Milestone Systems

XProtect Update Manager

User manual

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 supports all versions of XProtect VMS

It consists of the following elements:

Name	Description
XProtect Update Manager server	An update server that downloads and distributes hotfixes.
XProtect Update Manager agent	An 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?

In this initial release, you can:

- See a list of available hotfixes.
- Download hotfixes from the Milestone repository.
- Install hotfixes on XProtect client and server components.
- Uninstall XProtect hotfixes.
- 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
5009	**XProtect Update Manager Server**	Communication with the agents and the desktop application.
5019	**XProtect Update Manager Agent**	Communication with the update server.

Encryption between the XProtect Update Manager elements

To encrypt the connection, XProtect Update Manager requires certificates that are trusted by all hosts in the system.

Before you start the installation of XProtect Update Manager, install the certificates on all hosts that you want to be part of your VMS system:

- If you have a CA-signed certificate, install the pubilc key of that certificate on all hosts in your system. Install the certificate on the **Personal** store on the local computer. The certificate in the **Personal** store must be in .pfx format.
- To use a self-signed certificate, you must create a certificate for the update server. Then, install that certificate in the local computer's **Trusted Root Certification Authorities** and **Personal** stores on all hosts. The certificate in the **Personal** store must be in .pfx format.
- Give **Read** permission to the **Network Service** account to manage the private key of the SSL certificate. See Manage the private keys of a certificate on page 5.

You select a .pfx certificate file when you install the **XProtect Update Manager service**. You cannot install XProtect Update Manager without a valid certificate.

For more information about certificates, see the XProtect VMS certificates guide.

Manage the private keys of a certificate

The XProtect Update Manager service runs as the Network Service account. To make sure the communication between the different elements is encrypted, you must allow the service account to use the private key of the certificate.

After you have imported the SSL certificate to the private store on the local computer:

1. On the update server host, start **Manage computer certificates** and go to the certificates in the **Personal** store.
2. Right-click the certificate and select **All Tasks** > **Manage Private Keys**.
3. Add read permission for the Network service account.

Installation

Install XProtect Update Manager using the installation wizard

To install the relevant XProtect Update Manager elements:

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

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

   - **XProtect Update Manager Server** . The service downloads and stores the hotfixes and communicates with the agents. Install the service on a host in your network that is reachable by the agents.
   - **XProtect Update Manager Agent**. Install the 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 **Next**.
5. Select an installation folder and specify the following:

   - **Server address**. Specify the IP address or host name of the host that runs the XProtect Update Manager service.
   - **Select certificate**. Select a .pfx file to encrypt the connection between the XProtect Update Manager elements.

     

     All hosts with an XProtect Update Manager element must trust the certificate. You can reuse the VMS certificates or generate new ones. For more information, see the XProtect VMS certificates guide.

   Select **Next** to install XProtect Update Manager. Once the installation is complete, a list of the installed elements appears.

Install XProtect Update Manager using command-line arguments

You must install the relevant XProtect Update Manager elements on all hosts that run an XProtect component.

To see the prerequisites for installation, see System requirements. To see a list of the command-line arguments, see Overview of the command-line arguments on page 9.

To install any XProtect Update Manager element with encryption, you generate an arguments file, specify the configuration details, and then deploy XProtect Update Manager using the deployment file.

The arguments file contains your information in plaintext. The system generates a deployment file that encodes your password. Both files are saved in the folder where you store the XProtect Update Manager executable.

1. Run Windows Command Prompt as administrator and navigate to the XProtect Update Manager's executable file.
2. To generate the options file, enter:

   ```
   "XProtect Installation Manager Installer.exe" --exportoptions options.json
   ```

3. To generate an arguments file with your data, enter:

   ```
   "XProtect Installation Manager Installer.exe" --encryptoptions options.json
   deployment.json
   ```

4. Open the options.json file with a text editor and specify the configuration details, such as the update server's address and service account credentials for the agent and update server in the **"Value"** fields.

   - **"ServerAddress"** - the update server's address

   An example:

   ```
   [
     {
       "ProductName": "XProtect Installation Manager Client"
     },
     {
       "ProductName": "XProtect Installation Manager Agent",
       "Options": [
         {
           "Name": "ServerAddress",
           "Value": "localhost"
         }
       ]
     }
   ]
   ```

5. (Optional) Remove elements to install. To install only specific elements on a host, from the options.json file, remove the content inside the curly brackets that contain the selected **ProductName** key. For example, the script below will only install the desktop application and the update server.

```
[
  {
    "ProductName": "XProtect Installation Manager Client"
  },
  {
    "ProductName": "XProtect Installation Manager Service"
  }
]
```

6. To install the selected XProtect Update Manager element, enter:

```
"XProtect Installation Manager Installer.exe" --deploymentfile
deployment.json Location="[install location]"
```

You can generate the deployment.json file on one host, then do only steps one and five on all hosts on which you want to install XProtect Update Manager.

Overview of the command-line arguments

XProtect Update Manager supports the following command-line arguments:

Command	Action
--quiet	Install XProtect Update Manager silently.
--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 elements on this host.
--install	Install an XProtect Update Manager element on this host.

Command	Action
--uninstall	Uninstall an XProtect Update Manager element on this host.
--exportoptions	Export the options,json file.
--encryptoptions	Encrypt the options file and generate a deployment file.
--deploymentfile	Install the selected XProtect Update Manager elements using the encrypted deployment file.
--certificateserialnumber	Specify the serial number of a certificate on this host.
--showcertificates	View a list of the available certificates on this host.
/?	View the XProtect Update Manager command line help.

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 **Connect**.

Managing hotfixes

You can view downloaded and available hotfixes and remove the hotfixes from the update server's local storage from the **Updates** tab in XProtect Update Manager.

> To see a list of available hotfixes, you must enable the update server to check for updates online. See Settings tab on page 14.

When the update server is connected to the internet, you see a list of available and downloaded hotfixes. If the update server is not connected to the internet, you see only the hotfixes 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 a hotfix from the Milestone repository by selecting  .
- Remove a hotfix 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 agents to install hotfixes on hosts

Before installing any hotfixes on a host, you must authorize the agent.

To authorize an agent:

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

You can now install hotfixes on these hosts.

Install hotfixes for an XProtect component on a single host

You can install hotfixes for one, some, or all XProtect components that run on a host. To install hotfixes on a single host, see Install hotfixes for an XProtect component on some or all hosts on page 12.

Before you install hotfixes on a host, verify that the agent is authorized for that action. See Authorize agents to install hotfixes on hosts on page 11.

To install hotfixes on a single host:

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

   If you have not downloaded any hotfixes for the components that run on a host, the host will appear as **All 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 a hotfix.

   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 **Available Updates** panel, select the check boxes next to the components on which you want to install a hotfix and select **Update**.

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

   If the hotfix requires a host restart, the host status icon becomes yellow. To complete the update, you must restart the host. You will not be able to install new hotfixes before restarting the host.

Install hotfixes for an XProtect component on some or all hosts

You can install hotfixes on one, some, or all XProtect components that run on multiple hosts. To install hotfixes on a single host, see Install hotfixes for an XProtect component on a single host on page 12.

Before you install hotfixes on a host, verify that the agent is authorized for that action. See Authorize agents to install hotfixes on hosts on page 11.

To install hotfixes on some or all hosts:

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

   > If you have not downloaded any hotfixes for the components that run on a host, the host will appear as **All 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 hotfixes.

   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 **Available Updates** panel, select the check boxes in front of the components you want to install a hotfix 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 hotfix requires a host restart, the host status icon becomes yellow. To complete the update, you must restart the host. You will not be able to install new hotfixes before restarting the host.

View XProtect components

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 a hotfix

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

To uninstall a hotfix from XProtect Update Manager:

1. Go to the **Hosts** tab and select the host with the component you want to uninstall the hotfix from. On the left, you see the components that are installed on that host.
2. To uninstall a hotfix 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 **Next**. The wizard removes the selected element.
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 **Delete** 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 XProtect Update Manager 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
Server local packages folder	A folder on the update server host that contains the available hotfixes. You can copy existing hotfixes to this location or use XProtect Update Manager to download available hotfixes from the Milestone repository.
Check for updates online	To view and download new hotfixes from the Milestone repository, you must enable this setting.
Online update interval	Select how often the update server will connect to the Milestone repository to check for new hotfixes. You can manually refresh the list of available hotfixes using the **Refresh** button in the **Updates** tab.
Offline hosts timeout interval	Select how much time should pass before the server considers the host unavailable.
Remote hosts batch size	To prevent the network flooding, you can select the maximum number of hosts to be updated simultaneously.

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 elements 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`

Hotfixes

Error in the agent log file when installing a hotfix: A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

If the root certificate auto-update is disabled, XProtect Update Manager might fail to install a hotfix on a host. To enable this setting, see https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc734054(v=ws.10)#turn-off-automatic-root-certificates-update.

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/.