# Milestone Systems

XProtect Management Server Failover

milestone

# Contents

# Copyright, trademarks, and disclaimer

### Trademarks

This document contains trademarks owned by Milestone Systems A/S such as Milestone, Arcules, BriefCam, and XProtect.

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.

# XProtect Management Server Failover

If a standalone computer running the management server or 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 is an XProtect VMS extension that can help you when:

- A server fails – you can run the system components 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.

To configure XProtect Management Server Failover, you install the management server, log server, and event server on two computers. If the first computer stops working, the VMS components start running on the second computer. Additionally, you can benefit from a secure real-time replication of the VMS databases when SQL Server runs in the failover cluster.

# What's new?

In XProtect Management Server Failover 2025 R1

External Public Key Infrastructure (PKI) certificates

- You can now use your certificates to connect to the failover web console. See Use custom server certificates for communication with the failover web console.

SQL Server

- You can use custom locations for the data and log files of the SQL Server databases. See Configuring the failover cluster without database replication.

## In XProtect Management Server Failover 2023 R3

Failover recording server:

- You can now configure XProtect Management Server Failover and a failover recording server in a workgroup environment. See Prerequisites for running a recording server or failover recording server on the cluster nodes.

Troubleshooting:

- To see a list of the most common issues with XProtect Management Server Failover, go to Troubleshooting XProtect Management Server Failover .

## In XProtect Management Server Failover 2023 R2

Recording server:

- You can now install a recording server on the failover cluster nodes. See Prerequisites for running a recording server or failover recording server on the cluster nodes.

External SQL Server:

- You can now connect the XProtect Management Server Failover to your external SQL Server. See SQL Server prerequisites.

Workgroups:

- You can now configure the failover cluster in a workgroup environment. See Network and computer prerequisites.

User certificates:

- User certificates are no longer required to log in to the failover web console. To log in to the failover web console, you must now install a server certificate and authenticate with a user name and password. See Open the failover web console.

## In XProtect Management Server Failover 2023 R1

Authentication for the failover web console:

- 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.

Behavior of a node after restart:

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

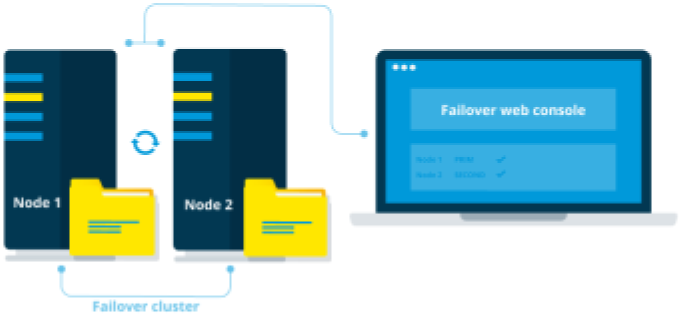
# Compatibility

XProtect Management Server Failover is compatible with:

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

# XProtect Management Server Failover elements

XProtect Management Server Failover consists of the following elements:



**Failover cluster** - It consists of two independent computers that work together to maintain high availability of the management server, log server, event server, and SQL Server. If one of the computers fails, the other computer in the cluster takes over the workload of running the VMS server components.

**Primary and secondary computers** - Typically, the primary computer is the computer you have a running VMS installation on. To configure the failover cluster, you install a VMS product on the secondary computer that mirrors the one on the primary computer.

**Nodes** - The failover cluster consists of two computers called nodes. The primary computer is referred to as Node 1, and the secondary computer is referred to as Node 2. The names of the nodes do not change but they can have different states. During normal operation, the node the VMS servers run on is in PRIM state and the standby node is in SECOND state.

**Virtual IP** - The virtual IP serves as a cluster address and allows the remote servers to connect seamlessly to the running management server. The virtual IP is an address you define during the configuration of the failover cluster.

Related topics:

- Failover steps
- The failover web console
- Node states

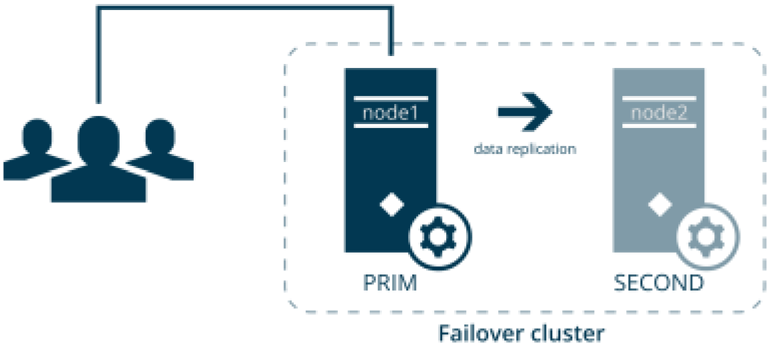
# Failover steps

In a typical scenario, you install these components on both nodes:

- XProtect Management Server
- XProtect Log Server
- XProtect Event Server
- SQL Server

The failover steps in a typical scenario are:

1. The management server, event server, log server, and SQL Server run on Node 1 (in PRIM state). If you have installed SQL Server on the nodes, XProtect Management Server Failover replicates the data from these system components on Node 2 (in SECOND state).

   Every second, the nodes exchange heartbeats.

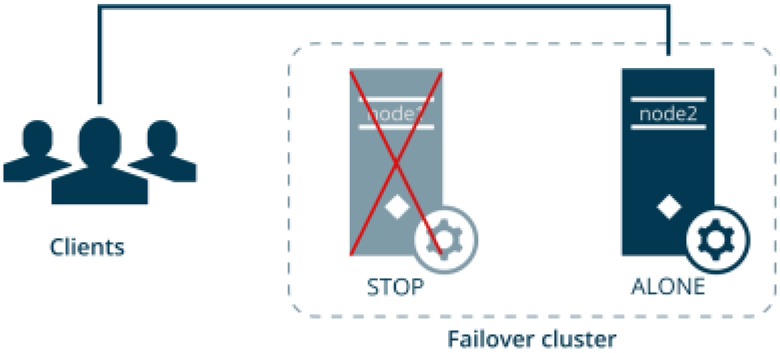
2. If the management server on Node 1 becomes unavailable for 30 seconds, Node 2 takes over.

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

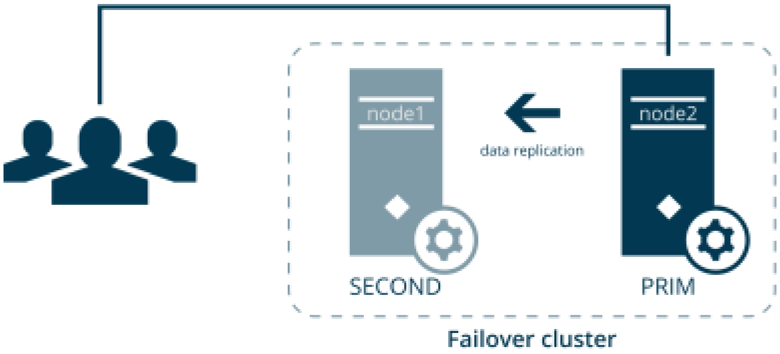
   a. Node 2 comes into ALONE state, and the data replication stops.

   b. The management server, event server, log server, and SQL Server start running on Node 2.

   c. The management server, event server, and log server store data on the SQL Server on Node 2.



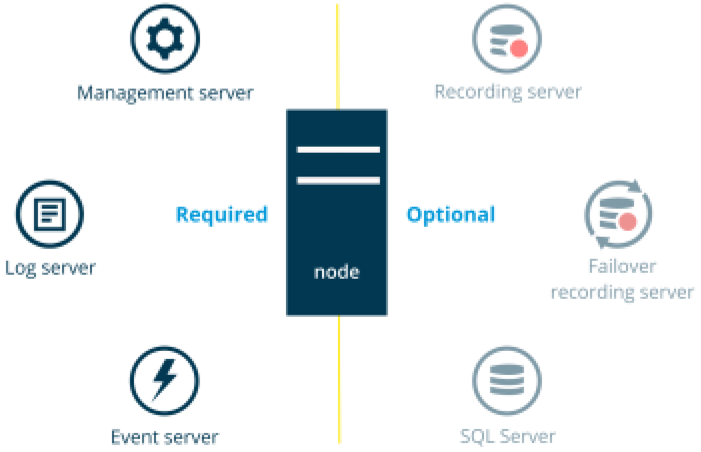
3. You identify and fix the issue that caused the failover and start Node 1 from the failover web console. The data that was modified on Node 2 replicates to Node 1.



The VMS system components still run on Node 2 (in PRIM state), and the data replicates on Node 1 (in SECOND state). If needed, you can swap the states of the nodes from the failover web console.

# Required and optional XProtect VMS components

Depending on the size of your VMS installation and resources, you can configure XProtect Management Server Failover in different ways. You can install the following system components on Node 1 and Node 2 in a domain or workgroup environment:



On the failover cluster nodes, you must install:

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

Additionally, you can install the following system components:

## SQL Server

You can use internal or external SQL Server instances.

To use an internal SQL Server instance, you must install SQL Server on both nodes. When using an internal SQL Server instance, XProtect Management Server Failover replicates the contents of the SQL Server databases and triggers failover if the SQL Server instance fails. See Prerequisites for SQL Server with data replication

If you have a large VMS installation, you can use an external SQL Server instance and exclude SQL Server from the failover cluster. In this scenario, the XProtect Management Server Failover solution does not monitor and replicate the SQL Server databases. Milestone recommends regular backups of the SQL Server databases as a disaster recovery measure. See Prerequisites for SQL Server without data replication.

## Recording Server

You can install a recording server on one or both nodes.

XProtect Management Server Failover does not provide failover for the recording server. You must configure the failover recording server yourself.

See Prerequisites for running a recording server or failover recording server on the cluster nodes.

## Failover Recording Server

You can install a failover recording server on one or both nodes.

If you have limited resources, you can use the failover cluster nodes to host a recording server and a failover recording server. You configure the failover recording server from XProtect Management Client.

For system resiliency, Milestone recommends installing the recording server on Node 2 and the failover recording server on the Node 1.

> ⚠ When part of the failover cluster, the failover recording server can work only in a Hot standby setup.

# XProtect Management Server Failover licenses

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

To use the failover cluster for unlimited period, you must purchase a license and provide your Milestone representative with the Node 1 and Node 2 hostnames. The license is issued specifically for these hostnames and can only be used with them.

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

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

# Before you configure the failover cluster

To prepare your system for the configuration of the failover cluster, check the prerequisites below:

**Network and computer**

Network and computer prerequisites

**SQL Server**

Prerequisites for SQL Server without data replication

Prerequisites for SQL Server with data replication

**VMS**

XProtect VMS prerequisites

Prerequisites for running a recording server or failover recording server on the cluster nodes

**Encryption**

Encryption considerations

Encrypting the connection to the failover cluster

Server certificate for the failover web console

# Network and computer prerequisites

Prepare your infrastructure for the configuration of the failover cluster.

- **Operating system** - Install two identical operating systems on Node 1 and Node 2. To see a list of supported operating systems, go to https://www.milestonesys.com/systemrequirements/.
- **Addresses** - In the same subnet, assign static IPv4 addresses to the nodes and reserve an IPv4 address for the virtual IP. The virtual IP allows the remote servers to connect seamlessly to the running management server.

> ⚠ If the host name and address of a node does not resolve as expected by the system, the configuration might fail. See DNS lookups .

> Do not assign IPv6 addresses to the computers that run the management server and external SQL Server. XProtect Management Server Failover does not support the IPv6 protocol.

- Domain or workgroup environment - Configure the failover cluster in an Active Directory (AD) domain or workgroup environment.

## Domain

Use the same AD domain on both nodes.

## Workgroup

| Prerequisite | Description |
|---|---|
| Workgroup membership | Add Node 1 and Node 2 to the same workgroup. |
| (When without DNS server) Host name mapping | Map the host names of the nodes to their IP addresses. See Map the host names of the nodes. |
| Windows group | You must add a new Windows group in XProtect Management Client on both nodes.<br>Go to **Roles** and add the `BUILTIN/Administrators` Windows group to the **Administrators** role. |
| Basic user | To make sure you can always log in, add a basic user to the Administrators role in XProtect Management Client for the VMS installations on both nodes.<br>Go to **Roles** and add an existing basic user or create a new one. |

- **Time** - Synchronize the time and time zones between the nodes.
- **ICMP traffic** - Allow inbound ICMP traffic through all device firewalls.
- **PowerShell execution policy** - Set your PowerShell execution policy to **Unrestricted**. This allows the configuration wizard to run PowerShell scripts on both nodes. See about_Execution_Policies.
- **Windows Defender Advanced Thread Protection Service** - You must disable Windows Defender Advanced Thread Protection Service. See Disable Windows Defender Advanced Thread Protection Service.

# Prerequisites for SQL Server with data replication

When you install SQL Server on the nodes, XProtect Management Server Failover replicates the contents of the SQL Server databases and triggers failover if the SQL Server instance fails.

To use data replication with XProtect Management Server Failover, the SQL Server installations must be identical on both nodes. You can see a lits supported SQL Server editions for your VMS product at https://www.milestonesys.com/systemrequirements/.

Also, consider the following prerequisites:

| Prerequisite | Description |
|---|---|
| Database backup | Back up any existing databases to avoid loss of data.<br>During the failover cluster configuration, the wizard replicates the SQL Server databases on Node 1 to the SQL Server databases on Node 2. All data on the SQL Server databases on Node 2 is overwritten. |
| SQL Server service account | The SQL Server service must run under the same user account as the XProtect services. |

| Prerequisite | Description |
|---|---|
| | To change a service account for the XProtect VMS, see Changing the service account that runs a VMS service |
| Database location | You can use the default or custom location for the VMS databases data and log files.<br>The default configuration is as follows:<br>• The VMS databases data and log files are stored in the **DATA** folder.<br>• The SQL Server error logs, trace log files, and log events are stored in the **Log** folder.<br>• The **DATA** and **Log** folders belong to the same parent folder.<br>The default locations are:<br>• `C:\Program Files\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\DATA`<br>• `C:\Program Files\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\Log`<br>{nn} is the version number.<br>To use custom locations, place the data (.mdf) and log (.ldf) files in a folder called **DATA**. Then, create an empty **Log** folder in the same parent folder. |
| Virus scanning exclusions | In your antivirus program, exclude the locations of the **DATA** and **Log** folders from virus scanning. |
| Instance name | Verify that the instance name of your SQL Server is **MSSQLSERVER**. See View the SQL Server instance name. |

# Prerequisites for SQL Server without data replication

You can set up a failover cluster with an external SQL Server instance not running on the nodes. With this configuration, XProtect Management Server Failover does not monitor the SQL Server databases.

> The failover server configuration with external SQL Server does not work in a workgroup environment.

| Prerequisite | Description |
|---|---|
| Permissions for the SQL Server user | In Microsoft SQL Server Management Studio, add a Windows user to the **public** role and map the user to the **db_owner** database role for the following databases:<br>• **Surveillance**<br>• **Surveillance_IDP** |

| Prerequisite | Description |
|---|---|
| | • **Surveillance_IM**<br>• **LogserverV2** |
| Connection | Verify that the VMS installations on both nodes:<br>• Are connected to the external SQL Server instance.<br>• The VideoOS IIS application pools on Node 1 are running.<br>• The VMS services on Node 1 are running. |
| Service account | Make sure that the Management Server service on both nodes runs under the Windows user you added on the SQL Server computer.<br>If your SQL Server runs under a different user, you can change the account that runs the Management Server service. See Changing the service account that runs a VMS service. |

# XProtect VMS prerequisites

Install two identical VMS products under a common user account with administrator permissions. To learn more about the general prerequisites for installing XProtect VMS, see the XProtect VMS administrator manual.

> When working in a domain environment, select AD users for the service accounts and only give them the permissions required to run the relevant services.

**XProtect components**

On both nodes, install the following system components:

- XProtect Management Server
- XProtect Event Server
- XProtect Log Server
- XProtect Management Server Failover
- XProtect API Gateway
- XProtect Recording Server (optional), see Prerequisites for running a recording server or failover recording server on the cluster nodes.

Install all other server components not mentioned above on different computers.

**Other considerations**

Depending on your system configuration, consider the following:

- **Plug-ins for the XProtect VMS** - Some third-party and custom plug-ins might not work with XProtect Management Server Failover. Always check with your Milestone sales representative if your plug-ins are supported.

- **System configuration password** - To assign a system configuration password, use the same password for the VMS installations on both nodes.

# Encryption considerations

If you want to encrypt the connection between the failover cluster nodes and other VMS components, you must consider the following:

- **VMS certificates** - To encrypt the connection to and from the running management server, you must install the CA certificate and an SSL certificate on both nodes. See Encrypting the connection to the failover cluster.

- **Failover certificates** - The failover cluster communicates with the failover web console through HTTP or HTTPS. You can use your own certificate or let the configuration wizard generate one for you. See Server certificate for the failover web console and Use custom server certificates for communication with the failover web console.

- **Identity Provider** - To ensure that users can log in to the running management server, you must set up data protection and update the data protection keys. See Update the data protection settings for Identity Provider.

# Prerequisites for running a recording server or failover recording server on the cluster nodes

Installing the recording server or failover recording server on the cluster nodes requires additional steps.

You can install a recording server or failover recording server on one or both nodes. For example, you can install:

- A recording server on Node 1.

- A recording server on Node 1 and a failover recording server on Node 2.

- A recording server on Node 1 and Node 2.

Before you configure the management server failover, consider the following:

- **Environment** - The nodes can run in a domain or workgroup environment.

- **Failover recording server setup** - If you configure a failover recording server on any of the nodes, you must use it in a hot standby setup.

- **Encryption** (optional)- To encrypt the connection between the VMS components, you must install the SSL certificate for the recording server on the recording server computer. Then, you must enable encryption for the recording server from the recording server's Server Configurator.

- **Services** - The XProtect Recording Server service and the configuration wizard for XProtect Management Server Failover need port 9001 to operate. To avoid conflicts, you must either use another port for the Milestone XProtect Recording Server service or stop the service when you configure or remove the configuration from the failover cluster.

To learn more about the configuration of the recording server and the failover recording server, see the XProtect VMS administrator manual.

# Server certificate for the failover web console

> You can connect to the failover web console over an HTTP or HTTPS connection. This section is only relevant if you want to use an HTTPS connection.

To secure the communication with the failover web console, you need a server certificate, see The failover web console .

The server certificate is a .crt file that you install on your computer. You must add the certificate to the computer's "Trusted Root Certification Authorities" store so that your computer trusts that certificate. If you do not install the certificate, your connection will remain secure, but:

- You will get a security warning the first time you open the failover web console.
- The system will not trigger an event in case of failover.

The wizard creates and downloads a server certificate from a local web service while configuring the failover cluster on Node 1. The wizard downloads a new server certificate whenever you configure the failover cluster. You can remove the previous certificates from the "Trusted Root Certification Authorities" store.

If you lose the server certificate, you can download it again from the **Manage your configuration** page on Node 1. See Download the server certificate to access the failover web console.

The server certificate is valid for five years. You will not receive a warning when a certificate is about to expire. If a certificate expires, your browser will no longer trust that certificate. To renew the server certificate, you must configure a new failover cluster.

Install the server certificate on all computers from which you want to access the failover web console, see Install the server certificate on a computer.

# Encrypting the connection to the failover cluster

To connect securely to the running management server, the remote servers must trust all nodes.

To enable encryption between the management servers and the remote servers, you must install the following certificates on all nodes:

- The public CA certificate
- The SSL certificate for the failover cluster

> To learn how to generate and install certificates, see the XProtect VMS certificates guide.

To enable encryption for a new VMS installation, you must:

1. Create a private and a public CA certificate.
2. Install the public certificate on the hosts where you have installed a VMS client component.
3. Create an SSL certificate for the failover cluster that includes the node name and the address of the cluster.
4. Install the SSL certificate for the failover cluster on the nodes.
5. Enable encryption for the Management Server service on the nodes.
6. Create and install certificates on the hosts where you installed a VMS server component.
7. Enable encryption on the hosts where you installed a VMS server component.

# Update the data protection settings for Identity Provider

When you set up the management server in a cluster, you must update the Identity Provider configuration data to make the data protection settings identical on both nodes.

> ⚠ You must have imported your certificate to the Personal store for the user running **VideoOS IDP AppPool** and given it Read permissions. If you use a self-signed certificate, you must add it to the

Trusted Root Certificates Authorities store on your local computer.

To set up data protection and update the data protection keys for the user running the **VideoOS IDP AppPool** application pool:

1. On Node 1, locate the appsettings.json file in the installation path of the Identity Provider (`[Install path]\Milestone\XProtectManagement Server\IIS\IDP).`
2. In the **DataProtectionSettings** section, make the following changes:
   - To set up data protection, set the thumbprint of the certificate that's used by the IDP application pools and the Management Server service. See How to: Retrieve the Thumbprint of a Certificate.
   - To remove the old certificate key, set CleanUpNonCertificateKeys to true.

   ```
   "DataProtectionSettings": {
     "ProtectKeysWithCertificate": {
       "Thumbprint": ""
       "CleanUpNonCertificateKeys": true
     }
   },
   ```

3. Repeat steps 1-2 on Node 2.

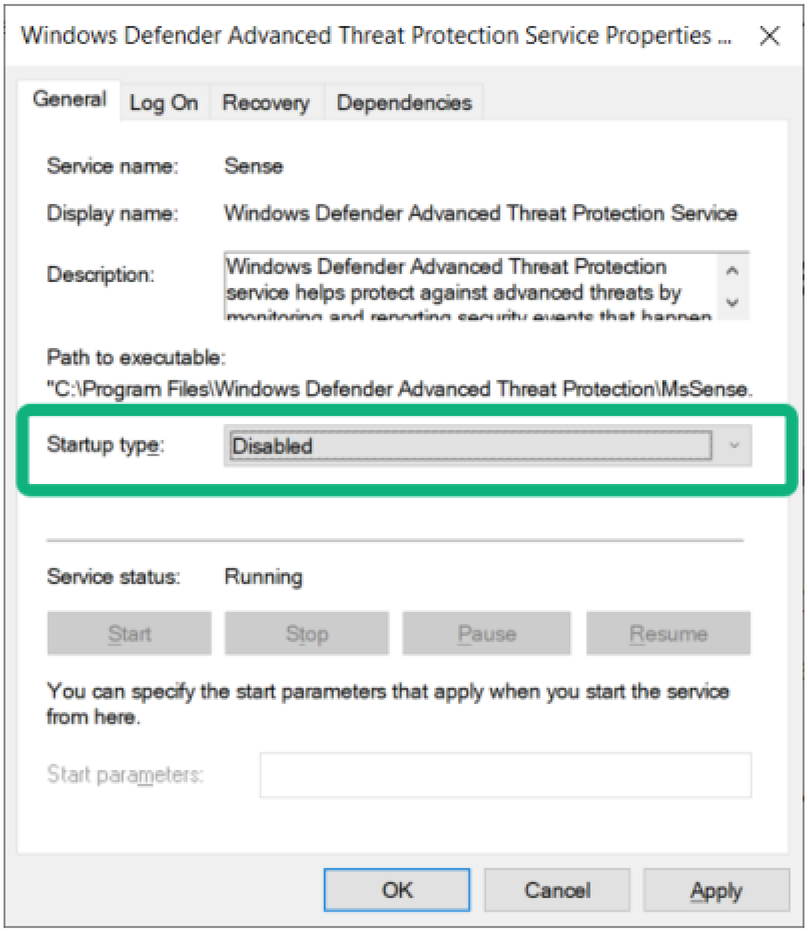
# Disable Windows Defender Advanced Thread Protection Service

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

1. On Node 1, open the **Start** menu, and enter **services.msc** to open **Services**.
2. Scroll down to **Windows Defender Advanced Threat Protection Service**.
3. Check the status of the service. If the status field is blank, this means that the service is not running.
4. To prevent the service from starting at system startup, right-click the service and select **Properties**. On the **General** tab, change the **Startup type** to:
   - **Disabled** if the service is running.
   - **Manual** is the service is stopped.

   Then, select **OK** to save your changes.

   You must have the necessary user permissions in Windows to perform this operation.



Windows Defender Advanced Threat Protection Service Properties ...
General
Log On
Recovery
Dependencies
Start
Stop
Pause
Resume
OK
Cancel
Apply

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:

5. Repeat steps 1-4 on Node 2.

# 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 host name that is related to an IP address

To make sure that the IP addresses and the host names of the nodes are resolved as expected, you must perform the queries on Node 1 and Node 2:

| Query name | Command | Perform on | Expected result |
|---|---|---|---|
| Forward DNS lookup | **Resolve-DnsName [Node 2 host name]** | Node 1 | The host name of Node 2 corresponds to the first IP address on the list. |
| Forward DNS lookup | **Resolve-DnsName [Node 1 host name]** | Node 2 | The host name of Node 1 corresponds to the first IP address on the list. |
| Reverse DNS lookup | **Resolve-DnsName [Node 2 IP address]** | Node 1 | The IP address of Node 2 corresponds to the first host name on the list. |
| Reverse DNS lookup | **Resolve-DnsName [Node 1 IP address]** | Node 2 | The IP address of Node 1 corresponds to the first host name on the list. |

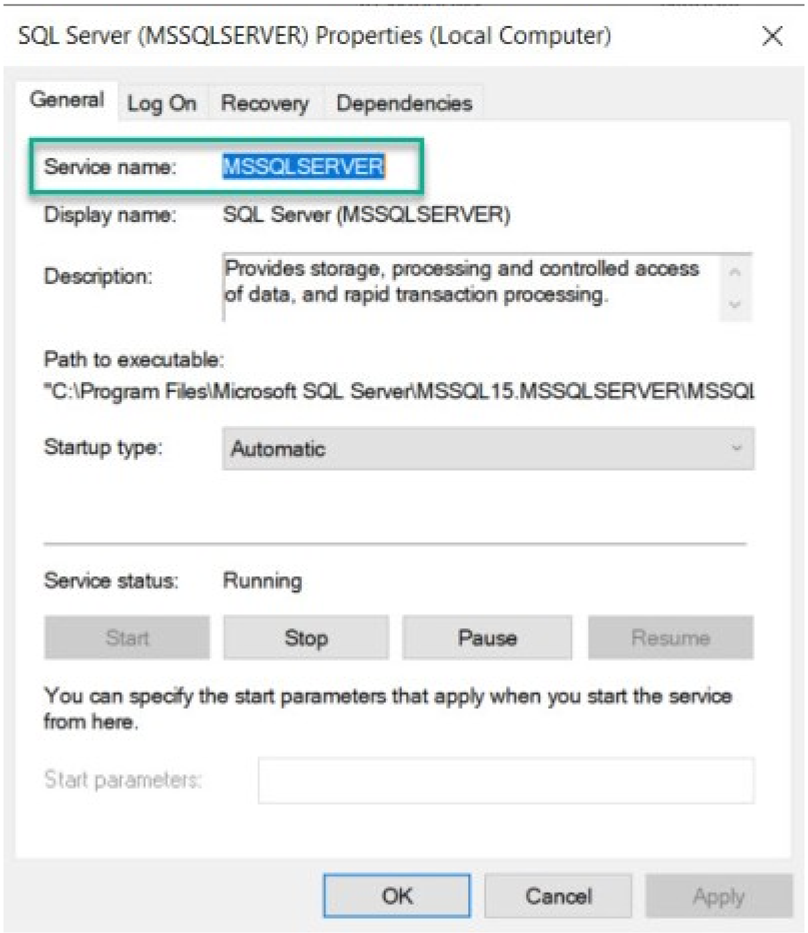
# View the SQL Server instance name

This section is only relevant if you want to use an internal SQL Server instance.

XProtect Management Server Failover uses a hardcoded name for the SQL Server instance name **MSSQLSERVER** and, If the instance name differs, the configuration will fail.

You must check the SQL Server instance name on both nodes.

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:

# Changing the service account that runs a VMS service

A Microsoft service account is an account used to run one or more services or applications in a Windows environment. The VMS services use the service accounts to register and communicate with the other VMS components. You select the service account for the VMS during the installation of the XProtect VMS, such as Network Service, but you can change the service account afterward.

To make sure that the different VMS components can communicate with each other after you have changed the service account, you must do the following:

1. Add the selected Windows user to the Administrator role in XProtect Management Client.
2. In Microsoft SQL Server Management Studio, add a Windows user to the **public** role and map the user to the **db_owner** database role for the following databases:
   - **Surveillance**
   - **Surveillance_IDP**
   - **Surveillance_IM**
   - **LogserverV2**
3. Stop the VMS services, see Start or stop a VMS service.
4. Stop the IIS application pools for the VMS, see Start or stop an Internet Information Services (IIS) application pool.
5. Change the identity of an IIS application pool, see Change the identity of an IIS application pool for XProtect.
6. Change the Windows service account, see Change the service account for a Windows service.
7. Register the management server from the Server Configurator.

   The registration triggers a restart of the server services. Once the services start, a confirmation appears, stating that registration on the management server has succeeded. If the services did not start automatically, you can start them from the Windows Services Manager, see Start or stop a VMS service.

# Start or stop a VMS service

The VMS services use the service accounts to register and communicate with the other VMS components. To start or stop a VMS service:

1. Open the Start menu, and enter services.msc to open **Services**.
2. Right-click a **Milestone XProtect** service and select **Start** or **Stop**.

   The VMS services for XProtect Management Server Failover are:
   - The **Milestone XProtect Management Server** service
   - The **Milestone XProtect Log Server** service
   - The **Milestone XProtect Event Server** service
   - The **Milestone XProtect Data Collector** service
   - (Optional) The **Milestone XProtect Recording Server** service

# Start or stop an Internet Information Services (IIS) application pool

The management server communicates with the remote servers through IIS.

To start or stop an IIS application pool:

1. Open the Start menu, and enter inetmgrc to open **Internet Information Services (IIS) Manager**.
2. On the **Connections** pane, double-click on your server to expand the list menu, then select **Application Pools**.

3. Right-click an application pool that starts with **VideoOS** and select **Start** or **Stop**.

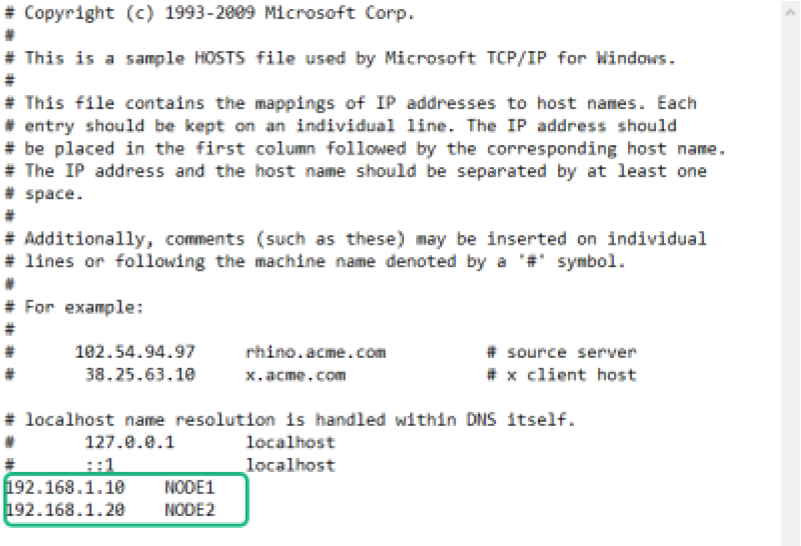
4. Repeat step 3 for all **VideoOS** application pools.

# Map the host names of the nodes

If you do not have a DNS server to resolve the host names of Node 1 and Node 2, you must map their IP address to host names manually.

1. On Node 1, go to `C:\Windows\System32\drivers\etc` and open the **hosts** file as administrator with a text editor such as Notepad.

2. Under the section `localhost name resolution is handled within DNS itself`, specify the IP address of Node 1 and its host name. On a new line, add the IP address of Node 2 and its host name.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.168.1.10    NODE1
192.168.1.20    NODE2
```

Repeat the same steps on Node 2.

# Change the identity of an IIS application pool for XProtect

To change the identity of an IIS application pool:

1. Open the Start menu, and enter inetmgrc to open **Internet Information Services (IIS) Manager**.

2. On the **Connections** pane, double-click your server to expand the list menu, then select **Application Pools**.

3. Right-click an application pool that starts with **VideoOS** and select **Advanced settings...**

4. Under **Process Model**, change the **Identity** with the selected Windows account.

5. Repeat steps 3-4 for all **VideoOS** application pools.

6. Start all **VideoOS** application pools.

# Change the service account for a Windows service

To change the service account for a Windows service:

1. Open the Start menu, and enter services.msc to open **Services**.

2. Right-click on the service you want to change the service account for and select **Properties**. The Windows services used by XProtect are:
    - The **Milestone XProtect Management Server** service
    - The **Milestone XProtect Log Server** service
    - The **Milestone XProtect Event Server** service
    - The **Milestone XProtect Data Collector** service
3. On the **Log On** tab, select **This account** and specify or browse for your account.
4. Enter the password and select **OK** to save your changes.

# Install XProtect Management Server Failover

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, you must install the XProtect Management Server Failover component on two separate computers, referred to as nodes.

**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.

**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.

# Configuring the failover cluster without database replication

You exclude the SQL Server databases from data replication by connecting to a SQL Server instance hosted on your network.

## SQL Server prerequisites

| Prerequisite | Description |
|---|---|
| Permissions for the SQL Server user | In Microsoft SQL Server Management Studio, add a Windows user to the **public** role and map the user to the  **db_owner** database role for the following databases:<br>• **Surveillance**<br>• **Surveillance_IDP**<br>• **Surveillance_IM**<br>• **LogserverV2** |
| Connection | Verify that the VMS installations on both nodes:<br>• Are connected to the external SQL Server instance.<br>• The VideoOS IIS application pools on Node 1 are running.<br>• The VMS services on Node 1 are running. |
| Service account | Make sure that the Management Server service on both nodes runs under the Windows user you added on the SQL Server computer.<br>If your SQL Server runs under a different user, you can change the account that runs the Management Server service. See Changing the service account that runs a VMS service. |

To configure the failover cluster, you switch between Node 1 and Node 2 in the following order:

Step I: Start the configuration on Node 2.

Step II: Continue the configuration on Node 1. Once done, move to Node 2.

Step III: Finish the configuration on Node 2

⚠ During the configuration, the XProtect VMS users won't be able to log in to any XProtect client during configuration.

# Step I: Start the configuration on Node 2

After you have checked the prerequisites and prepared your system, you can start with the configuration of the failover cluster without data replication.

If you have two or more running management servers that are connected to the same SQL Server databases, your data might be corrupted.

To avoid potential database conflicts, before you start the configuration, go to Node 1 and:

- Stop all VMS services. You can start the services after you have configured the failover cluster. See Start or stop a VMS service.
- Stop all Internet Information Services (IIS) application pools for the VMS. You can start the application pools after you have configured the failover cluster. See Start or stop an Internet Information Services (IIS) application pool.

On Node 2:

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.**
3. Make sure that you have installed the required system components and scheduled downtime.
4. On the **Select connection protocol** page, select a protocol for communication with the failover web console:
   - To use a system-generared certificate, select **HTTPS** to secure your connection. During configuration, the wizard takes the first DNS entry from your DNS servers list to generate the certificate. If the DNS server is down, the failover cluster configuration might fail.
   - If you want to use a custom certificate for encryption or you do not want to encrypt your connection, select **HTTP**.
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 Node 1.

The wizard prepares the node and informs when successfully completed.

(For HTTPS only) Save the security code. To establish a secure connection between the nodes, you must specify the security code on the Node 1.

You are now ready to continue on Node 1. See Step II: Continue the configuration on Node 1.

## Step II: Continue the configuration on Node 1

After you have prepared Node 2, you are ready to configure Node 1.

Before you run the failover configuration wizard, start the following IIS application pools and VMS services on Node 1. See Start or stop an Internet Information Services (IIS) application pool and Start or stop a VMS service.

On Node 1:

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**.

   To exclude SQL Server from the failover cluster, select **Use an external SQL Server**.

   > ⚠ If you select to use external SQL Server, XProtect Management Server Failover will not replicate the data on the SQL Server databases. To keep your SQL Server databases safe, you must configure a backup solution yourself.

3. If you have prepared Node 2, select **Confirm** to continue.

4. On the **Select connection protocol** page, select the same connection protocol you selected on Node 2.

5. On the **Connect to the secondary computer** page, specify the required system information.

| Name | Description |
|---|---|
| **Secondary computer's FQDN (recommended), host name, or IPv4 address** | Specify the address of Node 2 depending on your environment:<br>◦ **For AD domains**, specify the Fully Qualified Domain Name (FQDN) of Node 2.<br>◦ **For workgroup environment**, specify the host name (recommended) or IP address of Node 2. |
| **Failover license** | If you have purchased an XProtect Management Server Failover license, you can add it now on this node.<br>⚠ If you do not add a license within three days, the Management Server service will stop.<br>⚠ You must add the same XProtect Management Server Failover license on both nodes. |
| **Virtual IPv4 address** | The remote servers will communicate with this IPv4 address instead of the management server address. Specify an available IPv4 address in your network to replace the actual address of the management server. |
| **Security code** (for HTTPS only) | To establish a secure connection between the nodes, specify the security code you got from Node 2. |

If you have not added a license, a message informs you that the management server becomes unavailable after three days.

6. On the **Set a password for authentication** page, enter the password that you set on Node 2 in step 5.

   The wizard configures the failover cluster. The wizard configures the failover cluster. The time may vary depending on the system load, connection speed and the size of the SQL Server databases that are replicated.

7. (For HTTPS only) On the **Select destination folder for the server certificate** page, specify a destination folder. If you do not select a destination folder, the wizard will export the certificate to `C:\Users\{user}\Documents`.

   The wizard saves the certificate to the selected folder.

When the configuration of Node 1 succeeds, go to Node 2 to finish the configuration. See Step III: Finish the configuration on Node 2.

## Step III: Finish the configuration on Node 2

After you have prepared Node 2 and configured Node 1, go to Node 2 to finish the configuration:

1. Confirm that you have completed the configuration on Node 1.

2. On the **Add a failover license on this computer** page, you can add your failover license.

3. When the configuration is successful, the failover web console opens automatically on Node 2. Node 1 comes into the PRIM state, and Node 2 comes into the SECOND state.

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

You can enforce a node failover to ensure that the setup is correct. You can then swap the nodes again to revert to the original state of the nodes.

To continue with the setup, see After you configure the failover cluster .

If the configuration fails, remove the current configuration and start the process again, see Remove the existing failover cluster configuration.

# Configuring the failover cluster with database replication

If you have installed the Management Server component with SQL Server on both nodes, you can use data replication of the SQL Server databases.

## SQL Server prerequisites

| **Prerequisite** | **Description** |
|---|---|
| Database backup | Back up any existing databases to avoid loss of data.<br>During the failover cluster configuration, the wizard replicates the SQL Server databases on Node 1 to the SQL Server databases on Node 2. All data on the SQL Server databases on Node 2 is overwritten. |
| SQL Server service account | The SQL Server service must run under the same user account as the XProtect services.<br>To change a service account for the XProtect VMS, see Changing the service account that runs a VMS service |
| Database location | You can use the default or custom location for the VMS databases data and log files.<br>The default configuration is as follows:<br>• The VMS databases data and log files are stored in the **DATA** folder.<br>• The SQL Server error logs, trace log files, and log events are stored in the **Log** folder.<br>• The **DATA** and **Log** folders belong to the same parent folder.<br>The default locations are:<br>• `C:\Program Files\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\DATA`<br>• `C:\Program Files\Microsoft SQL Server\MSSQL{nn}.MSSQLSERVER\MSSQL\Log`<br>{nn} is the version number.<br>To use custom locations, place the data (.mdf) and log (.ldf) files in a folder called **DATA**. Then, create an empty **Log** folder in the same parent folder. |

| Prerequisite | Description |
|---|---|
| Virus scanning exclusions | In your antivirus program, exclude the locations of the **DATA** and **Log** folders from virus scanning. |
| Instance name | Verify that the instance name of your SQL Server is **MSSQLSERVER**. See View the SQL Server instance name. |

To configure the failover cluster, you switch between Node 1 and Node 2 in the following order:

Step I: Start the configuration on Node 2. Once you prepare Node 2, move to Node 1.

Step II: Continue the configuration on Node 1. Once done, move to Node 2.

Step III: Finish the configuration on Node 2

⚠ During the configuration, the XProtect VMS users won't be able to log in to any XProtect client during configuration.

## Step I: Start the configuration on Node 2

After you have checked the prerequisites and prepared your system, you can start with the configuration of the failover cluster with data replication.

On Node 2:

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.**

3. Make sure that you have installed the required system components and scheduled downtime.

4. On the **Select connection protocol** page, select a protocol for communication with the failover web console:

   - To use a system-generared certificate, select **HTTPS** to secure your connection. During configuration, the wizard takes the first DNS entry from your DNS servers list to generate the certificate. If the DNS server is down, the failover cluster configuration might fail.

   - If you want to use a custom certificate for encryption or you do not want to encrypt your connection, select **HTTP**.

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 Node 1.

The wizard prepares the node and informs when successfully completed.

(For HTTPS only) Save the security code. To establish a secure connection between the nodes, you must specify the security code on the Node 1.

You are now ready to continue on Node 1. See Step II: Continue the configuration on Node 1.

## Step II: Continue the configuration on Node 1

After you have prepared Node 1, you are ready to configure Node 2.

On Node 2:

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**.
3. If you have prepared Node 2, select **Confirm** to continue.
4. On the **Select connection protocol** page, select the same connection protocol you selected on Node 2.
5. On the **Connect to the secondary computer** page, specify the required system information.

| Name | Description |
|---|---|
| **Secondary computer's FQDN (recommended), host name, or IPv4 address** | Specify the address of Node 2 depending on your environment:<br>◦ **For AD domains**, specify the Fully Qualified Domain Name (FQDN) of Node 2.<br>◦ **For workgroup environment**, specify the host name (recommended) or IP address of Node 2. |
| **Failover license** | If you have purchased an XProtect Management Server Failover license, you can add it now on this node.<br>⚠ If you do not add a license within three days, the Management Server service will stop.<br>⚠ You must add the same XProtect Management Server Failover license on both nodes. |
| **Virtual IPv4 address** | The remote servers will communicate with this IPv4 address instead of the management server address. Specify an available IPv4 address in your network to replace the actual address of the management server. |
| **Security code** (for HTTPS only) | To establish a secure connection between the nodes, specify the security code you got from Node 2. |

   If you have not added a license, a message informs you that the management server becomes unavailable after three days.

6. On the **Set a password for authentication** page, enter the password that you set on Node 2 in step 5.

   The wizard configures the failover cluster. The wizard configures the failover cluster. The time may vary depending on the system load, connection speed and the size of the SQL Server databases that are replicated.

7. (For HTTPS only) On the **Select destination folder for the server certificate** page, specify a destination folder. If you do not select a destination folder, the wizard will export the certificate to `C:\Users\{user}\Documents`.

   The wizard saves the certificate to the selected folder.

When the configuration of Node 1 succeeds, go to Node 2 to finish the configuration. See Step III: Finish the configuration on Node 2.

## Step III: Finish the configuration on Node 2

After you have prepared Node 2 and configured Node 1, go to Node 2 to finish the configuration:

1. Confirm that you have completed the configuration on Node 1.

2. On the **Add a failover license on this computer** page, you can add your failover license.

3. When the configuration is successful, the failover web console opens automatically on Node 2. Node 1 comes into the PRIM state, and Node 2 comes into the SECOND state.

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

You can enforce a node failover to ensure that the setup is correct. You can then swap the nodes again to revert to the original state of the nodes.

To continue with the setup, see After you configure the failover cluster .

If the configuration fails, remove the current configuration and start the process again, see Remove the existing failover cluster configuration.

# After you configure the failover cluster

To make sure your VMS system can connect to the running management server seamlessly, you must make some addition configuration steps.

**Connection**

The remote servers and clients use the management server address to connect to the VMS system. To update the management server address on all components, you must:

- Connect the server VMS components to the system.

- Connect to the VMS system from the clients.

**Encryption**

Depending on the certificate you want to use to encrypt the connection to the failover web console, you must do one of the following actions:

- Install the failover certificate that the wizard generated during the configuration of the failover cluster. See Install the server certificate on a computer.

- Install your custom certificate. See Use custom server certificates for communication with the failover web console.

# Connect the server VMS components to the system

To connect a server component to the failover cluster, you must register the following server components with the cluster address.

- Recording Server service

- Mobile Server service

- DLNA Server service

- Milestone Open Network Bridge

- API Gateway

**Change the management server address on the recording server**

1. On the recording server computer, right-click the server manager tray icon and click **Server Configurator**.
2. In Server Configurator, click **Registering servers**.
3. Specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **Register**.

If the change is successful, a confirmation window appears.

**Change the management server address on the mobile server**

1. On the mobile server computer, right-click the Mobile Server Manager tray icon and click **Management server address**.
2. Specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **OK**.

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

**Change the management server address on the DLNA server**

1. On the DLNA Server computer, right-click the XProtect DLNA Server Manager tray icon and click **Management server address**.
2. Specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **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 that runs Milestone Open Network Bridge, right-click the Milestone ONVIF Bridge tray icon and click **Configuration**.
2. On the **Surveillance Server Credentials** page, in the **Management server** field, specify the cluster address and the selected protocol (HTTPS or HTTPS) and click **OK**.

If the change is successful, a confirmation window appears.

# Connect to the VMS system from the clients

Replace the hostname of the management server with the cluster address when logging in from the following clients:

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

You replace the hostname on the clients mentioned above to ensure your users always connect to the running management server and your system remains operational when a failure on the management server host occurs.

# Install the 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 Node 1 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 Node 1 and Node 2, 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.

# Use custom server certificates for communication with the failover web console

When setting up secure communication between the nodes in your cluster, each node will need a certificate that proves its identity. These certificates are created using PKI (Public Key Infrastructure), a system that uses public and private keys to establish trust and security.

⚠ Without certificates that are trusted by both nodes, your connection is not secure.

During configuration, the wizard generates a server certificate that encrypts the communication with the failover web console. If you want to encrypt the connection to the failover web console with a custom certificate (your enterprise PKI or commercial PKI), you can do that after you have configured the failover cluster with HTTP.

**Requirements**

You need the following files:

| File | Description |
|---|---|
| Server certificates | You need a server certificate for each node in the .crt format signed by the root or intermediate CA certificate. Make sure each client certificate contains the following Subject Alternative Name (SAN) details:<br>• The hostnames and FQDNs of both nodes as **DNS** values.<br>• The virtual IP of the failover cluster as an **IP address** value. |
| Private keys | You need the private unencrypted keys of the server certificates. |
| Client certificates | Client certificates signed by the same root or intermediate CA that you used to sign the server certificates. You can use client certificates in the .pfx or .p12 format that are issued to a specific Windows user. Make sure the client certificates have the following properties:<br>• The **Key Usage** field is set to **Client Authentication**.<br>• The name of the Windows user in the **Common Name** subfield under the **Subject** field. |
| A CA certificate | You need the root or intermediate CA certificate for signing the server and client certificates. It must be an X.509 certificate in the .pem format. |

**Install the CA certificates**

You need a CA certificate that signs the server certificates.

1. On Node 1, rename the CA certificate for the servers to `cacert.crt`.
2. Rename the CA certificate for the clients to `clcacert.crt`.
3. Copy the `cacert.crt` certificate file and paste it to `C:\Program Files\Milestone\XProtect Management Server Failover\safekit\conf`.
4. Copy the `clcacert.crt` certificate file and paste it to `C:\Program Files\Milestone\XProtect Management Server Failover\safekit\web\conf`.
5. Repeat steps 1-4 on Node 2.

**Install the server certificates**

To make sure the failover web console knows which certificate to use, you must copy the certificate and its private key to the configuration folder:

1. On Node 1, rename the server certificate to `server.crt` and the private key file to `server.key`.
2. Copy the certificate and key files and paste them to `C:\Program Files\Milestone\XProtect Management Server Failover\safekit\conf`
3. Repeat step 1 and 2 on Node 2.

**Install the client certificates**

To connect to the failover console from a computer that is not part of the failover cluster, you need a client certificate.

1. Double-click on the certificate to start the installation wizard.
2. Select to import the certificate in the store of the **Current User** and click **Next**.
3. Specify the password for the certificate and click **Next**.
4. Select Place all certificates in the following store and click **Browse**. Then, select the **Personal** store.
5. On the **Completing the Certificate Import Wizard** dialog, select **Finish**.
6. Verify that the server certificate is listed in the center view of the **Personal** subtree.

After you have completed these steps, try logging in to the failover web console.

If you are not able to log in to the console, verify that you have added the necessary exceptions to your Windows Firewall. See Ports used by XProtect Management Server Failover services and modules.

# Configure XProtect Management Server Failover (wizard)

When you select **Configure XProtect Management Server Failover** 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.

## 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.

## Select the step in your configuration flow

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

## Manage your configuration

From this page you can:

- **Apply failover license**, see Add a license for XProtect Management Server Failover.
- **Download server certificate on your computer**, see Download the server certificate to access the failover web console.
- **Change current password for authentication**, see Change the password for authentication.
- **Remove existing configuration**, see Remove the existing failover cluster configuration.

# 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 XProtect Management Server Failover (wizard).
- After the failover cluster configuration, from the **Manage your configuration** page.

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

You must add the same license on both nodes.

1. On Node 1, in the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. Select **Apply failover license** and select **Continue**.
3. 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.

4. Repeat steps 1 to 4 on Node 2.

# Download the server certificate to access the failover web console

To establish a secure connection with the failover web console, you need a certificate that your browser trusts. To learn more about the server certificate, see Server certificate for the failover web console.

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

> ⚠ If you have a running recording server on Node 1, you must stop the XProtect Recording Server service on that node until you have completed the steps. Then, you must manually start the service. See Start or stop a VMS service.

> You can only download the server certificate from Node 1.

To download the server certificate 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 **Download server certificate on your computer** and then select **Continue**.

3. On the **Select a destination folder for the server certificate** page, select a destination folder. If you do not select a destination folder, the wizard will export the certificate to `C:\Users\{user}\Documents`.

4. Select **Continue**. The wizard downloads the server certificate to the selected destination.

You can now install the server certificate, see Install the server certificate on a computer.

# Remove the existing failover cluster configuration

Remove your failover cluster configuration when you make changes in your VMS configuration, for example when you change the location of a SQL Server database or the system configuration password.

To remove the failover cluster configuration successfully and make sure the work of the VMS users is restored:

- Use a Windows user that has administrative permissions for XProtect.

- Replace the virtual IP address with the address of the running management server on all clients and remote servers.

- If the XProtect Recording Server or XProtect Failover Recording Server services run on any of the nodes using port 9001, you must stop the service on that node.

- If you use external SQL Server and want to remove your configuration, see Removing the failover cluster configuration when connected to an external SQL Server instance.

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

To remove the existing failover cluster configuration:

1. On Node 2, 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. Wait for the Management Server service to start.

> (When in a workgroup environment) If the Management Server service does not start automatically, register the management server with the local address from the management server's Server Configurator.

5. Repeat steps 1-4 on Node 1.

# Removing the failover cluster configuration when connected to an external SQL Server instance

To avoid any potential issues with your external SQL Server, you must take extra steps when you remove the existing failover configuration:

1. Backup your existing SQL Server.
2. Stop Node 1 and Node 2 from the failover web console. See Start or stop a node
3. Remove the existing failover cluster configuration from Node 2. See Remove the existing failover cluster configuration.
4. Stop the VMS services on Node 2 or change the address of SQL Server. See Start or stop a VMS service.
5. Remove the existing failover cluster configuration from Node 1. See Remove the existing failover cluster configuration.

# 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:

1. On Node 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 Node 2.

# Uninstall XProtect Management Server Failover

> ⚠ Before you uninstall XProtect Management Server Failover, you must remove the failover management server configuration from both nodes.

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 that can connect to Node 1 and Node 2.

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

- On Node 1 and Node 2, 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 either Node 1 or Node 2.

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.

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

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

# Browser requirements for the failover web console

Use the failover web console to manage the failover cluster. To learn more, see The failover web console .

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**.

# User interface details

The failover web console consists of two main tabs:

## Control

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

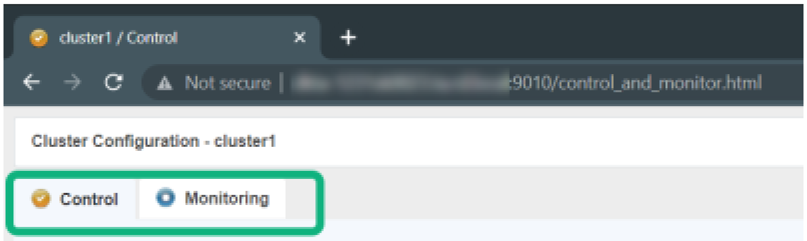
| Tab | Description |
|---|---|
| **Resources** | View the resources status of the module. Place the mouse cursor over the resource name to get the internal name of the resource. |
| **Module Log** | Read the execution log of the module. Set or clear the verbose log's checkbox to display the short log (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

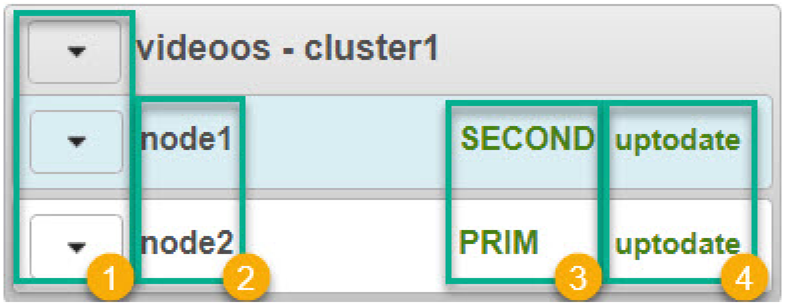
The **Monitoring** tab presents a simplified view of the current state of the module instances.

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


cluster1 / Control
Not secure | [redacted]9010/control_and_monitor.html
Cluster Configuration - cluster1
Control
Monitoring

## Cluster options

The control panel consists of four columns:



videoos - cluster1

node1 SECOND uptodate

node2 PRIM uptodate

**Node actions**

Node actions menu ❶ shows the options to change the state of a node:

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

**Nodes**

Nodes ❷ are the members of the failover cluster. node1 corresponds to the computer you selected as the primary computer, while node2 corresponds to the computer you selected as the secondary computer.

**Node states**

The node state ❸ column shows the current state of a node:

| 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). |

**Color**

A color indicates if the node is available:

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

**Data synchronization status**

The node data synchronization status ❹ column shows the current data synchronization status of a node. The column is not available when the failover cluster is connected to external SQL Server.

| 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

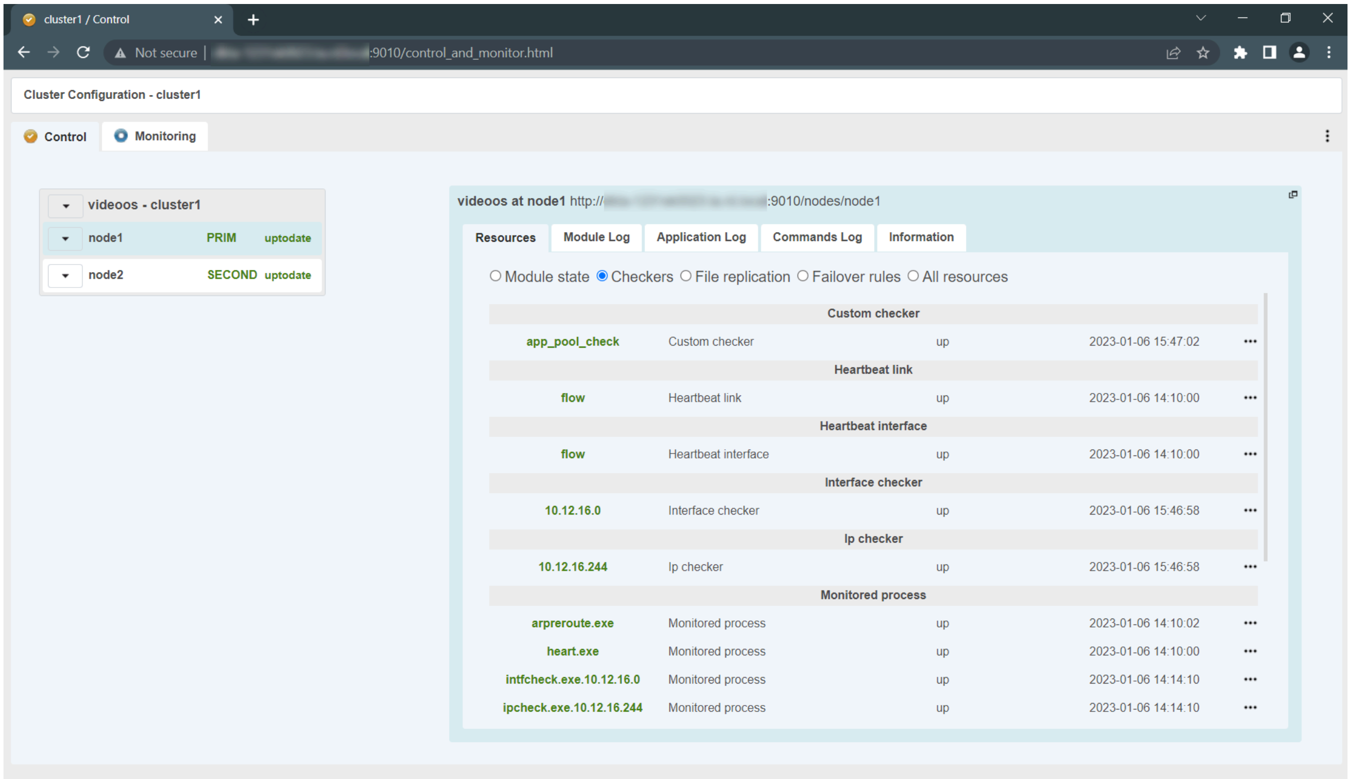
1. On a computer that has access to the failover cluster, open a browser and specify the URL of the failover web console using this format: http://[computername.domainname]:9010 or https://[computername.domainname]:9453.

   The [computername.domainname] is the FQDN of either Node 1 or Node 2.

   > On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

The failover web console opens:



cluster1 / Control

Not secure | [redacted]:9010/control_and_monitor.html

Cluster Configuration - cluster1

Control | Monitoring

videoos - cluster1

| | | |
|---|---|---|
| node1 | PRIM | uptodate |
| node2 | SECOND | uptodate |

videoos at node1 http://[redacted]:9010/nodes/node1

Resources | Module Log | Application Log | Commands Log | Information

○ 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 either Node 1 or Node 2.

   > On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

3. 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.

# 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 either Node 1 or Node 2.

   > On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

3. 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 either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

3. 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, Log Server, Event Server, and the SQL Server services stop, and there is no data replication. Once the roles are swapped, and the services 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 either Node 1 or Node 2.

   On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

3. Select one of the nodes.

4. Select the **Information** tab.

5. 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 either Node 1 or Node 2.

   > On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

3. Select the arrow next to a node and select **Admin** > **Configure boot start**.

4. 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 either Node 1 or Node 2.

   > On Node 1 and Node 2, double-click the icon of the XProtect Management Server Failover web console on your desktop.

2. 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.

3. 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.

4. 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.

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

6. 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. |
| 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. |

# XProtect Management Server Failover upgrade

XProtect Management Server Failover is part of the VMS, so you do not have to download additional files. To upgrade XProtect Management Server Failover, you must upgrade your XProtect VMS. See Upgrade best practices

Before you upgrade, you must remove the existing failover cluster configuration. See Remove the existing failover cluster configuration.

After you upgrade your XProtect VMS, Milestone recommends that you restart the nodes.

If you want to configure the failover cluster afterward, you do not need to add the XProtect Management Server Failover license or install the certificates again.

# XProtect Management Server Failover FAQ

## What happens if a node restarts unexpectedly?

By default, when a node restarts, it 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 determine if a 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 Server databases and the XProtect system configuration.

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

All users of Node 1 and Node 2 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 nodes..

## I have configured the failover cluster and I want to change or add a system configuration password. What should I do?

You must remove the failover cluster configuration on both nodes every time you want to:

- Assign a password
- Change a password

- Remove a password

You must use one system configuration password for the VMS installations on both nodes. Once you have applied your password changes, you can configure the failover cluster again.

## I have an external SQL Server installation connected to the failover cluster. What should I do to update my SQL Server?

Before you start, you must stop the nodes from the failover web console. Once you have updated your external SQL Server, you can start the nodes.

# Troubleshooting XProtect Management Server Failover

System log file

To troubleshoot system errors, you can find the `ManagementServerFailover.log` file on the computer where you have installed XProtect Management Server Failover at `C:\ProgramData\Milestone\XProtect Management Server\Logs`.

**The configuration of the failover cluster has failed**

## Error: <primary machine fqdn> not in server certificate

If you have multiple network adapters on Node 1 or Node 2, the wizard might not resolve their IP addresses or host names.

Solution: Check the address resolution on the nodes using DNS lookups . If the IP address or host name of a node does not resolve as expected, disable all network adapters except the one you use for the failover cluster. You can re-enable the network adapters after you configure the failover cluster.

## Error: Cannot find any service with service name 'MSSQLServer'. Service MSSQLServer was not found on computer.

The failover cluster configuration fails because the SQL Server instance name does not match the name in the configuration files.

Solution: Check the SQL Server instance names on Node 1 and Node 2. See View the SQL Server instance name. If the instance name of your SQL Server is not **MSSQLServer**, you need to update the contents of the configuration files.

> ⚠ Before you make any changes, make a backup of the configuration files.

You can find the configuration files at `C:\Program Files\Milestone\XProtect Management Server Failover\scripts`. You must replace **MSSQLServer** with the name of your SQL Server instance:

- **ConfigureServices.ps1** - you can open the file with a text editor.
- **videoos.safe** - open the file with a file archiver such as 7zip and go to the **bin** folder. Edit the **start_prim.cmd** and **stop_prim.cmd** files.

## Error: StartCertificateServerException occured during RunConfigurationStepsAsync: No connection to certificate authority service.

The system uses port 9001 to connect to the safecaserv service and generate a server certificate. If the port is in use by another service, for example the Recording Server service, the configuration fails..

Solution: Stop all services that use port 9001 on Node 1 and Node 2. Then, configure the failover cluster. The safecaserv service is necessary only during configuration.

## Error: PSSecurityException occured during RunConfigurationStepsAsync: File C:\Program Files\XProtect\XProtect Management Server Failover\scripts\ConfigureNativeFailoverServices.ps1 cannot be loaded because running scripts is disabled on this system

During the configuration of the failover cluster, the wizard runs PowerShell scripts in the background. Your PowerShell execution policy might block the scripts from running.

Solution: Set your PowerShell execution policy to **Unrestricted** and configure the failover cluster again. See Execution Policies.

**The failover cluster does not function properly**

## Failover events are not triggered

When you log in to XProtect clients and services as a basic user, your request goes to the Identity Provider. The Identity Provider keeps the certificate keys that were generated during the initial VMS configuration. To ensure the users have access to the resources you have allowed them to, you must remove the certificate keys before you configure the failover cluster.

Solution: Remove the failover cluster configuration, then set up data protection and remove the existing certificate private keys for the Identity Prover, then configure the failover cluster again. See Update the data protection settings for Identity Provider.

**Cannot remove configuration**

## Error: StartCertificateServerException occured during RunConfigurationStepsAsync: No connection to certificate authority service.

The system uses port 9001 to connect to the safecaserv service to remove the stored server certificate. If the port is in use by another service, for example the Recording Server service, the configuration fails.

Solution: Remove the existing failover cluster configuration, then stop all services that use port 9001 on Node 1 and Node 2. After you have removed the configuration, you can start the services that use port 9001.

**The VMS services do not start after removing the configuration**

## The Management Server and Event Server services will not start (when in a domain environment)

If you have removed the configuration and you have logged in as a standard user in Windows or administrator user that is not added to administrator role in XProtect, the services may fail to register.

Solution: Log in to the computer with an AD user that has administrative permissions in XProtect and remove the configuration.

## The Management Server and Event Server services will not start (when in a workgroup environment)

The services fail to register as the configuration still keeps the virtual IP of the failover cluster.

Solution: From the Server Configurator, register the management server and event server with the address of the management server computer.

## 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/.