

MAKE THE  
WORLD SEE

# Milestone Systems

---

XProtect Management Server Failover 2022 R3

Administrator manual



# Contents

- Copyright, trademarks, and disclaimer** ..... **4**
- Overview** ..... **5**
  - XProtect Management Server Failover (explained) ..... 5
  - Compatibility ..... 5
  - Failover steps (explained) ..... 6
- Licensing** ..... **8**
  - XProtect Management Server Failover license ..... 8
- Requirements and considerations** ..... **9**
  - Before you configure ..... 9
    - Network and computer prerequisites ..... 9
    - SQL Server prerequisites ..... 10
    - VMS prerequisites ..... 10
  - DNS lookups (explained) ..... 11
  - View the instance name of the SQL Server ..... 11
  - Encrypting the connection to and from the failover cluster ..... 12
  - Certificates for the failover web console (explained) ..... 12
  - Browser requirements for the failover web console ..... 13
- Installation** ..... **14**
  - Install XProtect Management Server Failover on a computer ..... 14
    - Install XProtect Management Server Failover with a new VMS installation ..... 14
    - Add XProtect Management Server Failover to an existing VMS installation ..... 14
- Configuration** ..... **15**
  - Configure failover management server (wizard) ..... 15
  - Configure the failover cluster ..... 15
  - Register remote servers ..... 19
    - Change management server address on the recording server ..... 20
    - Change management server address on the mobile server ..... 20
    - Change management server address on the DLNA server ..... 20
    - Change management server address for Milestone Open Network Bridge ..... 21
  - Add a license for XProtect Management Server Failover ..... 21

Add a license from the Manage your configuration page .....	21
Installing certificates .....	21
Generate certificates to access the failover web console .....	22
Install a server certificate on a computer .....	22
Install a user certificate on a computer .....	23
<b>Maintenance .....</b>	<b>25</b>
Remove existing failover cluster configuration .....	25
Uninstall XProtect Management Server Failover .....	26
Failover web console (explained) .....	26
Enable basic authentication for the failover web console .....	27
User interface details .....	28
Control tab .....	28
Monitoring tab .....	29
Control panel .....	29
Node actions .....	29
Node states .....	30
State colors .....	31
Node data synchronization statuses .....	31
Open the failover web console .....	31
View the status of the nodes .....	32
Start or stop a node .....	33
Swap the state of the nodes .....	33
Identify the host name of a node .....	33
Create snapshots of a module for support .....	34
Ports used by XProtect Management Server Failover services and modules .....	35
XProtect Management Server Failover services .....	35
Failover cluster modules .....	35
<b>Upgrade .....</b>	<b>36</b>
Upgrading XProtect Management Server Failover .....	36

## Copyright, trademarks, and disclaimer

Copyright © 2022 Milestone Systems A/S

### 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.

## Overview

### XProtect Management Server Failover (explained)

If a standalone computer running the Management Server service and a SQL Server has a hardware failure, it does not affect recordings or the recording server. However, these hardware failures can result in downtime for operators and administrators who are not already logged in to the clients.

XProtect Management Server Failover provides high availability and disaster recovery for the management server. Thanks to the synchronous data replication between the computers in the failover cluster, there is no data loss in case of hardware failure.

XProtect Management Server Failover is configured between two computers represented as nodes.

To make the failover work, the following system components must run on each node:

- Management Server service
- Event Server service
- Log Server service
- SQL Server

If the management server becomes unavailable on one node, the other node takes over the tasks of running the system components. The remote servers connect to the node that runs the system components.

The SQL database contents are replicated in real-time in a secure manner between the computers.

XProtect Management Server Failover can help you mitigate system downtime. There are a number of reasons why you would want to use a cluster:

- Server failure – If a server fails, you can run the Management Server service and SQL Server from another node in your management server failover configuration while you resolve the problems
- System updates and security patches – Applying security patches on a standalone management server can be time-consuming, resulting in extended periods of downtime. When you have a failover management server configuration, you can apply system updates and security patches with minimal downtime
- Seamless connection – Because clients and applications always connect to a running management server, failover is seamless

## Compatibility

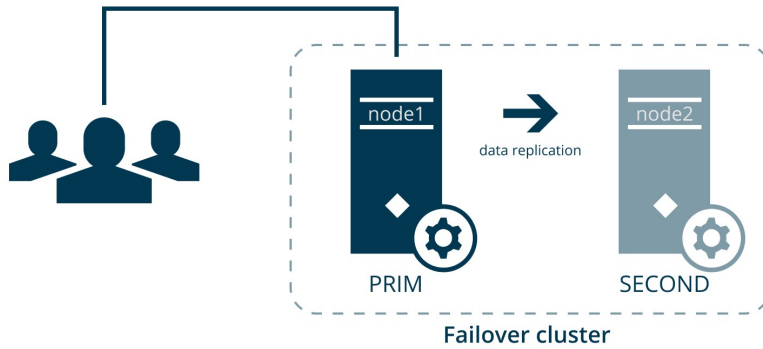
XProtect Management Server Failover is compatible with:

- XProtect Corporate 2022 R1 and later
- XProtect Expert 2022 R1 and later

## Failover steps (explained)

The failover cluster is configured between two computers represented as nodes.

- I. The Management Server service, Event Server service, Log Server service, and the SQL Server run on node1. XProtect Management Server Failover replicates the data from these system components to node2.

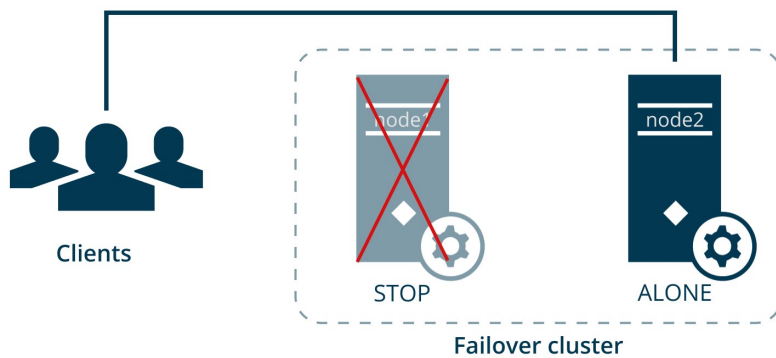


Every second, the computers exchange heartbeats.

- II. If the management server on node1 becomes unavailable for 30 seconds, node2 takes over.


The failover time depends on the start-up time of the Management Server service.

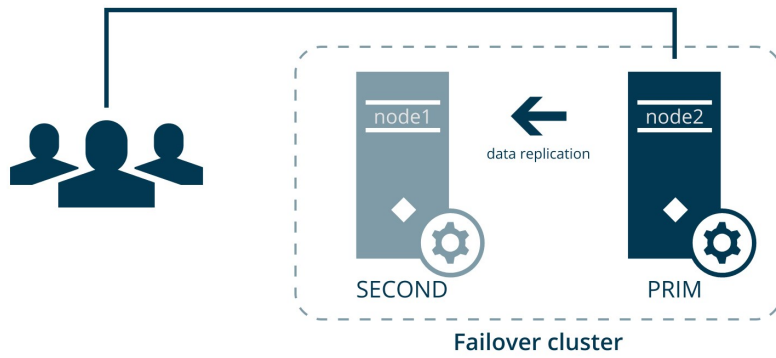
1. Node2 comes into state ALONE, and data replication stops.
2. The Management Server service, Event Server service, Log Server service, and the SQL Server start running on node2.
3. The Management Server service, Event Server service, and Log Server service store data on the SQL Server on node2.



- III. You identify and fix the issue that caused the failover and start node1 from the failover web console. The data that was modified on node2 is replicated to node1.

The VMS system components still run on node2, and data is replicated to node1.

 You have the option to swap the states of the nodes.



## Licensing

### XProtect Management Server Failover license

XProtect Management Server Failover comes with a three-day demo license.

To use the failover cluster for an unlimited period of time, register the host names of the primary and the secondary computer and add your XProtect Management Server Failover license.



If you do not add your XProtect Management Server Failover license, your management server stops working after three days.

To obtain a license for XProtect Management Server Failover, contact your reseller.

You have the option to add the license during the failover cluster configuration or afterward. See [Add a license for XProtect Management Server Failover on page 21](#).



# Requirements and considerations

## Before you configure

XProtect Management Server Failover is configured between two computers represented as nodes: a primary computer and a secondary computer.

During the failover cluster configuration, the wizard replicates the data from the primary computer to the secondary computer.

Milestone recommends that you schedule downtime for the failover cluster configuration.



The primary and the secondary computer cannot be used in other cluster configurations.

### Network and computer prerequisites

- Install two identical operating systems on the primary and the secondary computer. To see the list of supported operating systems, go to the Milestone website (<https://www.milestonesys.com/systemrequirements/>)
- Assign an IPv4 address for the computers. Both computers must belong to the same subnet  
XProtect Management Server Failover does not support IPv6.
- Use one Active Directory (AD) domain
- On both computers, install XProtect using the same AD user account with administrator rights
- Synchronize the time and the time zones between the computers
- Reserve an unused IPv4 address that will serve as the virtual IP of the failover cluster. This IPv4 address must be in the same subnet as the IP addresses for the primary and secondary computers



To make sure that the reserved IPv4 address is never distributed, you can exclude it from the DHCP pool.

- Allow inbound ICMP traffic through Windows Defender Firewall
- Disable Windows Defender Advanced Threat Protection Service from Services
- Perform the forward and reverse DNS lookup queries in Windows PowerShell. See [DNS lookups \(explained\) on page 11](#)

### SQL Server prerequisites

- Back up any existing databases



During the failover cluster configuration, all SQL databases on the secondary computer are overwritten. The data cannot be restored.

- Install identical SQL Server versions on the primary and the secondary computer using the same AD user account as XProtect
- Make sure that only one SQL Server is installed on the primary and the secondary computer
- Verify that the instance name of your SQL Server is MSSQLSERVER. See [View the instance name of the SQL Server on page 11](#)

### VMS prerequisites

Install identical VMS products on the primary and the secondary computers. Make sure that you have installed only the following system components:

- XProtect Management Server
- XProtect Event Server
- XProtect Log Server
- XProtect Management Server Failover



The XProtect Recording Server component and all other components not mentioned above must be installed on other computers.

Depending on your system configuration, consider the following:

- Encryption: to encrypt the connection to and from the running management server, you need to install two certificates for the Management Server service on the primary and the secondary computer. See [Encrypting the connection to and from the failover cluster on page 12](#)
- System configuration password: if you want to assign a system configuration password, use the same password on the primary and the secondary computer



Do not add or change the system configuration password after you have configured the failover cluster.

- External IDP: if you use an external IDP, set up data protection. For more information, see [Install in a cluster](#).
- API Gateway: if you want to use API Gateway, install it on both computers

## DNS lookups (explained)

For successful failover cluster configuration, Milestone recommends that you test the domain name translation for the cluster members in Windows PowerShell:

- Use forward DNS lookup to obtain an IP address by searching the domain
- Use reverse DNS lookup to obtain the domain name that is related to an IP address

To make sure that the IP addresses and the host names are resolved as expected, you must perform the forward and reverse queries on the primary and the secondary computer:

Query name	Command	Perform on	Expected result
Forward DNS lookup	<b>Resolve-DnsName</b> [secondary computer host name]	Primary computer	The host name of the secondary computer corresponds to the first IP address on the list.
Forward DNS lookup	<b>Resolve-DnsName</b> [primary computer host name]	Secondary computer	The host name of the primary computer corresponds to the first IP address on the list.
Reverse DNS lookup	<b>Resolve-DnsName</b> [secondary computer host name]	Primary computer	The host name of the secondary computer must correspond to the first IP address on the list.
Reverse DNS lookup	<b>Resolve-DnsName</b> [primary computer host name]	Secondary computer	The host name of the primary computer must correspond to the first IP address on the list.

## View the instance name of the SQL Server

Milestone recommends that you check the instance name before you start the configuration for the failover cluster.

XProtect Management Server Failover uses a hardcoded name for the SQL service name - MSSQLSERVER.



If the instance name is not MSSQLSERVER, the configuration will fail.

1. Select the Windows start bar and type **services.msc**.
2. Scroll down to **SQL Server [Display name]**.
3. Right-click the service and select **Properties**. The value in the **Service name** field is the instance name.

If the instance name is not MSSQLSERVER, see

<https://supportcommunity.milestonesys.com/s/article/Management-Server-Failover-Configuration-fails-if-SQL-is-installed-separately-troubleshooting>.

## Encrypting the connection to and from the failover cluster

XProtect Management Server Failover reroutes the data packets to the running management server. To establish a secure connection with the running management server, the remote servers must trust both the primary and the secondary computer.

Before you configure the failover cluster, create, import, and install an SSL certificate on the primary and the secondary computer.



If you want to enable encryption after you have configured the failover cluster, you need to remove the existing failover cluster configuration, enable encryption on the Management Server service on the primary and the secondary computer, and then configure the failover cluster again.

1. Create a private and a public CA certificate.
2. Install the public certificate on all client computers.
3. Create a SSL certificate for the failover cluster.
4. Install the SSL certificate for the failover cluster on the primary and the secondary computer.
5. Enable encryption for the Management Server service on the primary and the secondary computer.
6. Create and install certificates on the remote servers.
7. Enable encryption on the remote servers.

For more information, see the [certificates guide about how to secure your XProtect VMS installations](#).

## Certificates for the failover web console (explained)

During the failover cluster configuration, you must select a connection protocol. If you select an HTTPS connection, your computers need certificates to access the failover web console.

The system generates two certificates: a server and a user certificate. Install the server and the user certificate on every computer that you want to have access to the failover web console. You can create one server certificate and as many user certificates as needed.

- The server certificate is a .CRT file. It is installed in the Trusted Root Certification Authorities store of the computer that connects to the failover web console
- A user certificate is a .P12 file. It is a password-protected certificate that belongs to a user

## Browser requirements for the failover web console

The failover web console allows you to manage the failover cluster from your browser. It is accessible from any computer that can reach the primary and the secondary computer.

To make sure that the contents of the failover web console are correctly displayed:

- Network, firewall, and proxy configuration must allow access to the administration network of all the servers that are administered with the web console
- JavaScript must be available and enabled in the web browser
- To avoid security popups in Internet Explorer, you may add the addresses of the primary and the secondary computer into the Intranet or Trusted zone
- The messages in the failover web console are displayed in French, English, Japanese languages, according to the preferred language configured into the web browser (for not supported languages, English is displayed)
- To see the list of supported browsers, go to the Milestone website (<https://www.milestonesys.com/systemrequirements/>)

## Installation

### Install XProtect Management Server Failover on a computer

XProtect Management Server Failover is part of the XProtect installer. You can install it with a new VMS installation or add it later.



To set up a failover cluster, install XProtect Management Server Failover on two separate computers. For more information, see [Before you configure on page 9](#).

#### Install XProtect Management Server Failover with a new VMS installation

Follow the steps for Custom installation and select XProtect Management Server Failover as a component you want to install.



Do not install the recording server on the primary or the secondary computer.

#### Add XProtect Management Server Failover to an existing VMS installation

1. Open **Add or remove programs** on Windows and select Milestone.
2. Select **Modify** to launch the Milestone XProtect VMS wizard.
3. On the **Uninstall or change Milestone XProtect VMS components**, select **Change one or more Milestone XProtect VMS components**. Select **Continue**.
4. Select XProtect Management Server Failover. Select **Continue** to install the component.
5. When the installation is complete, a list shows the components that are installed on the computer.

## Configuration

### Configure failover management server (wizard)

When you select **Configure failover management server** from the Management Server Manager tray icon, you get one of the following messages:

#### **Your XProtect product does not support XProtect Management Server Failover**

To learn more about the supported products, see [Compatibility on page 5](#)

#### **No failover management server installed on this computer**

Make sure that XProtect Management Server Failover is installed on the primary and the secondary computer, see [Install XProtect Management Server Failover on a computer on page 14](#)

#### **Select the step in your configuration flow**

You have started the setup process. Before you continue, verify that your system meets the requirement and schedule downtime. If you want to learn more about the prerequisites, see [Before you configure on page 9](#).

The setup process consists of two parts:

- [Configure the failover cluster on page 15](#)
- [Register remote servers on page 19](#)

#### **Manage your configuration**

From this page you can:

- **Apply failover license**, see [Add a license for XProtect Management Server Failover on page 21](#)
- **Generate certificates**, see [Generate certificates to access the failover web console on page 22](#)
- **Remove existing configuration**, see [Remove existing failover cluster configuration on page 25](#)

### Configure the failover cluster

The Management Server service is not available during the configuration. Milestone recommends that you schedule downtime during the configuration.

During the configuration process, you switch between the primary and the secondary computer. To configure the failover cluster successfully:

1. Start from the secondary computer. Once you prepare the secondary computer, move to the primary computer.
2. Configure the primary computer. Once done, move to the secondary computer.
3. Finish the configuration on the secondary computer.



The wizard replicates the data from the primary to the secondary computer. To keep your existing VMS data, select your current management server as the primary computer.

### On the secondary computer

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Configure the secondary computer**, then **Continue**. A message appears.
3. Before you continue, make sure that you have installed the required system components and scheduled downtime. Select **Confirm** to continue.
4. On the **Select connection protocol** page, select a protocol for communication with the failover web console. Select **Continue**. The wizard prepares the secondary computer.



Milestone recommends that you use HTTPS to connect to the failover web console.



By default, HTTP does not provide user authentication. If you select HTTP and do not enable basic user authentication, all users from your network can access the failover web console and stop the management server.

A new page opens, informing you that the preparation of the secondary computer has succeeded.

If you have selected HTTPS: save the security code. You need to specify the security code on the primary computer to establish a secure connection between the primary and the secondary computer.



You are now ready to configure the primary computer.

### On the primary computer

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. In the **Failover management server** wizard, select **Configure the primary computer**, and then **Continue**. A message appears.
3. If you have prepared the primary computer, select **Confirm** to continue.
4. On the **Select connection protocol** page, select the same connection protocol you selected on the secondary computer. Select **Continue**.



- On the **Connect to the secondary computer** page, specify the required system information:

Name	Description
<b>Secondary computer (FQDN)</b>	Specify the fully qualified domain name of the secondary computer. It should follow this format: [hostname].[domain name]. Example: host.domain.com.
<b>Failover license</b>	<p>If you have purchased a failover license, you can add it now on this computer. If you leave the field blank and continue, you can still configure the failover management server using a demo license and add a license later.</p> <div data-bbox="459 696 1385 828" style="border: 1px solid #ccc; background-color: #fff9e6; padding: 10px; margin-bottom: 10px;">  If you don't add a license, the management server stops after three days.                 </div> <div data-bbox="459 875 1385 1008" style="border: 1px solid #ccc; background-color: #fff9e6; padding: 10px;">  You must add the same XProtect Management Server Failover license on both computers.                 </div>
<b>Virtual IP address</b>	This is the IPv4 address that is shared between the computers. Specify an available IPv4 address in your network that will replace the actual address of the management server. All remote servers, including the recording server, communicate with this address.
<b>Security code (for HTTPS only)</b>	Specify the security code from the secondary computer to establish a secure connection between the primary and the secondary computer.

Then select **Continue**.

- If you have not added a license, a message informs you that the management server becomes unavailable after three days with the demo license. Select **Continue**.

The wizard configures the failover cluster and copies the SQL databases and content from the primary computer to the secondary computer. It may take 5 to 10 minutes, depending on the system load and connection speed.

7. (For HTTPS only) On the **Generate certificates** page, create a user name and password for the admin role, then select a folder on your computer to save the certificates. If you do not select a destination folder, the certificates are exported to C:\Users\{user}\Documents.

Select **Continue**. The wizard generates the certificates and saves them to the selected folder. If needed, you can create more certificates later.

A new page opens, informing you that the configuration of the primary computer has succeeded.

Navigate to the secondary computer to finish the configuration.

### On the secondary computer

1. Confirm that you have completed the configuration on the primary computer, and then select **Continue**.
2. On the **Add a failover license on this computer** page, add the failover license that you have purchased.



If you leave the field blank, the system will use a three-day demo license.

Select **Continue**.

### 3. The complete the setup:

- **If the configuration failed**

You can remove the current configuration and start the configuration process again, see [Remove existing failover cluster configuration on page 25](#).

- **If the configuration succeeded**

You can close the wizard. The failover web console opens automatically on the secondary computer.



If you have selected HTTPS as the connection protocol, you won't be able to see the web console until you install the server certificate and a user certificate. See [Installing certificates on page 21](#).

The primary computer (node1) takes a PRIM state and the secondary computer (node2) takes a SECOND state. If needed, the states can be swapped.



To complete the setup, you must register the remote servers. See [Register remote servers on page 19](#).

If you have not added a license during the configuration, you can add one from the **Manage your configuration** page. See [Add a license for XProtect Management Server Failover on page 21](#).

A shortcut to the failover web console is added to your desktop.

## Register remote servers

The virtual IP address reroutes the data packets from the remote servers to the running Management Server service, Event Server service, and Log Server service.

You must register all remote servers with the virtual IP address of the failover cluster.



If the remote servers are not registered with the virtual IP address, the data packets will not be rerouted to the running management server during failover.

Change the address of the Management Server on the following system components:

- Recording Server service
- Mobile Server service
- DLNA Server service

- Milestone Open Network Bridge
- API Gateway

Use the virtual IP address of the management server when logging in from the following clients:

- XProtect Management Client
- XProtect Smart Client
- XProtect Mobile client
- XProtect Web Client



There is no hostname associated with the virtual IP address.

### Change management server address on the recording server

1. On the computer where the Recording Server service is installed, right-click the server manager tray icon, and select **Server Configurator**.
2. In Server Configurator, select **Registering servers**.
3. Specify the virtual IP address of the failover cluster and the selected protocol (HTTPS or HTTPS), and select **Register**.

If the change was a success, a confirmation window appears.

### Change management server address on the mobile server

1. On the computer where the Mobile Server service is installed, right-click the Mobile Server Manager tray icon, and select **Management server address**.
2. Specify the virtual IP address of the failover cluster and the selected protocol (HTTPS or HTTPS), and select **OK**.

The Mobile Server service restarts, and the tray icon turns green.

### Change management server address on the DLNA server

1. On the computer where the XProtect DLNA Server service is installed, right-click the XProtect DLNA Server Manager tray icon, and select **Management server address**.
2. Specify the virtual IP address of the failover cluster and the selected protocol (HTTPS or HTTPS), and select **OK**.

The XProtect DLNA Server service restarts, and the tray icon turns green.

### Change management server address for Milestone Open Network Bridge

1. On the computer where the Milestone ONVIF Bridge service is installed, right-click the Milestone ONVIF Bridge tray icon, and select **Configuration**.
2. On the **Surveillance Server Credentials** page, in the **Management server** field, specify the virtual IP address of the failover cluster and the selected protocol (HTTPS or HTTP), and select **OK**.

If the change was a success, a confirmation window appears.

## Add a license for XProtect Management Server Failover

You receive the XProtect Management Server Failover license in your email.

You have the option for when to add the license:

- During the failover cluster configuration (see [Configure failover management server \(wizard\) on page 15](#))
- After the failover cluster configuration, from the **Manage your configuration** page on the primary and the secondary computer

### Add a license from the Manage your configuration page

You must add the license on the primary and the secondary computer.

1. Go to one of the computers that are part of the failover cluster.
2. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
3. Select **Apply failover license** and select **Continue**.
4. On the **Add a failover license on this computer** page, select **Browse** and select your XProtect Management Server Failover license. Select **OK**, then **Continue**. A message informs you that the failover management server is configured successfully.
5. Repeat steps 1 to 4 on the other computer that is part of the failover cluster.

## Installing certificates

Certificates provide a secure connection with the failover web console. You can generate one server certificate and as many user certificates as needed.

To set up a secure connection to the failover web console, follow these steps:

1. [Generate certificates to access the failover web console on page 22](#)
2. [Install a server certificate on a computer on page 22](#)
3. [Install a user certificate on a computer on page 23](#).

## Generate certificates to access the failover web console

To establish a secure connection with the failover web console, you need certificates that are trusted by your browser. To learn more about certificates, see [Certificates for the failover web console \(explained\) on page 12](#).

You must install both a server and a user certificate on every computer that needs access to the failover web console.



You can create a server and a user certificate only from the computer that you selected as the primary computer during the failover cluster configuration.

To generate certificates after you have configured the failover cluster:

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Generate certificates** and then select **Continue**.
3. On the Generate certificates page:
  - Create a user name
  - Create a password. The password must be between 6 and 32 characters long. You can use a combination of letters, numbers, and any of the following characters ( ) \* \_ - .
  - Select a destination folder. The server and user certificates are exported there. If you do not select a destination folder, the certificates are exported to C:\Users\{user}\Documents
4. Select **Continue**. The wizard creates a server certificate and a user certificate, and exports them to the selected destination. When the process is completed, install the created certificates.

## Install a server certificate on a computer

Install the server certificate on all the computers that need to access the failover web console.

1. Copy the serverCert.crt file from the primary computer to the computer that needs to access the failover web console.
2. Right-click the server certificate and select **Install Certificate**.
3. In the **Certificate Import wizard**, choose the **Store Location**:
  - on the primary and the secondary computer, select **Local Machine**
  - on all other computers, select **Current User**

Select **Next** to continue.

4. Select **Place all certificates in the following store** and specify a folder.
5. Select **Browse**, and then **Trusted Root Certification Authorities**.

6. Select **OK** and **Next**.
7. On the **Completing the Certificate Import Wizard** dialog, select **Finish**.



If you receive a security warning that you are about to install a root certificate, select **Yes** to continue.

If the import has succeeded, a confirmation dialogue box appears.

8. Verify that the server certificate is listed in the center view of the **Trusted Root Certification Authorities** subtree.

You are now ready to install the user certificates.

## Install a user certificate on a computer

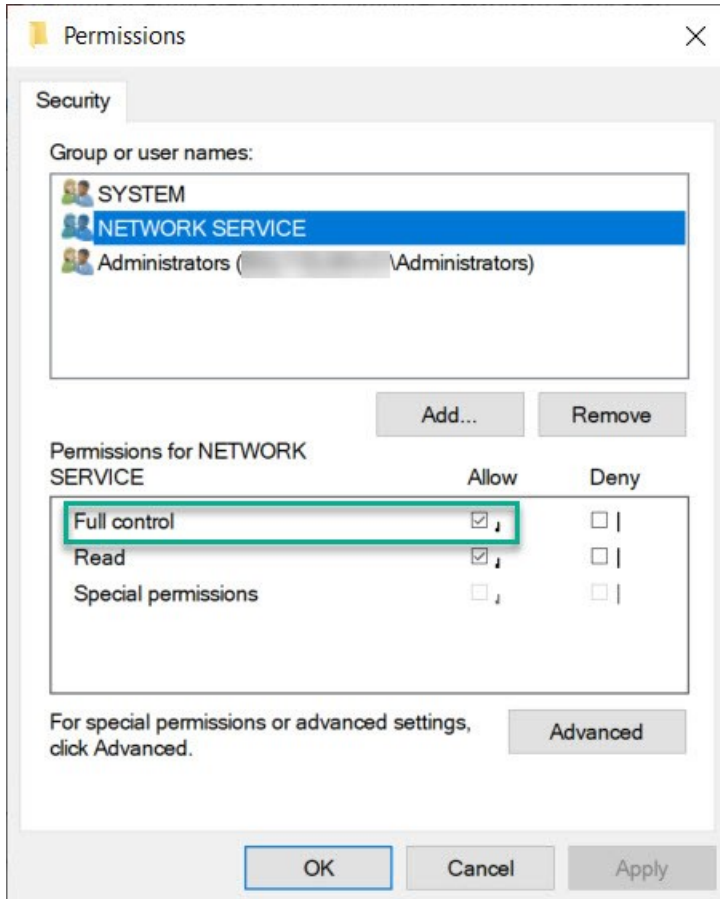
Install the user certificate on the same computer where you have installed the server certificate.

1. Copy the [user name].p12 file from the primary computer to the computer that needs access to the failover web console.
2. Right-click the user certificate and select **Install Certificate**.
3. In the **Certificate Import wizard**, choose the **Store Location**:
  - On the primary and the secondary computer, select **Local Machine**
  - On all other computers, select **Current User**

Select **Next**.

4. Browse to the certificate file and select **Next**.
5. Specify the password for the private key from when you created the server certificate, and select **Next**
6. Place the file in the **Certificate Store: Personal** and select **Next**.
7. Verify the information and select **Finish** to import the certificate.

8. On the primary and the secondary computer, allow the user that runs the Management Server service to use the private key of the user certificate:
  1. From the same computer, start **Manage computer certificates**.
  2. Select **Personal** and **Certificates**, and then select the user certificate that you have just installed.
  3. Right-click the certificate and select **All Tasks > Manage Private Keys**.
  4. Add full control permission for the user that runs the Management Server service. The default user is **Network Service**:



9. Install the server and a user certificate on every computer that you want to use for access to the failover web console.

If you had opened the web page of the failover web console before you installed the certificates, refresh the web page.

Your browser may prompt you to select a user certificate.



## Maintenance

### Remove existing failover cluster configuration

Remove your failover cluster configuration when:

- The failover cluster configuration was not successful
- Upgrading to a newer version of XProtect Management Server Failover
- Changing the SQL database location
- Updating the SQL Server version
- Enabling or disabling encryption between the management server and the recording server
- Changing the system configuration password
- Troubleshooting an issue



When you remove an existing failover cluster configuration, the XProtect Management Server Failover license, the SQL databases, and the server and user certificates are not removed.



Before you remove the failover cluster configuration, replace the virtual IP address with the address of a running management server on all clients and remote servers.

To remove the existing failover cluster configuration from the primary and the secondary computer:

1. In the notification area, right-click the Management Server Manager tray icon.
2. Select **Configure Failover Management Server**.
3. Select **Remove existing configuration** and then **Continue**. The wizard removes the failover management server configuration from the computer.
4. Select **Close** to exit the wizard.

Repeat the steps on the other computer that is part of the failover cluster.

## Uninstall XProtect Management Server Failover



Before you uninstall XProtect Management Server Failover, you must remove the failover management server configuration from the primary and the secondary computer.

1. Open the Windows **Control Panel**. Then double-click **Add or remove programs** and select **Milestone**.
2. Select **Modify** to launch the Milestone XProtect VMS wizard.
3. On the **Uninstall or change Milestone XProtect VMS components** page, select **Change one or more Milestone XProtect VMS components**. Select **Continue**.
4. Clear the check box for the XProtect Management Server Failover component and select **Continue**.
5. When the installation completes, a list shows the components that are currently installed on the computer.

## Failover web console (explained)

The failover web console allows you to manage the failover cluster. You can access the failover web console from any computer that can reach the failover cluster.



To restrict access to the web console, Milestone recommends that you use HTTPS connection.

How you open the failover web console depends on the computer:

- On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop
- On all other computers, type the URL of the failover web console in your browser: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`  
[Computername.domainname] is the FQDN of the primary or the secondary computer.

The primary and the secondary computers are represented as nodes. A module consists of two nodes: node1 corresponds to the computer you had selected as the primary computer when you configured the failover cluster, while node2 corresponds to the computer you had selected as the secondary computer.

From the failover web console, you can:

- [View the status of the nodes on page 32](#)
- [Swap the state of the nodes on page 33](#)
- [Start or stop a node on page 33](#)

- [Identify the host name of a node on page 33](#)
- See your license information
- View logs entries

## Enable basic authentication for the failover web console

By default, the HTTP connection does not provide any authentication, and anyone on your network can connect to the failover web console. However, you can configure basic user authentication to restrict access to the console.

The user name is always **administrator**, and you can only define a password for this user name.

To enable basic authentication and define a password:

1. On node1, open your preferred command-line shell. To open Windows **Command Prompt**, open the Windows **Start** menu and type **cmd**.

To change your current directory, type the following command:

```
cd C:\Program Files\Milestone\XProtect Management Server  
Failover\safekit\web\bin
```

2. Run the following command:

```
htpasswd.exe -cb "C:\Program Files\Milestone\XProtect Management Server  
Failover\safekit\web\conf\user.conf" administrator {enter your password}
```

3. Open **File Explorer** and navigate to C:\Program Files\Milestone\XProtect Management Server Failover\safekit\web\conf. Open the **httpd.conf** file with a text editor, for example **Notepad**.
4. Search for **Define usefile** and remove the # symbol before it. Save the file and close the text editor.
5. Open Windows **Command Prompt** and navigate to C:\Program Files\Milestone\XProtect Management Server Failover\safekit. To change your current directory, type the following command:

```
cd C:\Program Files\Milestone\XProtect Management Server Failover\safekit
```

6. Run the following command:

```
safekit.exe webserver restart
```

7. To enable basic authentication on both nodes, repeat the steps on node2. Since the **httpd.conf** file is

not replicated, specify the same password on both nodes.

8. Refresh the failover web console page. Your browser prompts you for a user name and password. Enter **administrator** as your user name and the password you defined in step 3.

## User interface details

The **Cluster Configuration** panel has two tabs:

- **Control**
- **Monitoring**

You can view and manage the nodes on both tabs from the **Cluster Configuration** panel.

### Control tab

On the **Control** tab, you can view the following:

Tab	Description
<b>Resources</b>	View the resources status of the module. Place the mouse cursor over the resource name to get the internal name of the resource.
<b>Module Log</b>	Read the execution log of the module. Set or clear the verbose log's checkbox to display the short log (with only E messages) or the verbose log (all messages including debug ones).
<b>Application Log</b>	Read application output messages of start and stop scripts. These messages are saved on the server side in SAFEVAR/modules/AM/userlog.ulong (where AM is the module name).
<b>Commands Log</b>	Display the commands that have been executed on the node (commands applied on the module and all global commands).
<b>Information</b>	Check the server level and the module configuration.



On the **Module Log**, **Application Log** and **Commands Log** tabs, click on the refresh button to get the last messages or on the save button to locally save the log.

### Monitoring tab

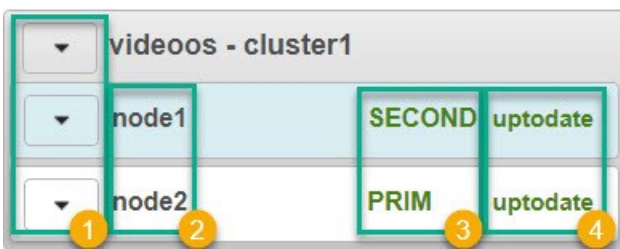
The **Monitoring** tab presents a simplified view of the current state of the module instances.

### Control panel

The control panel allows you to:

- Start or stop nodes and perform other actions. See also [Node actions on page 29](#)
- See the state of a node. See also [Node states on page 30](#)
- See the data synchronization status of a node. See also [Node data synchronization statuses on page 31](#)

The control panel consists of four columns:



- Node actions menu **1** allows you to change the state of a node
- Node1 and node2 **2**: node1 corresponds to the computer you selected as the primary computer, while node2 corresponds to the computer you selected as the secondary computer
- Node state **3** column shows the current state of a node
- The node data synchronization status **4** column shows the current data synchronization status of a node

### Node actions

Option	Description
Start	Start a node.
Stop	Stop a node.
Restart	Restart a node.
Swap	Swap the states of the nodes.

Option	Description
<b>Expert</b>	Stop and start a node, swap without data sync, force start or estimate the data sync.
<b>Admin</b>	Configure boot starts, suspend or resume the error detection of module processes, start or stop all checkers, and set the failover attribute to on or off.
<b>Support</b>	Collect logs, dumps, or snapshots for troubleshooting.

### Node states

Tab	Description
<b>PRIM</b>	The data is replicated from this node.
<b>SECOND</b>	The data is replicated to this node.
<b>ALONE</b>	No data replication. The node acts as a single unit.
<b>STOP</b>	The node is stopped, and no redundancy is available.
<b>WAIT</b>	The node is starting up (magenta) or waiting for the availability of a resource(red).

### State colors

Tab	Description
Green	The node is available.
Magenta	The node status is transient.
Red	The node is unavailable.

### Node data synchronization statuses

Tab	Description
<b>uptodate</b>	The replicated files are up-to-date.
<b>not uptodate</b>	The replicated files are not up-to-date.
<b>connection error</b>	Cannot connect to the node.
<b>not configured</b>	The configuration is missing from the node.

## Open the failover web console

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`.

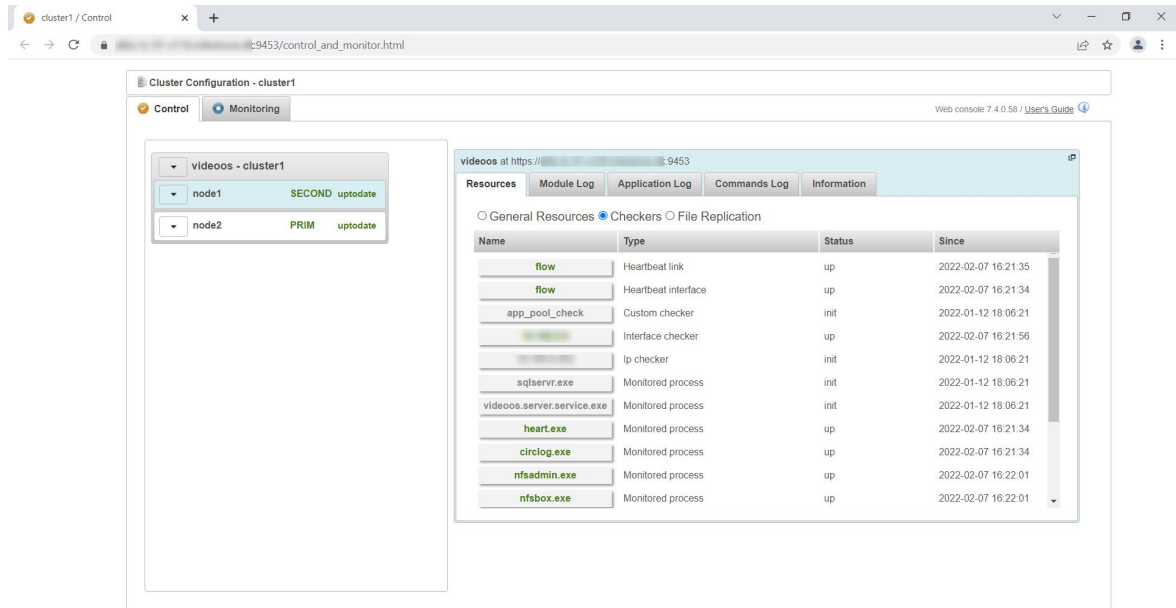
The `[computername.domainname]` is the FQDN of the primary or the secondary computer



On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

- (For HTTPS only) Select a user certificate to access the failover web console and specify the password.


The failover web console opens:



## View the status of the nodes

- On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`.

The [computername.domainname] is the FQDN of the primary or the secondary computer



On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

- On the left-hand side of the failover web console, select the **Monitoring** tab to view the current state of the module instances.



## Start or stop a node

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`.

The `[computername.domainname]` is the FQDN of the primary or the secondary computer



On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. On the left-hand side of the failover web console, select the button next to the node. Select **Start** or **Stop** to trigger action on the node. Wait until the console refreshes with the expected status.

You can run a global action on all nodes. Some local actions are only available on one node.

## Swap the state of the nodes

By default, after a failback, the failed node is stopped. If you decide to start the node, it gets the state **SECOND**.

To swap the state of the nodes:

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`.

The `[computername.domainname]` is the FQDN of the primary or the secondary computer



On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. Select the arrow next to the node in **PRIM** state and select **Swap**. A window appears. Select **Confirm** to swap the states of the nodes.

The Management Server service, Log Server service, Event Server service, and the SQL Server stop, and there is no data replication. The roles are swapped, and Management Server service, Log Server service, Event Server service, and the SQL Server start on the other node. The data replication between the nodes is restored.

## Identify the host name of a node

You can check the current state of a computer from the failover web console.

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`.

The `[computername.domainname]` is the FQDN of the primary or the secondary computer



On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. Select one of the nodes.
3. Select the **Information** tab.
4. In the **Server information**. area, you can see the host name of the computer.

## Create snapshots of a module for support

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console: `http://[computername.domainname]:9010` or `https://[computername.domainname]:9453`.

The `[computername.domainname]` is the FQDN of the primary or the secondary computer



On the primary and the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. In **Control** tab, click on the button of the node. It opens a menu with all actions that can be executed on the selected node.
3. Select the **Support** submenu, then **Snapshot** command. The web console relies on the web browser download settings for saving the snapshot file on your workstation.
4. Repeat this operation for the other node in the cluster.
5. Send snapshots to support.

The module snapshot action for a node is available in **Control** and **Monitoring** tabs.

A snapshot command creates a dump and gathers under `SAFEVAR/snapshot/modules/AM` the last 3 dumps and last 3 configurations to archive them in a .ZIP file.

A dump command creates a directory `dump_<date>_<hour>` on the server side under `SAFEVAR/snapshot/modules/AM`. The `dump_<date>_<hour>` directory contains the module logs (verbose and not verbose) and information on the system state and processes of the failover cluster at the time of the dump.

## Ports used by XProtect Management Server Failover services and modules

### XProtect Management Server Failover services

Service	Default ports	Purpose
safeadmin	Remote access on UDP port 4800 and local access on UDP port 6259	Communicate with other safeadmin instances on other computers. The main and mandatory administration service that is started at boot.
safewebserver	Local and remote TCP access on port 9010 for the HTTP web console or port 9453 for the HTTPS web console	The safewebserver service is a standard Apache web service that is mandatory for running the web console, the distributed command-line interface, and the <module> checkers.
safecaserv (optional)	Local and remote access on TCP port 9001	The safecaserv service is a web service for securing the web console with the SafeKit PKI.
safeagent (optional)	Local and remote access on UDP port 3600	The safeagent service for SNMP v2.

### Failover cluster modules

The ports values of one module are automatically computed depending on its module ID.

Module	Ports	Purpose
heart	port=8888 +(id-1)	UDP port used for sending heartbeats between the servers.
rfs	safenfs_port=5600 +(id-1)x4	TCP port used for replications requests between the servers.

# Upgrade

## Upgrading XProtect Management Server Failover

To upgrade XProtect Management Server Failover follow these steps:

1. Remove the existing failover cluster configuration from both the primary and the secondary computer. See [Remove existing failover cluster configuration on page 25](#).
2. Upgrade your VMS products on the primary and the secondary computer. See [Upgrade best practices](#).
3. Configure a new failover cluster. See [Configure failover management server \(wizard\) on page 15](#). You do not need to add the XProtect Management Server Failover license or install the certificates again.



[helpfeedback@milestone.dk](mailto: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/>.

