System Architecture Guide for IT Professionals

XProtect Corporate
XProtect Expert
XProtect Professional+

Prepared by:
John Rasmussen, Senior Product Manager
Milestone Systems

Date: August 2, 2017
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Purpose and target audience</td>
<td>3</td>
</tr>
<tr>
<td>Designed for network and IT systems</td>
<td>3</td>
</tr>
<tr>
<td>Overall system architecture</td>
<td>6</td>
</tr>
<tr>
<td>System components</td>
<td>6</td>
</tr>
<tr>
<td>Server components</td>
<td>7</td>
</tr>
<tr>
<td>Management server</td>
<td>7</td>
</tr>
<tr>
<td>Failover management server</td>
<td>8</td>
</tr>
<tr>
<td>Recording server</td>
<td>8</td>
</tr>
<tr>
<td>Failover recording server</td>
<td>9</td>
</tr>
<tr>
<td>Event server</td>
<td>9</td>
</tr>
<tr>
<td>Failover event server</td>
<td>10</td>
</tr>
<tr>
<td>Log server</td>
<td>10</td>
</tr>
<tr>
<td>Service channel</td>
<td>11</td>
</tr>
<tr>
<td>Mobile server</td>
<td>11</td>
</tr>
<tr>
<td>SQL server</td>
<td>11</td>
</tr>
<tr>
<td>Client components</td>
<td>12</td>
</tr>
<tr>
<td>Management Client</td>
<td>12</td>
</tr>
<tr>
<td>XProtect Smart Client</td>
<td>13</td>
</tr>
<tr>
<td>XProtect Web Client</td>
<td>13</td>
</tr>
<tr>
<td>Milestone Mobile</td>
<td>14</td>
</tr>
<tr>
<td>Additional products and components</td>
<td>14</td>
</tr>
<tr>
<td>XProtect Smart Wall</td>
<td>14</td>
</tr>
<tr>
<td>MIP SDK</td>
<td>15</td>
</tr>
<tr>
<td>Software Manager</td>
<td>15</td>
</tr>
<tr>
<td>System Implementation Guide</td>
<td>15</td>
</tr>
<tr>
<td>Standard system designs guide</td>
<td>16</td>
</tr>
<tr>
<td>Integration with standard IT technology</td>
<td>22</td>
</tr>
<tr>
<td>Benefits and summary</td>
<td>26</td>
</tr>
</tbody>
</table>
Introduction

XProtect Corporate®, XProtect Expert® and XProtect Professional+® are Milestone 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 “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 Corporate, XProtect Expert and XProtect Professional+ as the VMS, including introducing the system components and the system architecture. Furthermore, this white paper will give recommendations for system layout designs and provide references to more information on specific topics.

This white paper should enable the reader to understand the overall system architecture, the primary system components and their functions, as well as give guidelines to basic system design.

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, maintaining or expanding a VMS system.

The reader is assumed to have a general understanding of administrating IT and network installations. General knowledge about video encoding standards like MJPEG, MPEG4, H.264 and H.265 as well as transmission of video over IP networks is recommended but not required.

Designed for network and IT systems

Milestone XProtect VMS products are from a technical standpoint designed as an IT system, and their general network and client/server design, overall system logic and management principle should be very familiar for IT administrators used to working with large networks and IT systems.

Run on standard IT equipment

- Standard servers of your choice
- Standard storage and configuration of your choice, like SATA, SAS, SSD, DAS, SAN, NAS, iSCSI, etc.
- Standard network equipment with configuration and layout of your choice including support for VLAN, VPN, etc.
- Integrates with the standard Active Directory already present in most installations
- Use standard Microsoft SQL Server for storing the VMS configuration and logs
- Support for port customization and port forwarding to support routed networks and firewalls
**Wide choice of Microsoft® Windows® operating systems, for instance:**
- Microsoft Windows 7 - Professional SP1 and up
- Microsoft Windows 8 - Pro and up
- Microsoft Windows 8.1 - Pro and up
- Microsoft Windows 10 - Pro and up
- Microsoft Windows Server 2012 - Standard and Datacenter
- Microsoft Windows Server 2012 R2 - Standard and Datacenter
- Microsoft Windows Server 2016 - Essentials, Standard and Datacenter

(for an updated list: System Requirements)

**Support virtualization technology**
- Support for VMware
- Support for Microsoft Hyper-V
- All other virtualization technologies supporting Microsoft Windows

**Easy installation and upgrade**
- All XProtect VMS products are offered in trial versions that can be easily upgraded to a paid version without having to redo the installation or configuration
- XProtect Professional+ and XProtect Expert can seamlessly be upgraded to a more advanced XProtect product by applying a new license file; there is no need to reinstall or reconfigure the system
- Installers for server components and clients are hosted on the management server for easy download and distribution so there is no need to use CDs or USB drives to distribute the software
- Easy upgrade or addition of camera drivers on recording servers via dedicated device packs. This means there is no need to upgrade all VMS components and clients to support new camera models or camera firmware

**Flexible deployment that can be scaled over time**
- Scalable distributed system architecture with system components that can be run on one or more dedicated servers or on shared servers depending on system size and configuration. This enables the choice of the most cost-efficient hardware solution for the particular installation, whether it is a small or large 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 management is done through a single Management Client that can run on your local workstation eliminating the need to use remote desktop to access and configure the VMS
- Strict control of access rights to control who can see cameras and other devices as well as what functions users can access
• Built-in server and system monitoring including email notification on events and failures. Alternatively 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 software or hardware solutions, offering server and service failover functionality
• Dedicated hot-standby or cold-standby failover recording servers
• Camera and client networks can be separated to ensure reliable and secure operation of the video system and prevent interference, tampering or hacking via the client network.
• Should cameras be connected via the Internet or used in high-security installations, the camera to recording server communication can be secured by using HTTPS
• If web and mobile clients are used over the Internet the communication can be secured by using HTTPS. Furthermore, the mobile server can be placed in a DMZ (“demilitarized zone”) to protect the integrity of the VMS servers and network.
• For more information and recommendations on securing and hardening the servers, network and VMS installation:
  o White paper - Ensuring end-to-end protection of video integrity
  o Hardening Guide for XProtect VMS

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

Milestone XProtect VMS products are state-of-the-art products designed for advanced high-security, large-scale installations.

To scale to thousands of cameras across multiple sites, the VMS consists of several components handling specific tasks. All components can be installed on the same server if the server can handle the combined load, or the components can be installed on separate dedicated servers to scale and distribute the load. Smaller systems of about 50-100 cameras (depending on hardware and configuration) can run on a single server. For larger systems, it is recommended to use dedicated servers for some of the components.

Furthermore, not all components are needed in all installations, but can be installed if the functionality they offer is needed. For example, failover recording servers and mobile server for hosting and providing access to both the XProtect® Web Client and Milestone Mobile client.

System components

Note:
- XProtect® Smart Wall is an add-on product to XProtect Expert and not supported on XProtect Professional+
- Failover recording servers are not supported on 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 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 on USB sticks and hand carry them to the other servers.

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
When a system is upgraded to a new version the components on the download pages are also upgraded, so during the system upgrade the download page can also be used as a distribution point for other server 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 similar third-party software or hardware solutions, offering server and service failover functionality.

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

For more information on configuring a failover cluster using WSFC:  
[XProtect Advanced VMS - Failover clustering quick guide](#)

**Recording server**

The recording server is responsible for all communication with devices (cameras, video and audio encoders, input/output (I/O) modules, metadata sources, etc.), recording and event handling, for example:

- Retrieve video, audio, metadata and I/O event streams from the devices
- Record video, audio and metadata
- Provide access to live and recorded video, audio and metadata
- Provide access to device status
- Trigger system and video events on device failures, events, etc.
- Perform motion detection and generate Smart Search metadata

Furthermore, the recording server is responsible for communicating with other Milestone products when using the Milestone Interconnect technology.

For more information on Milestone Interconnect:  
[White paper - Milestone Interconnect](#)

**Device drivers**

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

The device drivers are by default installed as part of a device pack when the recording server is installed, but can later be updated by downloading and installing a newer version of the device pack. New device packs are typically released every other 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 is stored in the dedicated Milestone-developed, high-performance media database which is optimized for recording and storing video, audio and metadata.

The media database supports various unique VMS features like tiered multistage archiving, video grooming, Scalable Video Quality Recording™ (SVQR) encryption and adding a digital signature to the recordings. Furthermore, the tiered multistage storage architecture enables the “live” recording database and the archives to be distributed across different storage systems and technologies, making it possible to design and optimize the storage solution for both performance (recording), size (retention) and cost.

**Failover recording server**
The failover recording server is responsible for taking over the standard recording server tasks should a 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 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 in advance know which server to take over. This means that it cannot preload the configuration and startup its process until a recording server actually fails which adds time to the failover startup time.

In hot-standby mode the failover time is significantly shorter because the failover recording server already knows which recording server from which it should take over recording and thus can preload the configuration and start up completely - except for the last step of connecting to the cameras.

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

**Event server**
The event server handles various tasks related to events, alarms, maps and third-party integrations via the Milestone Integration Platform Software Development Kit (MIP SDK).

**MIP SDK - Events and actions:**
All system events are consolidated in the event server so there is one place and interface for partners to make plug-ins and integrations that use system events or introduce custom events and rule engine actions
Alarms:
The event server hosts the alarm feature, alarm logic, alarm state as well as handling the alarm database.

Maps and Smart Maps:
The event server hosts the “classic” maps and “new” Smart Map that are configured and used in 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 standardized access control plug-ins. When integrated both the video cameras 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 (license plate recognition) enables detection and registration of license plate information from vehicles and links the license plate information with video.

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

All data handled by the event server, such as alarms, maps and data from add-on products are stored in the same SQL server the management server uses.

Failover event 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 similar third-party software or hardware solutions, offering server and service failover functionality.

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

For more information on configuring a failover cluster using WSFC: XProtect Advanced VMS - Failover clustering quick guide

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

The system can log three types of logs:
- System log:
The system administrator can choose to log errors, warnings, information and combinations of these. 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

### Service channel

The service channel is responsible for communicating various service and configuration messages to the XProtect Smart Client and mobile server, and third-party components listening to the service channel. This could, for example, be communicating updates to an XProtect Smart Wall monitor layout or communicating that a failover server has now taken over for a recording server.

### Mobile server

The mobile server is responsible for hosting the XProtect Web Client and for providing access to the VMS for the XProtect Web Client and Milestone Mobile client users.

In addition to acting as a system gateway for the Milestone Mobile client and XProtect Web Client, the mobile server also transcodes video for the web and mobile clients. The reason video transcoding is needed is to ensure support for all video codecs and resolutions, like for instance H.264, H.265 and UHD/4K video, which natively are not supported by all web browsers and smart phones. Secondly, transcoding also may reduce the video resolution and lower the bandwidth needed to send the video.

Because the video streams to Milestone Mobile and XProtect Web Client always are transcoded, which is a resource-demanding task, it is highly recommended to install the mobile server on a dedicated server – preferably one that supports hardware accelerated transcoding using Intel Quick Sync Video.

### 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 and offer automatic backup functionality.

As with all other IT systems it is important to configure scheduled backup of the database so that configuration is not lost in case of failures.
Client components

Management Client

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

The VMS is designed for large-scale operation and the Management Client is thus designed to be run remotely from, for example, the 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.

Selecting a node will show the settings for this node, typically in a second tree structure because there often are more sub items that can be managed (2). When an item is selected, the settings are displayed in the properties dialog shown in the right side of the client (3). Items can have many settings, and if so the different settings are grouped on different tabs.

Selecting cameras, a preview of the selected group or camera are shown below the settings (4).
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 dedicated operators.

The XProtect Smart Client is designed to be run remotely on the operator’s computer and supports 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 tasks: live monitoring, playback and investigation; Sequence Explorer for investigation; alarms for alarm management and system monitor for monitoring the state of the system servers, cameras, storage, etc. Add-on products and third-party integrations can add additional tabs providing a dedicated user interface for their functions for instance for XProtect Access, XProtect LPR or XProtect Transact.

For more information about the XProtect Smart Client visit the Milestone website.

XProtect Web Client
The XProtect Web Client is the client designed for the occasional or remote user that needs easy access to live monitoring, playback, investigation, export and light alarm management.

For more information about the XProtect Web Client visit the Milestone website.

Compatible browsers can be found here on the XProtect Web Client tab:
System requirements and supported browsers
Milestone Mobile

Milestone Mobile is the client designed for the user on-the-go. It offers easy access to live and playback of cameras, as well as access to doing investigations and managing alarms.

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

Milestone Mobile is available for Apple®, Android™ and Windows Phone devices.

For more information about Milestone Mobile visit the Milestone website.

Compatible smartphone operating systems can be found here on the Milestone Mobile tab: 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 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 centers.

XProtect Smart Wall is fully integrated with XProtect Smart Client allowing users to control the XProtect Smart Wall in an easy and intuitive way and view shared content from the XProtect Smart Wall 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 using the VMS’ rule system on events and/or time schedule, or via MIP SDK integrations.
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 support for XProtect Professional+.

For more information about XProtect Smart Wall visit the Milestone website.

**MIP SDK**

The MIP SDK is a comprehensive tool that facilitates the integration of applications for Milestone’s VMS. The MIP SDK provides flexible access to video, audio, events, metadata and configuration data as well as optimized functions for access control integration. The MIP SDK extends the software’s functionality by allowing developers to create new and powerful surveillance solutions optimized for a specific system and purpose.

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 about the MIP SDK: Milestone Integration Platform Software Development Kit visit the Milestone website.

**Software Manager**

The Software Manager is a tool that from a central point can be used to remotely install and upgrade recording servers, recording server device packs and XProtect Smart Clients on servers or PCs in the network. For larger installations, the tool makes it easy and fast to upgrade the components that are installed remotely and in many places; namely the recording servers and their device packs as well as all the client PCs.

For more information about Software Manager visit the Milestone website.

**System Implementation Guide**

**VMS design:**

In addition to the system designs presented in the below guide, it is of course possible to design the VMS in other customized ways to suit specific cases as well as to use specialized or high-performance equipment and technologies like virtualization, hardware and software redundancy, etc.

**Number of cameras per recording servers:**

The guide and the designs do not consider the number of cameras you can run per recording server, but reflect a location (physical or virtual in a network) of the recording server. This means that the recording server symbol in the below designs should not be taken literally as one single recording server but more as an indication of the recording server functionality in the location, which then could be covered by one or more recording servers.
**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 the below design guide our pre-sales team can be contacted at presales@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 VMS installations with a “typical” design using off-the-shelf equipment, the below design guide can help illustrate the right way to implement the system.

![Surveillance Project Guide Diagram](image-url)
Design 1 – Single system. Less than five cameras / Demo system

This VMS design is the simplest possible design where everything is connected to the same network and all server components and clients run on the same server/PC.

Typically, you would run the management server, recording server and XProtect Smart Client(s) on separate servers/PCs, but if the server/PC is powerful enough or you just have a few cameras, everything could be installed on a single server (or laptop for demonstration purposes).

Design 2 – Single system. Up to 100 cameras

This VMS design is the basic design with all cameras, server components and clients connected to the same network.

Typically, you would run the management server and recording server on separate servers as shown in the diagram, but if the server is powerful enough or you have just a small number of cameras, the recording server could be installed on the same server as the management server.

If uninterrupted video operation is needed, a separate failover recording server can be added.
Note: When the system is larger than 300 cameras it is recommended to use a full version of the SQL server and run it on a dedicated server.

Furthermore, when having many cameras in the system, it is recommended to separate the client network from the camera network by creating a separate camera network for each recording server and its cameras.

Separating the client network from the camera 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 clients and other equipment on the client network cannot contact the camera directly and hack into the camera to change settings or in any other way interfere with the operation
- Dimensioning of the network is made easier because the load is separated to several different networks where the load, especially on the critical camera network, easily can be calculated
Design 4 – Single system, multiple sites. No direct user access in remote sites

This design is in essence the same as design 3, with the difference that each recording server is not located on the main site with the management server and users, but on separate physically remote sites.

The advantage of placing the recording servers on the remote sites is that the network connection to the central site does not need to be so fast that video from all cameras can be transferred to the central site simultaneously. The network bandwidth only needs to be fast enough for transferring the video from the number of cameras viewed in live or played back at the same time on the central site.

As an example:
Each recording server records 100 cameras at 1080p 25/30 FPS at 4 Mbit/s H.264
Users view max. 10 cameras at the same time per site

Placing recording servers on the central site, a bandwidth of 100 * 4Mbit/s = 400 Mbit/s is needed 24/7 per recording server. Placing recording servers on the remote sites, only bandwidth for the cameras viewed by users 10 * 4Mbit/s = 40 Mbit/s are needed – and this only during the periods where cameras actually are viewed 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 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 users access video locally on each of the sites, it is recommended to design the system using Milestone Federated Architecture. Milestone Federate Architecture requires that all sites are on the same Microsoft Windows domain or that a domain trust has been established between the different Microsoft Windows domains.

Furthermore, the network connections between the different sites must be fairly stable and have enough bandwidth for the required use. If this is not the case, log in may take a long time and the video experience may be poor.

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 on Milestone Federated Architecture:
White Paper - Milestone Federated Architecture
Design 6 – Multiple systems, multiple sites. Direct user access to remote sites using Milestone Interconnect

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, intermittent, have limited bandwidth or have servers which are not part of the central site’s Microsoft Windows domain, it is recommended to design the overall system using Milestone Interconnect.

With Milestone Interconnect, a Microsoft Windows domain trust is not needed, and furthermore sites running a broader range of Milestone VMS products and versions can be interconnected compared to Milestone Federated Architecture.

Milestone Interconnect is therefore well suited to connect VMS systems from multiple independent surveillance installations to a central site, for instance in a transportation or city surveillance installation

Milestone Interconnect 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 rights can be set and controlled per site
  - It is possible to interconnect a broader range of Milestone VMS products and versions compared to Milestone Federated Architecture
• Seamless access
  o Users on the central site can access the central and interconnected remote sites seamlessly via a single log-in
  o 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
  o With Milestone Interconnect it is possible to automatically retrieve the recordings made on the remote system when the network connection to the remote site is restored. This could for instance be used for surveillance in vehicles like cars, buses, trains and ferries
  o In addition to automatic retrieval, the system offers rule, schedule, user-activated and MIP SDK activated retrieval of recordings
  o Alternatively, recordings from the remote site can be played back seamlessly on the central site without first having to transfer them to the central site

• Network connection
  o With Milestone Interconnect the system can automatically handle unstable and intermittent network connections between the central and remote sites without impacting client log-on time, performance, operation or management of the central or remote site

In addition to the advantages listed above, Milestone Interconnect offers a long list of advanced functions and benefits. 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 the IT administrator. 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 is just video streams instead of files, transactions, business data, etc.

The below list are 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.

Furthermore, Active Directory provides time synchronization between servers, which is important for proper system operation.
**SQL server**

For installations with less than 300 cameras, the included free SQL Server Express edition can be used, but in general it is recommended to use a full version of Microsoft SQL Server as it offers better performance and most importantly, it offers scheduled backup of the database.

The whole system configuration is stored in the SQL server, so it is important to configure a regular backup of the VMS configuration database and not just make a manual one-time backup through the Management Client, because this backup will quickly become outdated due to configuration changes, such as replacing cameras, adding/deleting users, changing camera settings, etc.

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

**Virtualization**

Virtualization technologies like Microsoft Hyper-V and VMware can be used for all Milestone XProtect software and their individual components, and they are used widely within R&D in Milestone Systems during development, test, support, etc.

For the majority of installations, it is commonplace to run the management server and event server in a virtual environment and there are many benefits to doing so as the resource consumption normally is minimal and the benefits of high availability and zero downtime maintenance for these components are very desirable.

For the recording server or failover recording server the benefits of running them in a virtual environment is typically smaller as the recording server often uses a very high percentage of the server resources.

There are though some installations where virtualization of the recording servers may be desirable:

- If the physical recording servers require zero down time during maintenance, then features such as VMotion (for VMware) or Live Migration (for Hyper-V) would be beneficial.
  - VMotion and Live Migration have both been successfully tested with the recording server and failover recording server
- For use with a failover recording server to provide failover capability to multiple recording servers at the same time. As a single failover recording server only can provide failover capabilities to a single recording server at a time, virtualization can be used to accommodate multiple failover recording server instances on a single hardware platform

When using a virtual environment, each virtual server should be allocated at least the same resources as would be for a physical server.

**VLAN**

It is possible to use VLAN with Milestone XProtect software to segment and separate
the network and its traffic. If using VLAN to segment and share network equipment between standard network traffic and video surveillance traffic, 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 permanent load on the network because video from all cameras typically is streamed permanently to the recording servers.

A quick example: A recording server with 100 cameras configured with H.264 1080p resolution at 25/30 frames per second using 4 Mbit/s per camera amounts to a constant 400 Mbit/s load on the network to the recording server.

In addition to the constant traffic from the cameras to the recording server, the traffic from the recording server to the clients must also be taken into account.

**Firewall**
The video streams from the Milestone XProtect software can be streamed through firewalls by permitting/forwarding the used ports and protocols. This allows for cameras or clients to be located outside the local network, for instance on public Internet.

Please consult the software documentation or the system architecture document for an overview of used ports and protocols.

**VPN**
If clients or cameras are connected via public Internet, a standard VPN can be used to further protect and encrypt the audio and video streams and video surveillance system communication.

**IPv4 and IPv6**
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., standard IT monitoring products, and software already known by the IT administrators can also be used to monitor the health and status of the equipment running the VMS. This makes it easy to integrate Milestone XProtect software in existing IT infrastructure and work processes.

In extension to external system monitoring tools, Milestone XProtect Expert and XProtect Corporate support a built-in monitoring function with 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 like storage and network use per camera.

Note: The system monitor is not supported on XProtect Professional+

**Email**
In addition to the technical monitoring mentioned above, 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, when Edge Storage is used in the cameras or when the cameras are interconnected to a central XProtect Corporate system, it is necessary to set up a Network Time Protocol server (NTP) and configure the cameras and VMS servers to synchronize their time with the NTP server or Domain controller.

If this is not done, the video overlaid timestamps will, over time, drift and deviate from the VMS time stamps because the camera clocks are not very precise. When using Edge Storage and Milestone Interconnect the solution will stop working if the camera and/or interconnected systems server time are too far apart from the VMS server’s time.

**Windows reliability and performance monitor (Perfmon)**
Perfmon is a powerful performance monitoring tool that is built into Windows. It can be used to track various windows counters like CPU, network, disk load and I/O, etc., over time. 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 Perfmon counters that can be used to monitor the VMS’ performance and pinpoint issues or bottlenecks within the VMS or its use of the server hardware.

Perfmon can be found and started by typing “perfmon” in the start menu search/command field.
Benefits and summary

As discussed in this white paper, Milestone XProtect Corporate, XProtect Expert and XProtect Professional+ are built on a flexible multi-tiered client-server architecture, where the flexible architecture ensures compatibility with standard hardware, storage and IT technologies. This enables full system scalability of the VMS solution, from small single-server systems, to distributed multi-thousand camera systems that are integrated with standard IT systems, enabling the most optimal hardware technology platform to be selected for a given customer application considering cost and performance.

The modular system architecture also permits cost-efficient expansion and maintenance of systems in service as additional recording servers can be added when and as needed. Secondly the camera drivers, server components and client applications may be upgraded independently.

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.
About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit www.milestonesys.com

Milestone Systems Headquarters, DK
Tel: +45 88 300 300

Milestone Systems US
Tel: +1 503 350 1100