Whitepaper

Large-Scale VMS Design and Management

How to design and manage a video surveillance system with 100,000 highly-available cameras

Prepared by:
John Rasmussen, Senior Product Manager, Corporate Business Unit, Milestone Systems

Date: June 28, 2016
Table of Contents

Introduction.................................................................................................................................................. 3
Purpose and target audience ......................................................................................................................... 3
Large-scale design considerations .............................................................................................................. 4
Large-scale server recommendations .......................................................................................................... 5
  Management server recommendations ....................................................................................................... 6
  Event server recommendations .................................................................................................................. 7
  Recording server recommendations ......................................................................................................... 8
Large-scale VMS design .............................................................................................................................. 9
  Single site .................................................................................................................................................. 10
  Distributed sites ....................................................................................................................................... 12
  Distributed sites with remote locations ..................................................................................................... 14
Role and permission recommendations ....................................................................................................... 15
Additional design considerations ............................................................................................................... 16
  High availability ..................................................................................................................................... 16
  Virtualization .......................................................................................................................................... 19
  Domain controller recommendations ....................................................................................................... 19
Summary and benefits ................................................................................................................................. 21
Introduction
As the world’s leading Video Management Software (VMS) vendor\(^1\), Milestone Systems offers a range of products and technologies that address large-scale VMS installations.

Milestone XProtect® Corporate is designed to meet the needs of advanced, large-scale, multi-site VMS installations. Because of its modular and flexible architecture, it can address large-scale VMS projects of any size.

Additionally, using Milestone Federated Architecture (MFA) or Milestone Interconnect, XProtect Corporate can address large-scale VMS projects that are distributed across large geographical areas or across independent systems with different owners.

Purpose and target audience
This white paper can help you understand the architecture and technology needed to design large-scale XProtect Corporate systems with 100,000 or more cameras.

This whitepaper also covers these aspects of large-scale design:
- When to use MFA
- When to use Milestone Interconnect
- How to design for 99.999% high availability for live monitoring
- How to design for 99.99999% high availability for recording
- How to implement efficient user management

To fully benefit from the design examples and recommendations covered in this whitepaper, you must have a thorough understanding of Milestone XProtect Corporate, MFA and Milestone Interconnect.

The knowledge you need is available in the following whitepapers:
- XProtect Expert and XProtect Corporate – System Architecture Guide for IT Professionals
- Milestone Federated Architecture
- Milestone Interconnect

The primary audiences for this white paper are:
- Surveillance system architects and designers
- Large-scale surveillance project consultants
- Companies, organizations, universities, and governments with large-scale surveillance projects or installations

\(^1\) [https://www.milestonesys.com/press-releases/20160620-ihs11/]
Large-scale design considerations

Milestone XProtect Corporate is the third generation VMS software from Milestone Systems, and it was designed from the beginning with large-scale VMS deployments in mind.

The software is designed and developed to offer:

- No built-in scaling or performance limitations
- A flexible and distributed system architecture
- Technology to tie multiple discrete systems together in one large-scale VMS
- Dedicated servers (services) optimized for specific VMS tasks
- A single dedicated Management Client for centralized management
- Centralized storage of server and client configurations
- High availability for all server components
- Support for commonly used IT technologies and standards

Compared to designing VMS systems for a few thousand cameras, there are notably more aspects to consider when designing large-scale XProtect Corporate systems. Failing to properly consider and address these issues may reduce performance and can even require post-deployment re-design, which can be very costly.

It’s important to carefully consider the following questions. Their answers determine how to design the large-scale system.

- **Location of the cameras**
  - Centrally located, or distributed over a large geographical area?
  - How much bandwidth will be available from cameras to the recording servers?

- **Location of the primary users**
  - Centrally located users, or distributed across regions?
  - How much bandwidth will be available from recording servers to clients?

- **Centralize or regional management**
  - Manage entirely from a central location, or centrally and regionally, or only at the regional sites?

- **High availability needs**
  - High level of availability needed?

- **Server usage vs. cost of the servers**
  - Balance server load versus the cost of servers. For example, the number of cameras per recording server
Large-scale server recommendations

Although the scalability of XProtect Corporate is limited only by server performance and resources, it is not always the best choice to design with few but very large powerful servers.

When you calculate loads for servers, consider the resource cost per item (such as cameras) that you will run on the server. Then look at the price of a server that can support those items.

You may discover that it’s more cost effective to buy more, less powerful servers than a few very powerful ones.

In addition to the cost performance ratio of the hardware equipment, consider the cost of managing the system. In this case, the more cameras per server the more complex the configuration becomes. This can make it more complex and costly to manage.
This document offers general recommendations for the following key XProtect Corporate components when designing large-scale VMS systems.

- Management server
- Event server
- Recording server

Recommendations take in to account the performance versus cost information, and are based on large-scale testing done internally at Milestone, and at customer projects.

**Management server recommendations**

The management server is the central component of the XProtect Corporate system. It handles the system configuration, facilitates user authentication, and distributes configuration settings to system components, such as recording servers.

Configuration data is stored in Microsoft SQL Server. For large-scale systems, you must install SQL Server on a dedicated server and be dimensioned according to VMS configuration and usage.
Multiple factors impact the performance of the management server:

- Number of cameras in the system and their capabilities (number of streams, Pan/Tilt/Zoom (PTZ), image settings, etc.)
- Number of recording servers
- Client access and usage

Of these three factors, the number of cameras per management server has the greatest impact, and is typically the largest concern when designing large-scale VMS systems.

Milestone has determined that the optimal number of cameras per management server is around 8,000 to 12,000. This can vary, depending on configuration.

When the size of the VMS installation exceeds this number of cameras, or the installation will be distributed across multiple sites, MFA is used to increase the capacity or to distribute the system across multiple sites.

To make the large-scale design examples in this whitepaper easy to understand, 10,000 cameras are used as the standard per management server and site.

**Event server recommendations**

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

**Events:**
System events are consolidated in the event server. This gives partners a single place and interface for integrations that use system events.

Additionally, 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, and handles the alarm database.

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

**XProtect Access:**
The event server hosts the XProtect Access integration framework and the vendor specific XProtect Access plug-ins.
XProtect Transact:
   The event server hosts the XProtect Transact integration framework as well as the dedicated XProtect Transact connector plug-ins.

MIP SDK:
   Third-party plug-ins can be installed on the event server and access system events.

All data handled by the event server is stored in the SQL database that the management server uses.

Large-scale testing and event simulation internally in Milestone of the event server show that it can sustainably manage and store around 1,200 events, alarms, access events, and so on, per second. During peak periods it can handle around 6,000 per second.

Recording server recommendations

The recording server is a component that handles essential functions, like:

- Retrieve video, audio, metadata, and I/O event streams from 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, and so on
- Perform motion detection and generate Smart Search metadata

Video codec and motion detection

For large-scale design, the optimal codec is either MPEG-4 or H.264 with a group of pictures (GOP) length of 1 second or more. Additionally, motion detection in the recording server must be done only on key-frames. This gives lower load and higher performance on the recording server. Alternatively, you can disable motion detection on the recording server, and instead use the camera’s built-in motion detection, which even further lowers the load on the recording server.

Number of cameras per recording server

Milestone’s large-scale testing and simulation of the recording server show that the optimal cost to performance ratio is achieved when receiving and recording audio and video streams at the rate of 3Gbit/s in total. Assuming the video is 1080p full framerate (25 or 30 frames per second) streams at 3Mbit/s, that equals 1000 cameras per recording server.

Using this information, the large-scale VMS design recommendations for the recording server in this whitepaper are based on below specification:

- 1080p video stream at 25 or 30 FPS
- GOP length of 1 second
• 3 Mbit/s video streams in H.264 format
• Motion detection on key-frames only
• 1000 cameras per recording server

Large-scale VMS design

When designing a large-scale VMS, the primary things to consider are:

• Where will the cameras be placed in relation to the recording servers?
• What network infrastructure will be available between recording servers and cameras?
• Where will the primary users be located and how will they access the large-scale VMS?
• Where will the VMS servers be placed – centrally or regionally?
• What network infrastructure will be available between the client computers and the recording servers?
• What are the requirements for high availability?

Depending on these considerations, the design typically results in one of the following large-scale designs:

**Single site**
Typically used when:

• Most users are located in one location, or a few central locations
• The network infrastructure will support streaming all audio and video streams from the devices to a central location
• All servers will be placed in a central location, for easy network design and maintenance

**Distributed sites**
Typically used when:

• Most users are located in distributed sites, and focus mainly on cameras from their location
• The network infrastructure will not support streaming all audio and video streams from the devices to a central location
• The overall network load or cost should be reduced by streaming the audio and video to local sites

**Distributed sites with remote sites (using Milestone Interconnect)**
In addition to single site and distributed site designs, some setups also have to connect to smaller independent systems, or there may be locations with limited or unstable network connections. In these cases, use a combination of the single and distributed site designs and Milestone Interconnect.
Single site

Use the single site design when servers and users primarily are located at the same physical location. For example, a large airport, a university or a factory.

The single site design is the least complex large-scale VMS to design and implement because the core network, servers, storage, and clients are located in the same place. This makes it easier to:

- Dimension the network topology
- Ensure adequate bandwidth between servers and clients
- Design for high availability for network, servers, and storage
- Install and maintain the network, servers, storage, and clients

Having all servers, administrators, and users in one location also makes the system more robust and secure against external hacking and disturbances.

One scenario to consider carefully with the single site design is how far cameras are from the central location. For example, in city surveillance where cameras are distributed across a large area.

In this case carefully consider the bandwidth needs across the WAN (Wide Area Network):

- Upstream bandwidth for the individual cameras.
  - The network technology that connects each camera to the WAN must allow for the video stream (for example, 3Mbit/s for a 1080p video) to be sent to the central location without dropping data.
- Downstream bandwidth to the central site where the recording servers are located.
  - Recording 100,000 cameras in the central location when each camera is streaming video in at 3 Mbit/s requires at least 300 Gbit/s of downstream bandwidth.
- Network bottlenecks through the WAN.
  - The WAN will consist of multiple nodes, such as routers, switches, network connections, and so on. For each of these, calculate the bandwidth requirements and choose adequate equipment.
**Single site design recommendation**

Following the previously described server component recommendations, Milestone recommends the following design using MFA for a large-scale, single-site XProtect Corporate VMS system.

When designing a large-scale XProtect Corporate VMS with 100,000 cameras, divide the system into 10 logical systems, with 10,000 cameras per system. Each logical system consists of a complete XProtect Corporate system, including SQL server, management server, event server, and 10 recording servers. Each recording server connects to and records video from 1,000 cameras.

On top of the logical systems, is a top node system that consists of just an SQL server, a management server, and an event server. This top node system uses MFA to tie all logical systems together. VMS clients access the entire system via the top node, and depending on permissions, can seamlessly access logical sites and cameras.
Distributed sites

Use the distributed site design when the primary users are distributed over multiple physical sites, and cameras typically are monitored only at their local site. This design uses the same basic MFA structure and technology as the single site design. The difference is that instead of installing all the logical systems and servers in the same physical location, the systems and servers are distributed across multiple sites.

Because users typically monitor cameras only at their local site, it can be a benefit to place the logical systems in the user’s regions. This eliminates the need to send audio and video streams from the cameras to the central site and back to the users at the local sites.

Because the video streams primarily stay within the local site, only a small amount of traffic goes to the central location. Therefore, this design requires less bandwidth between the central and local sites. Users in the central location can still log-in and access all cameras across the entire system when needed.

Distributed sites design recommendation

Considering the design recommendations listed in the previous section, and using 20 remote sites of various sizes as an example, – Milestone recommends the following design using MFA for large-scale VMS systems of 100,000 or more cameras.

Depending on permissions, centrally located administrators and users can seamlessly access all remote sites and cameras. Additionally, administrators and users at the remote sites can access and manage their site’s cameras without having to authenticate or otherwise communicate with the central site. This makes the system more robust as each site can run independently should there be issues with the network connection to the central site.
Milestone Systems

White paper – Large-Scale VMS Design and Management

20 sites of various sizes – Some made of multiple logical systems

Site 3 (expanded)

1 to 10 recording servers, each recording up to 1,000 cameras

Recording server (expanded)

1,000 Cameras
Distributed sites with remote locations

Large-scale VMS systems sometimes need to connect to smaller sites at more remote locations. There can also be cameras at locations where the network is either unstable or there isn’t enough bandwidth to stream video to a central recording server.

In these cases, the single site and distributed sites designs can be extended to address these needs by using Milestone Interconnect.

On a basic level, Milestone Interconnect is similar to MFA in the sense that it ties separate systems together to form a larger system. However, the way that Milestone Interconnect ties sites together is a little different, and support additional unique capabilities, such as:

- Attach all Milestone XProtect VMS, Husky, or Arcus products to the central site
- Attach Milestone VMS systems owned and managed by third-parties to the central site
- Allow third-party Milestone VMS owners to specify which cameras and functions the central site can access
- Handle limited and intermittent network connections
- Upload recordings to the central site on manual activation, based on schedule, events, or via a third-party integration
- Control timeslot and bandwidth consumption when uploading recordings to the central site

**Distributed sites with remote locations design recommendation**

Unlike MFA, Milestone Interconnect connects sites through the recording servers. This enables connection to remote systems that have limited bandwidth, and a network connection that maybe aren’t always stable.

Additionally, connecting remote sites via the recording servers allows recordings to be transferred from the remote site and stored in the central site’s recording server. This enables use cases where recordings are stored at the remote site and retrieved only when there is a need to view them, or when the network connection is restored, or at a timeslot where the bandwidth is available.

For simplicity, the illustration shows only a single site in the large-scale VMS and its interconnected remote site.

Using standard user and permission settings in the interconnected VMS, the administrator of the local VMS has full control of the cameras, functions and recordings.
that the central VMS can access. For example, this enables local administrators to give access to outdoor cameras, but not interior cameras.

**Role and permission recommendations**

When designing and managing a large-scale XProtect Corporate system, consider how to set up and manage users and permissions.

If you set up users and permissions to the large-scale XProtect Corporate system one user and camera at a time, as done in smaller VMS systems, managing and controlling users and permissions can pose a real challenge. Therefore, use a structured approach to handle the many users and their permissions to cameras in the system.

Milestone recommends to create roles, which defines the detailed permissions to the VMS, for each area of responsibility, like: security guards, supervisors and administrators.

By doing this, you ensure that all users with this area of responsibility always have the same permissions. This also makes it easier to modify the permission for all the users in the role, should there be changes or additions to their role or the system.

Additionally, Milestone recommends creating Active Directory (AD) groups that correspond to the VMS responsibilities, and adding these AD groups to the corresponding VMS roles. When this is done, new VMS users can be granted access and assigned permissions in the VMS simply by creating users in AD and adding them to the right AD group.

![Example of VMS roles with an AD user group added to a role](image-url)
Additionally, in extension to the server side controlled and enforced permissions, XProtect Corporate supports customization of the XProtect Smart Client and XProtect Management Client interfaces. This is done using XProtect Smart Client profiles and XProtect Management Client profiles.

Finally, users can be added to multiple roles. In this case a specific user’s permissions will be a combination of all the roles that the user is a member of.

For more information about advanced security management in XProtect Corporate, see XProtect Corporate - Advanced Security Management.

Additional design considerations

When designing a large-scale XProtect Corporate system, there are often additional aspects to consider. The following sections cover some of the most frequent aspects.

High availability

Before a VMS of any size is designed, consider the following question: How critical is it if a server fails, and how should the administrators and users react?

In some cases, for instance a small retail shop, the operation of the VMS is not critical enough to warrant the cost of additional failover servers. Instead, the shop accepts that failures can be addressed within a day or two by fixing or replacing the server.

In large-scale VMS installations, an approach by simply replacing broken servers is typically not acceptable for the following reasons:

- VMS and cameras must be operational and record close to 99.999% of the time
- Many cameras are affected because each server runs roughly 1000 cameras
- Many users and their tasks, are affected
- It may take time to replace servers that are not standard, off-the-shelf servers

Management server and event server

In Milestone XProtect Corporate and XProtect Expert a 99.999% uptime is achieved by using Microsoft Clustering or equivalent high availability software or products, for the management server and event server.

Example: High availability for the management and event server using Windows clustering
Recording server
For the recording servers, 99.999% uptime is achieved by using one or more dedicated failover recording servers.

Milestone XProtect failover recording servers can run in two modes:
- Hot-standby
- Cold-standby

**Hot-standby**
Hot-standby is a 1:1 failover solution optimized for failover speed. The dedicated failover recording server is running in stand-by mode, and has the same configuration as the primary recording server preloaded. If the primary recording server fails, the failover recording server needs only to connect to the cameras to become operational.

The failover time, which is the time from the recording server failure to the time when the system shows video in the VMS clients again, depends on the camera brands and models. There is a difference in how fast different camera brands and models can provide a video stream to the failover recording server when it connects to them.

Using Hot-standby, the failover time is normally 10 to 15 seconds for cameras that perform well. This is true regardless of the number of cameras connected to the recording server.

![Recording servers and hot-standby failover recording servers in a 1:1 configuration](image)

**Cold-standby**
Cold-standby is a many-to-many failover solution optimized for cost. This is achieved by having one or more failover recording servers cover a larger set of recording servers. When a recording server fails, the first available failover recording server retrieves the configuration of the failed recording server, starts, and connects to the cameras.

Compared to hot-standby, cold-standby is a much more cost efficient solution because one failover recording server can be used for multiple recording servers. If the simultaneous failure of multiple recording servers is a concern, simply add more failover recording servers.

With cold-standby, the failover time is a bit longer compared to hot-standby. The reason for this is that with cold-standby, the failover recording server must first load
the recording server configuration, and then start the failover recording server. This adds around 20 seconds to the failover time.

The camera brands and models impact the failover time for the same reason as with hot-standby. There is a difference in how fast they provide a video stream to the failover recording server when it connects to them.

This means that using cold-standby, the failover time is normally around 30 to 35 seconds for cameras that perform well. This is true regardless of the number of cameras running on the recording server.

Additionally, it is possible to set up failover recording server groups to act as secondary backups to each other if all failover recording servers in the primary group are busy.

**Edge storage**
Video is not recorded during the period it takes the failover recording server to start. This means that, depending on the failover mode and the cameras used, a shorter or longer period of time is not recorded by the recording servers. However, this can be mitigated by using cameras that support edge storage, and enabling automatic retrieval of recordings from edge storage in the VMS.

For more information about edge storage, see [Milestone Edge Storage with flexible retrieval](#).

**Handling failover recordings**
After the failover recording server starts, recording follows the same rules as defined for the recording server.

When the primary recording server starts again, the following series of actions restores normal operations:

- The recording server connects to the cameras
- Clients currently connected to the failover recording server automatically reconnect to the recording server
- The failover recording server disconnects from the cameras and return to standby mode, making it ready for a new failover event
• Recordings made on the failover recording server are, via an auxiliary service on the failover recording server, transferred to the primary recording server.
• After the failover recordings are transferred they are deleted on the failover recording server. This makes room for recordings from a new failover event.
• If the cameras support edge storage, and automatic retrieval is enabled in the VMS, the recording server retrieves the recordings from the time the recording server failed to the time the failover recording server started recording.

The system is now back to normal, and recordings are available for seamless playback for the entire period where the recording server was offline.

Virtualization

When designing and deploying large-scale VMS systems, Milestone recommends that you base the server design and implementation on virtualization technology.

Virtualization technology offers a range of benefits when used in standard IT installations. These benefits also apply when used in large-scale VMS systems.

Some of the benefits virtualization offer:

• Cloning servers
• Portable server images
• High availability support
• Seamless migration of a running virtual server from one physical server to another. For example, this lets you:
  o Maintain the physical server
  o Replace servers or upgrade to more powerful servers
• Dynamic, on-the-fly allocation of memory, CPU and storage

Domain controller recommendations

When the VMS is distributed across multiple physical locations there is a risk that the network connection to the top node site fails. If this happens, the affected site cannot communicate with the domain controller (DC) in the headquarters. This can cause a range of issues.

The VMS servers and the user that is logged in are not affected. However new users cannot log in because the DC cannot authenticate them.
Additionally, in a MFA setup, the VMS server services will use an AD account to get domain permissions. If the VMS servers or services are restarted, the VMS server service cannot start because the account the service uses cannot be authenticated on the AD.

To avoid this, run a DC at each site, and configure it to synchronize with the DC at the top node site.

Having a DC in each site enables uninterrupted operation if the network connection to the headquarters fails. The local DC can perform authentications, which ensures that VMS servers and users are not affected.

When the network connection is reestablished, the local DC synchronizes changes with the headquarters DC.
Summary and benefits

The modular nature of Milestone XProtect Corporate, especially when combined with MFA and Milestone Interconnect, offers great flexibility when designing large-scale VMS systems.

XProtect Corporate can run 100,000 or more cameras in a large-scale VMS system deployment, regardless of whether the system is located on a single site, or distributed across multiple sites and managed by one or more authorities.

Additionally, you can deploy a large-scale VMS in phases, which makes design and deployment more manageable and cost effective. The distributed architecture also allows the large-scale VMS design to grow when the system needs to be expanded.

In large-scale VMS systems, high availability is often a concern. This is especially true with regards to achieving high availability for recording servers in a cost effective way. XProtect Corporate recording servers capable of recording 1,000 or more cameras per server, combined with a few cold-standby failover recording servers, address this concern in a very cost-effective way.

You can achieve high availability for the other XProtect Corporate servers by using a variety of standard IT products. This lets you choose the high availability level that fits the needs of a large-scale VMS system.
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