MAKE THE
WORLD SEE

# Milestone Systems

## XProtect® Management Server Failover 2023 R1

Administrator manual

milestone

# Contents

# Copyright, trademarks, and disclaimer

### Trademarks

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

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

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

### Disclaimer

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

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

Milestone Systems A/S 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

## What's new?

### In XProtect Management Server Failover 2023 R1

The failover web console requires authentication:

- You must authenticate with a password to log in to the failover web console. To set a password during the configuration of the failover cluster, see Configure the failover cluster on page 17.

You can change the default behavior of a node after restart:

- You can set a node to always stop or start after reboot, see Change the behavior of a node after restart on page 35.

## XProtect Management Server Failover

If a standalone computer running the Management Server service or the 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 have not logged in to the clients.

XProtect Management Server Failover provides high availability and disaster recovery for the management server. If the management server becomes unavailable on one computer, the other computer takes over running the system components. In cases of hardware failure, the secure real-time replication of the SQL database contents ensures that there is no data loss.

XProtect Management Server Failover can help you mitigate system downtime. You can benefit from a failover cluster when:

- A server fails – you can run the Management Server service and SQL Server from another computer while you resolve the problems.
- You need to apply 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 cluster, you can apply system updates and security patches with minimal downtime.
- You need seamless connection – users get continuous access to live and playback video, and to the system’s configuration at all times.

You configure XProtect Management Server Failover between two computers. To make the failover work, the following system components must run on each computer:

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

- SQL Server

## Compatibility

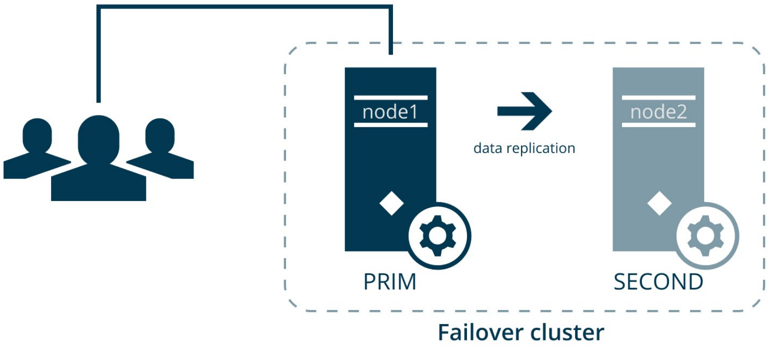
XProtect Management Server Failover is compatible with:

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

## Failover steps

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

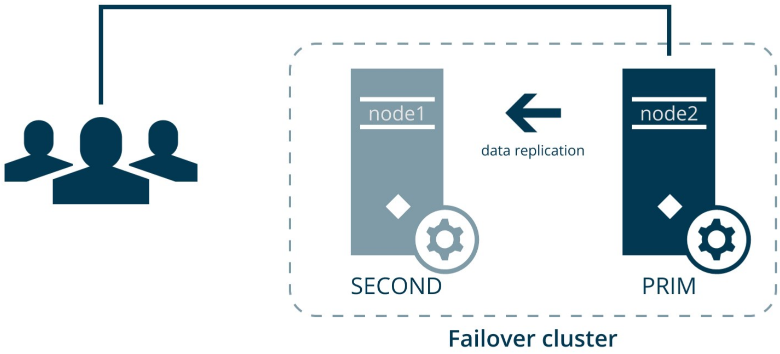
I. The Management Server service, Event Server service, Log Server service, and SQL Server run on node1 (in PRIM state). XProtect Management Server Failover replicates the data from these system components on node2 (in SECOND state).



Every second, the computers exchange heartbeats.

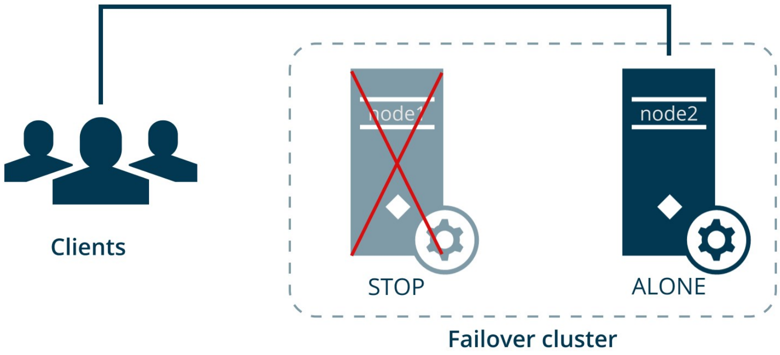
II. If the management server on node1 becomes unavailable for 30 seconds, node2 takes over.

The failover time depends on the startup time of the Management Server service.



1. Node2 comes into ALONE state, and the data replication stops.
2. The Management Server service, Event Server service, Log Server service, and 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 replicates on node1.



The VMS system components still run on node2 (in PRIM state), and the data replicates on node1 (in SECOND state).

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

# Licensing

## The 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, register the host names of the primary and secondary computers and add your XProtect Management Server Failover license.

> ⚠ If you do not add your XProtect Management Server Failover license, the Management Server service will stop after three days.

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

You can add the license during the failover cluster configuration or afterward. See Add a license for XProtect Management Server Failover on page 25.

# Requirements and considerations

## Before you configure

You configure XProtect Management Server Failover on two computers: a primary 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.

> ⚠ Do not use the primary and secondary computers in other cluster configurations.

### Network and computer prerequisites

To make sure that the primary and secondary computers can communicate with each other, the remote servers, and the clients:

- Install two identical operating systems on the primary and secondary computers. To see a list of supported operating systems, go to https://www.milestonesys.com/systemrequirements/.
- Assign static IPv4 addresses to the primary and secondary computers. Both computers must belong to the same subnet.

  XProtect Management Server Failover does not support IPv6.
- Reserve an unused IPv4 address on the subnet of the primary and secondary computers. The address serves as the virtual IP of the failover cluster.
- Use one Active Directory (AD) domain.
- Synchronize the time and the time zones between the computers.
- Allow inbound ICMP traffic through Windows Defender Firewall.
- Check if the Windows Defender Advanced Thread Protection Service is disabled. See Disable Windows Defender Advanced Thread Protection Service on page 11.
- Perform the forward and reverse DNS lookup queries in Windows PowerShell. See DNS lookups on page 11.

### SQL Server prerequisites

The SQL Server installations on the primary and secondary computer must be identical.

- Back up any existing databases to avoid loss of data.

> During the failover cluster configuration, the wizard overwrites all SQL databases on the secondary computer. The data cannot be restored.

- Make sure that the SQL Server service runs under the same AD user account as the XProtect services.
- Install only one SQL Server on the primary and secondary computers.
- Place the **DATA** and **Log** databases in the same folder. See View or Change the Default Locations for Data and Log Files.
- Verify that the instance name of your SQL Server is **MSSQLSERVER**. See View the instance name of the SQL Server on page 12.

**VMS prerequisites**

Install two identical VMS products under one AD user account with administrator permissions.

On the primary and secondary computers, install only the following system components:

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

> Install the XProtect Recording Server component and all other server components not mentioned above on different computers.

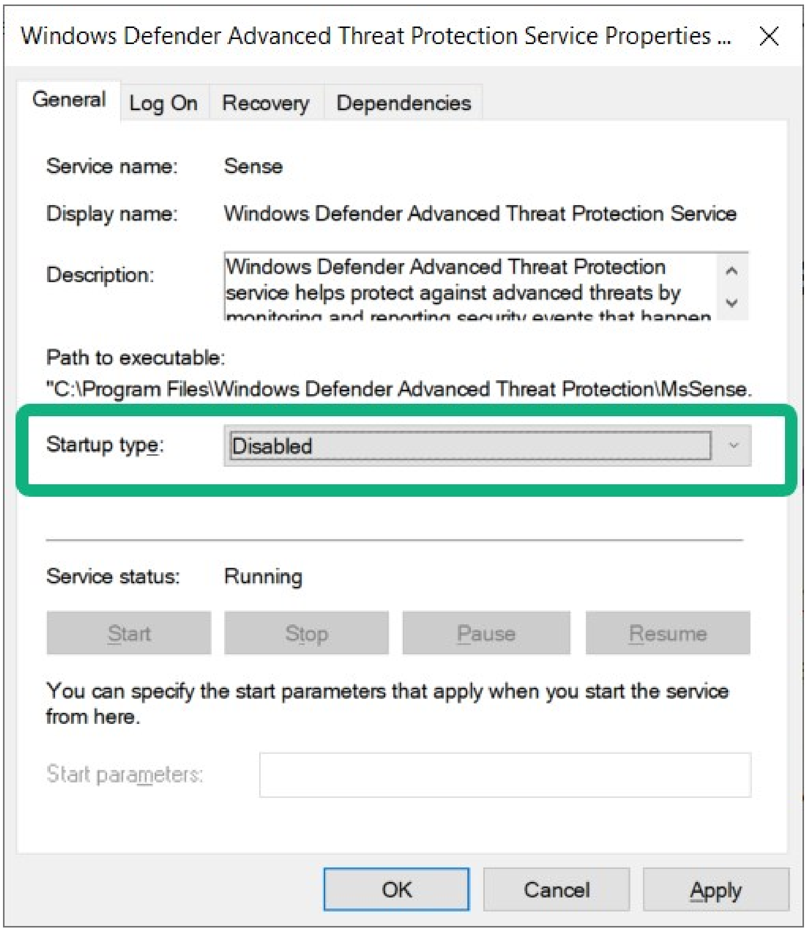
Depending on your system configuration, consider the following:

- 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 secondary computers. See Encrypting the connection to and from the failover cluster on page 13.
- System configuration password: to assign a system configuration password, use the same password on both the primary and secondary computers. Do not add or change the system configuration password after you have configured the failover cluster.
- External IDP: to use an external IDP, you must set up data protection. For more information, see Install in a cluster.
- API Gateway: to use API Gateway, you must install the component on both computers.

## Disable Windows Defender Advanced Thread Protection Service

The configuration of the XProtect Management Server Failover will fail if the Windows Defender Advanced Thread Protection Service is enabled.

1. Open the **Start** menu, and enter **services.msc** to open **Services**.
2. Scroll down to **Windows Defender Advanced Threat Protection Service**.
3. Right-click the service and select **Properties**. On the **General** tab, change the **Startup type** to **Disabled**. Then, select **OK** to save your changes.



Windows Defender Advanced Threat Protection Service Properties ...

Service name: Sense

Display name: Windows Defender Advanced Threat Protection Service

Description: Windows Defender Advanced Threat Protection service helps protect against advanced threats by monitoring and reporting security events that happen

Path to executable:
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.

Startup type: Disabled

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

## DNS lookups

For successful failover cluster configuration, Milestone recommends that you run DNS queries 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 of the primary and secondary computers are resolved as expected, you must perform the queries on the primary and secondary computers:

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

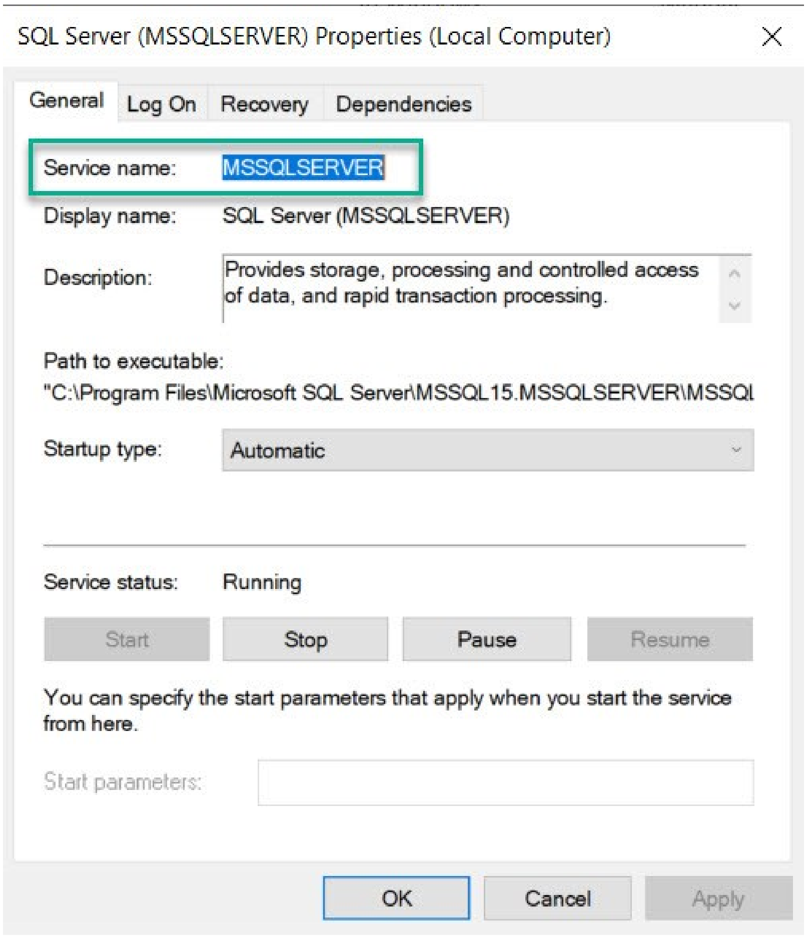
## View the instance name of the SQL Server

Milestone recommends that you check the SQL Server instance name before you start the configuration of the failover cluster.

XProtect Management Server Failover uses a hardcoded name for the SQL Server instance name: **MSSQLSERVER**.

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

1. Open the **Start** menu, and enter **services.msc** to open **Services**.
2. Scroll down to **SQL Server [Display name]**.
3. Right-click the service and select **Properties**. On the **General** tab, the value in the **Service name** field is the instance name.



SQL Server (MSSQLSERVER) Properties (Local Computer)

Service name: MSSQLSERVER

Display name: SQL Server (MSSQLSERVER)

Description: Provides storage, processing and controlled access of data, and rapid transaction processing.

Path to executable:
"C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

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 connect securely to the running management server, the remote servers must trust both the primary and the secondary computers.

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

> Do not enable encryption if the management servers are in a failover cluster.

1. Create a private and a public CA certificate.
2. Install the public certificate on all client computers.
3. Create an SSL certificate for the failover cluster.
4. Install the SSL certificate for the failover cluster on the primary and secondary computers.
5. Enable encryption for the Management Server service on the primary and secondary computers.
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

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 certificates on all computers from which you want to access the failover web console. You can create one server certificate and as many user certificates as needed.

- The server certificate is a CRT file. You install the certificate 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.

Related topics:

- Generate certificates to access the failover web console on page 25
- Install a server certificate on a computer on page 22
- Install a user certificate on a computer on page 23

## Browser requirements for the failover web console

Use the failover web console to manage the failover cluster. You can access the console from any computer that can reach the primary and secondary computers.

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/).
- After every VMS upgrade, clear the browser’s cache. To clear the cache only for the failover web console page, press **Ctrl**+**F5**.

# Installation

## Install XProtect Management Server Failover on a computer

The XProtect Management Server Failover component 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 the XProtect Management Server Failover component on two separate computers.

**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 XProtect Recording Server component on the primary or the secondary computer.

**Add the XProtect Management Server Failover component 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, the list displays the installed components.

To continue with the cluster configuration, see Configure the failover cluster on page 17

# 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 6.

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

Make sure that you have installed the XProtect Management Server Failover component on the computer, see Install XProtect Management Server Failover on a computer on page 16.

**Select the step in your configuration flow**

You have started the configuration process, see Configure the failover cluster on page 17.

**Manage your configuration**

From this page you can:

- **Apply failover license**, see Add a license for XProtect Management Server Failover on page 25
- **Generate certificates**, see Generate certificates to access the failover web console on page 25
- **Change current password for authentication**, see Change the password for authentication on page 27
- **Remove existing configuration**, see Remove the existing failover cluster configuration on page 26

## Configure the failover cluster

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

> ⚠ 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.

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

I. Start the configuration on the secondary computer. Once you prepare the secondary computer, move to the primary computer.

II. Continue the configuration on the primary computer. Once done, move to the secondary computer.

III. Finish the configuration on the secondary computer.

### Start the configuration 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**.
3. 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**.

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

5. On the **Set a password for authentication** page, specify a password for login to the failover web console. You need to set the same password on the primary computer.

   Select **Continue**.

The wizard prepares the secondary computer and informs when successfully completed.

> If you have selected HTTPS: save the security code. To establish a secure connection between the primary and secondary computers, you must specify the security code on the primary computer.

You are now ready to continue on the primary computer.

### Continue the configuration 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**.

5. On the **Connect to the secondary computer** page, specify the required system information and then select **Continue**.

| Name | Description |
|---|---|
| **Secondary computer (FQDN)** | Specify the fully qualified domain name of the secondary computer. It should follow this format: [host name].[domain name]. Example: host.domain.com. |
| **Failover license** | If you have purchased an XProtect Management Server Failoverlicense, you can add it now on this computer. If you leave the field blank and continue, you can still configure the failover cluster using a demo license and add a license later.<br>⚠ If you do not add a license, the Management Server service will stop after three days.<br>⚠ You must add the same XProtect Management Server Failover license on both computers. |
| **Virtual IP address** | The remote servers will communicate with this IPv4 address. Specify an available IPv4 address in your network to replace the actual address of the management server. |
| **Security code** (for HTTPS only) | Specify the security code from the secondary computer to establish a secure connection between the primary and secondary computers. |

6. On the **Set a password for authentication** page, enter the password that you set on the secondary computer in step 5, and then, select **Continue**.

7. 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.

8. (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.

When the configuration of the primary computer succeeds, navigate to the secondary computer to finish the configuration.

**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, and then select **Continue**.

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

3. When the configuration is successful, the failover web console opens automatically on the secondary computer.

   > (For HTTPS connection only) You cannot log in to the failover web console until you install the server certificate and a user certificate. See Installing certificates on page 22.

   The primary computer (node1) comes into the PRIM state, and the secondary computer (node2) comes into the SECOND state.

   The wizard adds a shortcut to the failover web console to your desktop.

   > To complete the setup you must register the remote servers. See Register remote servers on page 20.

If the configuration fails, you can remove the current configuration and start the process again, see Remove the existing failover cluster configuration on page 26.

## Register remote servers

A remote server is any server that is not installed on the primary and secondary computers. The virtual IP address reroutes the data packets from the remote servers to the computer that runs the 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 you have not registered the remote servers with the virtual IP address of the failover cluster, the communication with the running management server will fail if failover occurs.

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 host name that is associated with the virtual IP address.

### Change the 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 is successful, a confirmation window appears.

### Change the 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 the 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 the 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 HTTPS), and select **OK**.

If the change is successful, a confirmation window appears.

## Installing certificates

Certificates provide a secure connection to 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 25.
2. Install a server certificate on a computer on page 22.
3. Install a user certificate on a computer on page 23.

## Install a server certificate on a computer

Install the server certificate on all computers that will 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**:
   - For the primary and secondary computers, select **Local Machine**
   - For 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, and add full permissions on every computer from which you will access the failover web console.

**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**:
   - For the primary and secondary computers, select **Local Machine**
   - For 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.

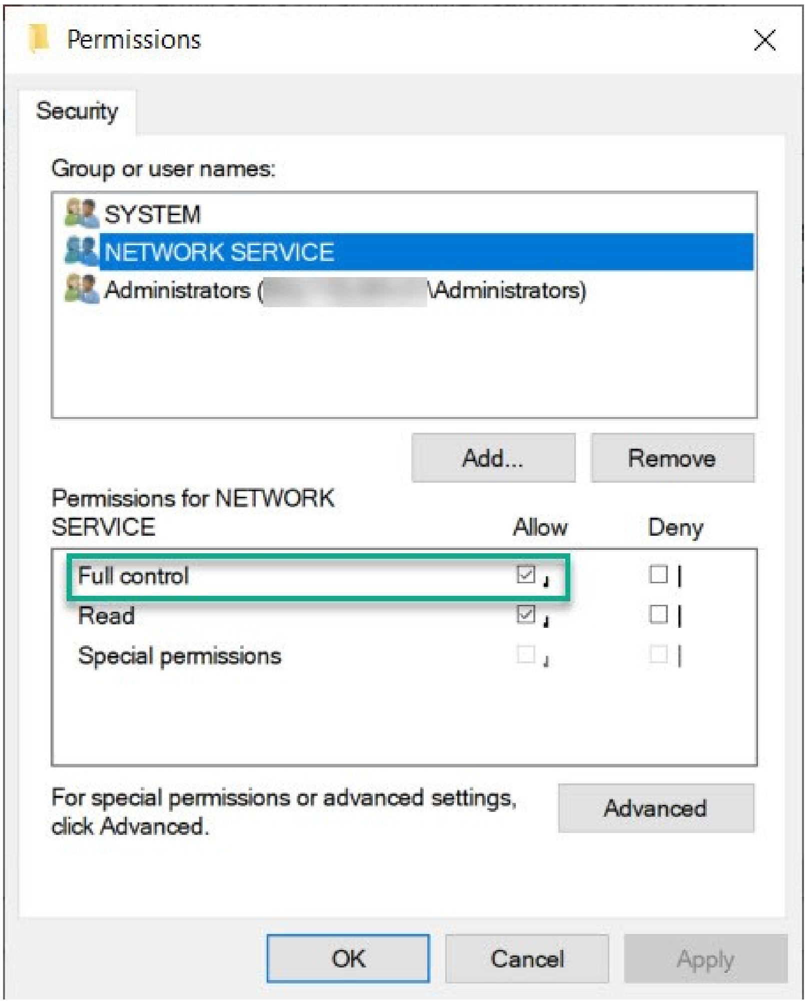
**Add full control permissions**

You need to allow the user that runs the Management Server service to use the private key of the user certificate.

To add full control permissions, on the primary and secondary computers:

1. Open the **Start** menu, and enter **certlm.msc** to open the **Certificate Manager tool** for the local device.
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**:



Group or user names:

- SYSTEM
- NETWORK SERVICE
- Administrators ([redacted]\Administrators)

| Permissions for NETWORK SERVICE | Allow | Deny |
|---|---|---|
| Full control | ☑ | ☐ |
| Read | ☑ | ☐ |
| Special permissions | ☐ | ☐ |

For special permissions or advanced settings, click Advanced.

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

## 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 17).
- 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 secondary computers.

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 configuration of the failover management server is successful.
5. Repeat steps 1 to 4 on the other computer that is part of the failover cluster.

## Generate certificates to access the failover web console

To establish a secure connection with the failover web console, you need certificates that your browser trusts. To learn more about certificates, see Certificates for the failover web console on page 14.

You must install 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 primary computer.

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 you can:
    - Create a user name.
    - Set 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. 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.

You can now install the created certificates.

Related topics:

- Install a server certificate on a computer on page 22
- Install a user certificate on a computer on page 23

## Remove the 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.

The wizard does not remove the XProtect Management Server Failover license, the SQL Server databases, and the server and user certificates.

⚠ 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 failover cluster configuration successfully, you need to use a Windows user that has administrative permissions in XProtect.

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

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.

## Change the password for authentication

To log in to the failover web console, you need to authenticate using a user name and a password.

You cannot change the predefined user name **admin**. During the configuration of the failover cluster, you must set a password for authentication.

To change the password for authentication on a computer:

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Change password for authentication** and then select **Continue**.
3. On the **Change password for authentication** page, specify and confirm a new password. Your password must be between 6 and 32 characters in length. You can use a combination of letters, numbers, and the following characters **( ) * _ - .**
4. Select **Continue** to set a new password.
5. Repeat steps 1-4 on the other computer that is part of the failover cluster configuration.

## Uninstall XProtect Management Server Failover

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

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 you have installed on the computer.

# The failover web console

Use the failover web console to manage the failover cluster. You can access the failover web console from any computer. Make sure that your network settings allow you to connect to the primary and secondary computers.

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

- On the primary and secondary computers, 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 secondary computer.

To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

The failover web console represents the primary and secondary computers as nodes: node1 corresponds to the computer you selected as the primary computer, while node2 corresponds to the computer you selected as the secondary computer.

From the failover web console, you can, for example:

- View the status of the nodes on page 33
- Swap the state of the nodes on page 34
- Start or stop a node on page 34
- Identify the host name of a node on page 35
- Change the behavior of a node after restart on page 35
- See your license information
- View logs entries

# User interface details

The failover web console consists of two main tabs:

**Control**

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

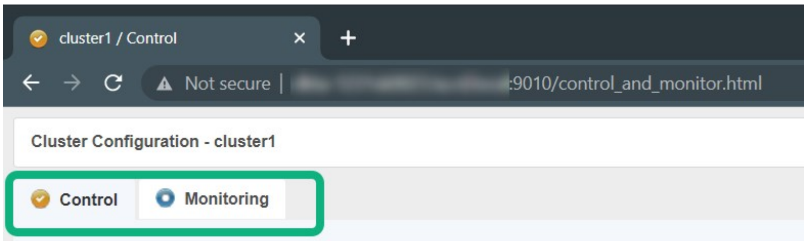
| Tab | Description |
|---|---|
| **Resources** | View the resources status of the module. Place the mouse cursor over the resource name to get the internal name of the resource. |
| **Module Log** | Read the execution log of the module. Set or clear the verbose log's checkbox to display the short log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

**Monitoring**

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

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

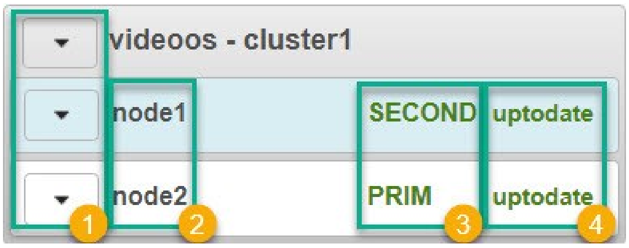

cluster1 / Control
Not secure
:9010/control_and_monitor.html
Cluster Configuration - cluster1
Control
Monitoring

### Cluster options

From the left-hand panel, you can:

- Start or stop nodes and perform other actions. See also Node actions.
- See the state of a node. See also Node states.
- See the data synchronization status of a node. See also Node data synchronization statuses.

The control panel consists of four columns:



- Node actions menu ❶ shows the options to change the state of a node.
- Node1 and node2 ❷: 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 ❸ column shows the current state of a node.
- The node data synchronization status ❹ 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. |
| **Expert** | Stop and start a node, swap without data sync, force start or estimate the data sync. |
| **Admin** | Configure boot start, suspend or resume the error detection of |

| Option | Description |
|---|---|
| | module processes, start or stop all checkers, and set failover to on or off. |
| **Support** | Save logs, dumps, or snapshots for troubleshooting. |

**Node states**

| Tab | Description |
|---|---|
| **PRIM** | The data replicates from this node. |
| **SECOND** | The data replicates to this node. |
| **ALONE** | No data replication. The node acts as a single unit. |
| **STOP** | The node stopped, and no redundancy is available. |
| **WAIT** | (Transient) 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 |
|---|---|
| **uptodate** | The replicated files are up-to-date. |
| **not uptodate** | The replicated files are not up-to-date. |
| **connection error** | Cannot connect to the node. |
| **not configured** | The configuration is missing from the node. |

## Open the failover web console

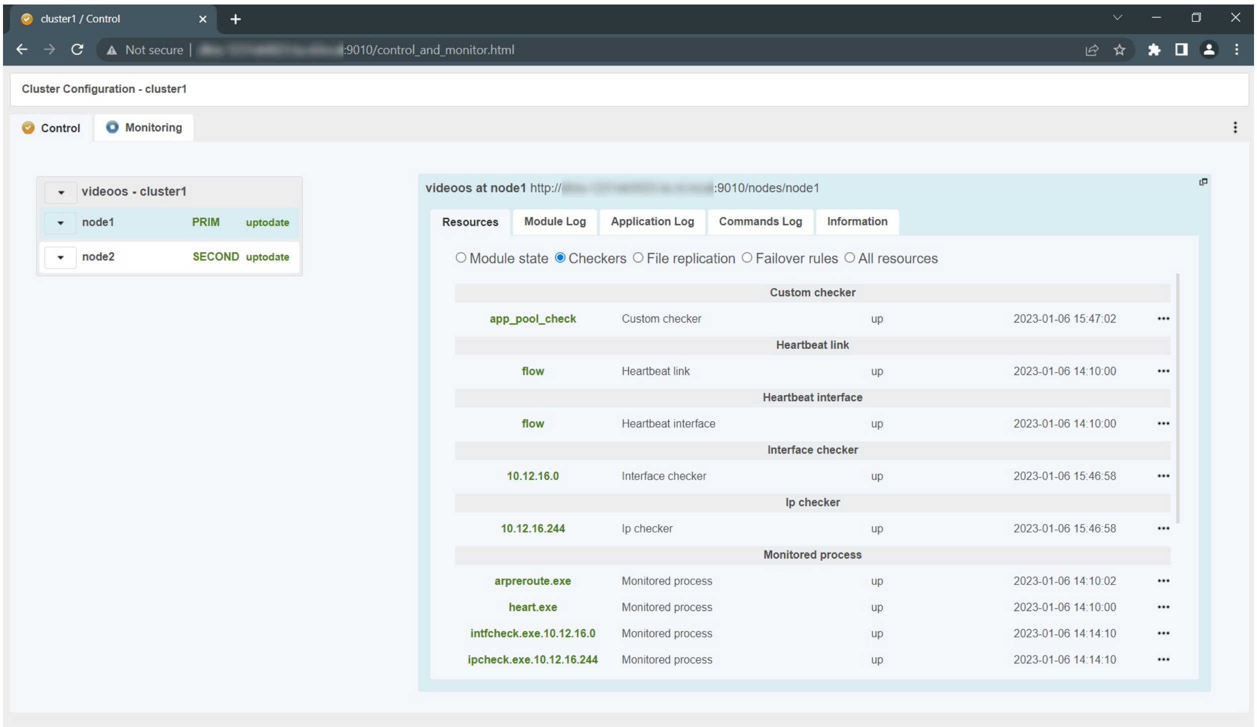
1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **http://[computername.domainname]:9010** or **https://[computername.domainname]:9453**.

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

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

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.
3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

The failover web console opens:



○ Module state ● Checkers ○ File replication ○ Failover rules ○ All resources

| | | | | |
|---|---|---|---|---|
| Custom checker | | | | |
| app_pool_check | Custom checker | up | 2023-01-06 15:47:02 | ••• |
| Heartbeat link | | | | |
| flow | Heartbeat link | up | 2023-01-06 14:10:00 | ••• |
| Heartbeat interface | | | | |
| flow | Heartbeat interface | up | 2023-01-06 14:10:00 | ••• |
| Interface checker | | | | |
| 10.12.16.0 | Interface checker | up | 2023-01-06 15:46:58 | ••• |
| Ip checker | | | | |
| 10.12.16.244 | Ip checker | up | 2023-01-06 15:46:58 | ••• |
| Monitored process | | | | |
| arpreroute.exe | Monitored process | up | 2023-01-06 14:10:02 | ••• |
| heart.exe | Monitored process | up | 2023-01-06 14:10:00 | ••• |
| intfcheck.exe.10.12.16.0 | Monitored process | up | 2023-01-06 14:14:10 | ••• |
| ipcheck.exe.10.12.16.244 | Monitored process | up | 2023-01-06 14:14:10 | ••• |

# View the status 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 using this format: **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 or the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.

3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

4. On the left-hand side of the failover web console, select the  **Monitoring** tab to view the current state of the nodes. To learn more about node statuses, see User interface details on page 28.

## 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 using this format: **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 or the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.

3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

4. On the left-hand side of the failover web console, select the arrow next to a node.

   > ✓ You can select the arrow next to **videoos-cluster1** to trigger an action on both nodes.

   Select **Start** or **Stop**. The console refreshes with the expected state.

## Swap the state of the nodes

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

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 using this format: **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 or the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.

3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

4. 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

The failover web console represents the primary computer as node1 and the secondary computer as node2. To see the host name that corresponds to 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 using this format: **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 or the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.

3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

4. Select one of the nodes.

5. Select the **Information** tab.

6. In the **Server information** area, you can see the host name of the computer.

## Change the behavior of a node after restart

By default, if a node restarts, it keeps its previous state. You can change that behavior and make a node to always start or stop after restart.

1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: **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 or the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.
3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.
4. Select the arrow next to a node and select **Admin** > **Configure boot start**.
5. From the **Module start at boot time** window, select:
   - **enabled** - the node starts automatically after restart and comes into SECOND state.
   - **disabled** - the node comes into STOP state after restart. You can start the node manually from the failover web console.

> To revert to the default behavior and set the node to keep the state from before the restart, you need to remove the existing failover configuration and configure the failover cluster again.

## 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 using this format: **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 or the secondary computer, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. (For initial connection over HTTPS only) Select a user certificate to access the failover web console and specify the password.

3. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see Change the password for authentication on page 27.

4. 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.

5. 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.

6. Repeat this operation for the other node in the cluster.

7. 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 comman-line interface, and the <module> checkers. |

| Service | Default ports | Purpose |
|---|---|---|
| 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

1. Remove the existing failover cluster configuration from the primary and secondary computers. See Remove the existing failover cluster configuration on page 26.

2. Upgrade your VMS on the primary and secondary computers. See Upgrade best practices.

3. Restart the primary and secondary computers.

4. Configure a new failover cluster. See Configure failover management server (wizard) on page 17. You do not need to add the XProtect Management Server Failover license or install the certificates again.

# FAQ

## XProtect Management Server Failover FAQ

**Can I install a recording server on the primary or the secondary computer?**

No, you cannot. The recording server must be installed on a separate computer or the failover cluster will not work.

**What happens if the primary or the secondary computer restarts unexpectedly?**

By default, when the primary or the secondary computer restarts, the node keeps the state from before the restart.

**What happens when the three-day demo license expires?**

The Management Server service stops every day and you have to start the service manually.

**How can I understand if the primary node has failed?**

You can view the states of the nodes from the failover web console or create an event in XProtect Management Client.

**Does XProtect supports events from the failover cluster?**

Yes, you can configure an event in XProtect Management Client when a failover occurs.

**What editions of SQL Server does XProtect Management Server Failover support?**

XProtect Management Server Failover supports all editions of SQL Server.

**Do I have to remove my existing VMS configuration before I can configure a failover cluster?**

You can configure a failover cluster with an existing VMS configuration. Before you start the configuration, backup the existing SQL databases and the XProtect system configuration. Make sure to select the computer where your current management server runs as the primary computer.

**Which Windows users can see the desktop icon for the XProtect Management Server Failover web console?**

All users of the primary and secondary computers can see the desktop icon for the XProtect Management Server Failover web console.

**I upgraded my VMS and tried to configure the failover cluster, but my configuration failed. What can I do?**

Before you start the configuration process again, remove the existing failover cluster configuration, then restart the primary and secondary computers.

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/.