Milestone

XProtect®

Corporate 5.0

Administrator's Getting Started Guide

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.

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.

XPCO50-agsg-1(a1)-220312

About This Guide

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

For more detailed feature descriptions, refer to the manuals available on the XProtect Corporate software DVD as well as on www.milestonesys.com. Furthermore, XProtect Corporate features a very comprehensive built-in help system (on page 38).

Also check our website (http://www.milestone.com) for updates to make sure you install the most recent version of our software.

Product Overview, XProtect Corporate

XProtect Corporate 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.

XProtect Corporate 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 **Smart Clients** and **Remote Clients**, which are both unlicensed and can be downloaded and installed for free (as many times as needed).

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

The system also offers the possibility of including the standalone XProtect Smart Client – Player when exporting video evidence from the Smart Client. The 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, XProtect Corporate handles an unlimited number of cameras, servers, and users—across multiple sites if required. XProtect Corporate is capable of handling IPv4 as well as IPv6.

System Requirements

IMPORTANT: XProtect Corporate no longer supports Microsoft® Windows® XP (however, clients can still be run/accessed from computers with Windows XP Professional).

It is recommended to have the Microsoft Active Directory® in place before you install XProtect Corporate. If you add the management server to the Active Directory after installing XProtect Corporate, 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 in an XProtect Corporate solution:

Computer Running Management Server

- **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® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Server 2003 (32 or 64 bit).

  Furthermore, to run clustering/failover servers, a Microsoft® Windows® Server 2003/2008 Enterprise or Data Center edition is needed.
- **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 Server

- **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® 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 2008 R2 (64 bit), 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) or Microsoft® Windows® Server 2003 (32 or 64 bit).
- **Software:** Microsoft .NET 4.0 Framework.

IMPORTANT: When formatting the hard disk of a recording/failover server device, it is important to 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 (see http://support.microsoft.com/kb/140365/en-us - http://support.microsoft.com/kb/140365/en-us).

Computer Running Management Client

- **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® 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 2008 (32 bit or 64 bit*), Microsoft® Windows® Server 2008 R2 (64 bit) or Microsoft® Windows® Server 2003 (32 bit or 64 bit*).

  * Running as a 32 bit service/application

- **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/ **(see http://www.microsoft.com/downloads/ -** http://www.microsoft.com/downloads/**).**

Computer Running Event Server

- **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® Server 2008 R2 (64 bit), 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

- **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® Server 2008 R2 (64 bit), 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

- **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® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit)*, Microsoft® Windows® Server 2003 (32 or 64 bit)*

  * Limited by Windows operating system to ten concurrent, incomplete outbound TCP connection attempts

- **Software:** Microsoft .NET 4.0 Framework, and Internet Information Services (IIS) 5.1 or newer

  If installing on Windows Server 2008, a standard IIS installation must furthermore be customized:

  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 Smart Client

- **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® 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 2008 R2 (64 bit), Microsoft® Windows® Vista Ultimate (32 bit or 64 -bi*), Microsoft® Windows® Vista Enterprise (32 bit or 64 bit*), Microsoft® Windows® Vista Business (32 bit or 64 bit*), Microsoft® Windows® Server 2008, Microsoft® Windows® Server 2003 (32 bit or 64 bit*), and Microsoft® Windows® XP Professional (32 bit or 64 bit*).

  *Running as a 32 bit service/application

- **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/ (see http://www.microsoft.com/downloads/ - http://www.microsoft.com/downloads/).

Computer Accessing Remote Client

- **CPU:** Intel Pentium® 4, minimum 2.4 GHz
- **RAM:** Minimum 256 MB (512 MB 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 1024 x 768 (1280 x 1024 recommended), 16-bit color
- **Hard Disk Space:** Minimum 10 MB free
- **Operating System:** 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*), Windows Vista Ultimate (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*), Windows Vista Business (32 bit or 64 bit*), Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008, Windows Server 2003 (32 bit or 64 bit*), aand Microsoft Windows® XP Professional (32 bit or 64 bit*)

  * Running as a 32 bit service/application

- **Software:** DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from http:// www.microsoft.com/downloads/ (see http://www.microsoft.com/downloads/ - http://www.microsoft.com/downloads/).

Active Directory

XProtect Corporate users are normally added from Active Directory, although users can also be added 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 wishing 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.

Important Port Numbers

XProtect Corporate uses particular ports when communicating with other computers, cameras, etc.

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, but not always, 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 viewing web pages.

When using XProtect Corporate, you must therefore make sure that certain ports are open for data traffic on your network.

The port numbers can be changed. Different port numbers may therefore be used in your organization. See Management Server Service and Recording Server Service (on page 35) for information about changing the recording server-related port numbers.

Tip: Consult the administrator of your organization's firewall if in doubt about how to open ports for traffic.

Virus Scanning Information

Virus scanning should in some cases be avoided—if 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 will most likely use 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 furthermore 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 different recording paths may have been specified in your organization).
- 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 reg. virus scanning, but it is important that the mentioned locations and files are exempt from virus scanning. If allowed, you should therefore 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 remote clients with XProtect Corporate 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 thus 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. It is therefore 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 (see http://support.microsoft.com/kb/816042/en-us - http://support.microsoft.com/kb/816042/en-us)
- Registry entries for the W32Time service (see http://support.microsoft.com/kb/223184/en-us - http://support.microsoft.com/kb/223184/en-us)

If these links do not work for you, try searching www.microsoft.com (see http://www.microsoft.com/ - http://www.microsoft.com/) for time server, time service, synchronize servers or similar.

It is also very important that 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 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 Smart Client and servers is tolerated.

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

Installation Overview

If upgrading from a previous version of XProtect Corporate , make sure you read the upgrade information (see "Upgrade from Previous Version" on page 25).

If you plan to run **Milestone Federated Architecture**, make sure to read about important prerequisites for running Milestone Federated Architecture.

Your XProtect Corporate installation process begins with the installation of the management server software.

- The **management server** is the center of your XProtect Corporate installation. It is typically installed on a dedicated server. See Management Server Installation (see "Install Management Server" on page 15).

Once the management server is installed, you are able to install key components required by the management server:

- The **recording server**, which is used for recording video feeds, and for communicating with cameras and other devices. The recording server is typically installed on one or more separate computers, rather than on the management server itself. See Install System Components (on page 29).

- The **Management Client**, which is used for configuration and day-to-day management of the system. The Management Client is typically installed on the system administrator's workstation or similar. See Management Client Installation (see "Management Client" on page 35).

Finally, you are able to install client software for access to the XProtect Corporate system:

- The Smart Client is the feature-rich client used for access to live and recorded video and other features from the surveillance system. The Smart Client client software must be installed on users' computers. See Install and Remove Smart Client (see "Installing the Smart Client" on page 25) for more information.

- Alternatively, the Remote Client lets you avoid installing client software, as the Remote Client is run straight from the XProtect Corporate system through a browser. It does, however, have significantly fewer features than the Smart Client. See Remote Client Introduction.

Tip: Video device drivers are small programs used for controlling/communicating with the cameras connected to a recording server. You get the drivers automatically during the initial installation of your XProtect Corporate system. However, new versions of the drivers are released from time to time.

As well on traditional servers, installation can also take place on virtualized servers.

Install Management Server

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from Previous Version" on page 25).

If you plan to run **Milestone Federated Architecture**, make sure to read about important prerequisites for running Milestone Federated Architecture.

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of XProtect Corporate.

Your XProtect Corporate installation process begins with the installation of the XProtect Corporate management server software. The management server is the center of your XProtect Corporate installation.

Prerequisites

- **Windows Installer 4.5 - only on Windows Server 2003**

  Before installing XProtect Corporate, it is important that you install Windows Installer 4.5. You can download the Windows Installer 4.5 **(see http://www.microsoft.com/downloads -**

http://www.microsoft.com/downloads**)** from this link: http://www.microsoft.com/downloads **(see http://www.microsoft.com/downloads/ -** http://www.microsoft.com/downloads/**).**

- **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 lightweight, yet powerful, version of a full SQL server) on the management server computer itself.

  Whatever SQL solution you choose, make sure to have Microsoft .NET Framework 3.5 Service Pack 1 installed on the management server computer running the SQL Server Express Edition (even though Microsoft .NET Framework 4.0 is already installed) **or** the separate server running the existing SQL Server. See also System Requirements (on page 8).

  Which SQL Server type is right for our organization? The SQL Server Express Edition is easy to install and prepare for use, and will often suffice for systems with less than 500 cameras. However, if you plan to perform frequent/regular backups of your database, using an existing SQL Server on the network is recommended (**Administrator rights** on the SQL Server are required). For large installations, such as installations with 500 cameras or more, using an existing SQL Server on the network is always recommended.

- **Windows Server 2003 Fix**

  If you use Windows Server 2003 it is recommended to install this supported fix (see http://support.microsoft.com/kb/925336 - http://support.microsoft.com/kb/925336) for Windows Server 2003 before starting: http://support.microsoft.com/kb/925336 (see http://support.microsoft.com/kb/925336 - http://support.microsoft.com/kb/925336). 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.

Installing

1. Shut down any Milestone software running. If upgrading, it is highly recommended that you remove any previous versions of the management server before upgrading. Note, however, that you may not want to remove the management server database, as it contains your XProtect Corporate configuration.

2. Insert the XProtect Corporate software DVD. If the *XProtect Corporate Management Server Installation* window does not open automatically upon inserting the DVD, run the following file from the DVD:

   `setup.exe`

   Tip: Alternatively, if you are installing a version downloaded from the internet, run the *setup.exe* file from the location you have saved it to.

3. A window will open, listing the steps involved in the installation:

4. Complete the steps outlined in the window.

   Tip: Depending on what is already installed on the computer which is going to act as management server, you may not need to complete all of the window's three steps. The step that currently requires your attention will be highlighted.

   Tip: When the management server software is installed, you are able to check the state of the management server by looking at the management server icon in the management server computer's notification area.

   See Management Server Service and Recording Server Service (on page 35) for more information.

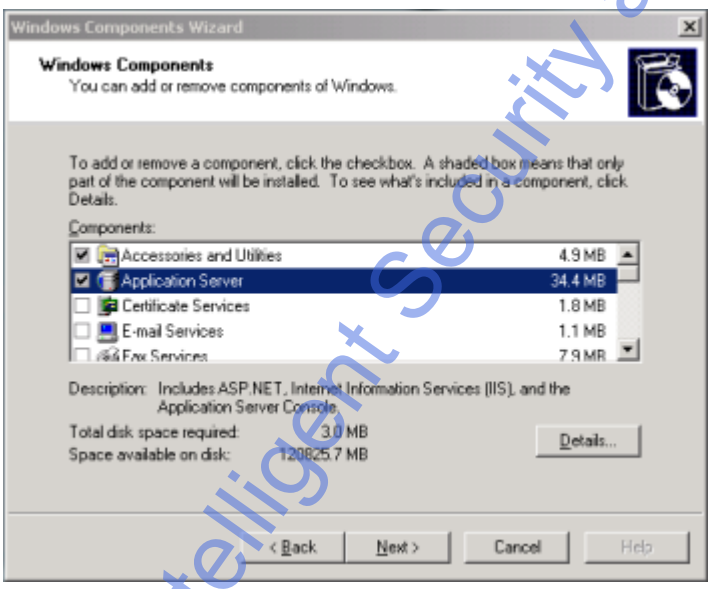
Step 1: Internet Information Services

XProtect Corporate Management Server Installation automatically detects if Internet Information Services (IIS) is already installed. If this step is not available, it is simply because IIS is already installed.

Internet Information Services includes a range of administrative features for managing web servers and web applications, and is required in order to run a XProtect Corporate management server.

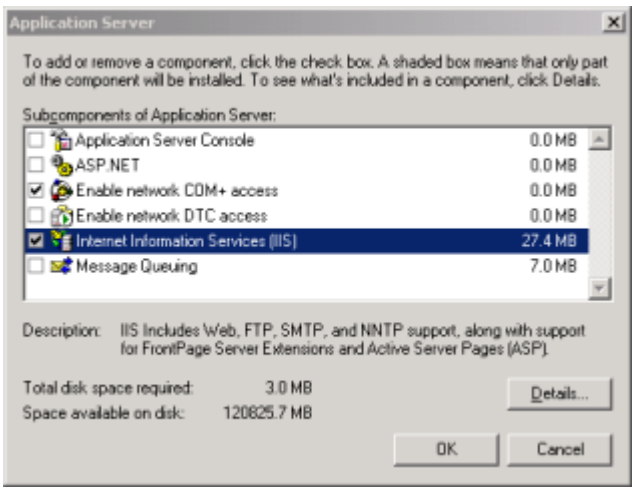
If installing on a server running Windows 2008 Server, IIS is automatically installed once you click the *Internet Information Services* step (should automatic installation fail, it is possible to do installation troubleshooting).

1. On Windows Server 2003, clicking the *Internet Information Services* step opens Windows' built-in *Windows Components* wizard:



2. In the wizard's *Components* list, select *Application Server*.

Click *Details*... and select *Internet Information Services (IIS)*.



3. Click *Details*... and verify that all IIS subcomponents are selected. Click *OK* to return to the *Windows Components* wizard.

4. In the *Windows Components* wizard, click *Next* and follow the wizard.

Tip: It is a good idea to have your Windows installation DVD ready; it may be required during the process.

When IIS is installed, you will be returned to the*XProtect Corporate Management Server Installation* window for the next step of the installation.

Step 2: XProtect Corporate Management Server Database

Before completing this step, click the *View Microsoft SQL Server 2008 Express End-user License Agreement* link to read the license agreement for the software.

This step opens the *Database Setup* wizard, which will guide you through the process of preparing a database for use with the management server.

In the *Database Setup* wizard you will get the choice of using an existing SQL Server on the network or setting up a SQL Server Express Edition (a lightweight, yet powerful, version of a full SQL server) on the management server computer itself.

Follow the wizard's steps by clicking *Next*.

IMPORTANT: We recommend 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 will prevent low disk performance.

IMPORTANT: During the database preparation process, you will be 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 XProtect Corporate, and you want to use your existing database, make sure you select *Use existing database*.

When you have prepared the database, you will be returned to the *Milestone XProtect Corporate Management Server Installation* window for the last step in the management server installation.

Step 3: XProtect Corporate Management Server

This step opens a wizard, which will guide you through the process of installing the management server software itself.

Opening page in *Management Server Setup* wizard

Follow the wizard's steps by clicking *Next*.

Tip: The wizard will ask you to specify the location of your temporary license (.lic) file. The system will verify your license file before you are able to continue. Therefore, have your license file ready.

On one of the wizard's steps, you will be asked to select between two installation options:

Typical (on page 19)

-or-

Custom (on page 19)

You install the XProtect service channel, XProtect event server and XProtect log server as part of the management server installation. But if required you can just as well install these on another server in your surveillance system:

- Installing the XProtect service channel enables automatic and transparent configuration communication between servers and clients in your XProtect Corporate installation.
- Installing the XProtect event server enables handling alarms and maps. Maps provide a physical overview of your surveillance system: Which cameras are placed where, and in what direction are they pointing? As mentioned it does not necessarily have to be installed on the management server - in fact, you can often achieve better performance by installing the event server on another server.
- Installing the XProtect log server provides the necessary functionality for logging information from your XProtect Corporate installation.

Typical

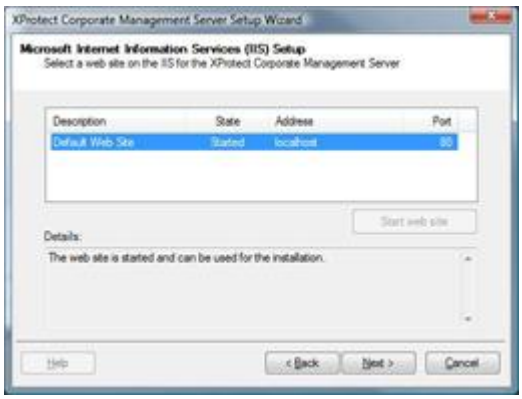
If you select *Typical* installation, the wizard will install all the management server components at their default location and with other default settings. A Typical installation is recommended for most users.

Custom

If you select *Custom* installation, you get the option to select where to install each individual management server component. A *Custom* installation is recommended for advanced users.

Only relevant if selecting *Custom* installation:

On one of the wizard's steps you will be asked to select an IIS (Internet Information Services) web site for the Management Server Service:



Select one of the listed web sites, and make sure the selected web site is started, then click *Next*. If the selected web site is not started, *Next* is disabled.

Tip: You may find that only a single IIS web site—the Default Web Site—is listed. In that case simply make sure that the web site is started, then click *Next*.

Towards the end of the wizard, in the *Service Log On Setup* window, you will be asked to select a user account under which the Management Server Service will run:

You will be able to select either a:

- predefined Network Service account (see "Select a Predefined Account; Network Service" on page 21) (in which case the service will run whenever the computer acting as management server is running).

  - or -

- particular user account (see "Select a Particular User Account" on page 21) (in which case the service will use the specified user account to log in to the computer acting as management server).

Tip: If the computer acting as management server is a member of a domain, you should either select *Network Service*, or make sure that you specify a user account which belongs to the domain in question.

What's Next?

Upon installation of the management server software, the management server's built-in web page automatically opens in a browser. The web page lets you install key components required by the management server, among these:

- One or more **recording servers** (for recording video feeds and for communicating with cameras and other devices)
- A **Management Client** (for configuration and day-to-day management of the system)

Even though the web page opens automatically on the management server computer, you will in most cases want to install the key components on other computers than the management server itself. This is no problem since installation takes place through the web page, which can easily be accessed from other computers. See Install System Components (on page 29) for further information.

Select a Predefined Account; Network Service

1. Select *This predefined account*.
2. Select *Network Service*.
3. Click *OK*.

Select a Particular User Account

1. Select *This account*.
2. Click *Browse...*. This will open the *Select User* window.
3. In the *Select User* window, verify that the required domain is specified in the *From this location* field. If not, click *Locations...* to browse for the required domain.
4. In the *Enter the object names to select* box, type the required user name.

   Tip: Typing part of a name is often enough. Use the *Check Names* feature to verify that the name you have entered is recognized.
5. Click *OK*.
6. Specify the password for the user account in the *Password* field, and confirm the password in the *Confirm password* field.

   The password fields must not be empty; the password for the account must contain one or more characters and/or digits.
7. Click *OK*.

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 interconnected 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 XProtect Corporate 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 XProtect Corporate Administrator's Manual for more information about prerequisites and installation guidelines for installing multiple management servers.

Milestone Federated Architecture

XProtect Corporate Milestone Federated Architecture™ (MFA) allows multiple individual XProtect Corporate systems to interconnect 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 prerequisites (see "Install Management Server" on page 15).

Management Server Installation Troubleshooting

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

Issue: Automatic IIS Installation for Mgmt. or Event Server Fails

If installing the management server or the Event Server (custom installation) on a server running Windows 2008 Server, Internet Information Services (IIS) is under normal circumstances automatically installed.

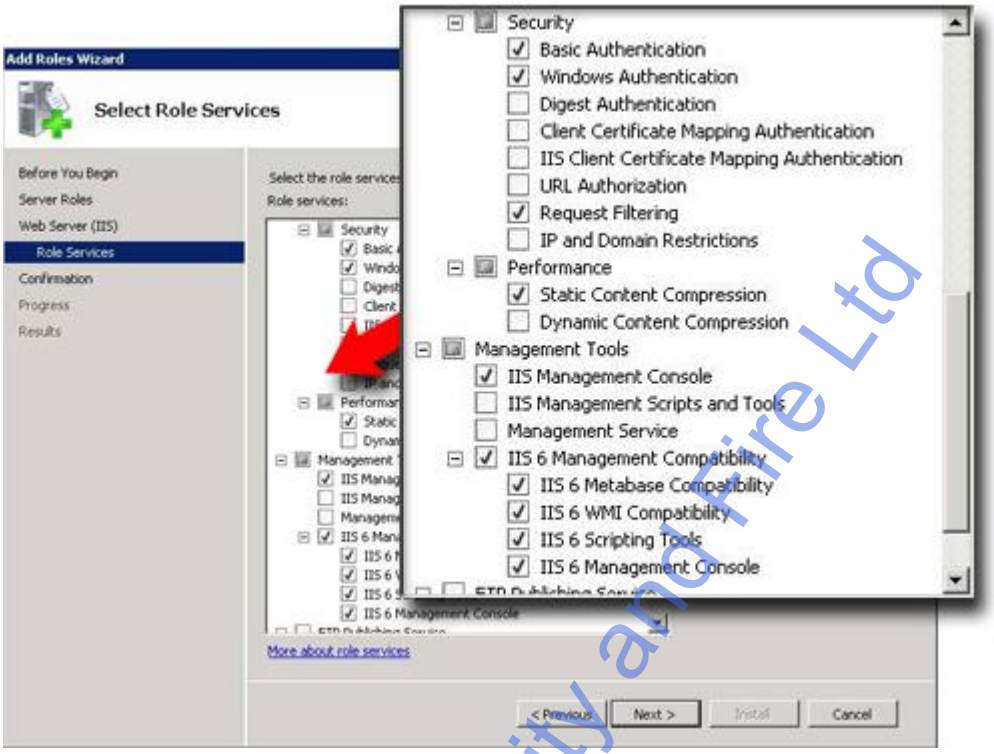
- For the management server, this happens when you click the Internet Information Services step in the XProtect Corporate Management Server Installation window.
- For the event server, this is only a problem if the event server is installed on a different server than the management server.

If the automatic installation fails, you can install IIS manually.

Solution: Install IIS Manually

1. If automatic IIS installation fails, you will see an error message asking you to install IIS manually. In the error message box, click *Install IIS Manually*.
2. You will now see the *Server Manager* window. In the left side of the window, select *Roles*, then the *Roles Summary*.
3. Now select *Add Roles* to start a wizard.
4. In the wizard, click *Next*, select *Web Server (IIS)*, and follow the wizard's steps.
5. When you reach the wizard's *Select Role Services* step, you will see that some role services are selected by default. However, you should select some additional role services:
   - Under *Security*, select *Basic Authentication* and *Windows authentication*.
   - Under *Management Tools*, select *IIS 6 Management Console*, expand it, and select *IIS 6 Metabase Compatibility*, *IIS 6 WMI Compatibility*, *IIS 6 Scripting Tools*, and *IIS 6 Management Console*.

- When ready, the relevant part of the *Role services* tree should look like this:



6. Complete the wizard by following the remaining steps.

Issue: Changes to SQL Server Location Prevents Database Access

This is an issue if using an MS SQL Server database as the XProtect Corporate management server database: If the location of the SQL Server is changed, for example by changing the host name of the computer running the SQL Server, access to the database will be lost.

Solution: Run Management Server Database Installation Step Again

See Management Server Installation (see "Install Management Server" on page 15). When running the database installation, you will - during the database preparation process - be asked whether you want to create a new database, use an existing database, or overwrite an existing database: Pointing to the new location of the SQL Server, select to use an existing database. This will update the SQL connection string used by the management server, and it will again be possible to access the database.

Failover Server Installation

For more details about failover servers and their installation, see the XProtect Corporate Administrator's Manual.

Log in to the Management Client

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

1. Click the XProtect Corporate Management Client desktop icon or—in Windows' *Start* menu—select *All Programs* > XProtect Corporate > *Management Client*. This will make the login window appear:

Management Client login window

2. The login window's *Server type* field will in many cases appear dimmed and pre-filled with the required information. If not, select XProtect Corporate.

3. In the *Server address* field, type the IP address or host name of the computer running the XProtect Corporate management server.

   Tip: If you have logged in before, you can select previously used server IP addresses or host names from the list.

4. By default, you will log in to the management server with your active Windows account. This means that if you are currently logged in as, for example, *JohnSmith*, you will by default log in to the management server as *JohnSmith* as well.

   - If you wish to log in to the management server with your active Windows account (this is the default login option), select *Windows Authentication (current user)* in the *Authentication* field.
   - If you wish to log in to the management server with a different Windows account, select *Windows Authentication* in the *Authentication* field, then type the required user name and password in the *User name* and *Password* fields respectively.

   Tip: If you have logged in with *Windows Authentication* before, you can select previously entered user names from the list.

   Tip: When using *Windows Authentication*, you have the option of selecting *Remember password*, in which case you will not have to type the password at subsequent logins.

5. Click *Connect* to open Management Client.

Installing the Smart Client

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

Example of the Smart Client, in this case displaying live video

Where can I find more information about the Smart Client? Once installed, the Smart Client has its own built-in help system. Alternatively, refer to the Smart Client User's Manual, available on the XProtect Corporate software DVD as well as from www.milestonesys.com.

The Smart Client must be installed locally on the remote user's computer, which can be done in three different ways. Naturally it can also subsequently be removed.

Upgrade from Previous Version

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

IMPORTANT: XProtect Corporate no longer supports Microsoft® Windows® XP. See System Requirements (on page 8).

The process of upgrading XProtect Corporate involves removing all of its components **except** the Database Server. The Database Server is one of the management server's components, it contains the entire system configuration (recording server configurations, camera configurations, rules, etc.). As long as you do not remove the Database Server, you will not need to reconfigure your surveillance system configuration in any way (although you may of course want to configure some of the new features in the new version).

Backward compatibility with recording servers from XProtect Corporate versions older than 3.0 is limited. You can still access recordings on such older recording servers; but in order for you to be able to change their configuration, they must be of version 3.0 or later. It is thus highly recommended that you upgrade all recording servers in your XProtect Corporate system.

When doing an update which includes updating your recording servers, you automatically update your Video Device Drivers as well. In this case, after restarting your system, it might take several minutes for your hardware devices to make contact with the new Video Device Drivers, so have patience. 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 will change when your SLC changes, so you are likely to have received a new license file when purchasing the new version. When you install the management server, the wizard will ask you to specify the location of your license (.lic) file, which the system will verify before you will be able to continue.

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

- Have your **new XProtect Corporate version** ready. If you have not purchased the software on a DVD, you can download it from www.milestonesys.com (see http://www.milestonesys.com/ - http://www.milestonesys.com/). Note that although you can download any version, you will only be able to install a version for which your license file is valid.

- The management server stores your XProtect Corporate 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, or 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 need 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 database owner of the management server's system configuration database on the SQL Server will suffice.

Upgrading the Management Server

The management server has several components. This describes removing old components—except the Database Server—and installing the new ones:

1. First remove the management server itself. See Remove System Components (on page 27).
2. Next, remove the XProtect Corporate Windows components.
3. If the XProtect Corporate Management Client is installed on the management server itself, remove the Management Client too. See Remove System Components (on page 27).
4. Run the installation file for the new version of XProtect Corporate. After a short while, the installation window will open. Out of the three installation steps for the management server, you will be asked to address step 3 (XProtect Corporate management server).
5. Click the installation window's step 3, and complete the XProtect Corporate management server installation. During this process you will be asked to specify the path to your license (.lic) file.
6. When the management server is installed, the management server's web page will appear in a browser. If you want to install the Management Client software on the management server itself, you can do it from the management server's web page.

Upgrading Recording Servers

Once the new management server is installed, you can remove the old recording server version, and install the new one:

What happens to the recording server's recordings? During the removal process, you will be asked whether you want to keep the recording server's recordings.

1. See Remove System Components (on page 27) for how to remove a recording server.
2. When the recording server has been removed, open a browser and connect to the management server's web page at the following address:

   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.
3. From the web page, install the new version of the recording server software.
4. Repeat for each recording server on your XProtect Corporate system.

When updating your recording servers, you automatically update your Video Device Drivers as well. After restarting your recording servers, it might take several minutes for your hardware devices to make contact with the new Video Device Drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Upgrading a Management Client

If the Management Client is installed on separate computers, such as the surveillance system administrator's workstation or similar, you should now remove the old version and install the new one:

1. See Remove System Components (on page 27) for details on removing a Management Client.
2. When the Management Client has been removed, open a browser and connect to the management server's web page at the following address:

   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.
3. From the web page, install the new version of the Management Client.

Upgrading the Smart Client

Smart Client users should now remove their old Smart Client versions and install the new one:

1. See Installing the Smart Client (on page 25) for how to remove a Smart Client.
2. When the Smart Client has been removed, open a browser and connect to the management server's web page at the following address:

   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.
3. From the web page, install the new version of the Smart Client.

Remove System Components

If you are not an XProtect Corporate system administrator, do not attempt to remove the management software.

The following procedure describes standard system component removal in recent Windows versions; the procedure may be slightly different in older Windows versions:

1. In Windows' *Start* menu, select *Control Panel*, and then...
   - If using *Category* view, find the *Programs* category, and click *Uninstall* a program.
   - If using *Small icons* or *Large icons* view, select *Programs and Features*.
2. In the list of currently installed programs, right-click the required program or service, select *Uninstall*, and follow the removal instructions.

Removing Management Server

XProtect Corporate management servers are most likely installed on a dedicated server.

To remove, follow the general removal procedure (see "Remove System Components" on page 27).

Removing Management Client or Service Channel

XProtect Corporate Management Client and **XProtect service channel** are all removed at the computer on which the program or service is installed.

To remove, follow the general removal procedure (see "Remove System Components" on page 27).

Removing Recording Server

To remove an **XProtect Corporate recording server**, use the following procedure on the computer on which the recording server is installed:

What happens to the recording server's recordings? During the removal process, you will be asked whether you want to keep the recording server's recordings.

1. Stop the recording server service by right-clicking the recording server icon in the computer's notification area (also known as the *system tray*), then selecting *Stop Recording Server Service*.

Example: recording server notification area icon

2. To remove, follow the general removal procedure (see "Remove System Components" on page 27). Right-click the *XProtect Corporate Recording Server* in step 2 of the process.

Install System Components

If upgrading from a previous version of XProtect Corporate, make sure you read the upgrade information (see "Upgrade from Previous Version" on page 25).

Installation of the following components is **not** covered in this section: XProtect event server, XProtect log server, management server (see "Install Management Server" on page 15) and XProtect service channel. See installation details for each.

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of Milestone XProtect Corporate.

IMPORTANT: As a prerequisite make sure of the following. During the installation process you will be asked to specify a user account under which the *Failover Server Service* will run. For the failover solution to work, the failover server has to use the same user account as the recording server. Furthermore, the user account you specify must have access to your XProtect Corporate system with administrator rights. **Do the following to make sure of this...**

To verify whether the user account has administrator access to your XProtect Corporate system, do the following:

1. In the Management Client's Site Navigation pane, expand Security and select *Roles*. In the overview pane's roles list, select the *Administrators* role.
2. In the properties pane's role settings list, verify that the required user is listed.
3. If the user is not listed, add the required user to the Administrators role by clicking *Add...* below the role settings list.

Part I—Downloading the Installer

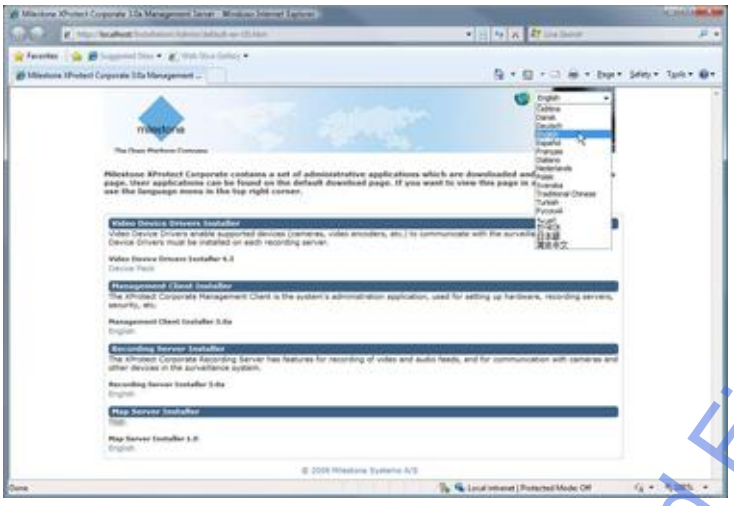
The following describes the installation process. The process is more or less similar for the component types mentioned, so replace *the component* with *the XProtect Corporate recording server*, *failover server* or *the Management Client*, depending on your needs.

1. On the computer on which you will install the component, shut down any Milestone software running. If upgrading, it is highly recommended that you remove (see "Remove System Components" on page 27) any previous versions of the component before upgrading.
2. With an Internet Explorer browser, connect to the XProtect Corporate management server at the following address:

   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.

This will open the management server's built-in web page. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.



3. The web page is available in a number of different languages. In this example, we assume that you view the web page in English, and that you want to install English versions of the Milestone XProtect Corporate components.

   On the web page find the relevant component's installer section, and then click the *English* link under the required recording server version (often, only one version will be available).

Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking *Run* or similar (exact button text depends on your browser version).

Part II—Installing the Component

Select the relevant component for a description of the process (if required, repeat the process on other computers where the component should be installed):

Recording Servers

1. This will open the XProtect Corporate *Recording Server Setup* wizard, which will guide you through the installation.

   On the first step of the wizard, click *Next*.

2. Select installation method:

   Typical (see "Recording servers (Typical)" on page 31)

   - or -

   Custom (see "Recording servers (Custom)" on page 31)

3. Click *Install*.

4. On the last step of the wizard, click *Finish*. The recording server is now installed. The recording server has no user interface as such; it is accessed and managed through the Management Client.

Tip: When the recording server software is installed, you are able to check its state.

See Management Server Service and Recording Server Service (on page 35) for more information.

Recording servers (Typical)

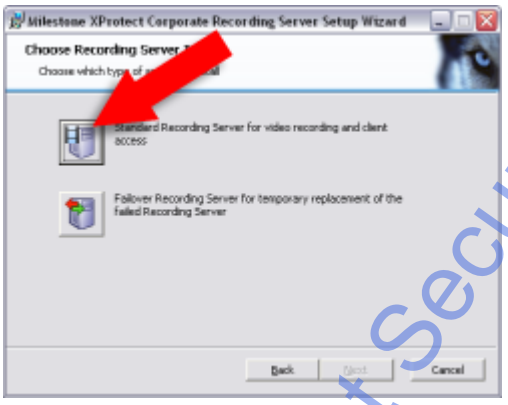
The *Typical* option installs the XProtect Corporate recording server with default settings. A *Typical* installation is recommended for most users.

1. Specify recording server setup parameters (see "Specify Recording Server Setup Parameters" on page 32).
2. Click *Next*.

Recording servers (Custom)

The *Custom* option lets you select where to install the XProtect Corporate recording server components. A *Custom* installation is recommended for advanced users.

1. Select required installation folder, then click *Next*.
2. When asked which type of server to install, click the *Standard recording server* [...] icon. This lets you install a regular recording server.



3. Specify recording server setup parameters.
4. Click *Next*.
5. The wizard will ask you to select a user account under which the XProtect Corporate *Recording Server Service* will run.

   You must select between:

   - a predefined system account (see "Select a Predefined System Account" on page 32)

     - or -

   - a particular user account (see "Select a Particular User Account" on page 32) (in which case the service will use the specified user account to log in to the computer acting as recording server).

     Tip: If the computer acting as recording server is a member of a domain, select the predefined account Local System or make sure you specify a user account which belongs to the domain in question.

     If using network drives, you should always specify a particular user account (which has access to the network drives in question), as the *Recording Server Service* will not be able handle the network drives otherwise.

6. Click *Next*.

7. In some cases it can be advantageous to install more than one instance of the recording server on the same physical server (see "Multiple Recording Server Instances" on page 33). Specify the required number of instances (default is 1), then click *Next*.

   - Only relevant if installing more than one instance of the recording server on the same physical server: For each instance, specify the IP address to use for the instance in question.

     IMPORTANT: Note that the IP addresses you specify must be assigned to the physical server in question. Furthermore, even though your organization will not use IPv6 addresses, make sure to assign both IPv6 and IPv4 on the server as these are needed by the software.

     Tip: Provided enough IP addresses are assigned to the server, the fields will be pre-filled.

8. Click *Next*.

Select a Predefined System Account

1. Select *This predefined account*.
2. Select *Local System, Local Service*, or *Network Service* as applicable.
3. Click *OK*.

Select a Particular User Account

1. Select *This account*.
2. Click *Browse...*. This will open the *Select User* window.
3. In the *Select User* window, verify that the required domain is specified in the *From this location* field. If not, click *Locations...* to browse for the required domain.
4. In the *Enter the object names to select* box, type the required user name.

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

5. Click *OK*.
6. Specify the password for the user account in the *Password* field, and confirm the password in the *Confirm password* field.

   The password must contain one or more characters and/or digits.

7. Click *OK*.

Specify Recording Server Setup Parameters

- **Name:** A name for the server in question. If required, you can later change the name through the XProtect Corporate Management Client.
- **Milestone XProtect Corporate management server:** The IP address (example: 123.123.123.123) or host name (example: ourserver) of the management server to which the server in question 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 or Failover Server Service.
- **MediaDB:** The path to the server in question's media database. The media database is the recording server's default storage area, i.e. 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, from the XProtect Corporate Management Client.

When should I choose a particular user account instead of a predefined? If using network drives you should always specify a particular user account (with access to the network drives in question). Otherwise the service in question is unable to handle the required network drives.

Multiple Recording Server Instances

It is only recommended to install multiple instances of the Recording Server Service on the same server under the following conditions.

If you:

- are upgrading from XProtect Corporate 4.1 or older

  —and—

- are already running more 32-bit Recording Server Service instances on the same server.

Since it is not possible to move devices/cameras from one recording server to another, setups running more than one 32-bit Recording Server Service instances on the same server, will need to maintain this structure.

For all other setups, the newer 64-bit recording server eliminates the need for running more 32-bit instances on the same server.

Recording Server Installation Troubleshooting

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

Issue: Recording Server Startup Fails due to Port Conflict

This is an issue if either the Simple Mail Transfer Protocol **(**SMTP) Service or an existing installation of XProtect Enterprise is running.

Both use port 25. If port 25 is already in use, it may not be possible to start the XProtect Corporate Recording Server Service. It is important that port number 25 is available for the recording server's SMTP service since many cameras are only capable of communicating via this port.

SMTP Service: Verification and Solutions

To verify whether SMTP Service is installed, do the following:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the left side of the *Add or Remove Programs* window, click *Add/Remove Windows Components*.
4. In the *Windows Components* wizard, select the *Internet Information Services (IIS)* item, and click *Details...*.
5. In the *Internet Information Services (IIS)* window, verify whether the *SMTP Service* check box is selected. If it is, SMTP Service is installed.

If SMTP Service is installed, select one of the following solutions:

Solution 1: Disable SMTP Service, or set it to manual startup

This solution lets you start the recording server without having to stop the SMTP Service every time:

1. From Windows' *Start* menu, select *Control Panel*.

2. In the *Control Panel*, double-click *Administrative Tools*.
3. In the *Administrative Tools* window, double-click *Services*.
4. In the *Services* window, double-click the *Simple Mail Transfer Protocol (SMTP)* item.
5. In the *SMTP Properties* window, click *Stop*, then set *Startup type* to either *Manual* or *Disabled*.

   Tip: When set to *Manual*, the SMTP Service can be started manually from the *Services* window, or from a command prompt using the command *net start SMTPSVC*.
6. Click *OK*.

Solution 2: Remove SMTP Service

Note that removing the SMTP Service may affect other applications using the SMTP Service.

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the left side of the *Add or Remove Programs* window, click *Add/Remove Windows Components*.
4. In the *Windows Components* wizard, select the *Internet Information Services (IIS)* item, and click Details....
5. In the *Internet Information Services (IIS)* window, clear the *SMTP Service* check box.
6. Click *OK, Next*, and *Finish*.

XProtect Enterprise: Verification and Solutions

To verify whether XProtect Enterprise is installed, do the following:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the *Add or Remove Programs* window, verify whether XProtect Enterprise appears in the list. If it does, XProtect Enterprise is installed.

If XProtect Enterprise is installed, select one of the following solutions:

Solution 1: Remove XProtect Enterprise

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the *Add or Remove Programs* window, select XProtect Enterprise, click *Uninstall/Change*, and then *OK*.

Solution 2: Set XProtect Enterprise Services to manual startup

This solution lets you start the recording server without having to stop the XProtect Enterprise Services every time:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Administrative Tools*.
3. In the *Administrative Tools* window, double-click *Services*.
4. In the *Services* window, repeat steps a-c for these items: *Milestone ImageImportService, Milestone ImageServer, Milestone LogCheckService, Milestone Recording Server.*
5. Double-click the item.

6. In the *<item> Properties* window, click *Stop*, then set *Startup type* to *Manual*.
7. Click *Close*.

Tip: With the startup type *Manual*, you can start and stop the XProtect Enterprise Services from a command file:

To start the XProtect Enterprise Services from a command file, create a file named e.g. *startx.cmd* with the following content:

```
net start "Milestone ImageImportService"
net start "Milestone ImageServer"
net start "Milestone LogCheckService"
net start "RecordingServer"
```

To stop the XProtect EnterpriseServices from a command file create a file named e.g. *stopx.cmd* with the following content:

```
net stop "Milestone ImageImportService"
net stop "Milestone ImageServer"
net stop "Milestone LogCheckService"
net stop "RecordingServer"
```

Management Client

1. In the *Select installer language* drop down box, select language to use during the installation. In this example, we assume that you prefer English.
2. Next to appear is the XProtect Corporate *Management Client Setup* wizard, which will guide you through the installation process. On the first step of the wizard, click *Next***.**
3. Select required installation folder, then click *Next*.
4. Click *Install* to begin installation; wait while the required components are installed.
5. When ready, click *Finish***.**
6. To get an overview of the Management Client, select *Launch XProtect Corporate Management Client.* This will start the Management Client right away.

Management Server Service and Recording Server Service

When the XProtect Corporate management server software is installed, you are able to check the state of the Management Server Service by looking at the *Management Server Service* icon in the notification area **of the computer running the management server**.

Likewise, when the XProtect Corporate recording server software is installed, you are able to check the state of the Recording Server Service by looking at the *Recording Server Service* icon in the notification area of the computer running the recording server in question.

The notification area icon also lets you start and stop the Management Server Service/Recording Server Service, view status messages, etc.

Tip: The notification area is also known as the *system tray.* It is located at the far right of the management / recording server's Windows taskbar.

IMPORTANT: When the **Recording Server Service** is running, it is **very** important that neither Windows Explorer nor other programs are accessing Media Database files or folders associated with your XProtect Corporate surveillance setup. Otherwise, the recording server might not be able to rename or move relevant media files.

Unfortunately, this might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server Service, close the program accessing the media file(s) or folder(s) in question, and simply restart the Recording Server Service.

Example: *Management Server Service* and *Recording Server Service* icons in notification area

Read Server Service State Icons

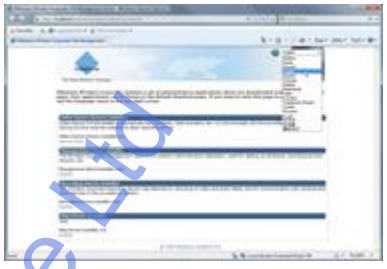
The following notification area icons represent the possible states of the management server service and recording server service:

Management Server Service	Recording Server Service	
		**Running.**
		**Stopped.**
		**Starting.** Appears when a server service is in the process of starting. Under normal circumstances, the icon will after a short while change to *Management server is running* or *Recording server is running*.
		**Stopp*ing*.** Appears when a server service is in the process of stopping. Under normal circumstances, the icon will after a short while change to *Management server is stopped* or *Recording server is stopped*.
Recording Server Service only		**In indeterminate state.** Appears when the *Recording Server Service* is initially loaded and until the first information is received, upon which the icon will, under normal circumstances, change to the *Recording server is starting* icon, and subsequently to the *Recording server is running* icon.
		**Running offline.** Typically appears when the *Recording Server Service* is running but the *Management Server Service* is not.
		**Must be authorized by administrator.** Appears when the *Recording Server Service* is loaded for the first time. Administrators authorize the recording server through the XProtect Corporate Management Client: In the Management Client's Site Navigation pane, expand the *Servers* list, select the *Recording Server* node then in the Overview pane right-click the required recording server and select *Authorize Recording Server*.

Use Download Manager

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

The web page is capable of displaying two sets of content:



- One targeted at system administrators, enabling them to download and install key XProtect Corporate components, such as recording servers (see "Install System Components" on page 29) and the Management Client (see "Install System Components" on page 29). This is the content you see during the XProtect Corporate installation process.
- One targeted at end users, providing them with access to client applications, such as the Smart Client and Remote Client, as well as various drivers, plugins, language packs, etc.

The example to the right shows the web page displaying content targeted at system administrators.

The web page automatically has some content; this is why you can use it straight away during the XProtect Corporate installation process. However, as a system administrator, you can customize what should be displayed on the web page, for example if particular language versions of the Smart Client are required in your organization. For this purpose you use the Download Manager.

Built-in Help System

Navigating the Built-in Help System

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

- ***Contents Tab***: Lets you 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 Tab***: Lets you 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 Tab***: What is a video encoder? What does PTZ mean? The *Glossary* tab provides a glossary of common surveillance and network-related terms. Simply select a term to view a corresponding definition in the small window below the list of terms.

The actual content of each help topic is displayed in the right pane of the help window. Help topic texts may contain various types of links, notably so-called expanding drop-down links.

Clicking an expanding drop-down link will display detailed information. The detailed information will be displayed immediately below the link itself; the content on the page simply expands. Expanding drop-down links thus help save space.

To print a help topic, navigate to the required topic and click the browser's *Print* button.

Tip: When printing a selected help topic, the topic will be 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.

Index

milestone

The Open Platform Company