milestone

The open platform company

White paper

XProtect Expert and XProtect Corporate - System Architecture Guide for IT Professionals

Prepared by:

John Rasmussen, Senior Technical Product Manager, Corporate Business Unit

Milestone Systems

Date: August 26, 2014

Table of Contents

Introduction

XProtect Expert® and XProtect Corporate® are high-end Milestone video management software (VMS) designed for complex and large-scale installations.

Throughout this white paper, XProtect Expert and XProtect Corporate are referred to as the "VMS" because they share the same architecture and components.

Purpose and target audience

The purpose is to provide insight to the benefits and ease of using Milestone XProtect Expert and XProtect Corporate 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 links 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 Expert and XProtect Corporate VMS products who are in the process of selecting, deploying, administrating, maintaining and 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 and H.264 as well as transmission of video over IP networks is recommended but not required.

Designed for network and IT systems

Milestone XProtect Expert and XProtect Corporate 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 and any 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
- 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
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

(See also: http://www.milestonesys.com/SystemRequirements/)

Support virtualization technology
- Support for VMware
- Support for Microsoft HyperV

Easy installation and upgrade
- Both products are offered in trial versions that can be easily upgraded to a paid version without having to redo the integration or configuration
- XProtect Expert can seamlessly be upgraded to XProtect Corporate by inserting a new license file; there is no need to reinstall or reconfigure anything
- 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 via dedicated device packs so there is no need to upgrade all 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 http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Federated_Architecture_with_synapsis.pdf
- Support for Milestone Interconnect™ to tie independent systems together http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Interconnect.pdf

Central management and monitoring

- All management is done through a single Management Client that can run on your local workstation so there is no need to use remote desktop to access and configure the VMS
- Strict control of access rights to control who can see the cameras and 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
- Camera and client networks can be separated to ensure reliable and secure operation of the video system, because any interference on the client network does not interfere with video recording from the camera network. Furthermore, because cameras cannot be accessed from the client network there is no risk that users or other unauthorized persons can access or hack cameras and tamper with settings or gain access to video
- 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
  http://www.milestonesys.com/SharePoint/White%20papers/Ensuring_end-to-end_protection_of_video_integrity.pdf
- Redundancy supported via Microsoft clustering on the management servers and dedicated hot-standby or cold-standby failover recording servers

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 IP/MAC). See supported hardware page for an overview of licenses needed per device type
    http://www.milestonesys.com/Supported-hardware-XProtect-Corporate/
  - o Mandatory Software Upgrade Plan for the first year gives access to new product versions for free
- No license cost on storage amount used
- No license cost on clients because they are free of charge
- Predictable maintenance cost because the system runs on standard IT equipment

Overall system architecture

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

In order to be able to scale to thousands of cameras across multiple sites, the VMS consists of several components that handle specific tasks. All components can be installed on the same server if the server is able to 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, where as it is recommended to use dedicated servers for some of the components in larger systems.

Furthermore, not all components are needed in all installations, but they 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.

The below diagram shows an overview of the different system components and further down there is a general description of each component.

System modules
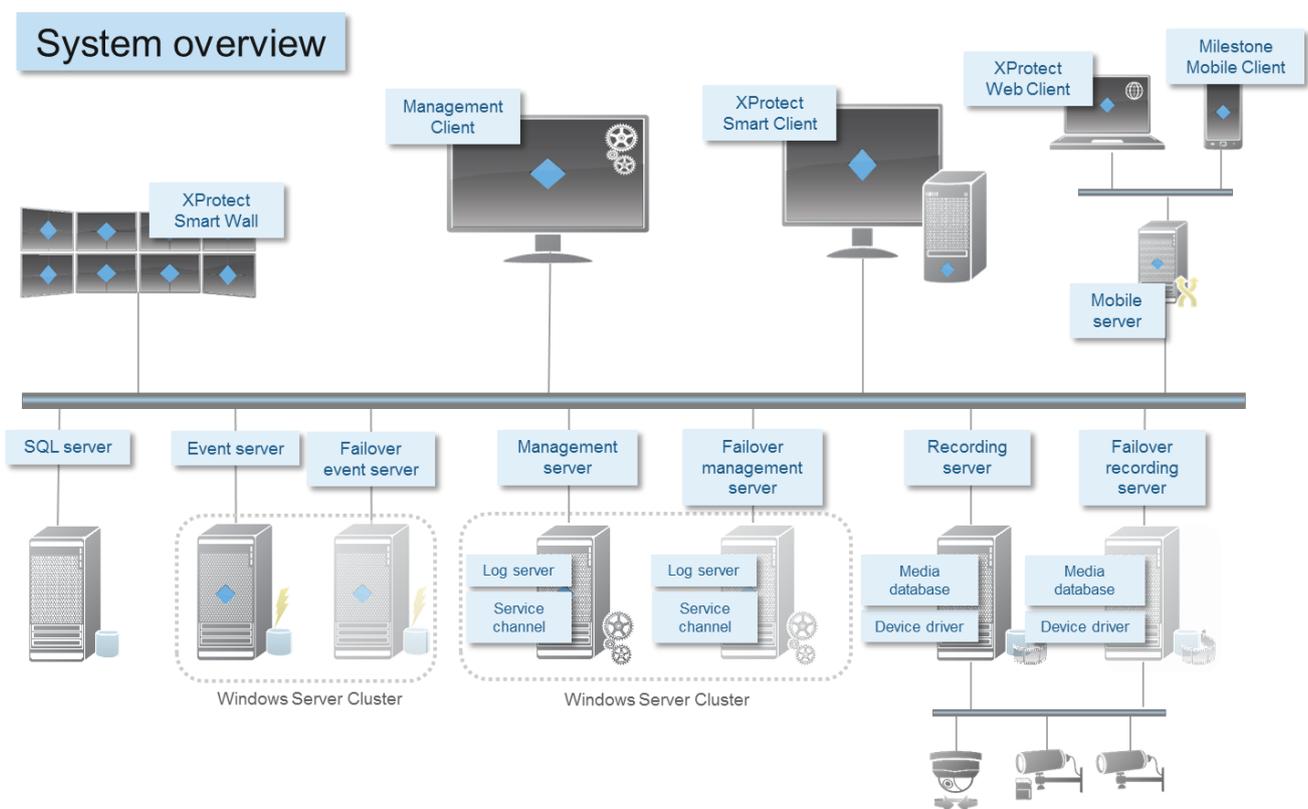
Note:
  - Failover recording servers are not supported in XProtect Expert
  - XProtect® Smart Wall is an add-on product to XProtect Expert

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 components and clients repository
In addition to the management server's VMS function, the management server also hosts a repository of all other system components. Two dedicated download pages for server components and client applications makes it easy and convenient for administrators or integrators to download and install the other system components and client applications on additional servers and workstations, without the need to copy the component installers on USB sticks and manually carry them to the other servers.

Client download page (does not require log in): http://[server-address]/installation/

Server component download page (may require log in): http://[server-address]/installation/admin
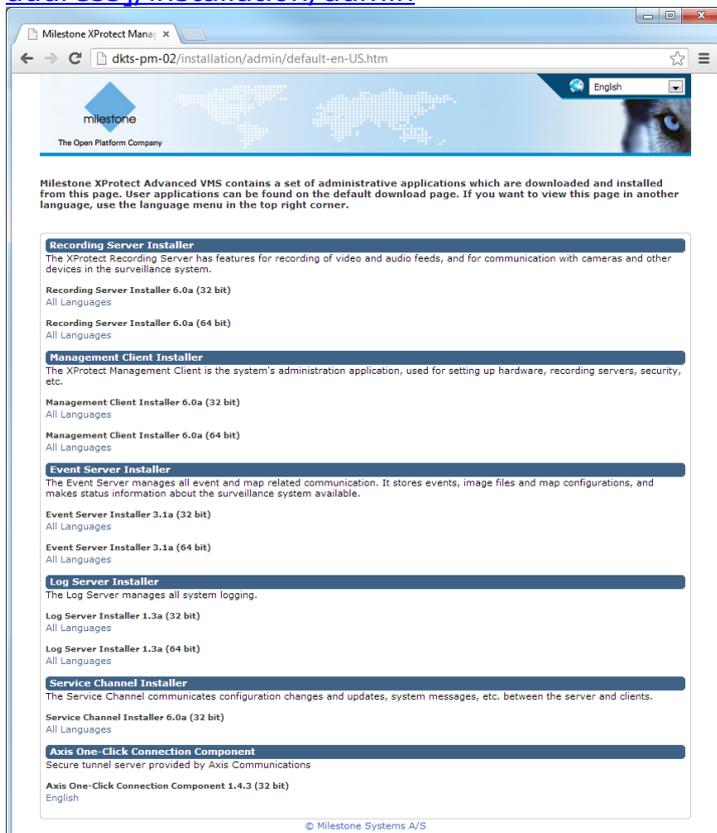
When a system is upgraded to a new version the components on the download pages are also upgraded, so during the system upgrade the download page can also be used as a distribution point for the other server components that should be upgraded. When Milestone releases new add-on components or versions of existing components or clients they can be downloaded from the Milestone website and placed on this download page for further download and distribution in the video surveillance installation.

Updated versions of the VMS, components and clients can be found here: http://www.milestonesys.com/downloads/. Look for "Server-side" installers on the web page to download and install updated components and clients on the VMS download page.

Failover management server

Failover support on the management server is achieved by installing the management server in a Microsoft Windows Cluster. The cluster will then ensure that another server takes over the management server function, should the first server fail.

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

For more information on configuring clustering in Microsoft Windows Server 2012 R2: http://technet.microsoft.com/library/hh831579.

Recording server

The recording server is responsible for all devices (cameras, video and audio encoders, input/output (I/O) modules, metadata sources, etc.) communication, 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: http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Interconnect.pdf.

Device drivers

An essential part of the recording servers is 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 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 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:
http://www.milestonesys.com/Supported-hardware-XProtect-Corporate/.

New device packs can be downloaded here:
http://www.milestonesys.com/Support/downloads/
(select "Device Packs" in the "Type" dropdown).

Media database
The retrieved video, audio and metadata is stored in the Milestone dedicated high-performance media database optimized for recording and storing video, audio and metadata.

The media database supports various unique features like tiered multistage archiving, video grooming, encryption and adding a digital signature to the recordings.
The media database supports a tiered storage architecture with "live" recording database and the archives 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.

For more information on the media database and the storage architecture:
http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Storage_Architecture_with_synapsis.pdf.

Failover recording server
The failover recording server is responsible for taking over the recording task should a recording server fail.

The failover recording server can operate in two modes:
- Cold-standby for monitoring multiple recording servers
- Hot-standby for monitoring a single recording server

The difference between the cold-standby and hot-standby failover modes is that in the standard failover mode the failover recording server does not know from which server to take over recording, so it cannot start until a recording server fails. In the 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 pre-load the configuration and start up completely, except for the last step of connecting to the cameras.

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).

Events:
> All system events are consolidated in the event server so there is one place and interface for partners to make integrations that use system events.
>
> Furthermore, the event server offers third-party access to sending events to the system via the generic events or analytics events interface.

Alarms:
> The event server hosts the alarm feature, alarm logic, alarm state as well as handling the alarm database.

Maps:
> The event server also hosts the maps that are configured and used in the XProtect® Smart Client.

MIP SDK:
> Finally, third-party developed plug-ins can be installed on the event server and access system events.

All data handled by the event server, such as alarms, maps and event logs, 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 Microsoft Windows Cluster. The cluster will then ensure that another server takes over the event server function should the first server fail.

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

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

Log server

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

The system can log three types of logs:
- **System log:** the system administrator can choose to log errors, warnings and information 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 now is active and the address of it.

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 Milestone Mobile and XProtect Web Client, the mobile server also offers video transcoding capabilities because the original camera video stream in many cases is too large to fit the bandwidth available for the mobile and web users.

The video streams to Milestone Mobile and XProtect Web Client by default are transcoded, so it is highly recommended to install the mobile server on a dedicated server, or install the video decoder plug-in in the browser so the streams can be retrieved and decoded in the original format without transcoding them.

SQL server

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

The XProtect Expert/XProtect Corporate installer includes Microsoft SQL Server 2012 Express that can be used freely.

For larger systems more than 300 cameras it is recommended to use the SQL Server 2008 R2 Standard or Enterprise edition on a dedicated server, because these editions can handle larger databases and offer 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 for XProtect®

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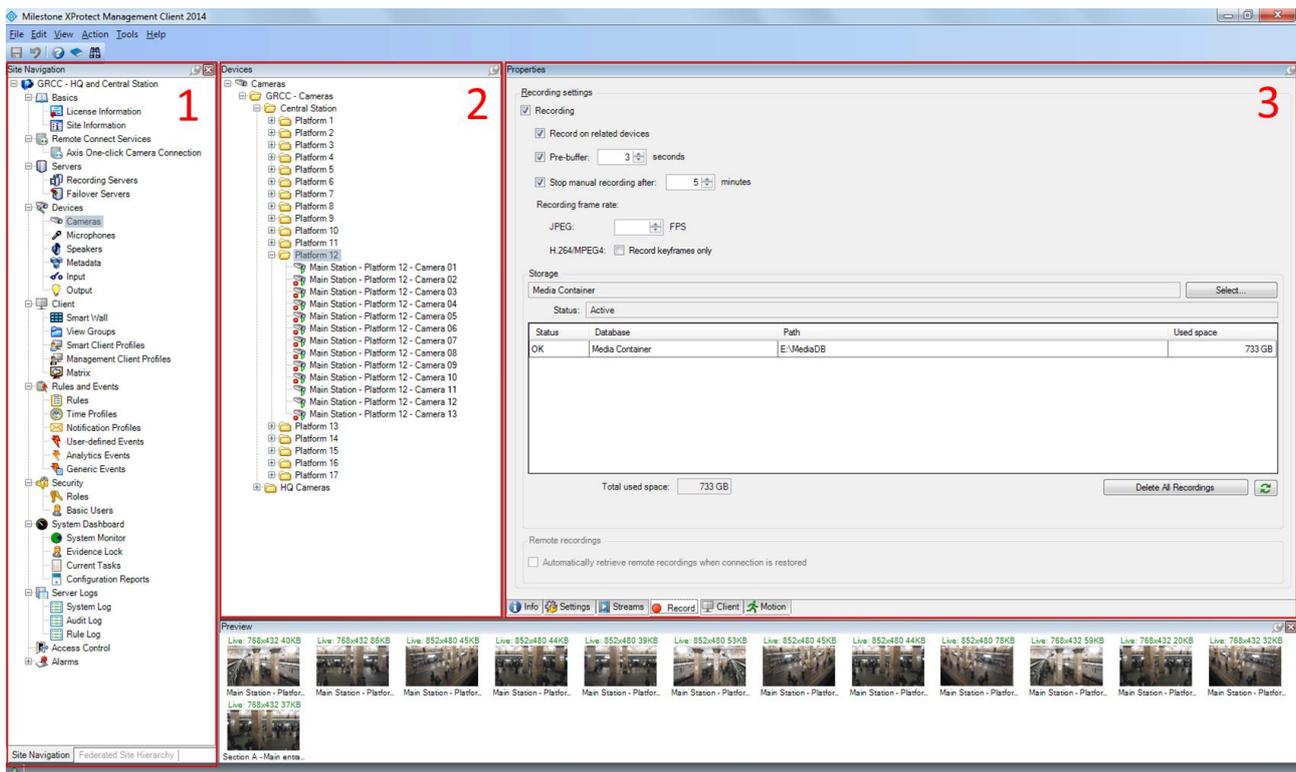
The Management Client has a "Site Navigation" tab (1), where nodes for various parts or functions of the system can be selected, for instance cameras, as shown on the above screenshot.

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.

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.
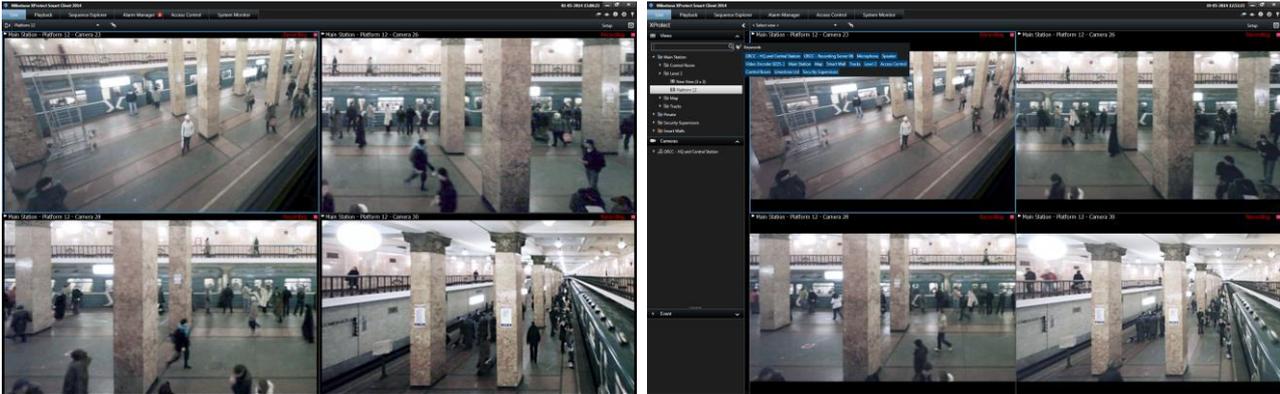
Furthermore, the XProtect Smart Client has tabs dedicated to different tasks: live monitoring, playback and investigation, Sequence Explorer for investigation, alarms for alarm management and system monitor for monitoring the state of the system servers, cameras, storage, etc. Add-on products and third-party integrations can add additional tabs providing a dedicated user interface for their functions.

For more information about the XProtect Smart Client:
http://www.milestonesys.com/xprotectsmartclient/.

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 and export. Furthermore, the XProtect Web Client gives access to activate system events and outputs.
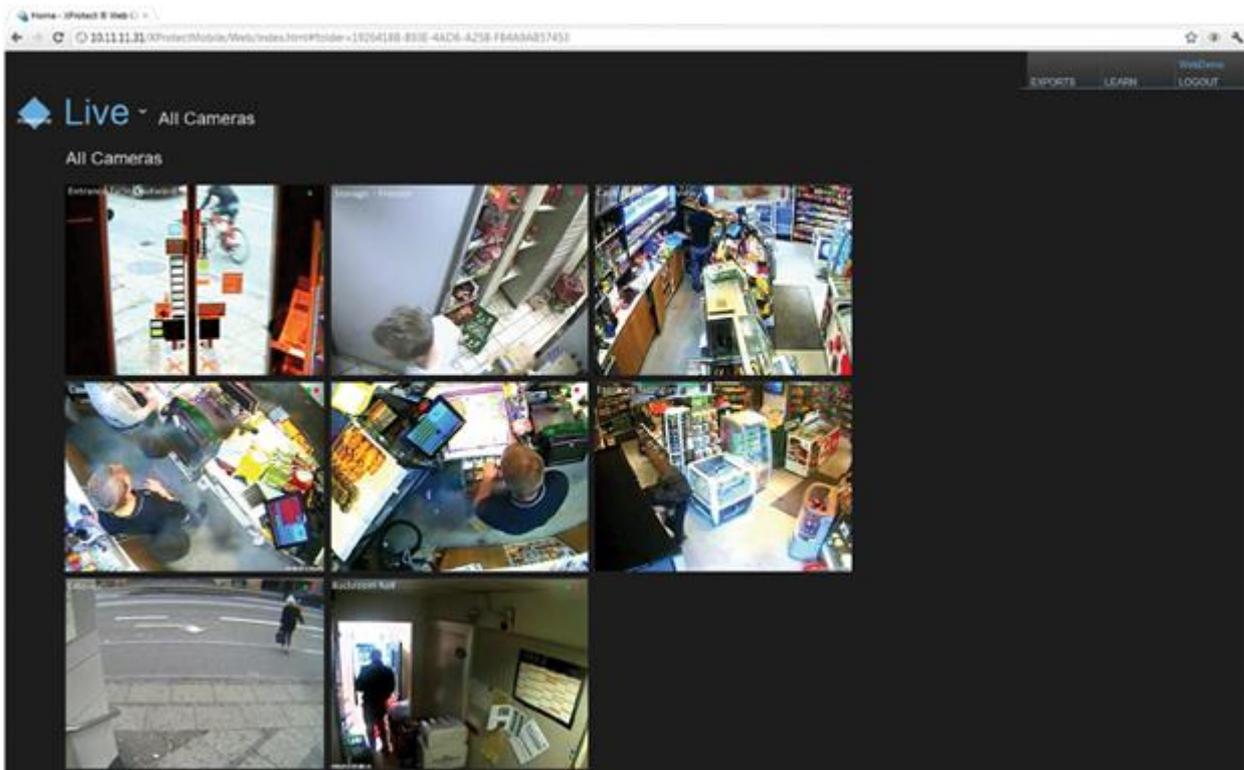
For more information about the XProtect Web Client:
http://www.milestonesys.com/xprotectwebclient/.

Compatible browsers can be found here: (click on XProtect Web Client)
http://www.milestonesys.com/SystemRequirements/.

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 activate system events and outputs.

Furthermore, the Milestone Mobile client can be used as a remote recording device by using the device's built-in camera and the Milestone Video Push feature. 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 8 devices.

For more information about Milestone Mobile:
http://www.milestonesys.com/xprotectmobile/.

Compatible smartphone operating systems can be found here: (click on Milestone Mobile)
http://www.milestonesys.com/SystemRequirements/.

Additional products and components

In addition to Milestone XProtect Expert and XProtect Corporate VMS, Milestone has a set of add-on products and utilities, of which the most important ones are highlighted below.

XProtect Smart Wall 2014

XProtect Smart Wall 2014 is a Milestone video wall product.

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

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

XProtect Smart Wall does not require installation of additional components or clients. All XProtect Smart Wall components are natively embedded in the VMS and the XProtect Smart Client. All that is needed is a license that includes XProtect Smart Wall.

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

For more information on XProtect Smart Wall:
http://www.milestonesys.com/xprotectsmartwall/.

MIP SDK

The MIP SDK is a comprehensive tool that facilitates the integration of applications for Milestone VMS. The MIP SDK provides flexible access to video, 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:
http://www.milestonesys.com/mipsdk/.

Software Manager

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

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

http://www.milestonesys.com/utilities/.

System Implementation Guide

Important notes:

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 redundancy, etc.

Number of cameras per recording serves: The guide and the designs do not consider the number of cameras you can run per recording server, but reflect a location (physical or in the 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 assistance with server requirements, larger VMS projects or projects with more specialized requirements than the ones covered in the below design guide, please use our request form on the web page below or contact your local Milestone representative.
http://www.milestonesys.com/serverspecs/.

Storage needs: Recording server storage estimators can be found here:

MPEG4/H.264 http://www.milestonesys.com/storagecalculatormpeg4/.

MJPEG http://www.milestonesys.com/storagecalculatorjpeg/.

Standard system designs guide

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

For VMS installations with a "typical" design and configuration running on off-the-shelf equipment, the below design guide can help illustrate the right way to implement the system.

Surveillance Project Guide

Physical Location
- Single site
- Multiple sites

Number of cameras (Single site)
- <5 cameras/Demo system
- 5-100 cameras
- >100 cameras

Reliable Network Connection (Multiple sites)
- Yes
- No

Local Site Access (Reliable Network Connection: Yes)
- No
- Yes

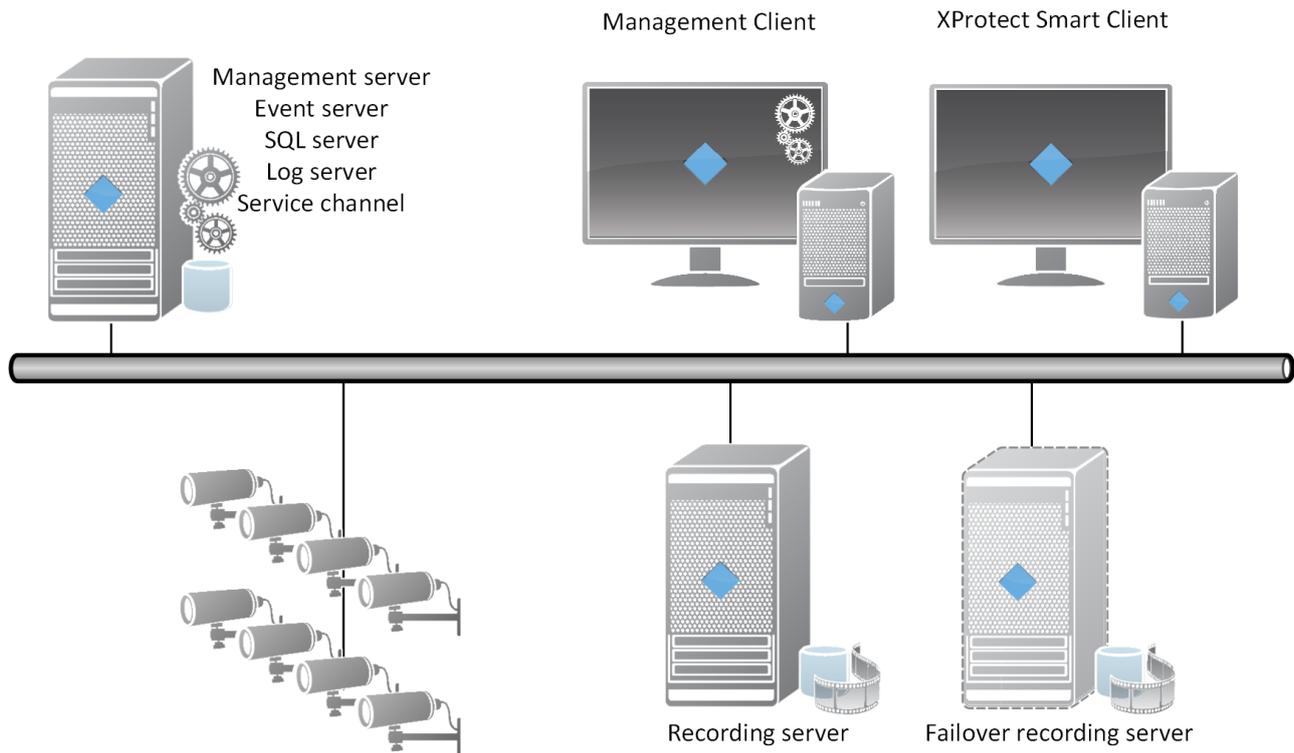| Design 1	Design 2	Design 3	Design 4	Design 5	Design 6
Single System <5 cameras / Demo System	Single System 5-100 cameras	Single System >100 cameras	Single System Multiple Sites	Multiple Systems Multiple Sites — Milestone Federated Architecture	Multiple Systems Multiple Sites — Milestone Interconnect

Design 1 – Single system. Less than five cameras / Demo system

Management Client
XProtect Smart Client

Management server
Recording server
Event server
SQL server
Log server
Service channel
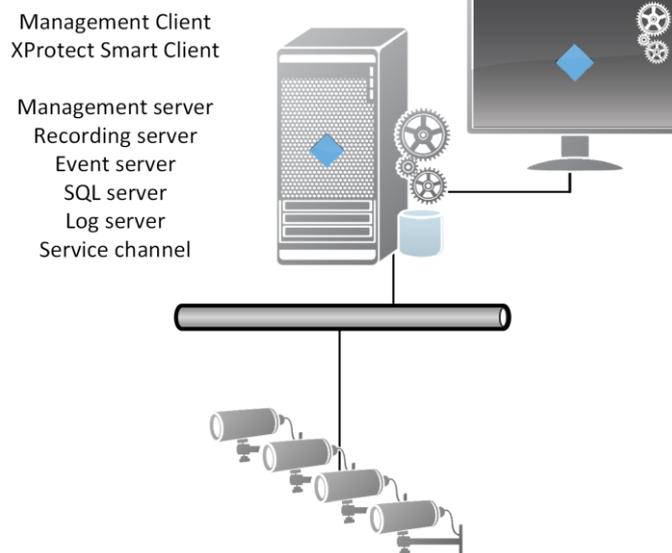
This VMS design is the simplest possible design where everything is connected to the same network and all server components and clients run on the same server/PC.

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 and 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

Management Client   XProtect Smart Client

Management server
Event server
SQL server
Log server
Service channel

Recording server   Failover recording server

This VMS design is the most 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 failover recording server can be added.

## Design 3 – Single system. More than 100 cameras
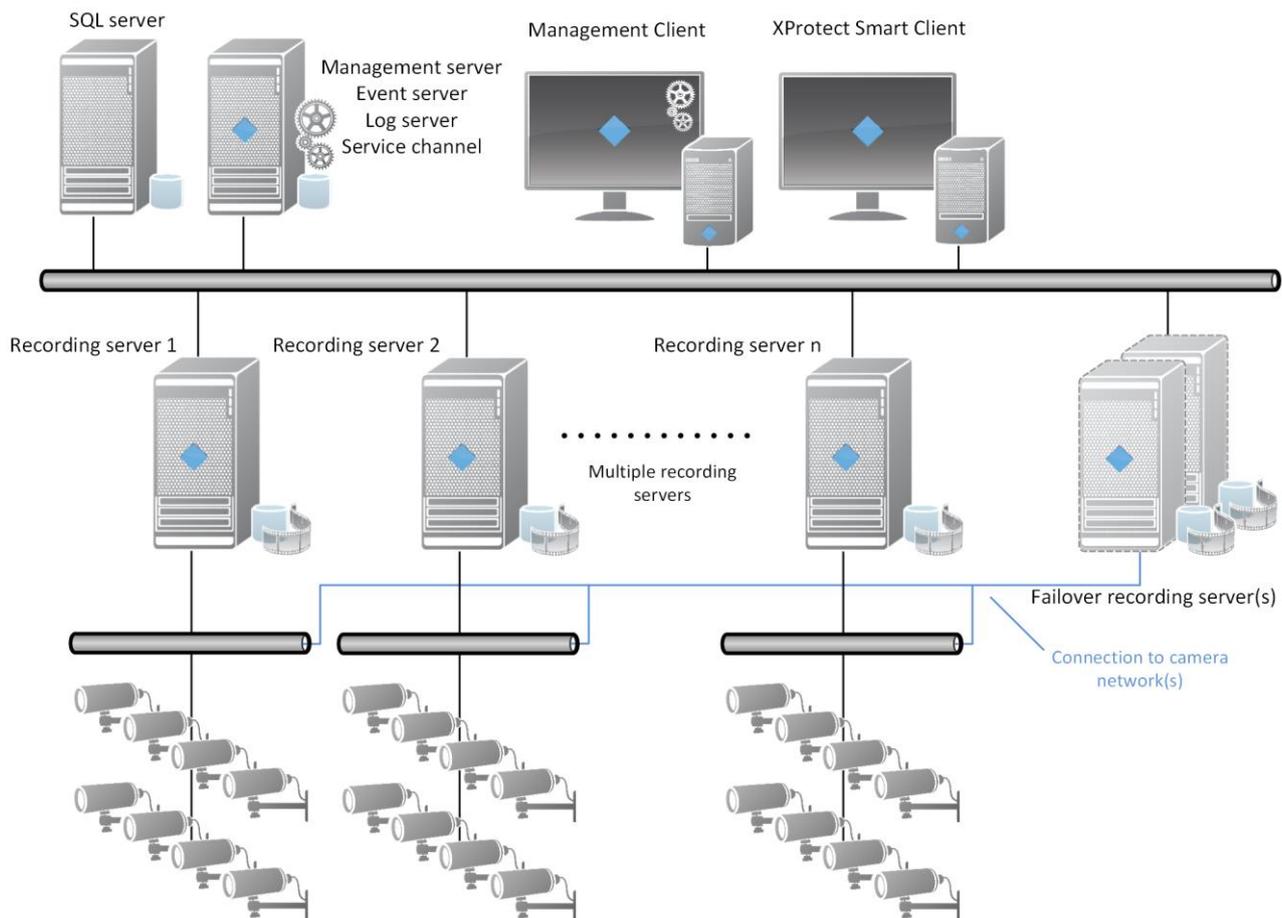
Note: When the system is larger than 300 cameras it is recommended to use a full version of the SQL server and run it on a dedicated server.

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 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
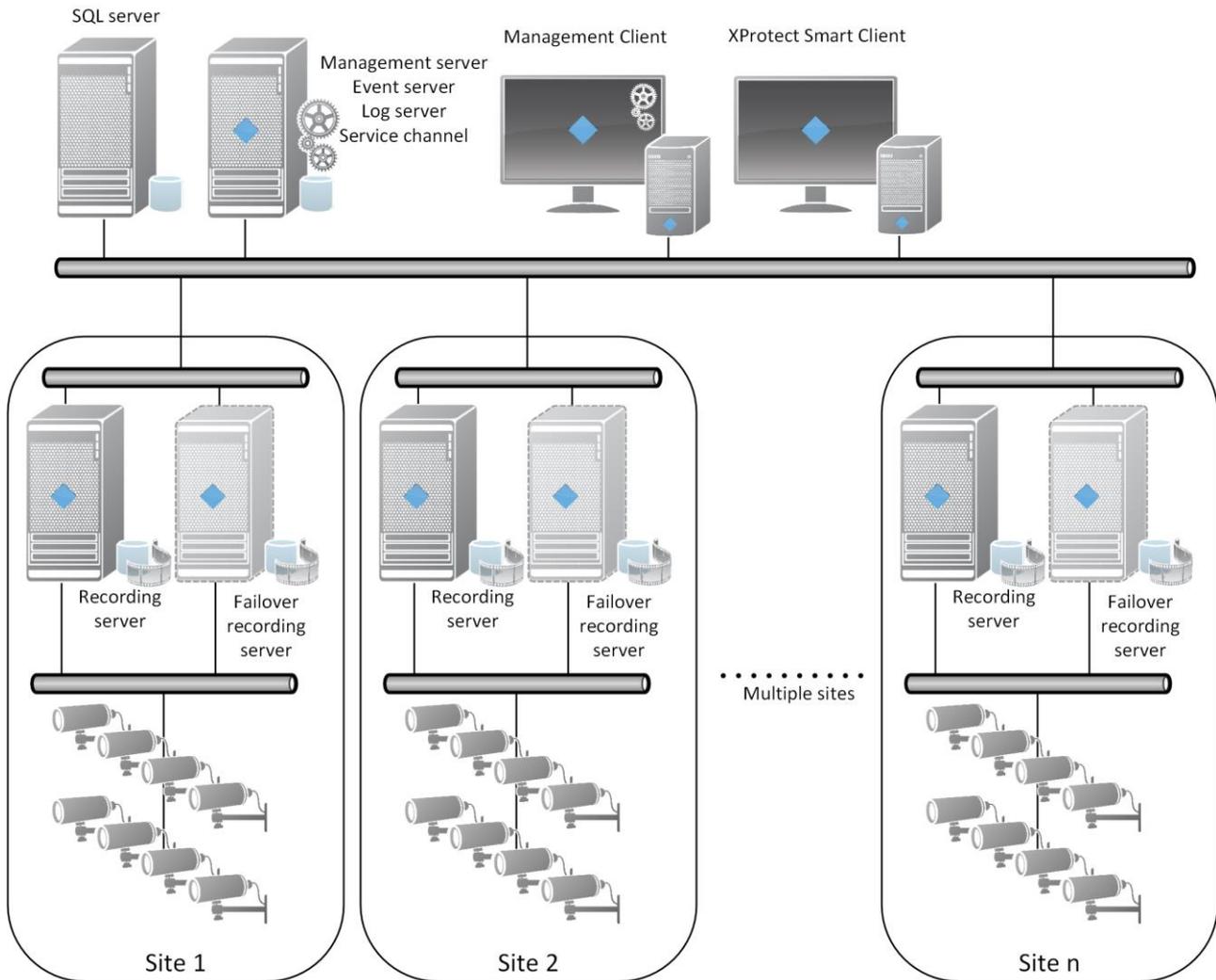
This design is in essence the same as design 2, with the difference that each recording server is not located on the main site with the management server and users, but on separate remote physical sites.

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.

The network connection from the remote sites to the main site only needs to have enough bandwidth for the number of cameras to be viewed live or played back at the same time.

Design 5 - Multiple systems, multiple sites. Direct user access to remote sites using Milestone Federated Architecture
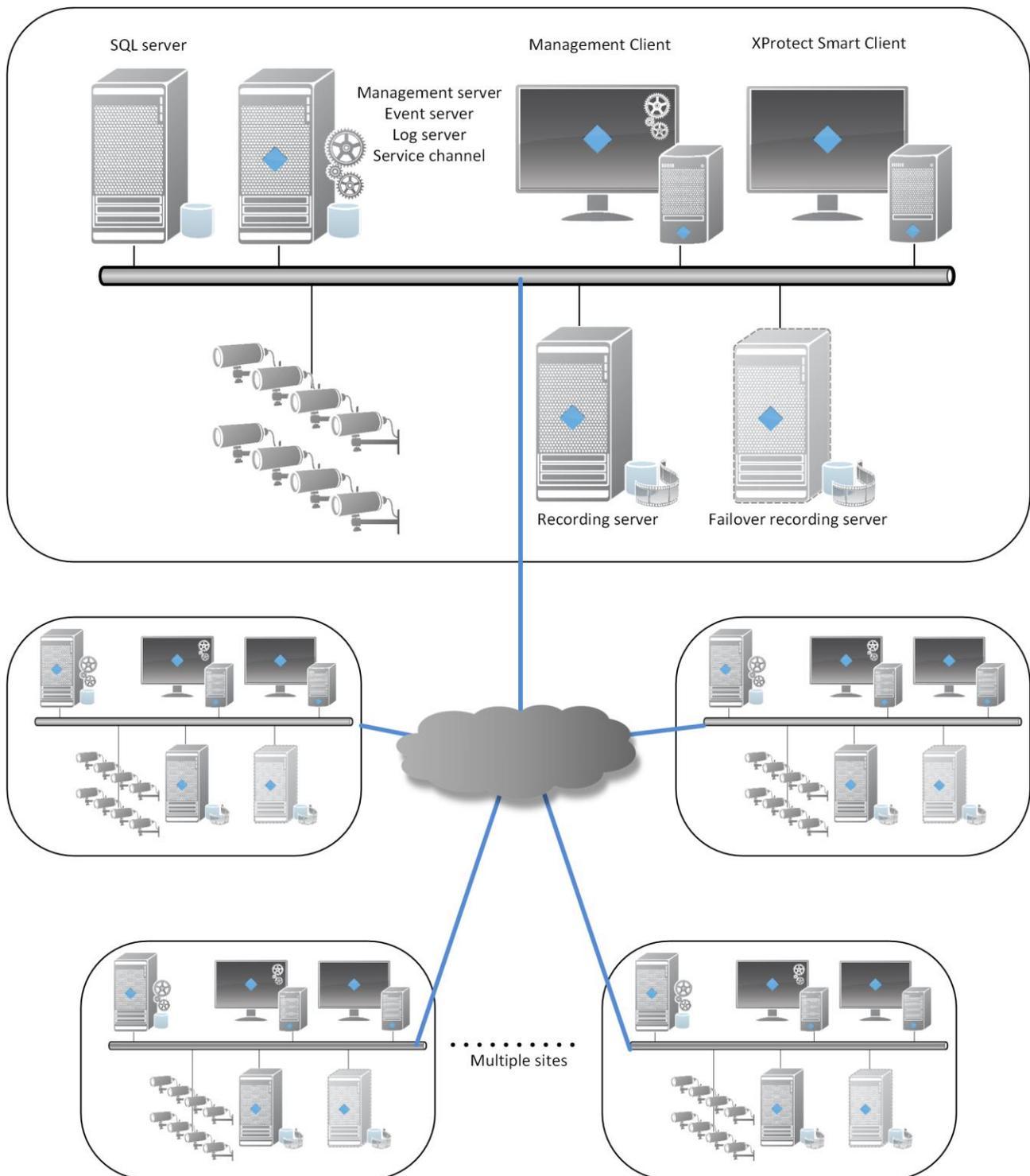
In a geographically distributed VMS system where users access video locally on each of the sites, it is recommended to design the system using Milestone Federated Architecture.

This solution 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, or log in may take a long time and the video experience may be poor.
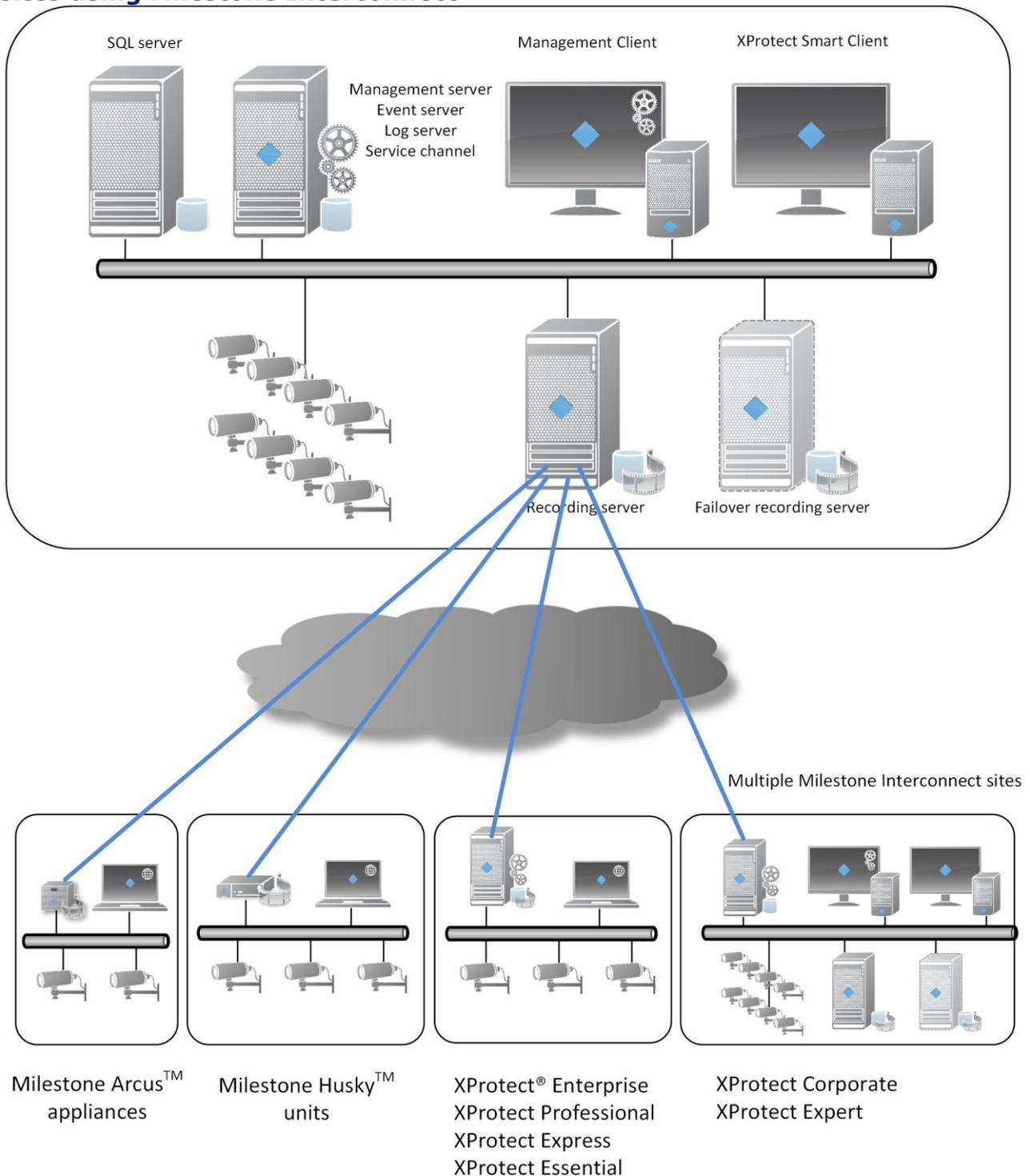
Milestone Federated Architecture offers a number of advantages:
- Independent design and configuration
  - Each site can be designed independently only taking the site's cameras and user requirements into consideration
  - Each site can be configured independently keeping the complexity of the overall system down
  - User and administrator rights 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 see:
http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Federated_Architecture_with_synapsis.pdf.

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

Milestone Arcus™ appliances

Milestone Husky™ units

XProtect® Enterprise
XProtect Professional
XProtect Express
XProtect Essential

XProtect Corporate
XProtect Expert

In a physically distributed VMS system, where there is a need for accessing the video directly by users on remote sites and where the network connections between the central and remote sites are unstable or intermittent, or the sites are not part of the same 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 the sites can run any Milestone VMS version. Milestone Interconnect is thus well suited to interconnect VMS systems from multiple customers to a central site, for instance with a city surveillance installation.

Milestone Interconnect offers a number of advantages:
- Independent design and configuration
  - Each site can be designed independently only taking the site's cameras and user requirements into consideration
  - Each site can be configured independently keeping the complexity of the overall system down
  - User and administrator rights can be set per site
  - It is possible to use any XProtect product on the remote sites
- Seamless access
  - Users on the central site can access the entire interconnected system seamlessly via a single log-in
  - Local users on a remote site can access the system on their site even if the connection to the central site is broken
- Flexible recording
  - With Milestone interconnect it is possible to automatically retrieve the recordings made on the remote system when the network connection to it is restored, for instance for surveillance in vehicles like cars, buses, trains and ferries
  - In addition to automatic retrieval, the system offers rule, schedule and user-activated retrieval of recordings
  - Alternatively, recordings can be played back directly from the remote site
- Network connection
  - With Milestone Interconnect the system can automatically handle unstable and intermittent network connections between the central and remote sites

In addition to the advantages listed above, Milestone Interconnect offers a long list of advanced functions and benefits. For more information see: http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Interconnect.pdf.

Integration with standard IT technology

Milestone XProtect Expert and XProtect Corporate 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 choose, deploy and administrate the VMS because the learning curve is low for people with IT knowledge. The Milestone XProtect VMS looks like and is managed like an IT system, the data is just video streams instead of files, transactions, business data, etc.

The below list are examples of how Milestone XProtect Expert and XProtect Corporate 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.

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.

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 A/S during development, test, support, etc.

In general, where it makes sense for the system integrator or administrator to use it, it is recommended to use virtualization because it provides a range of management, stability, scaling and failover benefits. However, when used, it is important to take into account that a recording server running many cameras can use a lot more CPU, network, system I/O and disk resources compared to what standard services running on virtual server normally use. This means that depending on the server specs, it may not be possible to run multiple virtual machines on the same host, if one of the virtual machines on the host is running a recording server with a high number of cameras.

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 is streamed permanently to the recording servers.

A quick example: 100 cameras on a recording server running at HD resolution at 25 or 30 frames per second using 2 Mbit/s per camera amounts to a constant 200 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 for an overview of used ports and protocols.

VPN

Standard VPN can be used to further protect and encrypt the video streams and video surveillance system communication, if the clients or cameras are connected via public Internet. As an alternative to pure port forwarding in a router or firewall, VPN can also be used to provide access to the VMS from the Internet.

IPv4 and IPv6

Milestone XProtect Expert and XProtect Corporate 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 the existing IT infrastructure and work processes.

In extension to external system monitoring tools, Milestone XProtect Expert and XProtect Corporate support a built-in function with dedicated user interface called System Monitor, which 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, System Monitor also provides an overview of VMS-specific parameters like storage and network use per camera.

Email

In addition to the technical monitoring mentioned above, Milestone XProtect Expert and XProtect Corporate VMS can use email to send notifications of technical issues, security events or events from third-party integrations. It is also possible to include still images and 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, it is necessary to set up a Network Time Protocol server (NTP) and configure the cameras to synchronize its time with the NTP server. The NTP server must be synchronized with the VMS servers' time source, typically a domain controller, so all parts of the VMS use the same time. 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, and for Edge Storage the solution will stop working once the camera and VMS time stamps are too far apart.

Windows reliability and performance monitor (Perfmon)
Windows Perfmon is a powerful performance monitoring tool that is built into Windows.

Perfmon 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 Expert and XProtect Corporate 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.
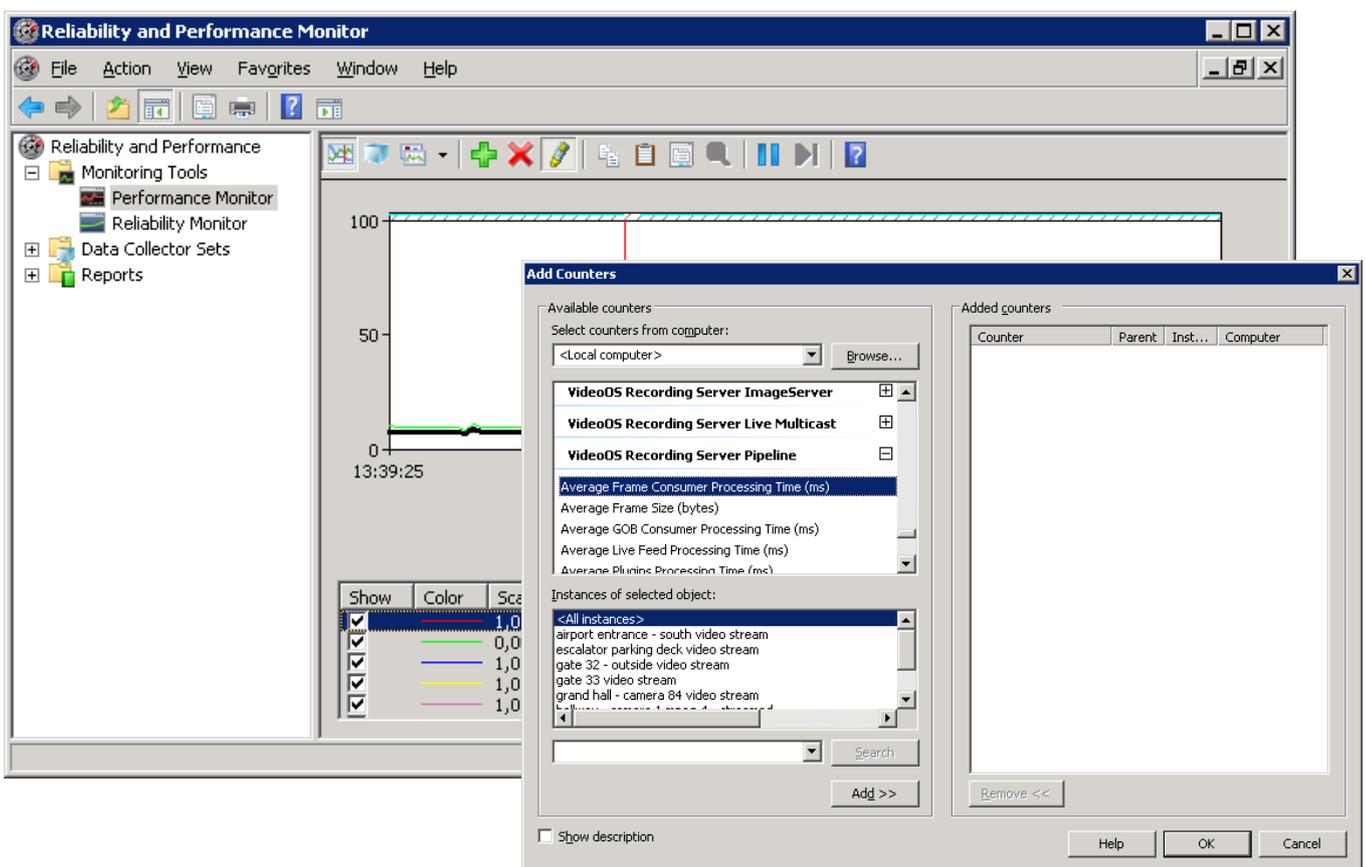
Benefits and summary

As discussed in this white paper, Milestone XProtect Corporate and XProtect Expert build on a flexible multi-tiered client-server system architecture, where the open 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, 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 because additional recording servers can be added when and as needed, and the camera driver layer, server components and client applications may be upgraded independently.

To meet the strictest needs for system security and reliability, XProtect Corporate and XProtect Expert 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 Corporate and XProtect Expert 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 clustering.

Embracing standard IT technologies and concepts, such as standard IPv4 and IPv6 network communication, Microsoft Active Directory, virtualization technologies, SQL databases and SNMP, XProtect Corporate and XProtect Expert 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