rules	N/A	N/A	-
3	Recording stream from the remote site recording server retrieved by the central site recording server	Configurable. The default is 7563*	TCP/IP	Sum of camera streams viewed
	* In XProtect Professional VMS the default port is 80, events 2233, central 1237 must be open. The recording server on the central site connects to the remote site in the same way as a XProtect Smart Client			
4	The stream is recorded in the central site recording server database based on rules.	N/A	N/A	-
	Recordings not available due to remote site link downtime can be retrieved automatically or based on schedule, event or request	-	-	Configurable by remote retrieval settings
5	The recorded stream(s) are retrieved by XProtect Smart Client on playback request	Configurable. The default is 7563	TCP/IP	Sum of camera streams viewed

Milestone DLNA Server



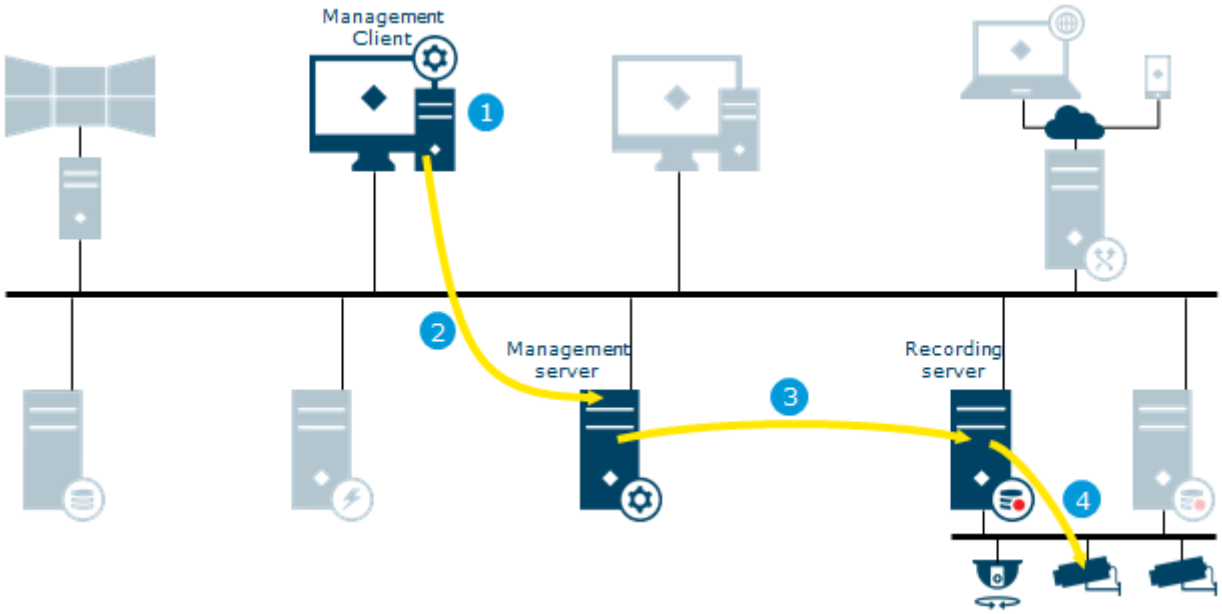
	Process	Port	Protocol	Bandwidth
1	The Milestone DLNA Server connects to the management server to authorize itself with the provided credentials	Configurable. Typically port 80 for an AD user and port 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
2	A DLNA device scans the network and connects to the XProtect system via the Milestone DLNA Server and requests a live camera video stream	Configurable. The default port is 9100	HTTP	Low 1 kbit/call
3	Milestone DLNA Server retrieves the requested camera video stream from the recording server	Configurable. The default port is 7563	TCP/IP	Usage dependable, sum of camera streams viewed
4	Milestone DLNA Server sends the live video stream from the requested camera to the DLNA device	Configurable. The default port is 9200	HTTP	Usage dependable, sum of camera streams viewed
	Only H.264 encoded camera streams are supported. If a camera supports multiple streams, only the default stream is sent. The system administrator manages the entire Milestone DLNA Server configuration from the Management Client. For example, selecting cameras available			

Milestone ONVIF Bridge



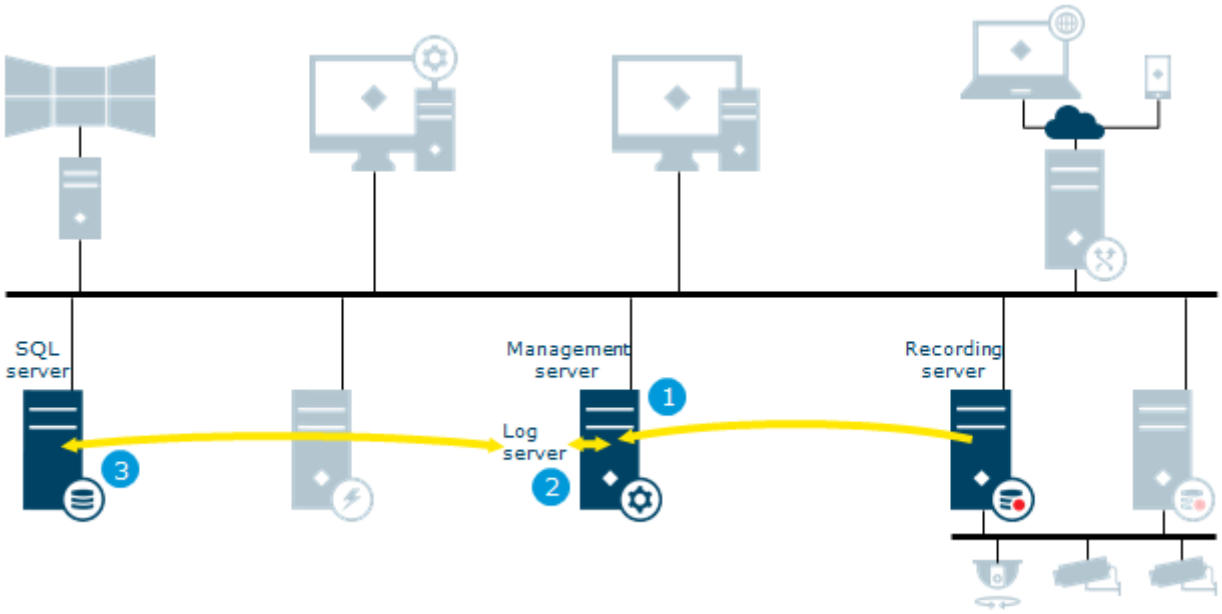
	Process	Port	Protocol	Bandwidth
1	Login, stream or PTZ request from ONVIF client received on the Milestone ONVIF Bridge server. The Milestone ONVIF Bridge is a gateway for non-Milestone clients to the Milestone VMS	Configurable. The default is 580	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
2	The Milestone ONVIF 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 ONVIF Bridge server	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
3	Requested live or playback stream from the recording server is retrieved by the Milestone ONVIF Bridge server	Configurable. The default port is 7563	TCP/IP	Usage dependable, sum of camera streams viewed
4	Video is streamed to the ONVIF client	Configurable. The default port is 554	RTSP	Usage dependable, sum of camera streams viewed

Management Client configuration update



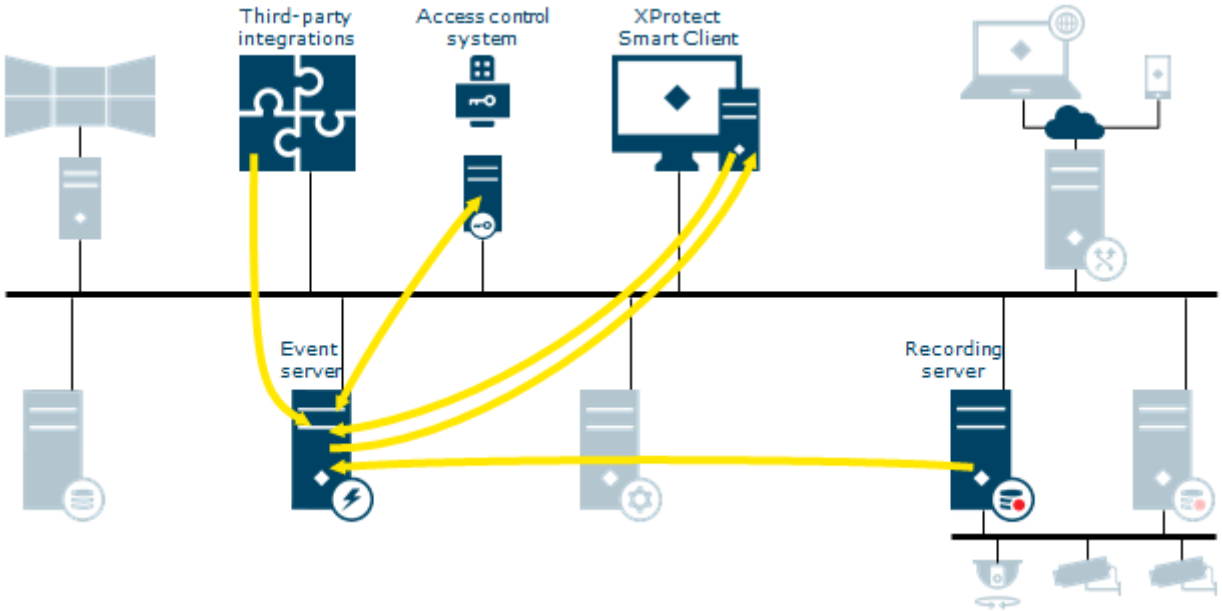
	Process	Port	Protocol	Bandwidth
1	Configuration updated on the Management Client	-	-	-
2	Changes are stored on the Management server	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 10 kbit/call
3	Configuration update sent to relevant components. In this case, the recording server	9993	TCP/IP	Low 1 kbit/call
4	If updates concern cameras, the recording server applies new settings	Configurable. Typically 80 for HTTP and 443 for HTTPS	HTTP or HTTPS	Low 1 kbit/call

Log server



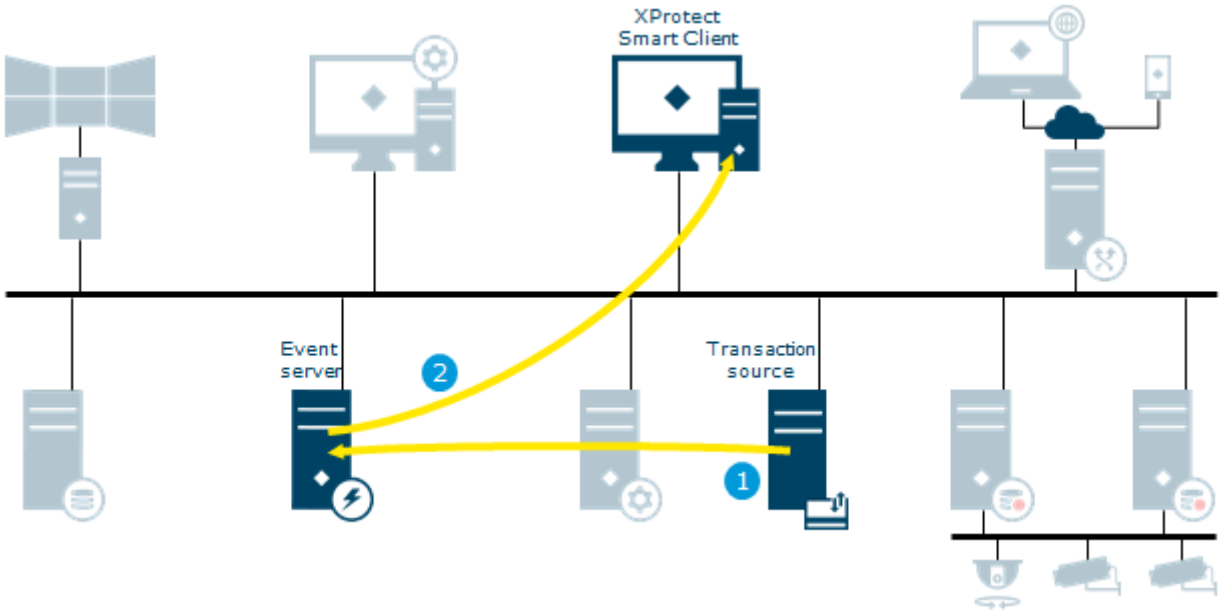
	Process	Port	Protocol	Bandwidth
1	The Management server or recording server creates a log message	9993	TCP	Low 1 kbit/call
2	The log message is forwarded to the log server	Configurable. The default is port 80	HTTP	Low 1 kbit/call
3	The log message is stored in the SQL server database	1433	TCP	Low 1 kbit/call

Event server



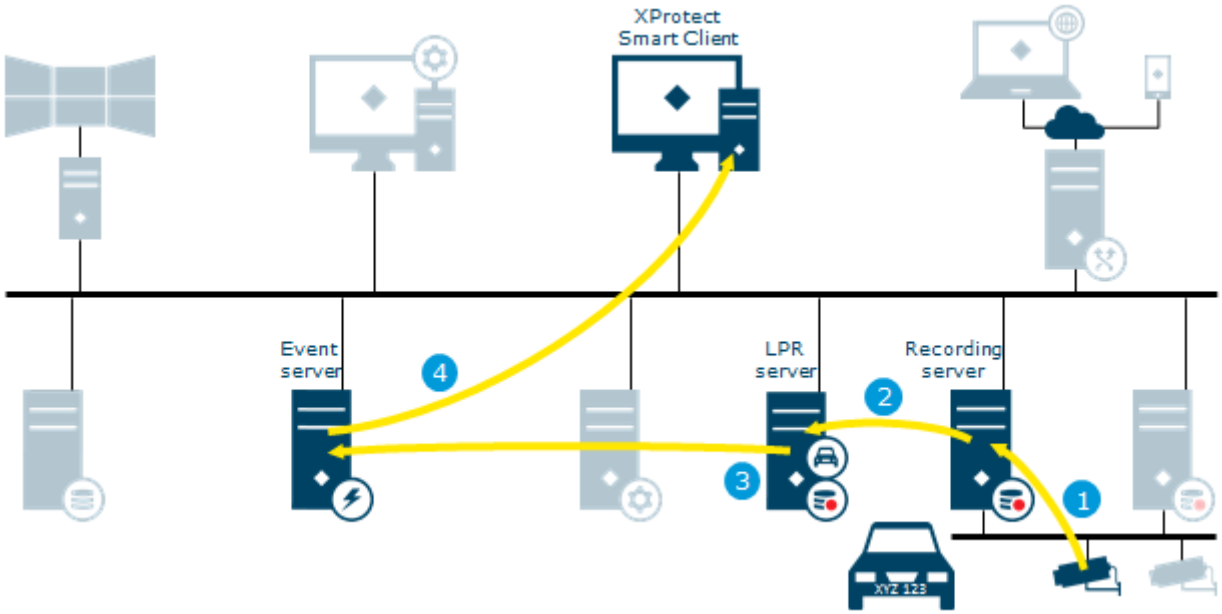
	Process	Port	Protocol	Bandwidth
	Data about alarms, access control or map updates are received by the event server	-	-	-
	Third-party integrations MIP message communication	22333	TCP/IP	Low 1 kbit/call
	Access control integrations	Depends on the integration	TCP/IP	Low 1 kbit/call
	XProtect Access. The event server Plug-in is a client to the access control system	Random or fixed. Paxton 8025	TCP/IP	Low 1 kbit/call
	Analytics events	Configurable. The default port is 9090	TCP/IP	Low 1 kbit/call
	Generic events	Configurable. The default ports are 1234 and 1235	TCP/IP, UDP	Low 1 kbit/call
	Recording server	7563	TCP	Low 1 kbit/call
	The event server sends data to XProtect Smart Client to show in alarm list, XProtect Access or the map overview. The XProtect Smart Client user responds to the notification and returns data to event server	-	-	-

XProtect Transact



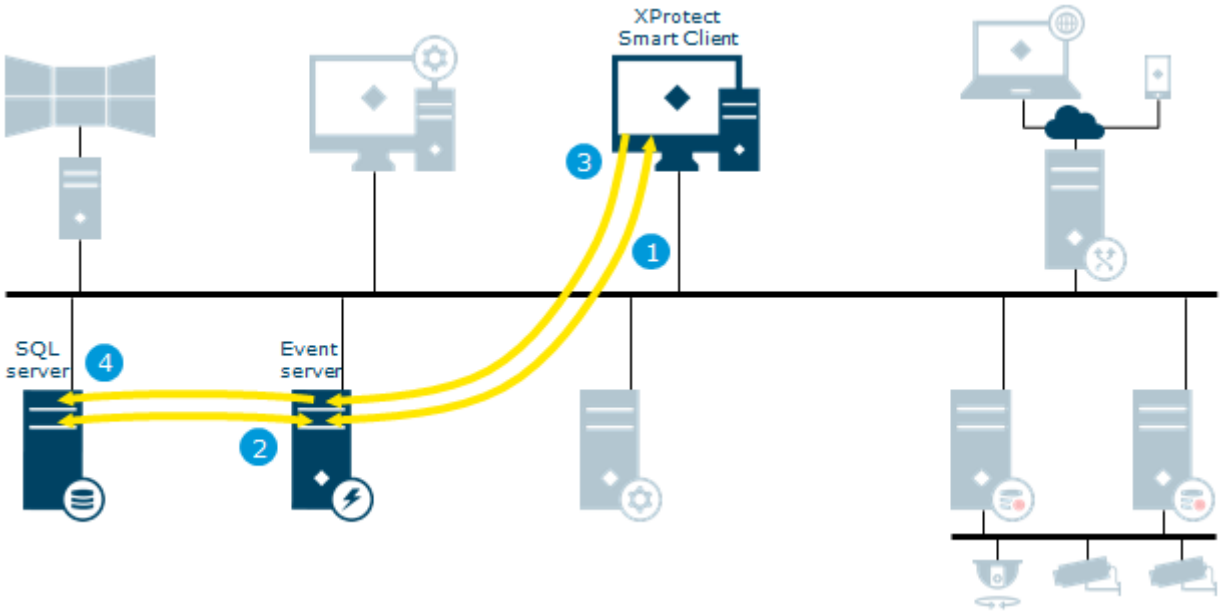
	Process	Port	Protocol	Bandwidth
1	Transaction data generated by the transaction source is sent to the event server and stored	Configurable. Typically 80	TCP/IP	Low 10 kbit/call
2	The event server sends transaction data to XProtect Smart Client and view items containing transaction data and the associated video is updated	Configurable. The default is 22331 22333	TCP/IP	Low 1 kbit/call
	The system administrator manages the entire XProtect Transact configuration from the Management Client. For example, setting up transaction sources, associated cameras, definitions and events	-	-	-

XProtect LPR



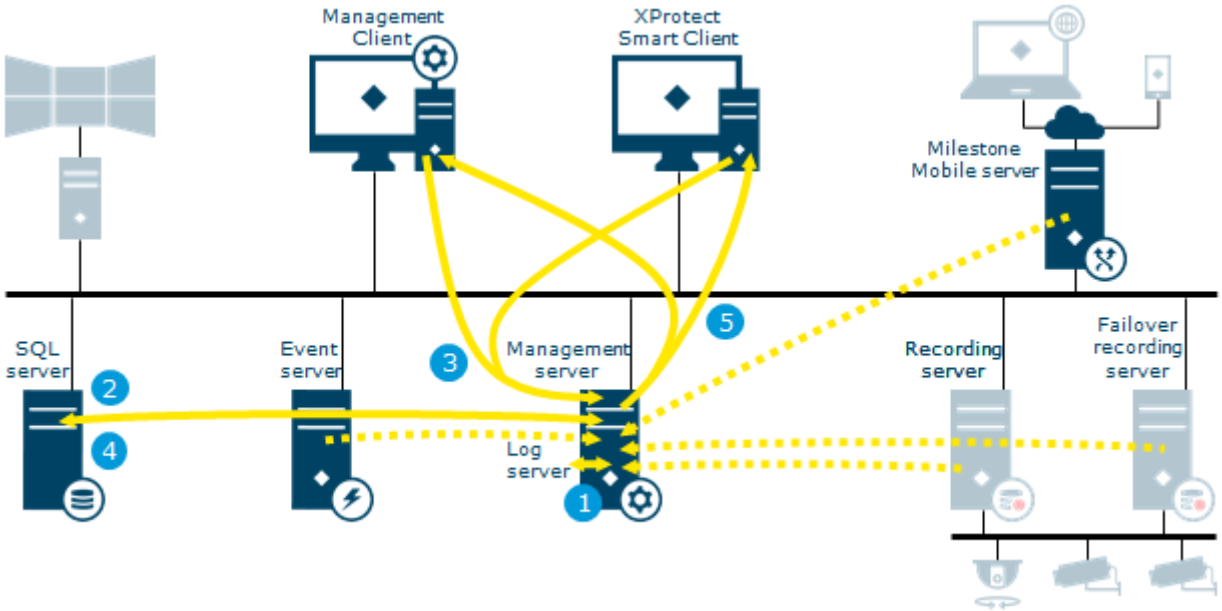
	Process	Port	Protocol	Bandwidth
1	Live streams from cameras configured for LPR (License Plate Recognition) retrieved by the recording server	Configurable. Typically 80	Configurable. Typically RTSP, UDP, TCP/IP	Device configurable. Typically 1-10 Mbit/s
2	Streams from the recording server retrieved by the LPR server	Configurable. The default is 7563	TCP/IP	Usage dependable, sum of camera streams viewed
3	The LPR server recognizes license plates by comparing them with the license plate characteristics of the installed country modules. Found license plates are compared with the license plate match list requests from the event server LPR plug-in	22334	TCP/IP	Low 1 kbit/call
4	The event server sends events and alarms to XProtect Smart Client when there is a match	Configurable. The default is 22331 22333	TCP/IP	Low 1 kbit/call
	The system administrator manages the entire XProtect LPR configuration, for example, setting up events, alarms, and match lists from the Management Client. To be able to configure XProtect LPR from the Management Client you must install the LPR plug-in on the Management Client computer	-	-	-

View and manage alarms



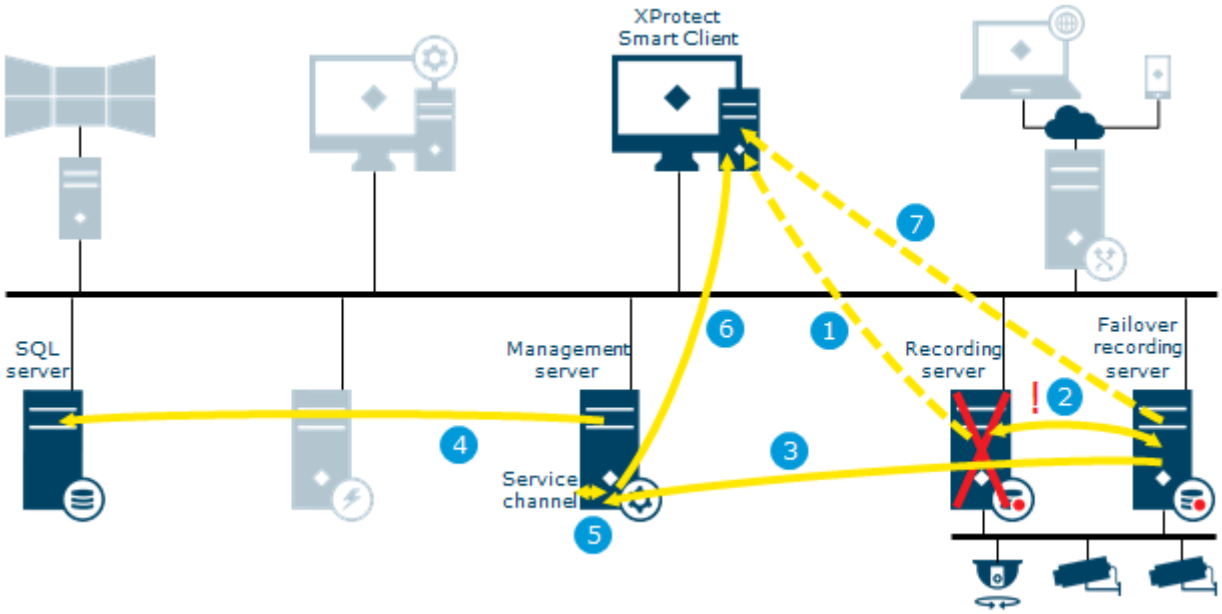
	Process	Port	Protocol	Bandwidth
1	XProtect Smart Client requests an alarm list from event server	Configurable. The default port is 22331	TCP/IP	Low 1 kbit/call
2	The alarm list is retrieved from the SQL server and returned to XProtect Smart Client	1433	TCP	Low 100 kbit/call
3	The alarm is handled and its state/details is updated by the user	-	-	-
4	New state/details stored on the SQL server	1433	TCP	Low 1 kbit/call

Data collector



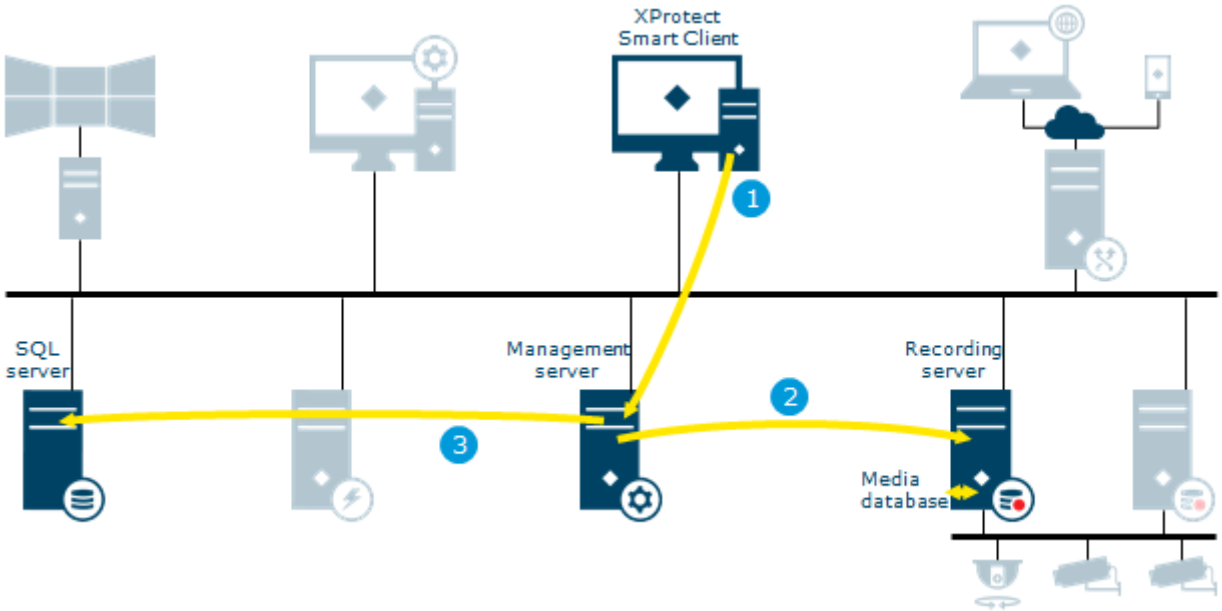
	Process	Port	Protocol	Bandwidth
1	System status received on management server delivered by: log server, event server, recording server, failover recording server and mobile server	7609	HTTP	Low 10 kbit/call
2	The collected data is stored on the SQL server	1433	TCP	Low 1 kbit/call
3	XProtect Smart Client or the Management Client requests status via System Monitor	80	HTTP	Low 1 kbit/call
4	Requested data is collected from the SQL server	1433	TCP	Low 100 kbit/call
5	Data returned to clients	80	HTTP	Low 100 kbit/call

Recording server failover



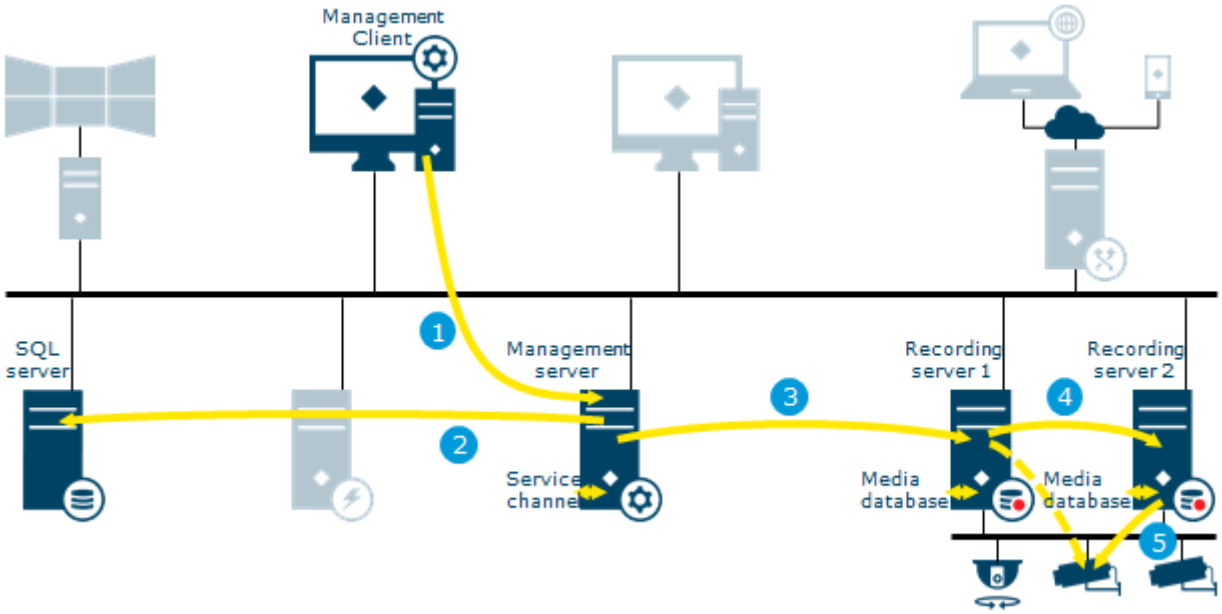
	Process	Port	Protocol	Bandwidth
1	Video streamed from the recording server	Configurable. The default port is 7563	Configurable. TCP/IP, UDP Multicast. Default TCP/IP	Sum of camera streams viewed
2	Alive messages exchanged between recording and failover recording server	Configurable. Default is 11000	Configurable, TCP/IP	Low 1 kbit/call
3	Cold standby: failover message sent, configuration retrieved, start failover Hot standby: failover message sent, start failover	80	HTTP	Configuration dependent
4	Configuration updated with active failover recording server	1433	TCP	Low 1 kbit/call
5	Update configuration message sent to service channel	80	HTTP	Low 1 kbit/call
6	Update message distributed to all clients	Configurable. Typically 80 for an AD user and 443 for a basic user	HTTP for an AD user and HTTPS for a basic user	Low 1 kbit/call
7	Video streamed from failover recording server	Configurable. The default port is 7563	Configurable. TCP/IP, UDP Multicast. Default TCP/IP	Sum of camera streams viewed
	Media retrieved from failover recording server when recording server is available	5210	TCP	-

Evidence lock



	Process	Port	Protocol	Bandwidth
1	The user creates an evidence lock in XProtect Smart Client. The information sent to the Management server	Configurable. Typically port 80 for an AD user and port 443 for a basic user	HTTP for AD User and HTTPS for a basic user	Low 1kbit/call
2	The Management server informs recording server to store and protect the locked recordings in the Media database	9993	TCP	Low 1kbit/call
3	Management server stores information about the evidence lock in the SQL server	1433	TCP	Low 1kbit/call

Move hardware



	Process	Port	Protocol	Bandwidth
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 configuration and stores it in the SQL server database	1433	TCP	Low 1kbit/call
3	The Management server sends update to Recording server 1	9993	TCP	Low 1kbit/call
4	The Management server sends update to Recording server 2	9993	TCP	Low 1kbit/call
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	5210	TCP	-
	The management server contacts service the channel with update information	80	HTTP	Low 1 kbit/call
	Clients connect to Recording server 2	-	-	-

Ports used by the system

All XProtect components and the ports needed by them are listed in individual sections 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 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 which need to be opened for a particular service. In order to figure out which ports need to be opened on a particular computer, you need to consider all services running on this computer.

Management Server service and related processes

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	All XProtect components	Main communication, for example, authentication and configurations.
443	HTTPS	IIS	XProtect Smart Client and the Management Client	Authentication of basic users.
6473	TCP	Management Server service	Management Server tray controller, local connection only.	Showing status and managing the service.
7475	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.

Port number	Protocol	Process	Connections from...	Purpose
8080	TCP	Management server	Local connection only.	Communication between internal processes on the server.
9993	TCP	Management Server service	Recording Server services	Authentication, configuration, token exchange.
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.

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 per 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.

Port number	Protocol	Process	Connections from...	Purpose
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. In XProtect 2014 systems or older, the port number was 6474.
7563	TCP	Recording Server Service	XProtect Smart Client, Management Client	Retrieving video and audio streams, PTZ commands.
8966	TCP	Recording Server Service	Recording Server tray controller, local connection only.	Showing status and managing the service.
11000	TCP	Recording Server Service	Failover recording servers	Polling the state of recording servers.
65101	UDP	Recording Server service	Local connection only	Listening for event notifications from the drivers.

Note that 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.	Listening for event messages from devices. The port is disabled per 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.
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.

Port number	Protocol	Process	Connections from...	Purpose
8844	UDP	Failover recording servers	Local connection only.	Communication between the servers.
8966	TCP	Failover Recording Server Service	Failover Recording Server tray controller, local connection only.	Showing status and managing the service.
8967	TCP	Failover Server Service	Failover Server tray controller, 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.

Note that 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	Mobil Server management (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 must have the LPR plug-in installed.
22334	TCP	LPR Server Service	LPR Server management (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.

Milestone 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.
9300	HTTP	DLNA Server Service	Milestone DLNA Server Manager	SysTray application.

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.

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.

Port number	Protocol	Connections from...	Purpose
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.

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.

Note that only a few camera models are able to establish outbound connections.

Client components (outbound connections)

XProtect Smart Client, XProtect Management Client, Milestone 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.

Web Client, Milestone Mobile client

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

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

Index

About Milestone Systems

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 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 is a stand-alone company in the Canon Group. For more information, visit: http://www.milestonesys.com.