MAKE THE
WORLD SEE

Milestone Systems

XProtect Update Manager

User manual

milestone

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 reserves 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 system installation folder.

Contents

Overview

XProtect Update Manager

XProtect Update Manager is a tool that helps you keep your distributed XProtect VMS up to date.

The tool is released independently on the main XProtect releases and works with all supported versions of the XProtect VMS. To see the list of supported XProtect verisions, go to https://www.milestonesys.com/support/software/product-lifecycle/xprotect-management-software/.

It consists of the following components:

Name	Description
XProtect Update Manager Service	An update server that downloads and distributes updates.
XProtect Update Manager Agent	An update agent that collects information about the XProtect components, reports to the update server, and installs the updates on a host.
XProtect Update Manager Client	A desktop application that provides an interface to view and update the XProtect components.

What's new?

XProtect Update Manager v. 1.1

Simplify encryption with a system-generated certificate:

- You can now use your own or system-generated certificates to secure the connection between the XProtect Update Manager components. See Encryption between the XProtect Update Manager components on page 6.

Additional components to install:

- You can now install AXIS Optimizer for the AXIS devices that are connected to the XProtect VMS. See Install the Axis Optimizer plugin for XProtect on page 17.

XProtect Update Manager v. 1.0

In this initial version, you can:

- See a list of available updates.
- Download updates from the Milestone repository.
- Install updates on XProtect client and server components.
- Uninstall XProtect updates.
- Get a list of the hosts that run XProtect components.
- Check if the XProtect components on an host are up to date.
- Restart a host remotely.
- Install XProtect Update Manager using the installation wizard or command-line arguments.
- Manage local files.

Requirements and considerations

Ports used by the tool

During installation, the wizard creates firewall exceptions for the ports that XProtect Update Manager uses.

Port	Service	Purpose
5119	**XProtect Update Manager Agent Service**	Communication with the update server.
5109	**XProtect Update Manager Central Service**	Communication with the update agents and the desktop application.

Encryption between the XProtect Update Manager components

To install XProtect Update Manager, you must use certificates for encryption that are trusted by all hosts in the system.

During the installation of the update server, you select the type of certificate to use:

- System-generated certificates are self-signed certificates created by the installation wizard. Every system-generated certificate comes with a secure connection key. You add the secure connection key on every update agent computer to establish a secure connection with the update server.
- Your own certificate. To see your certificate listed in the installation wizard, you must import a .pfx certificate to the **Personal** store on the computer.

Installation

Install XProtect Update Manager using the installation wizard

To install the relevant XProtect Update Manager components:

1. Download XProtect Update Manager from the Milestone software download page (https://www.milestonesys.com/download/).
2. Double-click on the file to launch the installer. The welcome window is displayed.

   Select **Continue**.
3. Read the Milestone End-user License Agreement. Select the **I accept the terms in the license agreement** check box and click **Continue**.
4. Select the components to install:

   - **XProtect Update Manager Service**. The server downloads and stores the update files and communicates with the update agents. Install the server on a host in your network that is reachable by the update agents.
   - **XProtect Update Manager Agent**. Install the update agent on every host with an XProtect component.
   - **XProtect Update Manager Client**. Install the desktop application on any host from which you want to view and update your XProtect components.

   Then, select **Continue**.
5. Select an installation folder. If you have selected to install the update agent or client on a computer without an update server, specify the update server address.

   

   Do not use localhost as the update server address.

   Select **Continue**.

6. When installing the XProtect Update Manager Service component.

   If you are installing the update server together with other components or standalone, specify the certificate you want to use to secure the connection between the XProtect Update Manager components:

   - System-generated certificate - let the wizard generate a self-signed certificate and install it in the Personal store of the local computer.
   - Your own certificate - select an existing certificate. The wizard displays only certificates in the .pfx format. The certificates must be installed in the Trusted Root Certification Authorities store on your local computer.

   Select **Continue**.

7. When installing the XProtect Update Manager Agent component. If you are installing the update agent together with the client component or standalone and you have selected to use a system-generated certificate, you must add the secure connection key.

   Select **Continue**.

Once the installation is complete, a list of the installed components appears.

Install XProtect Update Manager with a system-generated certificate using command-line arguments

After you have prepared your system and decided to use a system-generated certificate for secure connection between the XProtect Update Manager components, you are ready to begin.

To learn more about encryption, see Encryption between the XProtect Update Manager components on page 6.

You can install the component one-by-one.

1. Run Windows Command Prompt as administrator and navigate to the XProtect Update Manager's executable file.
2. To install the update server, type:

   ```
   "XProtectUpdateManagerInstaller.exe" --install Location="[LOCATION]"
   Index=1 CertificateMode=SelfSigned
   ```

   Where **LOCATION** is an installation folder on your computer.

   The installation starts. At the end of the installation, the system generates a secure connection key. Save the key to install the update agent on this or other computers.

3. To install the update agent, type:

```
"XProtectUpdateManagerInstaller.exe" --install Location="[LOCATION]"
Index=2 ServerAddress=[ADDRESS] CertificateMode=SelfSigned TrustedKey=[KEY]
```

   Where **LOCATION** is an installation folder on your computer, **ADDRESS** is the update server address (IP address, hostname or FQDN) and **KEY** is the secure connection key from the update server.

4. To install the client, type:

```
"XProtectUpdateManagerInstaller.exe" --install Location="[LOCATION]"
Index=3
```

   Where **LOCATION** is an installation folder on your computer.

You have installed all XProtect Update Manager components on your computer with a system-generated certificate.

Install XProtect Update Manager with your own certificate using command-line arguments

After you have prepared your system and decided to use your own certificate for secure connection between the XProtect Update Manager components, you are ready to begin.

To learn more about encryption, see Encryption between the XProtect Update Manager components on page 6.

You can install one or more components in any order.

1. Run Windows Command Prompt as administrator and navigate to the XProtect Update Manager's executable file.
2. Depending on the components you want to install, type:
    - For the update server

      ```
      "XProtectUpdateManagerInstaller.exe" --install Location="[LOCATION]"
      Index=1 CertificateMode=CertificateAuthority SerialNumber=[NUMBER]
      ```

      Where **LOCATION** is an installation folder on your computer and **NUMBER** is the serial number of the certificate. The certificate must be installed in the **Trusted Root Certification Authorities** store on your local computer.
    - For the update agent:

      ```
      "XProtectUpdateManagerInstaller.exe" --install Location="[LOCATION]"
      Index=2 ServerAddress=[ADDRESS] CertificateMode=CertificateAuthority
      SerialNumber=[NUMBER]
      ```

      Where **LOCATION** is an installation folder on your computer, **ADDRESS** is the update server address (IP address, hostname or FQDN), and **NUMBER** is the serial number of the certificate. The certificate must be installed in the Trusted Root Certificatation Authorities store on your local computer.
    - For the client:

      ```
      "XProtectUpdateManagerInstaller.exe" --install Location="[LOCATION]"
      Index=3
      ```

      Where **LOCATION** is an installation folder on your computer.

You have installed all XProtect Update Manager components on your computer with your own certificate.

Overview of the command-line arguments and parameters

XProtect Update Manager supports the following command-line arguments:

Command	Action
--quiet	Install XProtect Update Manager silently.

Command	Action
--ui	Open the installation wizard.
--showconsole	View installation logs in a separate window.
--list	View embedded products in the installer.
--requirements	View the requirements for the products in the installer.
--deployed	View the installed XProtect Update Manager components on this host.
--install	Install an XProtect Update Manager element on this host.
--uninstall	Uninstall an XProtect Update Manager element on this host.
--exportoptions	Export the options,json file. You can use this file to specify the properties for the components you want to install
--encryptoptions	Encrypt the options.json file and generate a deployment.json file. You can use the deployment file to speed up the installation process without the need to enter the same commands and parameters on every computer.
--deploymentfile	Install the selected XProtect Update Manager components using the encrypted deployment file.
--showcertificates	View a list of the available certificates on this host.
/?	View the XProtect Update Manager command line help.

Required parameters

Some of the commands require additional parameters to execute.

Parameter	Value	Description
Location	A directory on your computer.	A parameter for the **--install** command.

Parameter	Value	Description
Index or **Code** or **ID**	A component identifier.	Parameters for the **--install** or **--uninstall** commands. You must provide at least one component identifier for a component.
ServerAddress	The IP address, hostname, or FQDN of the update server.	A parameter for the **--install** command. You specify the address of the update server when you install the XProtect Update Manager Agent component.
CertificateMode	Select the certificate to use: • **SelfSigned** for system-generated certificates • **Current** to use your current system-generated certificate • **CertificateAuthority** to select your own certificate.	A parameter for the **--install** command. You must select a certificate to use when you install the XProtect Update Manager Service component.
TrustedKey	The secure connection key from the system-generated certificate.	A parameters for the **--install**. You must select a certificate to use when you install the XProtect Update Manager Agent component and you have used a system-generated certificate for the update server.
SerialNumber	The serial number of your certificate.	A parameter for the **--install**. You must specify the serial number of your own certificate when you install the XProtect Update Manager Service component. The certificate must be installed in the **Personal** store on your local computer and must be signed by a root or intermediate CA.

Component identifiers

Use one or more component identifiers to specify the component you want to install or uninstall.

Component	Index	Code	ID
XProtect Update Manager Service	1	506691BC-46CB-4432-A4F9-2A33181D50B2	5C5D9ABDFE
XProtect Update Manager Agent	2	84AC98F0-02F8-46CD-98E4-44BBE1189268	171766AC58
XProtect Update Manager Client	3	78992797-B7A1-48F7-B4EF-8D0A116B3609	2E2ECD5A98

Operation

Connect to an update server in your network

To view and update your VMS components, you must connect to an update server.

1. Select the XProtect Update Manager icon to start the application.
2. To connect to the update server, you must authenticate with Windows user credentials with administrator permissions on the update server host. Select one of these login types:
    - **Current user** - log in using the same Windows user credentials as your current login.
    - **Windows authentication** - specify a Windows user name and password.
3. Specify the update server's host name or IP address and select **Log in**.

If you are logging in for the first time and you use a system-generated certificate to connect to the update server, you get a security notification. By default, the self-signed certificate is not trusted by your computer. To connect securely to the update server, compare the certificate details from this page with the certificate details on the update server computer and click **Accept and continue**.

Managing updates

You can view downloaded and available updates and remove the updates from the update server's local storage from the **Updates** tab in XProtect Update Manager. From this tab, you can download and install updates and the Axis Optimizer plugin for your XProtect VMS

To see a list of available updates, you must enable the update server to check for updates online. See Settings tab on page 18.

When the update server is connected to the internet, you see a list of available and downloaded updates. If the update server is not connected to the internet, you see only the updates that you have downloaded or copied to the local storage.

From the **Updates** tab, you can:

- View the files that you have downloaded by selecting  .
- Download updates from the Milestone repository by selecting  .
- Remove updates from the update server's local storage by selecting  .

The list refreshes automatically according to the refresh interval you selected in **Settings**. The default refresh interval is 12 hours. To refresh the list manually, select **Refresh**.

Authorize update agents to install updates on hosts

Before installing any updates on a host, you must authorize the update agent to carry out the task on the computer.

If you change the user that runs the **XProtect Update Manager Agent Service**, you must authorize the host again.

To authorize an update agent:

1. On the **Hosts** tab, select the check boxes before the host names of the hosts on which you want to install updates.
2. Select **Authorize**.

You can now install updates on these hosts.

Update XProtect components on a single host

You can install updates for one, some, or all XProtect components that run on a host. To install updates on a single host, see Update XProtect components on some or all hosts on page 16.

Before you install updates on a host, verify that the update agent is authorized for that action. See Authorize update agents to install updates on hosts on page 15.

To install updates on a single host:

1. On the **Updates** tab, download the updates for your XProtect components by selecting .

   If you have not downloaded any updates for the components that run on a host, the host will appear as **Up-to-date** in the **Hosts** tab.

2. On the **Hosts** tab, select the check box before the host that runs the XProtect component on which you want to install an update.

   To find a host quickly, you can search by host name, or filter the results by host status, component name, or component version.

3. In the **Components to update and install** panel, select the check boxes next to the components on which you want to install an update and select **Update**.

   When the process is complete, the components' status changes to **Up-to-date** and the status icon becomes green.

   If the update requires a host restart, the host status icon becomes yellow. You must restart the host to complete the update and install new updates.

Update XProtect components on some or all hosts

You can install updates on one, some, or all XProtect components that run on multiple hosts. To install updates on a single host, see Update XProtect components on a single host on page 15.

Before you install updates on a host, verify that the update agent is authorized for that action. See Authorize update agents to install updates on hosts on page 15.

To install updates on some or all hosts:

1. On the **Updates** tab, download the updates for your XProtect components by selecting .

   If you have not downloaded any updates for the components that run on a host, the host will appear as **Up-to-date** in the **Hosts** tab.

2. On the **Hosts** tab, select the check boxes before the host names of the hosts on which you want to install the updates.

   To see the components that run on a host in the host components panel on the right, select the host name.

   To find a host quickly, you can search by host name, or filter the results by host status, component name, or component version.

3. In the **Components to update and install** panel, select the check boxes in front of the components you want to install an update on and select **Update**.

   When the process is complete, the components' status changes to **Up-to-date** in the host components panel and the status icon becomes green.

   If the update requires a host restart, the host status icon becomes yellow. You must restart the host to complete the update and install new updates.

Install the Axis Optimizer plugin for XProtect

AXIS Optimizer for the XProtect VMS allows you to manage your Axis devices from XProtect Management Client more efficiently. To learn more about Axis Optimizer, go to https://www.axis.com/products/axis-optimizer-for-milestone-xprotectr.

To see the Axis Optimizer plugin in the XProtect Update Manager client, you must enable the update server to check for updates online.

The Axis Optimizer plugin must be installed on a computer running the XProtect Smart Client or XProtect Management Client components. The Axis Optimizer component for the event server must be installed on the computer that runs the event server.

To install the plugin:

1. On the **Updates** tab, download the Axis Optimizer plugin by selecting .
2. On the **Hosts** tab, select the check box before the host you want to install the plugin on.
3. In the **Components to update and install** panel, select Axis Optimizer for Milestone XProtect and click **Update**.
4. Read and accept the license agreement.
5. Select if you want to install the event server component. With this component, you can create custom actions for Axis devices. It requires a restart of the Event Server service. You can also opt out from sharing usage data or device statistics to Axis.

   Then, click **Install**.

You can see the status of the installation on the component list on the right-hand side.

View XProtect components on a host

To get a better overview of your XProtect VMS, you can use XProtect Update Manager to view the XProtect components per host.

1. Go to the **Hosts** tab and select a host.

   > To find a host quickly, you can search by host name, or filter the results by host status, component name, or component version.

2. On the right-hand side, you can see a list of all XProtect components installed on that host.

Uninstall an update

You can revert to an older version of any XProtect component by uninstalling an update.

To uninstall an update from XProtect Update Manager:

1. Go to the **Hosts** tab and select the host with the component you want to uninstall the update from. On the left, you see the components that are installed on that host.
2. To uninstall an update from a component, select  .

Remove a host from XProtect Update Manager

To remove an host from the **Hosts** tab in the XProtect Update Manager client:

1. On the host, open the Windows **Control Panel**. Then double-click **Add or remove programs** and select the **XProtect Update Manager Installer**. Then, select **Uninstall**.
2. Select to uninstall the **XProtect Update Manager Agent** and then click **Continue**. The wizard removes the selected component.
3. Open the XProtect Update Manager client and connect to the update server on which you have added the host.
4. Go to the **Hosts** tab and click the **Remove** icon next to the host on which you have uninstalled XProtect Update Manager.

Managing local files

By default, XProtect Update Manager stores all files you download at `C:\Packages`. You can add or remove files you want to appear in XProtect Update Manager by copying or moving files to this directory. This is useful, for example, when your VMS installation runs offline and you don't want to connect the update server to the internet.

You can change the location from **Settings** in the XProtect Update Manager client.

If you have an internet connection and enabled XProtect Update Manager to check for updates online, your files might be overwritten.

Settings tab

On this tab, you can specify a number of settings related to the functionality of the tool.

Name	Description
Local storage	A folder on the update server host that contains the available updates. You can copy existing updates to this location or use XProtect Update Manager to download

Name	Description
	available updates from the Milestone repository.
Check for VMS updates online	To view and download new updates from the Milestone repository, you must enable this setting.
Check for VMS updates every...	Select how often the update server will connect to the Milestone repository to check for new updates. You can manually refresh the list of available updates using the **Refresh** button in the **Updates** tab.
Check hosts every...	Select how much time should pass before the server considers the host unavailable.
Maximum concurrent updates	To prevent the network flooding, you can select the maximum number of hosts to be updated simultaneously.

Manage users

When you install XProtect Update Manager Service on a computer, the wizard automatically add the user you are logged in with to the group of allowed users. This user can log in to the update server from the client. You can add or remove users to this group depending on your needs.

To manage the users who can manage your VMS installations from XProtect Update Manager:

1. On the computer where you have installed the XProtect Update Manager service, open the **Start** menu, and type **lusrmgr.msc** to open **Local Users and Groups**.
2. Go to **Groups** and click **XUM Allowed Users** to see a list of the users who can log in to XProtect Update Manager.
3. Add or remove Windows users.

When you add users, you can use the account to log in to XProtect Update Manager from any computer in your domain.

Change the update server address

You can change the update server address on an update agent without reinstalling it.

1. On the update agent computer, go to C:\ProgramData\Milestone\XProtect Update Manager\Agent and open the serversettings.json file.

   If you can't see the **ProgramData** folder, enable the setting to view **Hidden items** in File Explorer.

2. In **Hostname,** change the value with the new IP address of the update server. For example: `Hostname": "192.168.2.65",`.

You can now log in to the update server using the changed address.

Troubleshooting

Troubleshooting XProtect Update Manager

Log files

To troubleshoot system errors, you can find the log files on the hosts where you have installed the different XProtect Update Manager components in the following folders:

- On the hosts: `C:\ProgramData\Milestone\XProtect Update Manager\Agent\Logs`
- On the server: `C:\ProgramData\Milestone\XProtect Update Manager\Server\Logs`

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.