MAKE THE
WORLD SEE

Date: 14 September 2020

White Paper

System Architecture Guide for IT Professionals

XProtect® Corporate
XProtect® Expert
XProtect® Professional+

Prepared by:
John Rasmussen, Platform Architect, Milestone Systems

milestone

Table of Content

Introduction

XProtect Corporate, XProtect Expert and XProtect Professional+ are video management software (VMS) designed for medium to large-scale installations.

Throughout this white paper, XProtect Corporate, XProtect Expert and XProtect Professional+ are referred to as 'XProtect® VMS products' because they share the same architecture and components.

Purpose and target audience

The purpose of this whitepaper is to provide insight to the benefits and ease of using Milestone XProtect VMS products as the VMS. Furthermore, it introduces and describes the system components and overall system architecture.

This white paper should enable the reader to understand the overall system architecture of the XProtect VMS products and the primary system components and their functions. Furthermore, it provides recommendations for various system layout designs and includes references to more information on specific topics.

The primary audience for this white paper is system integrators and IT administrators with limited experience using Milestone XProtect VMS products who are in the process of selecting, deploying, administrating or expanding a Milestone XProtect VMS system.

The reader is assumed to have a general understanding of general IT and network infrastructure. In addition, it is recommended that the reader has general knowledge about video encoding standards like MJPEG, MPEG4, H.264 and H.265 as well as transmission of video over IP networks.

Designed for network and IT systems

From a technical standpoint, Milestone XProtect VMS products are designed and implemented as a regular IT infrastructure system. The product's system architecture, with a client-server design and management principles, should therefore be very familiar to IT and network administrators.

Run on standard IT equipment:

- Standard servers of your choice
- Standard storage of your choice; SATA, SAS, SSD, DAS, SAN, NAS, iSCSI, etc.
- Standard storage configuration of your choice; RAID 0, 1, 5, 6, 10, etc.
- Standard network equipment with configuration and layout of your choice including support for VLAN's, VPN, and firewalls etc.
- Standard certificate-based HTTPS encryption of network communication
- Integrates with the standard Microsoft Active Directory
- Use standard Microsoft SQL Server for storing the VMS configuration and logs

Wide choice of Microsoft® Windows® operating systems:

- Microsoft Windows 8.1 (64 bit) - Pro & Enterprise

- Microsoft Windows 10 (64 bit) - Pro & Enterprise
- Microsoft Windows 10 (64 bit) - Enterprise LTSB (v1607 or later)
- Microsoft Windows 10 (64 bit) - IoT Enterprise (v1803 or later) & IoT Core
- Microsoft Windows Server 2012 (64 bit) - Standard & Datacenter
- Microsoft Windows Server 2012 R2 (64 bit) - Standard & Datacenter
- Microsoft Windows Server 2016 (64 bit) - Essentials, Standard & Datacenter
- Microsoft Windows Server 2019 (64 bit) - Essentials, Standard & Datacenter

The newest updated list can be found here: System Requirements

Support for cloud hosting and virtualization technology:

- Support for VMware
- Support for Microsoft Hyper-V
- Support for Amazon AWS
- Support for Microsoft Azure Virtual Machines
- As well as all other virtualization technologies supporting Microsoft Windows operating systems

Easy installation and upgrade:

- All XProtect VMS products are offered in fully functioning trial versions
- Both trial and paid versions of XProtect Expert and XProtect Professional+ can easily be upgraded to a paid version or a more advanced XProtect product by simply applying a new license file to the running system – No need to reinstall, reconfigure or even restart the VMS
- Installers for the VMS server components and clients are hosted on the management server for easy download to new computers where VMS components should be installed – No need to manually distribute installers via USB thumb drives
- Easy upgrade or addition of new camera drivers via dedicated device packs - No need to upgrade all VMS components and clients to support new camera models or new camera firmware

Flexible deployment that can be scaled over time:

- Scalable system architecture with system components that allow everything to be run on a single server, or distributed over multiple servers when the requirements, configuration, system size or usage need it. This provides everyone with the option to choose the most cost-efficient hardware and VMS system design that fits their needs, whether the needs are for a small or large VMS installation.
- Support for Milestone Federated Architecture™ to tie related systems together
  - For more information: White paper - Milestone Federated Architecture
- Support for Milestone Interconnect™ to tie independent systems together
  - For more information: White paper - Milestone Interconnect

Central management and monitoring:

- All VMS management and configuration is done through a single Management Client that can be used on any computer, for instance on the IT or VMS administrator's local workstation. This eliminates the need to access the VMS servers directly to manage the VMS
- The XProtect VMS products support definition of an unrestricted number of user roles, each with support for controlling which cameras/devices, functions and features the users in the role can access or administrate
- Having the roles defined, users are then simply added to the roles they should have in the VMS

- Using Microsoft Active Directory (AD), it can be even simpler to manage the VMS users. This is because AD groups can be used in the VMS roles, which allows management of VMS access by simply assigning users to the right groups in the AD
- Built-in server and VMS performance monitoring includes email notification on events and failures. Alternatively, or in addition to the built-in monitoring, you can use standard IT tools to monitor the servers, storage, network, etc.

Secure and reliable architecture:

- Failover support on management and event servers via Microsoft Windows Server Failover Clustering (WSFC) or similar third-party solutions
- Dedicated hot-standby or cold-standby failover recording servers
- Certificate based HTTPS encryption of communication between VMS servers and clients, and between recording servers and cameras
- Support for separating client network and camera network, thus preventing users and other equipment on the client network to tamper with or hack the cameras, or in general interfere with video recording

For more information and recommendations on securing and hardening the servers, network, and VMS installation:

  - White paper - Ensuring end-to-end protection of video integrity
  - Hardening Guide for XProtect VMS

Predictable cost:

- Transparent and simple license structure
  - Base license: The base license unlocks all software functionality and can be used on multiple sites when owned by the same legal entity
  - Hardware device license per connected hardware device (one hardware license per device IP/MAC address).
  - Milestone Care Plus is mandatory for XProtect Corporate and XProtect Expert for the first year. Milestone Care Plus gives access to new product versions for free
  - Milestone Care Plus is optional for XProtect Professional+
- No license cost on number of recording servers used
- No license cost on storage amount used
- No license cost on number of clients used
- Predictable maintenance cost because the system runs on standard IT equipment

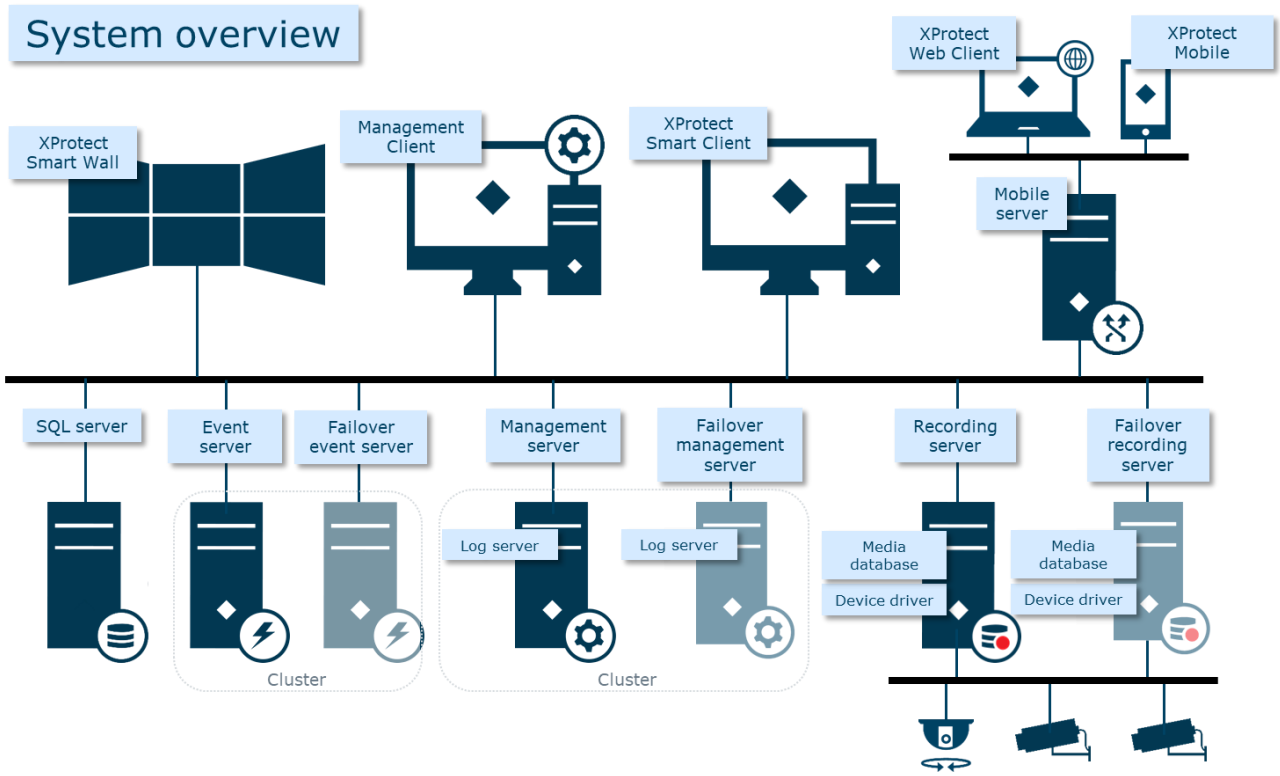
Overall system architecture

Milestone XProtect VMS products are state-of-the-art products designed for medium- to large-scale high-security installations. The XProtect VMS products consist of several components that can be installed across multiple servers in a single installation (site), as well as supporting Milestone Federated Architecture and Milestone Interconnect to support VMS installations that are distributed over multiple sites. That said, all components can also be installed on the same single server if the server can support the combined load.

Not all components are needed in all installations if the functionality they offer is not needed. For instance, the failover recording servers, which can take over recording if a standard recording server fails,

and the mobile server, which provides access to both the XProtect® Web Client and XProtect® Mobile, are optional components. Likewise, if the users only access the VMS using the XProtect Web and/or XProtect Mobile, the XProtect® Smart Client does not need to be installed.

System components



Note:

- XProtect® Smart Wall is included in XProtect Corporate, but is an add-on to XProtect Expert
- XProtect® Smart Wall and failover recording servers are not supported by XProtect Professional+

Server components

Management server

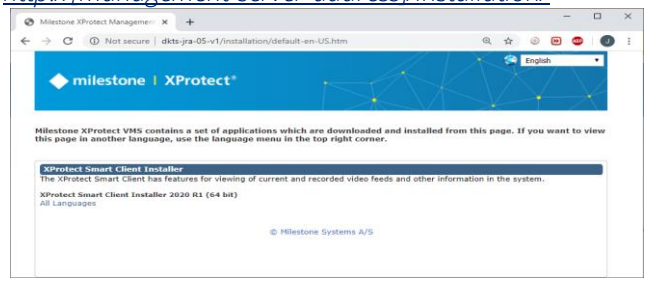
The management server is the central component of the VMS and is responsible for handling the system configuration, distributing configuration to other system components, such as recording servers, and for facilitating user authentication.

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

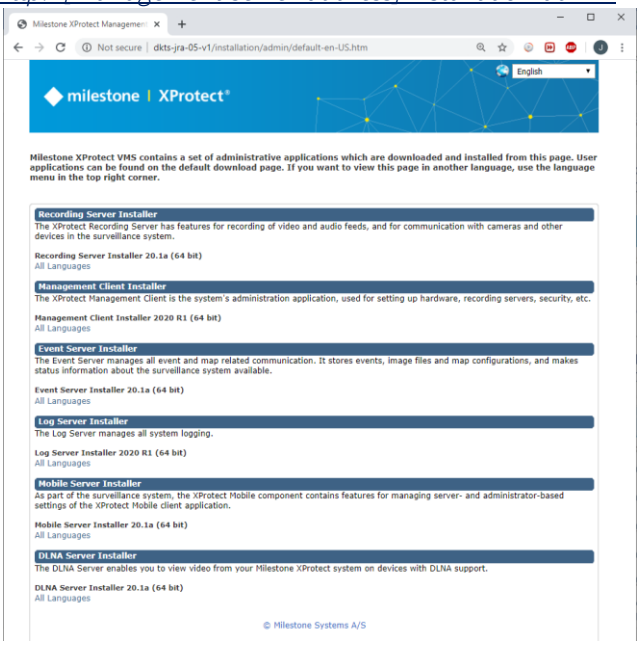
System component and client repository

In addition to the management server's VMS function, the management server also hosts two download pages with installers for all other system components and clients. This makes it easy and convenient for administrators or integrators to download and install system components and client applications on additional servers and workstations, without the need to copy the component installers to USB thumb drives and hand carry them to the other computers.

Client download page (does not require user authentication):
http://[management-server-address]/installation/



Server component download page (may require user authentication):
http://[management-server-address]/installation/admin



In upgrade scenarios, the management server will also host the new updated component versions once it has been updated. It can thus again be used as a distribution point for the other server and client components that should be upgraded.

Failover management server

Failover support on the management server is achieved by installing the management server in a failover cluster using Microsoft Windows Server Failover Clustering (WSFC) or by using third-party software that offers similar failover functionality – for instance this could be Evidian SafeKit.

Running the management server in a failover cluster will ensure that another server can take over the management server function, should the active server fail.

More information about Microsoft's Failover Clustering: Failover Clustering in Windows Server
More information about Evidian SafeKit: Milestone XProtect cluster with Evidian SafeKit

Recording server

The recording server is responsible for the core VMS functionality of communicating with cameras and surveillance devices, for recording, storing, and securing the retrieved media as well as providing VMS clients access to the live and recorded media.

The recording server handles these functions:

- Communication with devices – for instance cameras, audio and video encoders, I/O (input/output) modules, metadata sources, etc.
- Recording and storing video, audio and metadata media retrieved from the devices for the set retention time
- Encrypting and signing the recorded media in the media database
- Providing client access to live and recorded video, audio, and metadata
- Securing and controlling client access to live and recorded media
- Providing access to device status
- Performing motion detection and generate Smart Search metadata
- Triggering system and video events on device failures, events, etc.

Furthermore, when using Milestone Interconnect, the recording server is responsible for communication with the remote interconnected system.

For more information about Milestone Interconnect: White paper - Milestone Interconnect

Device drivers

An essential part of the recording servers are device drivers. These drivers work as the interface between the recoding server and the devices (cameras, video and audio encoders, I/O modules, metadata sources, etc.). A dedicated device driver is needed for each device or series of devices from the same manufacturer. In addition to the dedicated device drivers, the VMS also supports an ONVIF driver that can be used for ONVIF-compliant devices.

If a dedicated driver has not been developed for a specific device or video system, and the specific device or video system is not ONVIF compliant, then in many cases a 'universal' driver can be used. Alternatively, a custom dedicated driver can be developed for the specific device or video system by using the Milestone Integration Platform Software Development Kit (MIP SDK).

The device drivers are by default installed with the recording server. However, the drivers are installed as a separate device pack and can thus be updated later by downloading and installing a newer and updated device pack without having to update the recording servers or any other VMS components.

New device packs are released every second month.

For more information on supported devices: Supported hardware
New device packs can be downloaded here: Download device packs

Media database

The retrieved video, audio, and metadata are stored in the dedicated Milestone-developed, high-performance media database, which is optimized for recording and storing streamed real-time video, audio, and metadata.

The media database supports various unique features such as: multistage storage architecture, video grooming, Scalable Video Quality Recording™ (SVQR), encryption and digital signatures. The multistage storage architecture enables splitting the media database into a "live" database and one or more "archive" databases. This allows the storage system and media database to be distributed across different storage technologies making it possible to design and optimize the VMS and storage system for both performance (live recording), size (archive retention) and cost.

For more information about the media database and storage architecture: XProtect Storage Architecture and Recommendations

Failover recording server

The failover recording server is responsible for taking over the recording server tasks should a standard recording server fail.

The failover recording server can operate in two modes:

- Cold-standby - acting as failover for multiple recording servers
- Hot-standby - acting as a dedicated failover for a single recording server

The difference between cold-standby and hot-standby failover modes is that in cold-standby failover mode the failover recording server does not know which server to take over in advance. This means that it cannot preload the configuration and start its process until a recording server fails. Loading the configuration and starting the processes increases the failover startup time compared to hot-standby.

In hot-standby mode, the failover time is significantly shorter because the failover recording server already knows which recording server it should take over recording for and thus can preload the configuration and start up completely - except for the last step where it connects to the cameras. So, when a recording server is stopped or fails, the only thing the hot-standby failover recording server needs to do is to connect to the cameras and start recording, which takes very little time.

Note: Failover recording server is not supported in XProtect Professional+

Event server

The event server handles various tasks related to events, alarms, maps, XProtect® Access, XProtect® LPR, XProtect® Transact and third-party integrations via the Milestone Integration Platform Software Development Kit (MIP SDK). All data handled by the event server, such as alarms, maps and data from add-on products are stored in the same SQL server that the management server uses.

Events

All system events are consolidated in the event server (if a function is subscribing to them), making them available for the other features and integrations in the event server.

Alarms

The event server hosts the alarm feature, alarm logic, and alarm state, as well as manages the alarm database.

Maps and Smart Maps
The event server hosts the Maps and Smart Map features that are configured and used by the XProtect Smart Client.

Milestone XProtect Access
The event server hosts the XProtect Access add-on product. XProtect Access enables integration of access control systems using a standardized access control framework. When integrated, the VMS and the access control system can be controlled from one centralized interface.

Milestone XProtect LPR
The event server hosts the XProtect LPR add-on product. XProtect LPR enables detection and registration of license plate information from vehicles and links the license plate information with video from the VMS.

Milestone XProtect Transact
The event server hosts the XProtect Transact add-on product. XProtect Transact extracts transactional data from point-of-sale (POS) systems, barcode scanning systems and other data systems that generate textual data, and pairs that data with video from the time of the transaction.

MIP SDK
The MIP SDK enables integrations with the XProtect VMS products. In the event server, the MIP SDK can be used to create plug-ins for the event server, enabling integrations of the VMS and third-party systems.

Failover event server
As with the management server, failover support on the event server is achieved by installing the event server in a failover cluster using Microsoft Windows Server Failover Clustering (WSFC) or by using third-party software that offers similar failover functionality – for instance this could be Evidian SafeKit.

Running the event server in a failover cluster will ensure that another server can take over the event server function, should the active server fail.

More information about Microsoft's Failover Clustering: Failover Clustering in Windows Server
More information about Evidian SafeKit: Milestone XProtect cluster with Evidian SafeKit

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 combined load of the management and log server is too high for a single server.

The system can log three types of logs:

- System log:
  The system administrator can choose to log errors, warnings, information, and combinations of these. The default is logging errors only
- Audit log:

The system administrator can choose, in addition to log-in and administration logs, to log user activity in the clients

- Rule log:
  The rule log can be used by the system administrator to create logs on specific events

Mobile server

The mobile server is responsible for hosting the XProtect Web Client and function as a gateway to the VMS for the XProtect Web Client and XProtect Mobile users.

In addition to hosting the XProtect Web Client and function as a gateway to the VMS, the mobile server is also responsible for providing access to the video, either by streaming video directly to the clients, or by transcoding it to JPEG. Streaming the video directly or transcoding it to JPEG depends on the usage:

- For live viewing of H.264 and H.265 streams - Stream the video untouched through the mobile server
- For live viewing of all other codecs and for all playback regardless of codec - Transcode it to JPEG

The reason transcoding is needed for some codecs and playback is because not all browsers or smart phones support all of the codecs that the VMS and cameras support, and secondly, because more re-fined control and playback capabilities are needed for playback – for instance the ability to playback video backwards.

If many users playback recordings at the same time, or view live video from cameras configured with other codecs than H.264 and H.265, the mobile server will have to transcode a lot of video – which is a very resource demanding task. In these cases it is highly recommended to install the mobile server on a dedicated server - preferably on a server that has an Intel CPU with Intel Quick Sync Video support, or has an NVIDIA card installed, because the transcoding load in these cases will be offloaded to the GPU.

SQL server

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

The XProtect VMS products installer includes a Microsoft SQL Server Express edition that can be used freely.

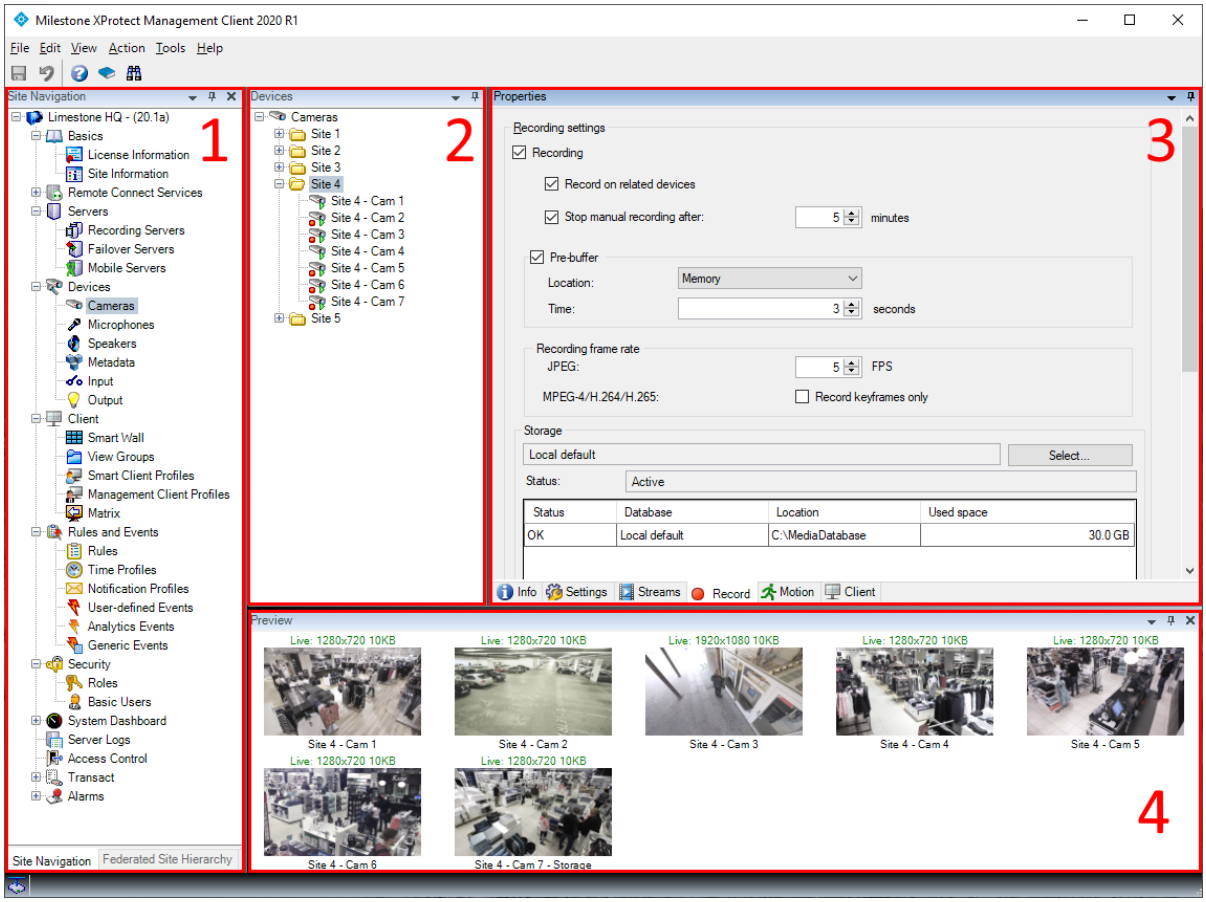
For larger systems with more than ~300 cameras, it is recommended to use Microsoft SQL Server Standard or Enterprise edition on a dedicated server. These editions can handle larger databases, have a better utilization of system resources, offer automatic backup functionality, as well as have 'Always On' functionality.

Client components

Management Client

The Management Client is the administration interface for the VMS.

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



The Management Client has a "Site Navigation" tab (1), where nodes for various parts or functions of the system can be selected, for instance 'Cameras' as shown on the screenshot.

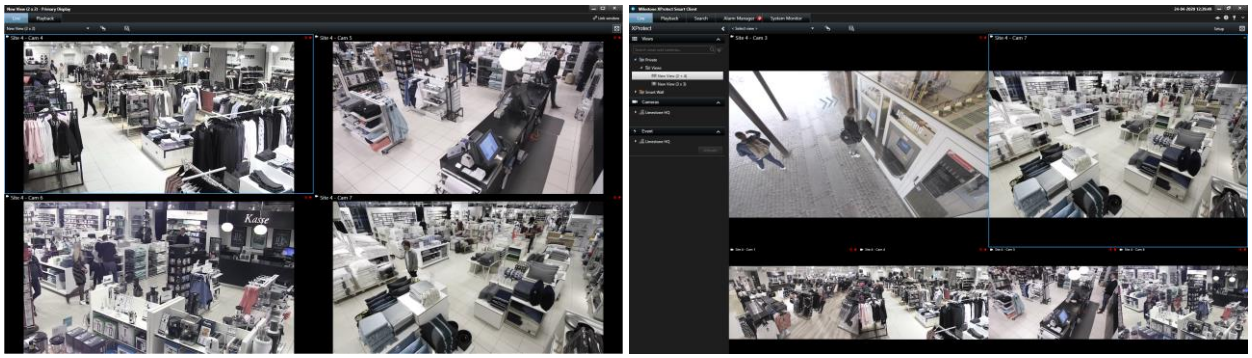
Selecting a node will show the settings for this node, typically in a second tree structure where more items of this kind can be selected (2). When an item is selected, the settings are displayed in the properties dialog, shown in the right side of the client (3). Since the selected items often have many settings, the settings are grouped on different tabs that are assigned to one area, for instance 'Recording' as shown on the screenshot.

When selecting a camera or a camera group, a preview of the camera(s) is shown in the preview pane (4). By default, the preview shows up to 64 cameras at a reduced framerate to avoid putting too much load on the computer that is running the Management Client. To conserve bandwidth and CPU load even more, the preview pane can be closed completely.

XProtect Smart Client

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

The XProtect Smart Client is designed to be run remotely on the operator's computer and supports hardware accelerated video decoding and multi-screen use in full-screen mode as shown below, or as floating windows where the windows can be resized and moved freely.



Furthermore, the XProtect Smart Client has tabs dedicated to different primary tasks:

- Live: Live monitoring
- Playback: Playback, investigation, and export
- Search: Searching for recordings based on search parameters
- Alarms: Alarm management
- System monitor: Monitor state and load of servers, storage, cameras, etc.

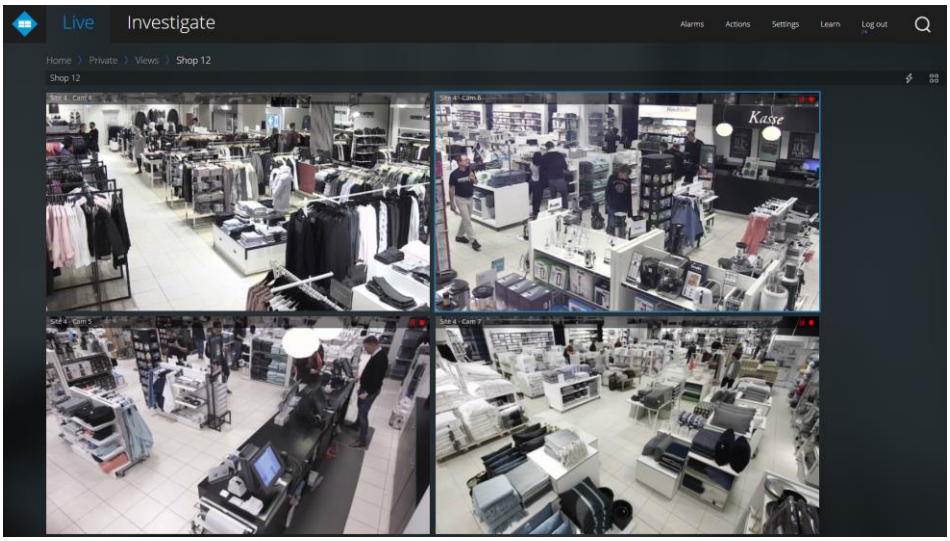
In addition to the standard tabs, the XProtect add-on products as well as third-party integrations can add additional tabs that provide user interfaces dedicated to specific functions - for instance:

- XProtect Access: Access control integrations
- XProtect LPR: License plate functionality
- XProtect Transact: Viewing transactional data

For more information: XProtect Smart Client

XProtect Web Client

The XProtect Web Client is designed for the occasional or remote user who needs access to the VMS from a standard browser.



Compatible browsers can be found on the XProtect Web Client tab listed here: System requirements

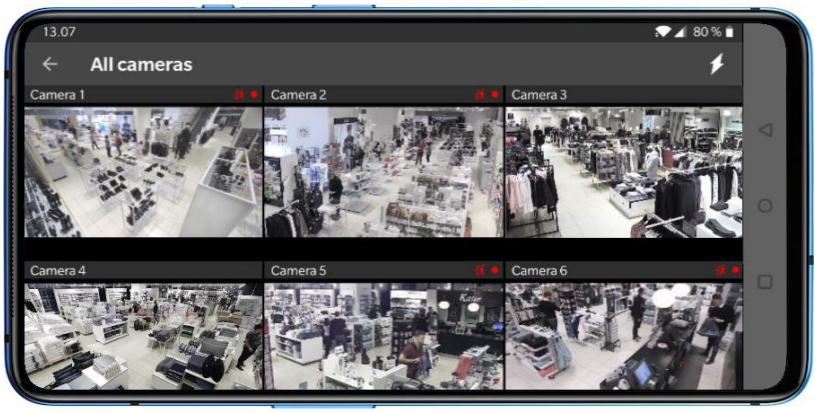
For more information: XProtect Web Client

XProtect Mobile

XProtect Mobile is the client that is designed for the user on-the-go. It offers easy access to live and playback of cameras, as well as access to doing investigations, triggering events, managing alarms, and controlling XProtect Access integrations.

Furthermore, the XProtect Mobile can be used as a remote camera for the VMS by using the device's built-in camera and microphone and the video push feature. When activated, the video and optionally audio from the device's camera and microphone is streamed back to the VMS and recorded like a standard camera and microphone.

XProtect Mobile is available for Apple® and Android™ devices.



For more information: XProtect Mobile

Compatible smartphone operating systems can be found on the XProtect Mobile tab listed here: System requirements

Additional products and components

In addition to the Milestone XProtect VMS products, Milestone has a suite of add-on products and utilities, of which a few are highlighted below.

XProtect Smart Wall

XProtect Smart Wall is Milestone's advanced video wall product that is designed to work as a flexible canvas to increase operators' situational awareness and improve response times. It displays relevant video cameras and other surveillance related content, giving operators a complete overview of large surveillance installations.

XProtect Smart Wall is fully integrated with XProtect Smart Client that allows users to control the XProtect Smart Wall in an easy and intuitive way. Furthermore, the content shared on the XProtect Smart Wall can also be displayed locally in the users' XProtect Smart Client.

In extension to user control of content on the XProtect Smart Wall, cameras and other content can automatically be sent to the XProtect Smart Wall by using the VMS' rule system that is based on events and/or time schedule. Alternatively, it can be controlled from third-party systems by using the MIP SDK.

XProtect Smart Wall is included in XProtect Corporate and can be purchased as an add-on for XProtect Expert. The XProtect Smart Wall is not supported for XProtect Professional+.

For more information: XProtect Smart Wall

MIP SDK

The MIP SDK is a comprehensive tool that facilitates the integration of third-party applications and systems with Milestone's XProtect VMS. The MIP SDK provides flexible access to the VMS and supports nearly all functions and features, for instance: viewing live/recorded video, audio and metadata, event integration, rule integration, viewing performance data and configuration of the VMS.

To support the integration of different third-party applications and systems, the MIP SDK has different integration methods, including protocol integration, component integration and a unique plug-in abstraction layer. Using the plug-in integration, solutions become a fully integrated part of the XProtect VMS user interface.

For more information: MIP SDK

Furthermore, the MIP SDK includes a plug-in framework for simple development and integration of access control systems.

For more information: XProtect Access

Finally, the MIP SDK includes a device driver framework for simple development of custom device drivers for video, audio or IoT devices that are not currently supported by the device drivers in the device pack.

For more information: Driver Framework

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 computers in the surveillance network. For larger installations, the tool makes it easy and fast to upgrade components such as recording servers and device packs that are installed on multiple servers.

For more information: Software Manager

VMS Design Guide

Notes to presented VMS designs:

This guide presents the VMS implementation designs that are recommended for the most typical installations. In addition to these typical implementation designs, it is of course possible to design and implement the VMS in other ways to suit specific needs.

Server specifications:

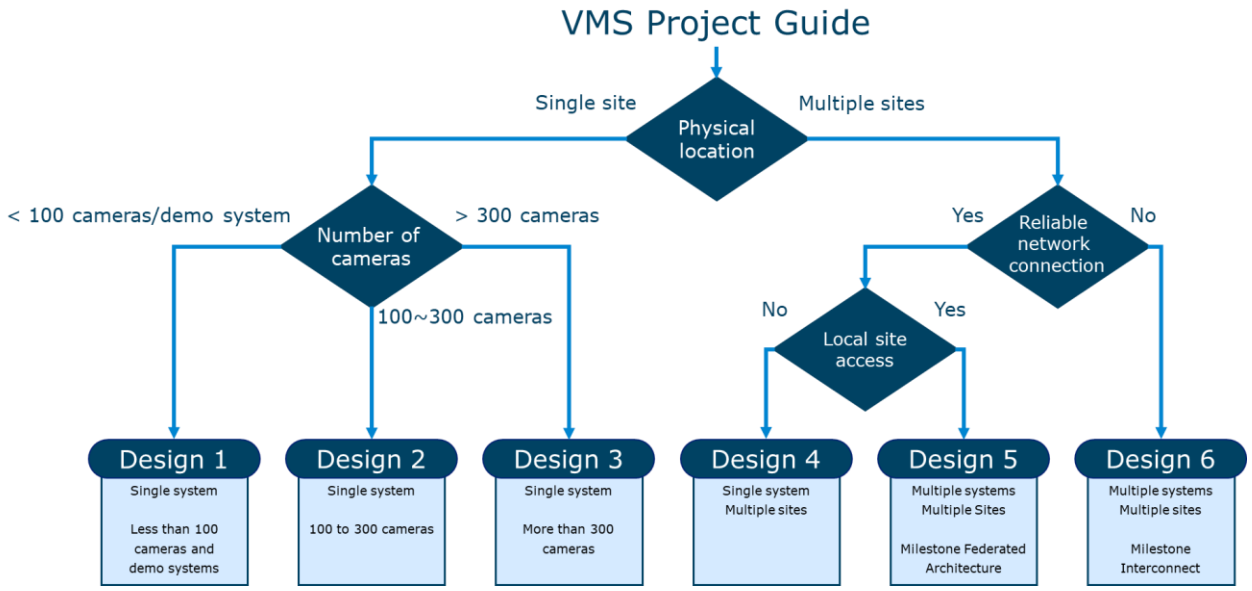
To get server recommendations for specific projects, use the XProtect Server Calculator (Note: requires a *My Milestone* login).

To get assistance with server requirements for larger VMS projects or projects with more specialized requirements than the ones covered in this design guide, contact the Milestone pre-sales team at pre-sales@milestonesys.com.

Standard system designs guide

When deciding how to implement the VMS, the first things to consider are the physical location of the sites that should be surveyed, where the users of the VMS are located, and the quality of the network infrastructure if the installation covers multiple physical locations.

For typical VMS installations, this design guide can help to choose the recommended way to implement the system.

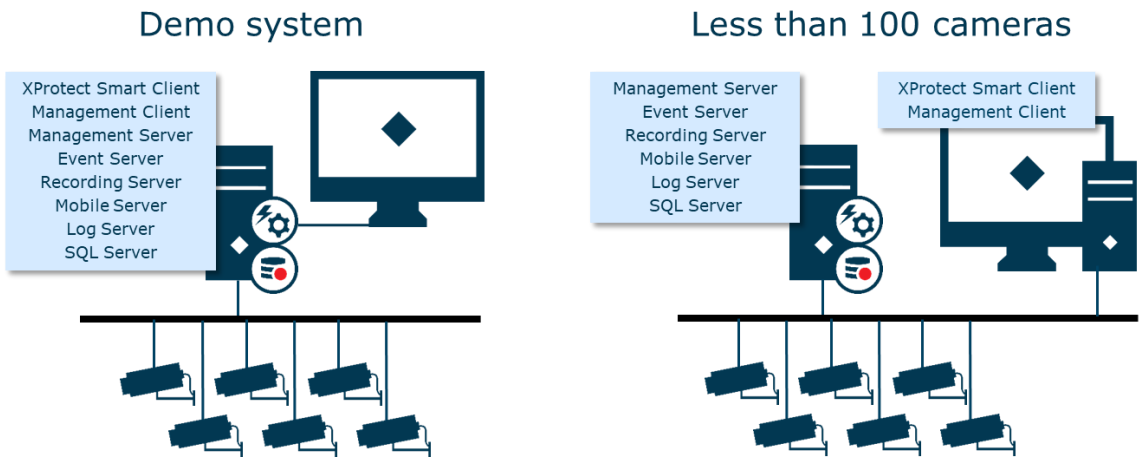


Note: The 'Number of cameras' decicion limits are based on cameras set to: H.264/H.265, 1080p, 25/30 FPS and a bitrate of 3-5 Mbit/s.

- With lower resolution/bitrates, the limits will be higher
- With higher resolution/bitrate, the limits will be lower

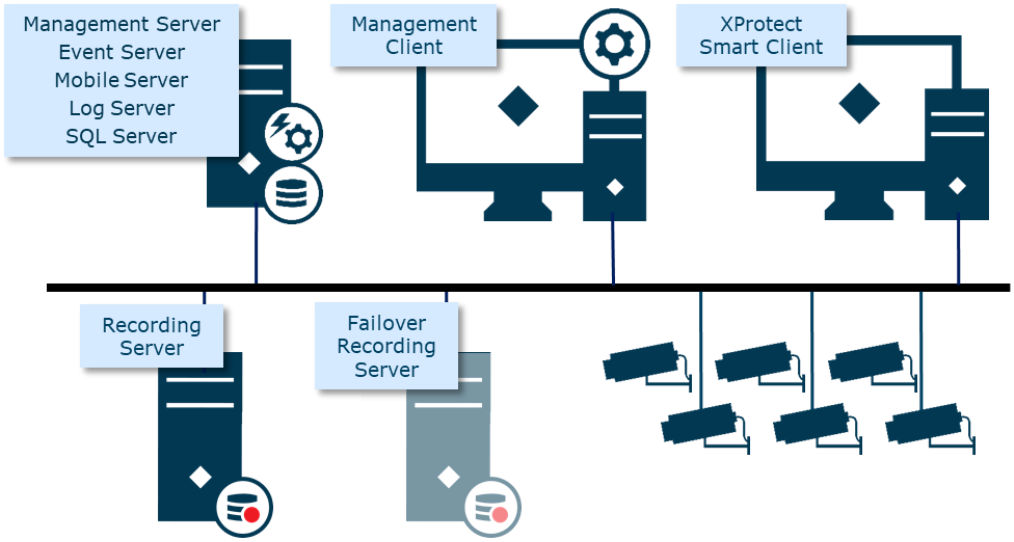
Design 1 – Single system - Less than 100 cameras / Demo system

This VMS design is the simplest possible design where everything is connected to the same network and all server components, and maybe even the clients, are installed on the same computer.



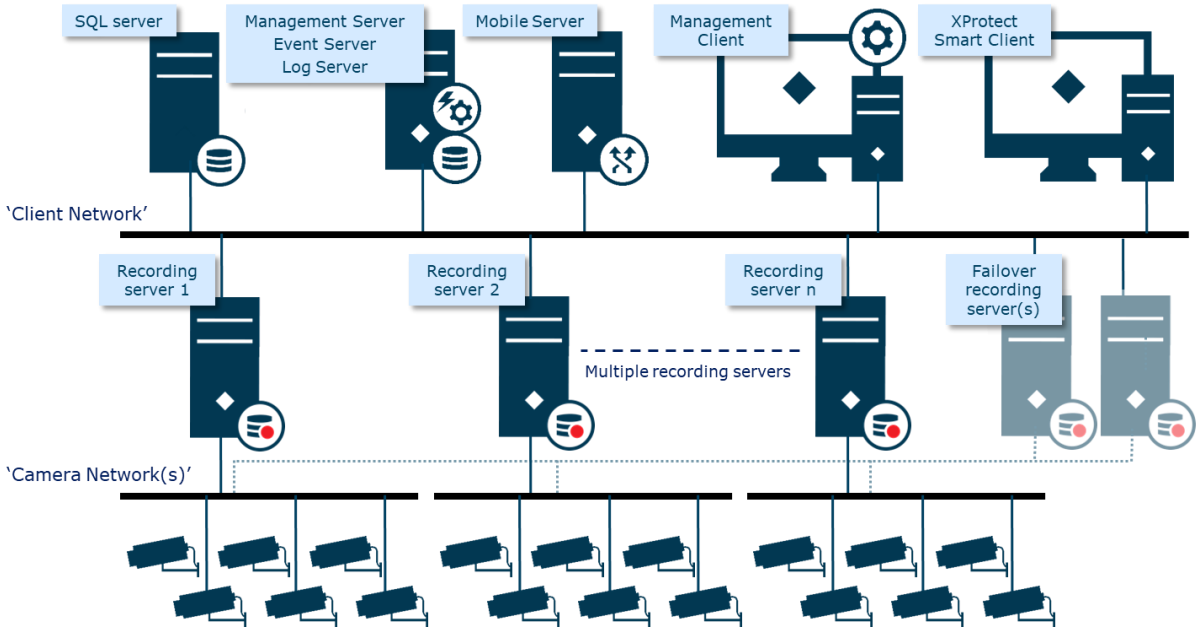
Typically, for real world usage, it is recommended that the VMS servers and VMS clients are installed on separate computers. However, if the computer is powerful enough, everything could be installed on the same computer – for instance, a laptop to try out or demonstrate the XProtect VMS.

Design 2 – Single system - Up to 300 cameras



With this design the recording server is installed on a dedicated server to ensure optimal performance. To provide live and recording capabilities in scenarios where the recording server has failed or is stopped for maintenance, a failover recording server can be added.

Design 3 – Single system - More than 300 cameras



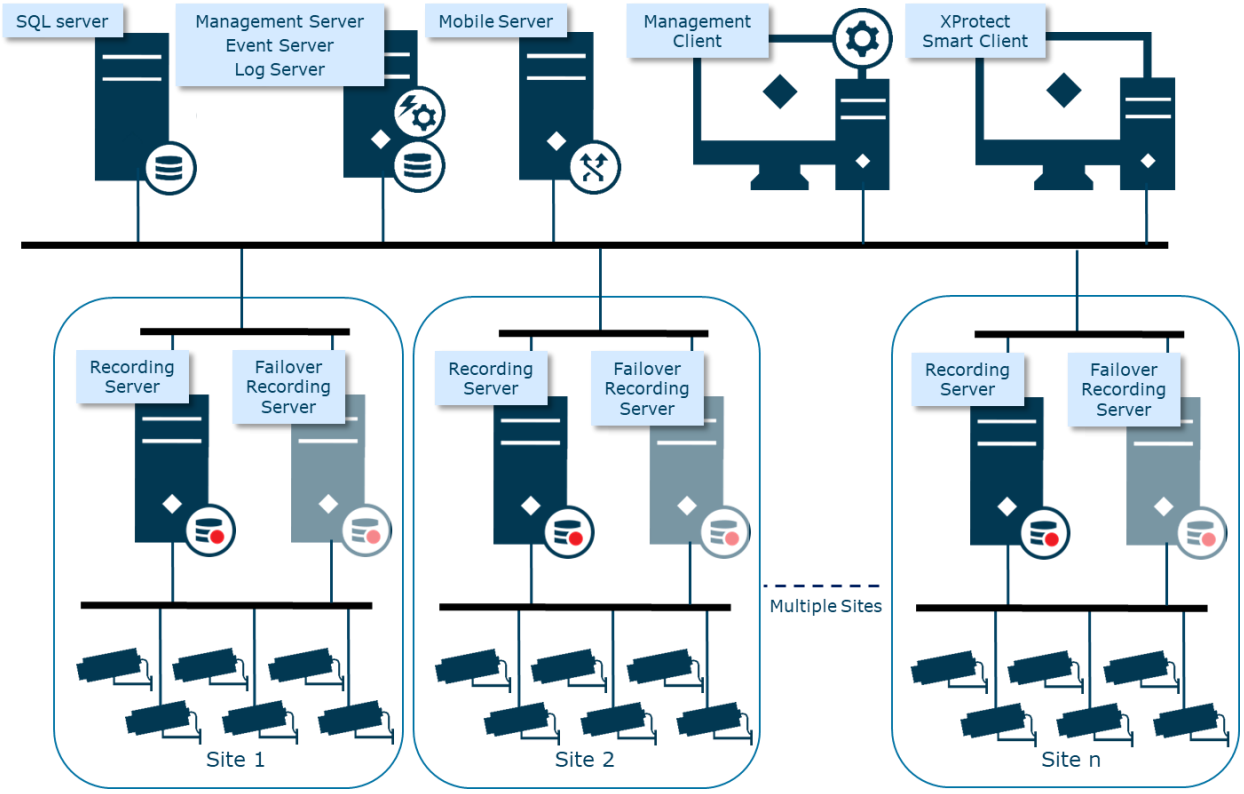
Note: When the system is larger than ~300 cameras, it is recommended to run the SQL server on a dedicated server and use either the Standard or Enterprise edition of the SQL server.

Furthermore, with many cameras in the system, it is recommended to separate the 'client network' from the 'camera network' by creating one or more separate networks for the recording server and the cameras.

Separating the camera network from the client network increases performance, stability and security and furthermore makes it easier to dimension the network.

- Performance is increased by separating the traffic to and from recording servers so any high load on the client network does not impact the recording performance
- Stability is increased because any network interference on the client network does not affect the camera network
- Security is increased because the cameras are protected behind the recording servers, and they can therefore not be accessed, hacked, or blocked by users or other equipment connected to the client network
- Dimensioning of the network is made easier because the load is separated to several different network segments where the load, especially on the critical camera network, can easily be calculated

Design 4 – Single system, multiple sites. No direct user access in remote sites



This design is essentially the same as design 3, though with the difference that the cameras and recording servers are located on physically remote sites, and not on the main site where the management server and the VMS users are located.

The advantage of this design is that the bandwidth from the remote sites to the central site can be much lower compared to recording all cameras from the remote sites on the central site. Basically, the network requirements are set by how many cameras must be viewable at the same time from the remote site.

An example with some requirements to illustrate it:

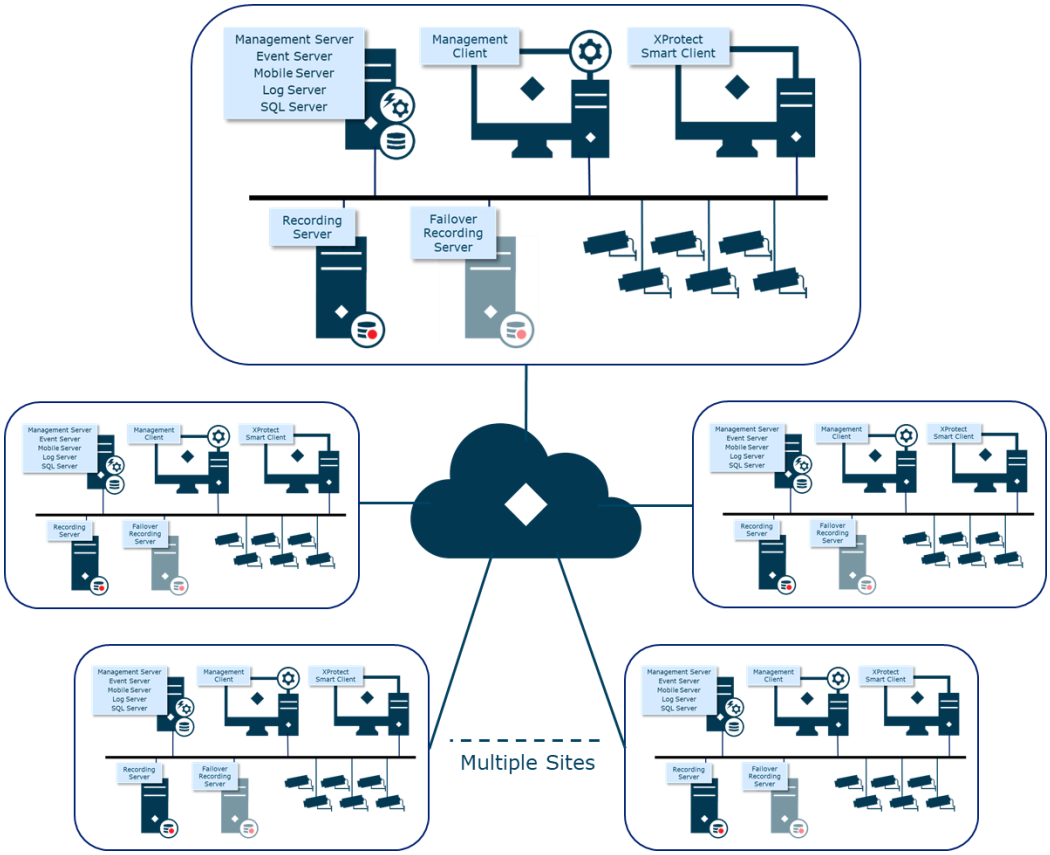
- *Each site has one recording server that record 100 cameras at: 1080p, 25/30 FPS, 4 Mbit/s, H.264/H.265*
- *The users on the central site must be able to view maximum 10 cameras at the same time for each remote site*

If the recording servers were placed on the central site, as shown on the previous design 3, a bandwidth of 100 * 4Mbit/s = 400 Mbit/s would be needed 24/7 from each remote site to the central site.

However, when placing the recording servers on the remote sites, only the bandwidth for cameras actively viewed by the users on the central site are needed. With a maximum of 10 cameras, only 10 * 4Mbit/s = 40 Mbit/s are needed – and this only during periods where the cameras are viewed actively by the users.

Should failover functionality be needed, it is recommended to place a failover recording server on each remote site to contain the traffic to the remote site in case of failure.

Design 5 - Multiple systems, multiple sites. Direct user access to remote sites using Milestone Federated Architecture



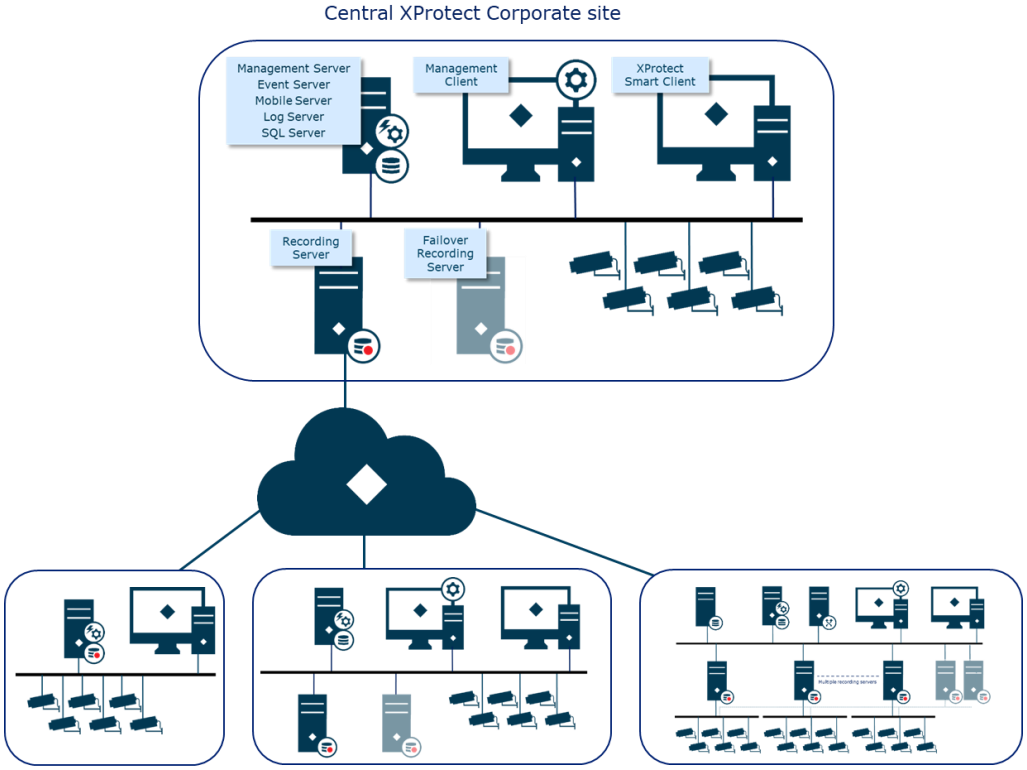
In a geographically distributed VMS system, where the network connection is stable and where users must access video locally on each of the remote sites, it is recommended to design the system using Milestone Federated Architecture.

Milestone Federated Architecture offers several advantages:

- Independent design and configuration
  - Each site can be designed independently, only taking the number of cameras and user requirements on the individual site into consideration
  - Each site can be configured independently, keeping the complexity of the overall system low
  - User and administrator permissions can be set per site
- Seamless access
  - Users on a central site can access the entire federated system seamlessly via a single log-in
  - Local users on the remote site can access the system on their site even if the connection to the central site is broken

For more information: White Paper - Milestone Federated Architecture

Design 6 – Multiple systems, multiple sites. Direct user access to remote sites using Milestone Interconnect



Multiple Milestone Interconnect sites of different size

In a physically distributed VMS system, where there is a need for accessing video locally by users on remote sites and where the network connections between the remote and central sites may be unstable or have limited bandwidth, it is recommended to use Milestone Interconnect.

Secondly, if the remote sites are on different domains, or maybe even use workgroups, it is also recommended to use Milestone Interconnect because it is domain agnostic. This means that any combination of domains and workgroups between the central and remote sites is supported.

Furthermore, Milestone Interconnect supports interconnecting all of the XProtect VMS products - except the free XProtect Essential+ product.

Milestone Interconnect offers several benefits:

- Independent design and configuration
  - Each site can be designed independently, only taking the number of cameras and user requirements on the individual site into consideration
  - Each site can be configured independently, keeping the complexity of the overall system low
  - User rights can be set and controlled per site
- Seamless access
  - Users on the central site can access the central and interconnected remote sites seamlessly via a single log-in

    - Local users on a remote site can access the system on their local site even if the connection to the central site is not working
- Flexible recording
    - In case the connection between the central site and remote site have been lost for a period and then later restored, the central site can automatically retrieve recordings made on the remote system during the period with network outage. This could for instance be used for surveillance in vehicles like cars, buses, trains, airplanes, ferries etc.
    - In addition to automatic retrieval upon network reconnection, the system offers user-activated, rule-activated, scheduled, and MIP SDK-activated retrieval of recordings
    - Alternatively, instead of recording or retrieving recordings on the central site, the interconnected systems can be configured so clients on the central site playback recordings directly from the remote sites without first having to transfer them to the central site
- Resilient
    - With Milestone Interconnect, the system can handle unstable and intermittent network connections between the central and remote sites without impacting client log-on time, performance or management of the central or remote site

For more information: White paper - Milestone Interconnect

Integration with standard IT technology

Milestone XProtect VMS products integrate seamlessly with commonly used IT technology and tools, and use terms and technologies commonly known by IT administrators. This makes it easy for IT administrators to understand, design and deploy the VMS, as well as operate and administrate it.

Milestone XProtect VMS products looks like, and are managed much like an IT system - the data the VMS handles are just video, audio and metadata streams instead of files, transactions, business data, etc.

The following list show examples of how Milestone XProtect VMS products integrate with and use standard IT technology:

Microsoft Active Directory (AD)

Users and groups from the AD can be used in the security roles in the VMS. This makes it easy via the AD groups to administrate who can access the VMS and what they can access. New users to the system are simply added to the right AD group(s) and they have access to the VMS.

SQL server

For installations with less than 300 cameras, the included free SQL Server Express edition can be used. For larger systems, it is recommended to use the Microsoft SQL Server Standard or Enterprise edition, because they offer better performance and most importantly, they offer scheduled backup of the SQL database.

The whole system configuration is stored in the SQL database, so it is important to configure a scheduled backup of the SQL database and not just make a manual one-time backup through the Management Client. The reason a scheduled backup is recommended over a manual backup is because the VMS administrators or system integrators who are managing the VMS may forget to make a manual backup each time something in the VMS is changed.

Note:
If you use full recovery mode in the SQL, a regular transaction log backup should be scheduled. This is to avoid an ever-increasing SQL transaction log. If you do not require full recovery mode, we recommend changing to use simple recovery, which will prevent the transaction logs from filling.

Virtualization

All virtualization technologies and platforms that support running Microsoft Windows operating systems can be used with every Milestone XProtect product. The virtualization technology or platform could for instance be Microsoft Hyper-V, VMware, Citrix, or virtual servers in the cloud, such as Microsoft Azure and Amazon AWS.

While all XProtect servers and clients can run in virtualized machines (VMs), running the mobile and recording servers in a VM may require some additional configuration of both the host and the VMs. The reason for this is that, by default the host GPU is not available in the VM and both the mobile and recording servers need access to a GPU for optimal performance to transcode video to the web or mobile clients or to decode video to do motion detection.

Depending on the virtualization platform used, enabling the host GPU to be available in the VM may require configuration of both the host and the VM, to make sure the GPU(s) are assigned to the right machine. Furthermore, a GPU can typically only be used with a single VM. Should more VMs with GPU support be hosted on the same machine, the host must have a dedicated GPU installed per VM.

VLAN

It is possible to use VLAN with Milestone XProtect software to segment the network to separate regular business and VMS network traffic.

When doing this, it is important to take into account that, depending on the number of cameras and their stream configuration, the video surveillance traffic can place a very high and continuous load on the underlying network because video, audio and metadata are streamed from the cameras to the recording servers, and from the recording serves to the clients.

A quick example: A recording server with 250 cameras configured with 1080p, 25/30 FPS, 4 Mbit/s, H.264/H.265 will put a continuous load of 1Gbit/s on the network into the recording server.

In addition to this, the network traffic from the recording server to the clients, which also can be substantial, must also be considered.

VPN

If clients or cameras are connected via the public internet, a standard VPN can be used to provide secure access from the internet to the VMS site, ensuring that video, audio and metadata streams, as well as other VMS communication are encrypted.

IPv4, IPv6 and multicast

Milestone XProtect VMS products support both IPv4 and IPv6, including multicast.

VMS, server, and network monitoring

Milestone XProtect software runs on standard IT equipment, such as servers, storage, network switches,

etc. Furthermore, standard IT monitoring products, and software already known by IT administrators can be used to monitor the health and status of the equipment running the VMS. This makes it easy to integrate Milestone XProtect software in the existing IT infrastructure and work processes.

In extension to external system monitoring tools, Milestone XProtect Corporate and XProtect Expert support built-in monitoring functions with a dedicated user interface called System Monitor.

The System Monitor gives an overview of the load and use of the servers and their storage, as well as the network in general. In addition to this, it also provides an overview of VMS-specific parameters such as storage and network use per camera.

Note: The System Monitor is not supported on XProtect Professional+

Email

In addition to the technical monitoring previously mentioned, Milestone XProtect VMS products can use email to send notifications of technical issues, security events or events from third-party integrations. Using email notifications, it is also possible to include still images and/or AVIs of the event in the email notification.

SNMP

It is possible to use SNMP traps to send notifications to a standard network monitoring product, for instance SolarWinds Kiwi Syslog.

NTP

When timestamps are enabled to be overlaid on the video from the cameras, or when Edge Storage is used in the cameras, or when the cameras are interconnected to a central XProtect Corporate system, it is essential that all cameras and VMS servers use the exact same time.

If time synchronization is not ensured, the video overlaid timestamps will drift over time, and deviate from the VMS timestamps since the camera clocks are not very precise over a longer period. Furthermore, when using Edge Storage and Milestone Interconnect, the solution will stop working if the camera and/or interconnected system's time are not synchronized with the central VMS site's time.

If VMS servers are joined to a domain, time synchronization of the servers are ensured by the domain controller. However, the cameras may not be joined to a domain. Instead, a Network Time Protocol (NTP) server must be installed, and the cameras be configured to synchronize their time with it.

In case the VMS servers are not joined to a domain, they can be configured to synchronize the time with the same NTP server as the cameras.

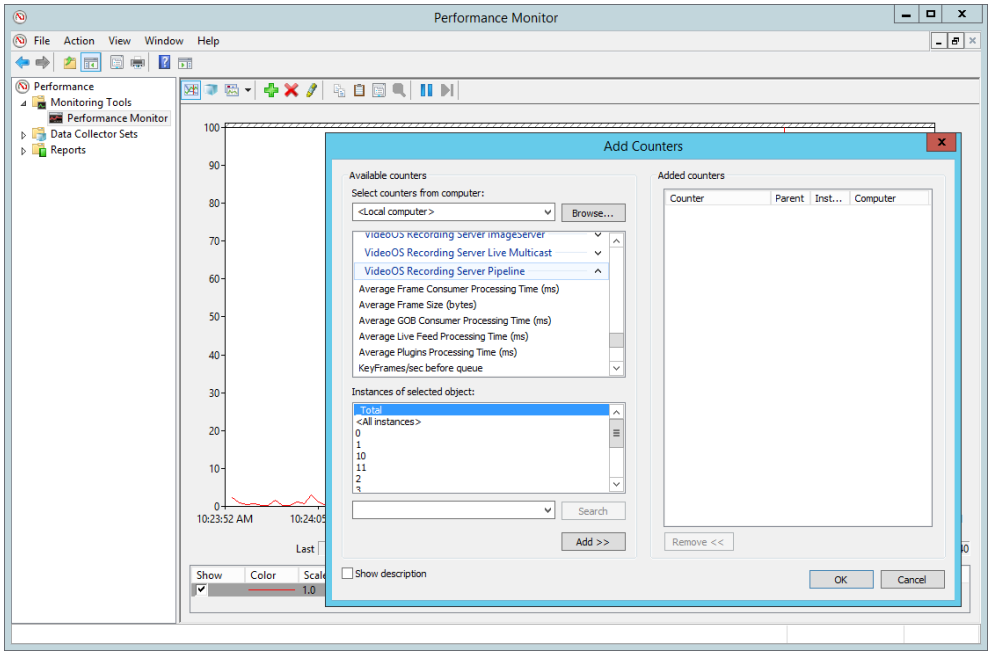
Note: When using both a domain and NTP, it is important to ensure that the domain and NTP are synchronized to the same time source. One way to do this is to install the NTP on one of the servers in the domain.

Windows reliability and Performance Monitor

Performance Monitor is a powerful tool that is built into Windows. It can be used to track various Win-

dows counters over time, such as CPU, network, disk load and I/O, etc.. In addition to the standard Windows counters, it can also monitor counters from other software services if they offer service-specific counters.

Milestone XProtect VMS products support a wide range of VMS-specific performance counters that can be used in the Performance Monitor to monitor the VMS' performance and pinpoint issues or bottlenecks within the VMS or its use of the server hardware.



The Performance Monitor can be started by typing "perfmon" in Windows start menu.

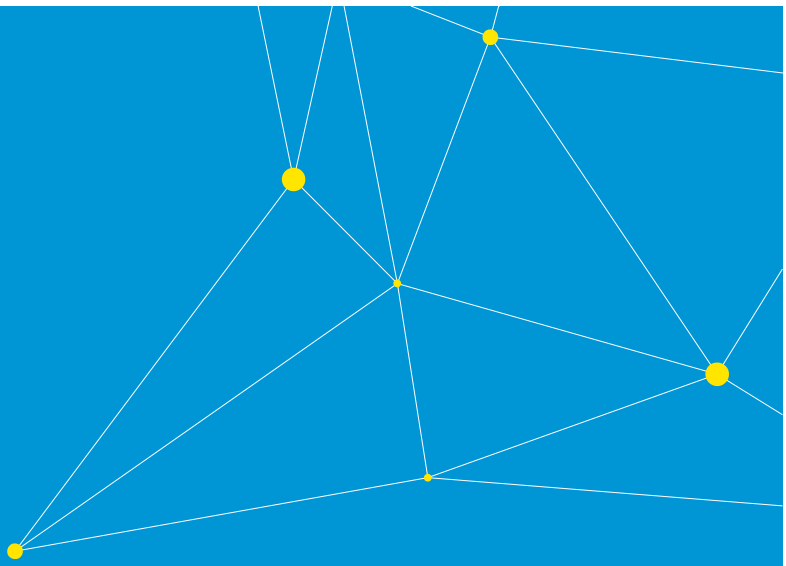
Benefits and summary

As covered in this white paper, Milestone XProtect Corporate, XProtect Expert and XProtect Professional+ are built on a flexible multi-tiered client-server architecture, where the architecture ensures a perfect fit with standard IT technologies, servers, network, and storage. The architecture also provides flexibility and scalability, making the VMS fit installations of any size ranging from small single-server systems with a few cameras, to distributed multi-server and multi-site installations handling thousands of cameras.

The modular system architecture also permits cost-efficient expansion and maintenance of deployed systems since additional recording servers can be added as needed. Secondly, the camera drivers, server components and client applications may be upgraded independently, making it simpler and flexible to upgrade the VMS.

To meet the strictest needs for system security and reliability, the XProtect VMS products offer the possibility to separate the camera network from the client network to eliminate any interference in the video communication between the cameras and the recording servers and traffic on the client network. This physical separation furthermore prevents users, or other unauthorized persons, from gaining access to video or tampering with camera settings. In addition to this, XProtect VMS products provide an array of built-in security and high-availability mechanisms, including support for secure camera communication via HTTPS, fault tolerance using cold-standby or hot-standby failover recording servers and Microsoft Windows Server Failover Clustering (WSFC) or similar third-party software or hardware solutions for other VMS components.

Embracing standard IT technologies and concepts, such as standard IPv4 and IPv6 network communication, VLAN, VPN, Microsoft Active Directory, virtualization technologies, SQL databases and SNMP, XProtect VMS products fit into the existing IT topology. This allows system administrators to apply existing knowledge and IT tools when managing the VMS system, as a complement to the native central management and monitoring functions available via the Management Client. This not only reduces the cost of equipment and training of system administrators, but it also reduces the overall cost of maintaining the system in production.



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 500,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.