Milestone Systems

XProtect® Advanced VMS 2013

Administrator's Getting Started Guide

milestone

The Open Platform Company

Contents

Copyright, trademarks and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file **3rd_party_software_terms_and_conditions.txt** located in your Milestone surveillance system installation folder.

About this guide

This guide briefly explains how to install your XProtect system as well as how to configure some of its key features.

For more detailed feature descriptions, see the manuals available on the software DVD as well as on the Milestone website. Your XProtect product also features a very comprehensive built-in help system.

Check our website for updates to make sure you install the most recent version of our software.

Product overview

This system is a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance, with support for devices from different vendors. The solution offers centralized management of all devices, servers, and users, and empowers an extremely flexible rule system driven by schedules and events.

Your system consists of the following main elements:

- The **management server** - the center of your installation
- One or more **recording servers**
- One or more **Management Clients,** which are unlicensed and can be downloaded and installed for free (as many times as needed).
- A **Download Manager**
- One or more **XProtect® Smart Clients**, which are unlicensed and can be downloaded and installed for free (as many times as needed). Possibly also one or more **XProtect Web Clients** and/or **Milestone Mobile clients**, which are also free of charge.

Your system also includes fully integrated Matrix functionality for distributed viewing of video from any camera on your surveillance system to any computer with XProtect Smart Client installed.

The system also offers the possibility of including the standalone XProtect® Smart Client – Player when you export video evidence from the XProtect Smart Client. XProtect Smart Client – Player allows recipients of video evidence (such as police officers, internal or external investigators, etc.) to browse and play back the exported recordings without having to install any software on their computers.

Finally, your system handles an unlimited number of cameras, servers, and users—across multiple sites if required. Your system can handle IPv4 as well as IPv6.

System requirements

IMPORTANT: Your system no longer supports Microsoft® Windows® XP (however, you can still run/access clients from computers with Windows XP Professional).

For easy user/group management, Milestone recommends that you have Microsoft Active Directory® in place before you install your system. If you add the management server to the Active Directory after installing, you must re-install the management server, and replace users with new users defined in the Active Directory.

The following are **minimum** requirements for the computers used:

Computer running management server

Name	Description
CPU	Intel® Xeon®, minimum 2.0 GHz (Dual Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 50 GB free (depends on number of servers, cameras, rules, and logging settings
Operating System	▸ Microsoft® Windows® 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2008 (32 or 64 bit) ▸ Microsoft Windows Server 2003 (32 or 64 bit) To run clustering/failover management servers, you also need a Microsoft Windows Server 2003/2008/2012 Enterprise or Data Center edition.

Software	Microsoft® .NET 3.5 SP1 and .NET 4.0 and Internet Information Services (IIS) 5.1 or newer

Computer running recording server or failover recording server

Name	Description
CPU	Dual Core Intel Xeon, minimum 2.0 GHz (Quad Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP, or PCI-Express, minimum 1024 x 768, 16-bit color
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 100 GB free (depends on number of cameras and recording settings)
Operating System	▸ Microsoft® Windows® 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2008 (32 or 64 bit) ▸ Microsoft Windows Vista® Business (32 or 64 bit) ▸ Microsoft Windows Vista Enterprise (32 or 64 bit) ▸ Microsoft Windows Vista Ultimate (32 or 64 bit) ▸ Microsoft Windows Server 2003 (32 or 64 bit)
Software	Microsoft® .NET 4.0 Framework.

IMPORTANT: When you format the hard disk of a recording/failover recording server device, you must change its **Allocation unit size** setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help at http://support.microsoft.com/kb/140365/en-us.

Computer running Management Client

Name	Description
CPU	Intel Core2TM™ Duo, minimum 2.0 GHz
RAM	Minimum 1 GB
Network	Ethernet (100 Mbit or higher recommended)
Graphics Adapter	AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit color
Hard Disk Space	Minimum 100 MB free
Operating System	▸ Microsoft® Windows® 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft Windows Vista® Ultimate (32 bit or 64 bit) ▸ Microsoft Windows Vista Enterprise (32 bit or 64 bit) ▸ Microsoft Windows Vista Business (32 bit or 64 bit) ▸ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 (32 bit or 64 bit) ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2003 (32 bit or 64 bit)
Software	Microsoft® .NET 4.0 Framework, DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from http://www.microsoft.com/downloads/.

Computer running event server

Name	Description
CPU	Intel® Xeon® , minimum 2.0 GHz (Dual Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)
Operating System	▸ Microsoft® Windows® 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2008 (32 or 64 bit) ▸ Microsoft Windows Server 2003 (32 or 64 bit)
Software	Microsoft® .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Computer running log server

Name	Description
CPU	Intel® Xeon® , minimum 2.0 GHz (Dual Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color

Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)
Operating System	▸ Microsoft® Windows® 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2008 (32 or 64 bit) ▸ Microsoft Windows Server 2003 (32 or 64 bit)
Software	Microsoft® .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Computer running service channel

Name	Description
CPU	Intel® Xeon® , minimum 2.0 GHz (Dual Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)

Operating System	▸ Microsoft® Windows® 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft® Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2008 (32 or 64 bit) ▸ Microsoft Windows Server 2003 (32 or 64 bit)
Software	Microsoft® .NET 4.0 Framework, and Internet Information Services (IIS) 5.1 or newer

If you are installing on Windows Server 2008, you must customize a standard IIS installation:

1. In Windows **Start** menu, select **Control Panel,** then select **Programs and Features.**
2. In the **Programs and Features** window, click **Turn Windows features on or off.** This opens the **Windows Features** window (window name may be different depending on which operating system you are installing the service channel on).
3. In the **Windows Features** window, expand **Internet Information Services.**
4. Expand and select **Web Management Tools**, then expand and select **IIS 6 Management Compatibility**, then select **IIS Metabase and IIS 6 configuration compatibility.**
5. Expand and select **World Wide Web Services,** then expand and select **Application Development Features,** then select the following:
   - .NET Extensibility
   - ASP
   - ASP.NET
   - ISAPI Extensions
   - ISAPI Filters.
6. Expand and select **Security**, then select **Windows Authentication**.
7. Click **OK.**

Computer running XProtect Smart Client

Name	Description
CPU	Intel Core2 Duo, minimum 2.0 GHz (Quad Core recommended for larger views)
RAM	Minimum 512 MB (1 GB recommended for larger views, 1 GB recommended on Microsoft® Windows® Vista®)
Network	Ethernet (100 Mbit or higher recommended)
Graphics Adapter	AGP or PCI-Express, minimum 1280 x 1024, 16 bit colors
Hard Disk Space	Minimum 500 MB free
Operating System	▸ Microsoft® Windows® 8 Pro (32 bit or 64 bit) ▸ Microsoft Windows 8 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Professional (32 bit or 64 bit) ▸ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ▸ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ▸ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ▸ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ▸ Microsoft Windows Server 2008 ▸ Microsoft Windows Server 2003 (32 bit or 64 bit) ▸ Microsoft Windows Vista Ultimate (32 bit or 64 -bit) ▸ Microsoft Windows Vista Enterprise (32 bit or 64 bit) ▸ Microsoft Windows Vista Business (32 bit or 64 bit) ▸ Microsoft Windows XP® Professional (32 bit or 64 bit).
Software	Microsoft® .NET 4.0 Framework, DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from http://www.microsoft.com/downloads/.

Active Directory

You normally add users from Active Directory, although you can also add users without Active Directory. Active Directory is a distributed directory service included with several Windows Server operating systems. It identifies resources on a network in order for users or applications to access them.

If you wish to add users through the Active Directory service, a server with Active Directory installed, and acting as domain controller, must be available on your network.

Port numbers of special interest

Your system uses particular ports when communicating with other computers, cameras, and so on.

What is a port? A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore, it is sometimes necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic which is used when you view web pages.

In your XProtect system, you must therefore make sure that certain ports are open for data traffic on your network.

Ports used by the system

If nothing else is stated, ports are both inbound and outbound.

Port 20 and 21: Used by **recording servers** to listen for File Transfer Protocol (FTP) information; some devices use FTP for sending event messages. FTP is a standard for exchanging files across networks.

Port 25: Used by **recording servers** to listen for Simple Mail Transfer Protocol (SMTP) information. Also, some devices use SMTP (e-mail) for sending event messages and /or for sending images to the surveillance system server via e-mail. SMTP is a standard for sending e-mail messages between servers.

Port 80: While not directly used by the system, but by **management servers**, port 80 is typically used by the Internet Information Services (IIS) Default Web Site for running the Management Server service.

Port 443: Used by the basic user authentication process where both **management server** and the **service channel** must keep this port open at all times.

Port 554: Used by **recording servers** for RTSP traffic which is used for controlling streaming from cameras.

Port 1024 and above (outbound only (except ports listed in the following)**):** Used by **recording servers** for HTTP traffic between cameras and servers.

Port 5210: Used for communication between **recording servers** and **failover recording servers** when databases are merged after a failover recording server has been running.

Port 5432: Used by **recording servers** to listen for Transmission Control Protocol (TCP) information; some devices use TCP for sending event messages.

Port 7563: Used by **recording servers** and **XProtect Smart Client.** The main entry to the recording server where the ImageServer interface is implemented. Also used for handling PTZ camera control commands and for retrieving image stream from clients etc.

Port 7609: Used by the **report server** to communicate with the **Data Collector Server service** and must always be keep open on the machine running the **Data Collector**.

Port 8080: Used for communication between internal processes on the **management server** only.

Port 8844: Used for User Datagram Protocol (UDP) communication between **failover recording servers**.

Port 9000: Used by **management servers** for communication between the system and **XProtect Transact**.

Port 9993: Used for communication between **recording servers** and **management servers**.

Port 11000: Used by **failover recording servers** for polling (i.e. regularly checking) the state of **recording servers**.

Port 12345: Used by **management servers** and **XProtect Smart Client** for communicating between the system and Matrix recipients.

Port 22331: Used for communication between **event server** and **XProtect Smart Client** and **event Server** and **Management Client**.

Port 65101: Used between processes on the same machine only – i.e. Inter Process Communication (IPC) on a single machine only.

Virus scanning information

In some cases, Milestone recommends that you avoid virus scanning, if this is allowed in your organization.

If you use virus scanning software on:

- recording data in databases on recording servers
- data being archived in archiving locations

It most uses a considerable amount of system resources on scanning.

This may affect system performance negatively, notably scanning of data in databases containing recordings. Some virus scanning software may also temporarily lock each file it scans, which may further impact system performance negatively. Virus scanning may even corrupt recording databases, and render your surveillance system recordings useless.

Therefore:

- Do not use virus scanning on recording server directories containing recording databases (by default *C:\MediaDatabase* and all folders under that location, but note that your organization may have specified different recording paths).
- Do not use virus scanning on archiving locations.
- Do not use virus scanning on files with the following file extensions (which are all surveillance system-related):
  - .blk
  - .idx
  - .pic
  - .pqz
  - .sts
  - .ts
- Do not use virus scanning on the management server.

Your organization may have strict guidelines regarding virus scanning, but it is important that the mentioned locations and files are exempt from virus scanning. If allowed, you should disable any virus scanning of recording servers' databases, of any archiving locations as well as on the management server. Consult your organization's IT system administrator if in doubt.

Servers and clients require time-synchronization

Part of the security surrounding the use of clients with your system is based on so-called time-based tokens.

Why servers require time-synchronization

When a client logs in to the surveillance system, the client receives a token from the management server. The token contains important security-related time information.

The management server also sends a similar token to the required recording server(s). This is partly due to the fact that recording servers may be located all around the world. Each recording server uses the token to validate the client's token against the local time in the recording server's own time zone.

The validity of a token expires after a while. Therefore, it is important that time on your management server and all of your organization's recording servers is synchronized (minute and second-wise; hours may of course be different in different locations around the world). If time on the servers is not synchronized, you may experience that a recording server is ahead of the management server's time.

When a recording server is ahead of the management server's time, it may result in a client's token expiring on the recording server earlier than intended by the management server. Under unfortunate circumstances, you might even experience that a recording server claims that a client's token has already expired when it receives it, effectively preventing the client from viewing recordings from the recording server.

How to synchronize time on your organization's servers depends on your network configuration, internet access, use of domain controllers, etc. Often, servers on a domain are already time-synchronized against the domain controller. If so, you should be fine as long as all required servers belong to the domain in question.

If your servers are not already time-synchronized, it will be necessary to synchronize the servers' time against a time server, preferably the same time server.

The following articles from Microsoft® describe what to do in different situations:

- How to configure an authoritative time server in Windows Server 2003
- Registry entries for the W32Time service

If these links do not work for you, try searching www.microsoft.com for time server, time service, synchronize servers or similar.

It is also very important that XProtect Smart Client s are time-synchronized with the management server.

Why clients require time-synchronization

Because configuration communication is facilitated by the service channel, it is advantageous that XProtect Smart Client s are also time-synchronized with the management server and the computer

running the service channel service. A time difference of five minutes between XProtect Smart Client and servers is tolerated.

If an XProtect Smart Client is not time-synchronized with the management server and the computer running the service channel service, the XProtect Smart Client is not updated with information about configuration changes made by other users in XProtect Smart Client in Setup mode. This means that users risk overwriting each other's configuration changes.

Installation overview

Note that the **Milestone Mobile server** and **Axis One-click Connection Component** are not installed by the common installer. These must be install from the management server's download website (see "Download Manager/download web page" on page 35) (controlled by the Download Manager) once the management server is installed. The same goes for failover recording server(s) (see "Install failover recording server (recording server)" on page 24).

In general, your installation (or upgrade scenario) is handled by one common installer. Depending on your selections, this installer installs all or some of the following components:

- **Management server,** the center of your system installation. Typically installed on a dedicated server.
- **Recording server**, used for recording video feeds, communicating with cameras (via video device drivers) and other devices. Typically installed on one or more separate computers, rather than on the machine where the management server is installed. The needed video device drivers are automatically installed along with the recording server.

  Tip: Video device drivers are small programs used for controlling/communicating with the cameras connected to a recording server. As mentioned, you get the drivers automatically during installation. However, new versions of the drivers are released from time to time and must be downloaded from the management server's download web page and installed manually.
- **Management Client**, used for configuration and day-to-day management of the system. Typically installed on the system administrator's workstation or similar.
- **XProtect Smart Client**, feature-rich client used for accessing live and recorded video and other features from your XProtect system. Must be installed on users' computers (see "Install XProtect Smart Client" on page 31).
- **Service channel,** enables automatic and transparent configuration communication between servers and clients in your system. By default installed on the management server but, if you need to increase performance, it can be installed on another server.
- **Event server,** handles alarms and maps. Does not have to be installed on the management server, better performance can often be achieved by installing it on another dedicated server.
- **Log server,** provides the necessary functionality for logging information from your system. By default installed on the management server but, if you need to increase performance, it can be installed on another server.

  When installing the event server or log server, the URL address of the management server is expressed like this: *http//123.123.123.123*. If installing the event server or log server on the management server itself, this should be specified as *localhost*. The address can also include a port, like this: http://123.123.123.123:2356 or http://Localhost:2356.

The common installer saves all components on the management server's download web page no matter whether you install them or not. Once you have run the installer, single components can be (re-)installed from the management server download web page (see "Download Manager/download web page" on page 35). Refer to Download Manager's standard installers (users) to see what component are available for separate download.

Since most single component installer elements are identical to the common installer elements, single component installers are not described in detail. Only exception is the **failover recording server** installer (see "Install failover recording server (recording server)" on page 24).

As well as installing on physical servers, your XProtect system installation can also take place on **virtualized servers** (see "**Install your system on virtual servers**" on page 25).

Install your system - preconditions

If you are upgrading from a previous version, refer to Upgrade from previous version (on page 32).

If you plan to run **Milestone Federated Architecture™**, refer to About Milestone Federated Architecture.

If you run **workgroups**, make sure to ignore the normal installation guidelines and use the alternative method for installing for workgroups indicated in the following.

- **Microsoft® Windows® Installer 4.5 - only on Windows Server 2003:**

  Before installing your XProtect system, it is important to install Windows Installer 4.5**.**

- **SQL Server:**

  The management server requires access to a relational database. Later in this installation process you must choose between using an existing SQL Server on the network (**Administrator rights** on the SQL Server are required) or setting up a SQL Server Express Edition (a lighter version of a full SQL server) on the management server itself.

  If you select an SQL Server Express Edition, you might need to have Microsoft® .NET Framework 3.5 Service Pack 1 installed on the server running the SQL Server (even though Microsoft .NET Framework 4.0 is already installed). Refer to System requirements (on page 7).

- **2 x Windows Server 2003 Fix:**

  If you use Windows Server 2003, Milestone recommends that you install two supported fixes before starting: Fix 1 and Fix 2. Otherwise, the installation of your management server might fail due to Microsoft Windows Installer process having insufficient contiguous virtual memory to verify that the *.msi* package or the *.msp* package is correctly signed.

- **Alternative installation for workgroups:**

  If you do not use a domain setup but a workgroup setup, do the following when installing:

1. Log in to Windows using a common administrator account.

2. Depending on your needs, start the management or recording server installation and click **Custom**.

3. Depending on what you selected in step 2, select to install the Management or Recording Server service using a common administrator account.

4. Finish the installation.

5. Repeat steps 1-4 to install any other systems you want to connect. They must all be installed using a common administrator account.

This approach however, can not be used when **upgrading** workgroup installations, refer to Alternative upgrade for workgroup (on page 32).

Install your system - Single Server option

In an upgrade scenario (see "Upgrade from previous version" on page 32), you might **not** want to remove the management server database as it contains your system configuration.

1. If you are installing a version downloaded from the Internet, run the `MilestoneAdvancedXProtectVMSSystemInstaller.exe` file from the location where you saved it. Alternatively, insert the software DVD. If the dialog does not open automatically, run the `MilestoneAdvancedXProtectVMSSystemInstaller.exe` file from the DVD.

2. The installation files unpack. Depending on your security settings, one or more Windows security warnings may appear. Accept these and the unpacking continues. When done, the **Milestone Advanced XProtect VMS** dialog appears. In the coming steps, do the following:

   a) Select the **Language** to use during the installation (this is **not** the language your system will use once installed, this is selected later). Click **Continue**.

   b) In **Type the location of the license file**, enter your license file from your XProtect provider. Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.

   c) Read the *Milestone End-user License Agreement*. Select the **I accept the terms in the license agreement** check box. Optionally, select the **Sign me up for the Customer Experience Improvement Program** check box. Follow the on-screen *Read more* link for further information on this.

   d) Consider the following installation methods:

   - **Single Server**, installs all management server components, recording server, and clients on the current computer. You only need to make a minimum of selections and all components are selected in the component list, which cannot be edited.

   - **Distributed**, installs all management server components and clients on the current computer. However, you must install the recording server on a separate machine. This means that the recording server is cleared in the component list which you cannot edit.

   - **Custom**, lets you select freely among management server components to install on the current computer. The only exception is the management server. By default, recording server is cleared in the component list, but you can edit this.

3. Select **Single Server**. A list of components to install appears (you cannot edit this list). Click **Continue**.

4. Select **Files location** for the program file. In **Product language**, select the language in which your XProtect product should be installed. Click **Install**.

5. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

   If you do not have Microsoft® IIS installed, this is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security settings, one or more Windows security warnings may appear. Accept these

and the installation continues. When done, your XProtect installation completes and you can get started with your surveillance system.

Install your system - Distributed option

1. Refer to Install your system - Single Server option (on page 22), steps 1-2.
2. Select **Distributed.** A non-editable list of components to be installed appears. Click **Continue**.
3. Choose the type of SQL server database you want (see "Select SQL type" on page 28). Also specify the name of the SQL server. Click **Continue**.
4. Select either **Create new database** or **Use existing database** and name the database (see "Select SQL type" on page 28). If you choose the latter, select to **Keep** or **Overwrite** existing data. Click **Continue**.
5. Refer to Install your system - Single Server option (on page 22), step 4-5.

Install your system - Custom option

Note that with this option you can select or clear all of the components to install, except the management server. The management server is by default selected in the component list and will always be installed. If one is already installed, it will be updated.

1. Refer to Install your system - Single Server option (on page 22), steps 1-2.
2. Select **Custom**. A list of components to be installed appears. Apart from the management server, all elements in the list are optional. The recording server is by default deselected, but you can change this if needed. Click **Continue**.
3. Choose the type of SQL server database you want (see "Select SQL type" on page 28). If relevant, also specify the name of the SQL server. Click **Continue**.
4. Select either **Create new database** or **Use existing database** and name the database (see "Select SQL type" on page 28). If you choose the latter, select to **Keep** or **Overwrite** existing data. Click **Continue**.
5. Select either **This predefined account** or **This account** to select the service account (see "Select service account" on page 29). If needed, enter a password and confirm this. If you are installing a recording server and a recording server is also already installed on the same machine, this dialog is shown twice. Click **Continue**.
6. Specify recording server properties (see "Recording/failover recording server install properties" on page 28). Click **Continue**.
7. If you have more than one available IIS website, you can select any of these. However, if any of your websites have HTTPS binding, select one of these. Click **Continue**.
8. Refer to Install your system - Single Server option (on page 22), step 4-5.

Install failover recording server (recording server)

IMPORTANT: During the installation process, you are asked to specify a user account under which the **Failover Server service** should run. This user account must have administrator rights in the system. Note also that if you run workgroups, you should ignore the normal installation guidelines for installing recording servers and use the alternative installation method for workgroups (see "Install your system - preconditions" on page 21).

Once you have installed the management server using the common installer, you can download the separate recording server installer from the management server's web page (see "Download Manager/download web page" on page 35) (controlled by the Download Manager). As part of this installer, you can specify whether the installer should result in a standard recording server or a failover recording server.

1. Go to the Management server's download web page and select the Recording Server installer suitable for your needs. Save the installer somewhere appropriate and run it from here or run it directly from the web page.
2. Select the **Language** you want to use during the installation (this does not affect the language of your system, choose this later in the process). Click **Continue**.
3. From a selection list of:
   - **Typical**, which installs a standard recording server with default settings
   - **Failover**, which installs a recording server as a failover recording server
   - **Custom**, which installs a standard recording server and offers configuration options, for example, letting you install more than one recording server instance on the current machine.

   Select **Failover.**
4. Specify failover recording server properties (see "Recording/failover recording server install properties" on page 28). Click **Continue**.
5. When installing a failover recording server it is mandatory to use a particular user account (**This account**) (see "Select service account" on page 29). If needed, enter a password and confirm this. Click **Continue**.
6. Refer to Install your system - Single Server option (on page 22), step 4-5.

When the failover recording server is installed, you can check its state from the **Failover Server service** icon and start using it.

Install other components (such as Milestone Mobile server)

All XProtect system components, including the Milestone Mobile server, are available for separate download and installation from the management server's download web page (see "Download Manager/download web page" on page 35) (controlled by the Download Manager). You may need these separate component installers for installing, for example:

- the Milestone Mobile server

- a component on a dedicated server
- one or more failover recording servers.

Some components are only available from here.

About installing the Milestone Mobile server

Once you have installed the Milestone Mobile server, you can use Milestone Mobile (a smartphone and tablet compatible client) and XProtect Web Client with your system. To reduce the overall use of system resources on the computer running the management server, install the Milestone Mobile server on a separate computer. For more information about how to do this, refer to Milestone Mobile Administrator's Manual http://clouddownload.milestonesys.com/XProtect%20Mobile%2020a/Manuals/MilestoneXProtectMobile_Administrators_Manual_en_US.pdf.

Install your system on virtual servers

You can run all system components on virtualized (see "Installation overview" on page 20) Windows® servers, such as - for example - VMware® and Microsoft® Hyper-V®. Contact your IT department for more information.

Tip: Virtualization is often preferred to better utilize hardware resources. Normally, virtual servers running on the hardware host server do not load the virtual server to a great extent, and often not at the same time. However, recording servers record all cameras and video streams. This puts high load on CPU, memory, network, and storage system. So, when run on a virtual server, the normal gain of virtualization disappears to a large extent, since - in many cases - it will use all available resources.

If run in a virtual environment, it is important that the hardware host has the same amount of physical memory as allocated for the virtual servers and that the virtual server running the recording server is allocated enough CPU and memory - which it is not by default. Typically, the recording server needs 2-4 GB depending on configuration. Another bottleneck is network adapter allocation and hard disk performance. Consider allocating a physical network adapter on the host server of the virtual server running the recording server. This makes it easier to ensure that the network adapter is not overloaded with traffic to other virtual servers. If the network adapter is used for several virtual servers, the network traffic might result in the recording server not retrieving and recording the configured amount of images.

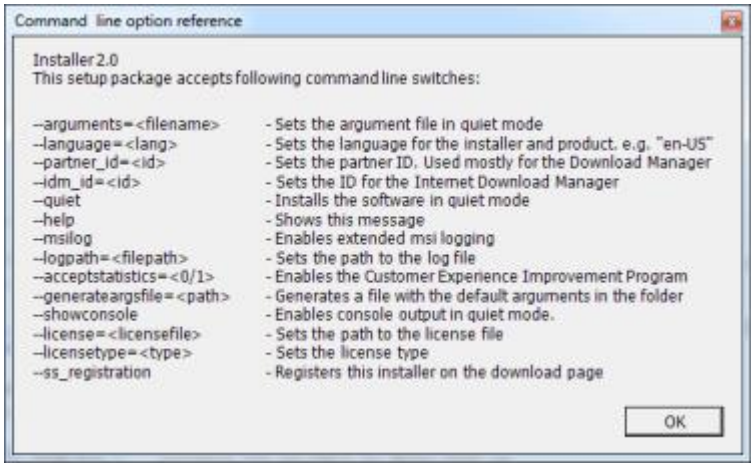
About installer commands

As an administrator, you have a set of installer command you can use when you work with XProtect installers.

1. On the machine where you want to enter an installer command, go to Window's **Start**, and open a Command Prompt window.
2. In the *Command Prompt*, execute the required installer command - possible with a prefix. Note that there is a [space] before -- in all installer command lines.

   Example: *RecordingServer_setup_x64.exe --ss_registration*

Tip: To get an overview of installer commands, in the *Command Promt,* type [space]*--help* and the following window appears:



Troubleshoot management server installation

The following issue may occasionally occur during or upon installation of management servers.

Issue: Changes to SQL server location prevents database access

This is an issue if the location of the SQL Server is changed, for example by changing the host name of the computer running the SQL Server. The result of this issue will be that the access to the database is lost.

Solution: Use the update SQL address tool found at the tray icon, aka Systray.

More about installing

Recording/failover recording server install properties

Fill out the following properties when you install a standard recording server (see "Install your system - Custom option" on page 23) or a failover recording server (see "Install failover recording server (recording server)" on page 24):

Name	Description
Recording server name:	A name for the server in question. If required, you can later change the name.
Management server address:	The IP address (example: *123.123.123.123*) or host name (example: *ourserver*) of the management server to which the server should be connected. If required, you can later change the management server IP address/host name as part of the basic administration on the Recording server service/Failover Server service.
Media database:	The path to the media database. The media database is the recording server/failover recording server's default storage area that is the default location in which recordings from connected cameras are stored in individual camera databases. If required, you can later change the path, and/or add paths to more storage area locations.

Select SQL type

In the installer dialogs (see "Install your system - Custom option" on page 23), you must decide what to do regarding SQL database (see "Install your system - Distributed option" on page 23). The options are **Install SQL Server 2008 Express on this computer** / **Use the installed Microsoft SQL Server Express database on this computer** or **Use an existing SQL Server on the network**. As indicated, the wording used for selecting SQL server type varies depending on whether you already have installed an SQL database on the current machine:

- First option when you have **no** SQL database installed: **Install SQL Server 2008 Express on this computer**
  First option when you have **an** SQL database installed: **Use the installed Microsoft SQL Server Express database on this computer**
- Second option: **Use an existing SQL Server on the network** is the second option.

However, it can be difficult to determine which SQL server type is right for your organization. The Microsoft SQL Server Express Edition is a "lightweight" version of a full SQL server. It is easy to install and prepare for use, and often suffices for systems with less than 300 cameras. However, if you plan to perform frequent/regular backups of your database, Milestone recommends using an existing SQL server on the network (you must have administrator rights on the SQL server). For large installations (300 cameras or more), Milestone recommends using a full-scale existing SQL server on a dedicated machine on the network.

IMPORTANT: Milestone recommends that you install the database on a dedicated hard disk drive that is not used for anything else but the database. Installing the database on its own drive prevents low disk performance.

IMPORTANT: If relevant, during the database preparation process, you are asked whether you want to create a new database, use an existing database, or overwrite an existing database. For a new installation, you would typically select the default option **Create new database.** However, if you are installing the database as part of upgrading to a newer version of the system, and you want to use your existing database, make sure you select **Use existing database**.

Select service account

In the installer dialogs (see "Install your system - Custom option" on page 23), you are asked to select a service account under which the Management Server service runs:

- With a predefined network service account (**This predefined user account**), the service always runs when the server (computer) are running - no matter which account is used. The account matters for access to various resources.
- With a particular user account (**This account**), the service uses the specified user account to run the service under the account as management server. If the server acting as management server is a member of a domain, you should either select the suggested **Network Service** or specify a user account for the domain in question.

  Note that if the server in question is a failover recording server, it is **not** possible to select **This predefined account,** and when selecting **This account**, it is **only** possible to select to specify a user account for the domain in question.

When should I choose a particular user account instead of a predefined? If you use network drives, you should always specify a particular user account (with access to the network drives in question). Otherwise, the relevant service cannot access the required network drives.

Choose between a predefined network service account and a particular user account:

1. Select **This predefined account**.

a) Select **Network Service**.

b) Click **OK**.

- or -

1. Select **This account**.

a) Click **Browse...**. This opens the **Select User** window.

b) Verify that the relevant domain/workgroup is specified in the **From this location** field. If not, click **Locations...** to browse for the required domain/workgroup.

c) In the **Enter the object names to select** box, type the required user name. Click **OK**.

Tip: Typing part of a name is often enough. Use the **Check Names** feature to verify that the name you have entered is recognized.

d) In the **Password** field, specify the password for the user account and in the **Confirm password** field, confirm the password. The password fields cannot be empty. The password for the account must contain one or more characters and/or digits. Click **OK**.

Log in to the Management Client

Access to the Management Client requires certain user rights. Consult your surveillance system administrator if in doubt.

1. Click the Management Client desktop icon or—in Windows' **Start** menu—select **All Programs** > **Milestone** > **XProtect Management Client**. This makes the login window appear.
2. In the **Computer** field, type the name of the computer running the management server **(leaving out** http/https in front).
3. You have three different options when logging in: **Windows Authentication (current user)**, **Windows Authentication**, and **Basic Authentication**.
4. By default, you log in with your active Windows account. This means that if you are currently logged in as, for example, **JohnSmith**, by default you log in to the management server as **JohnSmith** as well.
5. Depending on how you wish to log into the management server, in the **Authentication** field select:
   - **Windows Authentication (current user)** if you want to log in with your active Windows account (this is the default login option).
   - **Windows Authentication**, if you want to log in with a different Windows account.
   - **Basic Authentication**, if you want to log in with a basic user authentication.

     For **Windows Authentication** and **Basic Authentication** also fill in the **User name** and **Password** fields respectively.

   Tip: If you have logged in with a specific user type before (**Windows Authentication**, **Basic Authentication,** or both) you can select previously entered user names in the user name list.
6. Click **Connect** to open Management Client.

Install XProtect Smart Client

The XProtect Smart Client provides remote users with a feature-rich access to the surveillance system and enables them to view live and recorded video and to access other features from the system. The XProtect Smart Client supports IPv6.

You must install XProtect Smart Client locally on the remote user's computer. This can be done in three different ways: from a server, from a DVD or through a silent install. You can also remove XProtect Smart Client at a later time.

Find more information about XProtect Smart Client in its own built-in help system which is available after installation, or see the XProtect Smart Client User's Manual, available on the software DVD as well as from http://www.milestonesys.com/downloads.

Upgrade from previous version

This information is only relevant if you are upgrading a previous XProtect installation.

IMPORTANT: Your XProtect system no longer supports Microsoft Windows XP (see "System requirements" on page 7).

When upgrading, all components— **except** the management server database and if you selected so also your video device drivers—are automatically removed and replaced. The management server database is the management server's component, it contains the entire system configuration (recording server configurations, camera configurations, rules, and so on). As long as you do not remove the management server database, no reconfiguration of your system configuration is needed (although you may want to configure some of the new features in the new version).

Backward compatibility with recording servers from versions older than this current version is limited. You can still access recordings on such older recording servers, but to be able to change their configuration, they must be of the same version as this current one. Therefore, it is highly recommended to upgrade all recording servers in your system.

When you do an upgrade including your recording servers, you are asked whether you want to **update** or **keep** your video device drivers. If you choose to update, it might take a few minutes for your hardware devices to make contact with the new video device drivers after restarting your system. This is due to several internal checks being performed on the newly installed drivers.

Prerequisites

- Have your **temporary license (***.lic***) file** ready. The license file changes when your SLC changes, so you are likely to have received a new license file when you purchased the new version. When you install the management server, the wizard asks you to specify the location of your license (*.lic*) file, which the system verifies before you can continue.

  If you do not have your license file, contact your XProtect product vendor.

- Have your **new product version** ready. If you have not purchased the software on a DVD, you can download it from http://www.milestonesys.com/downloads.

- The management server stores your system's configuration in a database. The system configuration database can be stored in two different ways:

1. In a SQL Server Express Edition database on the management server itself

2. In a database on an existing SQL Server on your network.

   If using 2), **Administrator rights on the SQL Server** are required whenever you want to create, move or upgrade the management server's system configuration database on the SQL Server. Once you are done creating, moving or updating, being the database owner of the management server's system configuration database on the SQL Server is sufficient.

Alternative upgrade for workgroup

If you do not use a domain setup, but a workgroup setup, you must do the following when upgrading:

1. On the recording server, create a local Windows user.
2. From the Windows **Control Panel,** find the **Milestone XProtect Data Collector service.** Right-click it, select **Properties**, and select the **Log on** tab. Set the Data Collector service to run as the local windows user you just created on the recording server.
3. On the management server, create the same local Windows user (with the same user name and password).
4. In the Management Client, add this local Windows user to the **Administrator**'s group.

For installing with workgroups, see Install your system - preconditions (on page 21).

Multiple management servers

Using multiple management servers may be relevant for your organization. Basically, there are two scenarios where multiple management servers can be relevant: One is using multiple management servers in a clustering setup for peace of mind. The other is using not just multiple management servers, but multiple XProtect Corporate systems in a federated architecture.

Clustering

The management server software can be installed on multiple servers within a cluster of servers. This ensures that your system has very little down-time: if a server in the cluster fails, another server in the cluster will automatically take over the failed server's job running the management server. The automatic process of switching over the Management Server service to run on another server in the cluster only takes a very short time (up to 30 seconds). See the Administrator's Manual for more information about prerequisites and installation guidelines for installing multiple management servers.

Milestone Federated Architecture

This section is only relevant if you run XProtect Corporate.

Milestone Federated Architecture™ (MFA) allows multiple individual XProtect Corporate systems to connect in a parent/child hierarchy of federated sites. Each individual site in the federated hierarchy is a standard XProtect Corporate system, complete with management server, SQL Server, one or more recording server(s), failover server(s) and a number of cameras as well as users and administrators.

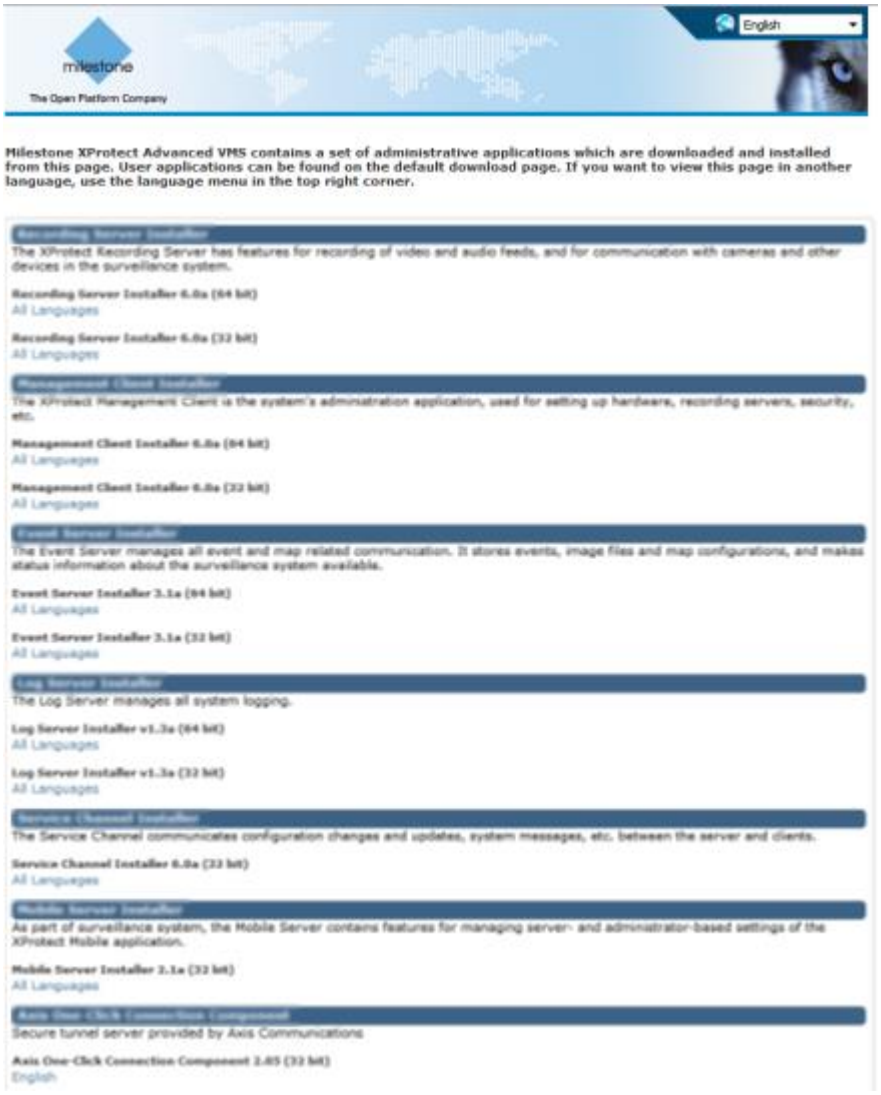
Once several XProtect Corporate systems are added into a federated hierarchy, they appear as one big system to administrators and users, while still being individually manageable. Based on user rights on each system, federated architecture offers users access to video, audio and other resources across all individual sites in the federated hierarchy. Furthermore, it offers administrators access to remote management of all sites from only one login—again based on administration rights on the individual systems.

In principle, there is no limit to the number of sites you can add to a federated hierarchy and how they can be linked, offering you unlimited scaling, flexibility and accessibility.

If you plan to run MFA, make sure to read the management server installation (see "Installation overview" on page 20) prerequisites.

Download Manager/download web page

The management server has a built-in web page. This web page enables administrators and end users to download and install required XProtect system components from any location, locally or remotely.



The web page is capable of displaying two sets of content, both by default in a language version matching the language of the system installation:

- One is targeted at **administrators**, enabling them to download and install key system components. Most often the web page is automatically loaded at the end of the management server installation and the default content is displayed. Otherwise the web page can be accessed by entering the URL:

  http://[management *server address]:[port]/installation/admin/*

where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.

- One targeted at end **users**, providing them access to client applications with default configuration. The content is displayed when the web page is accessed by entering the URL:

  http://[management *server address]:[port]/installation/*

  where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

The two web page(s) automatically has some default content so they can be used straight away after the installation process. As administrator however, by using the Download Manager, you can customize what should be displayed on the web page(s). You are also able to move components between the two versions of the web page, i.e. between the one targeted at system administrators and the one targeted at end users. To move a component, right-click it, and select the web page version you want to move the component to.

Even though the Download Manager lets you control which components users can download and install, you cannot use it as a users' rights management tool. Such rights are determined by roles defined in the Management Client.

You access the Download Manager on the server running the management server software. From Windows' **Start** menu, select **All Programs**, **Milestone**, **XProtect Download Manager**.

Navigate the built-in help system

You can always freely navigate between the help system's contents. To do this, use the help window's three tabs: **Contents**, **Search**, and **Glossary,** or use the links inside the help topics.

Tab	Description
Contents	Navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer. To go straight to the help system's **Contents** tab, click **Contents...** button in the Management Client's toolbar.
Search	Search for help topics containing particular terms of interest. For example, you can search for the term **zoom** and every help topic containing the term **zoom** will be listed in the search results. Clicking a help topic title in the search results list will open the required topic. To go straight to the help system's **Search** tab, click the **Search...** button in the Management Client's toolbar.
Glossary	What is a video encoder? What does PTZ mean? The **Glossary** tab provides a glossary of common surveillance and network-related terms. Select a term to view a corresponding definition in the small window below the list of terms.

Clicking an expanding drop-down link displays detailed information. The detailed information is displayed immediately below the link itself and the content on the page expands. To print a help topic, navigate to the required topic and click the browser's **Print** button.

Tip: When you printing a selected help topic, the topic is printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links, click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you require.

Index

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.