

MAKE THE  
WORLD SEE

# Milestone Systems

---

XProtect® Management Server Failover 2023 R2

Administrator manual



# Contents

<b>Copyright, trademarks, and disclaimer</b> .....	<b>4</b>
<b>Overview</b> .....	<b>5</b>
What's new? .....	5
In XProtect Management Server Failover 2023 R2 .....	5
XProtect Management Server Failover .....	5
Compatibility .....	6
Failover steps .....	6
System architecture and XProtect Management Server Failover .....	8
<b>Licensing</b> .....	<b>10</b>
XProtect Management Server Failover licenses .....	10
<b>Requirements and considerations</b> .....	<b>11</b>
Before you configure .....	11
Encrypting the connection to the failover cluster .....	14
The server certificate for the failover web console .....	15
Browser requirements for the failover web console .....	16
Disable Windows Defender Advanced Threat Protection Service .....	16
DNS lookups .....	17
View the instance name of the SQL Server .....	18
Prerequisites for advanced configurations .....	19
Prerequisites for configuring the failover cluster in a workgroup environment .....	19
Prerequisites for using external SQL Server .....	20
Prerequisites for installing a recording server on the primary or secondary computer .....	21
Changing the service account that runs a VMS service .....	22
Start or stop a VMS service .....	23
Start or stop an Internet Information Services (IIS) application pool .....	23
Map the host names of the primary and secondary computers .....	24
Change the identity of an IIS application pool for XProtect .....	24
Change the service account for a Windows service .....	25
<b>Installation</b> .....	<b>26</b>
Install XProtect Management Server Failover on a computer .....	26

<b>Configuration</b>	<b>27</b>
Configure failover management server (wizard)	27
Configure the failover cluster	27
Register remote servers	31
Install the server certificate on a computer	33
<b>Maintenance</b>	<b>34</b>
Add a license for XProtect Management Server Failover	34
Download the server certificate to access the failover web console	34
Remove the existing failover cluster configuration	35
Removing the existing configuration when the failover cluster is connected to external SQL Server	36
Change the password for authentication	36
Uninstall XProtect Management Server Failover	37
The failover web console	37
User interface details	38
Open the failover web console	41
View the status of the nodes	42
Start or stop a node	43
Swap the state of the nodes	43
Identify the host name of a node	44
Change the behavior of a node after restart	44
Create snapshots of a module for support	45
Ports used by XProtect Management Server Failover services and modules	46
<b>Upgrade</b>	<b>48</b>
XProtect Management Server Failover upgrade	48
<b>FAQ</b>	<b>49</b>
XProtect Management Server Failover FAQ	49

## Copyright, trademarks, and disclaimer

Copyright © 2023 Milestone Systems A/S

### Trademarks

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

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

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

### Disclaimer

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

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

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file `3rd_party_software_terms_and_conditions.txt` located in your Milestone system installation folder.

## Overview

### What's new?

#### In XProtect Management Server Failover 2023 R2

##### Recording server:

- You can now install a recording server on the primary and secondary computers. See [Prerequisites for installing a recording server on the primary or secondary computer on page 21](#).

##### External SQL Server:

- You can now connect the primary and secondary computers to your external SQL Server. See [Prerequisites for using external SQL Server on page 20](#).

##### Workgroups:

- You can now configure the failover cluster in a workgroup environment. See [Prerequisites for configuring the failover cluster in a workgroup environment on page 19](#).

##### 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 on page 41](#).

#### 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 on page 27](#).

##### 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 on page 44](#).

## XProtect Management Server Failover

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

XProtect Management Server Failover provides high availability and disaster recovery for the management server. If the management server becomes unavailable on one computer, the other computer takes over running the system components.

You can use the secure real-time replication of the SQL Server databases to ensure there is no loss of data in case of hardware failures.

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

- A server fails – you can run the Management Server service and SQL Server from another computer while you resolve the problems.
- You need to apply system updates and security patches – applying security patches on a standalone management server can be time-consuming, resulting in extended periods of downtime. When you have a failover cluster, you can apply system updates and security patches with minimal downtime.
- You need seamless connection – users get continuous access to live and playback video, and to the system's configuration at all times.

You configure XProtect Management Server Failover between two computers. To make the failover work, you install on each computer:

- XProtect Management Server
- XProtect Event Server service
- XProtect Log Server service
- Microsoft SQL Server (recommended)

## Compatibility

XProtect Management Server Failover is compatible with:

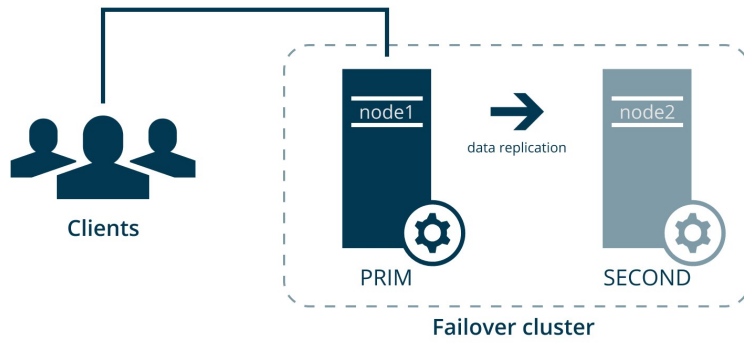
- XProtect Corporate 2022 R1 and later
- XProtect Expert 2022 R1 and later

## Failover steps

You configure the failover cluster on two computers represented as nodes.

The failover steps in a typical scenario are:

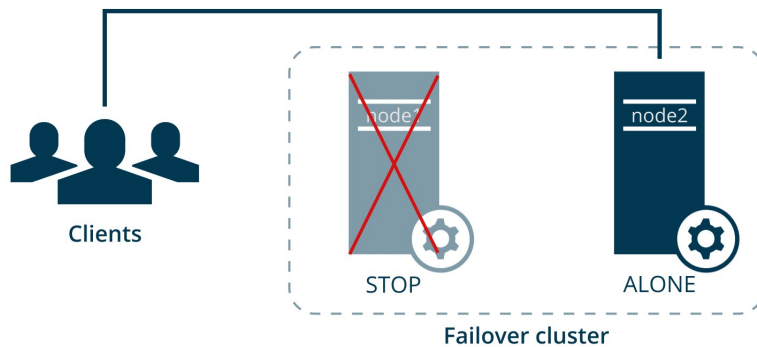
- I. The Management Server, Event Server, Log Server, and SQL Server services run on node1 (in PRIM state). XProtect Management Server Failover replicates the data from these system components on node2 (in SECOND state).



Every second, the computers exchange heartbeats.

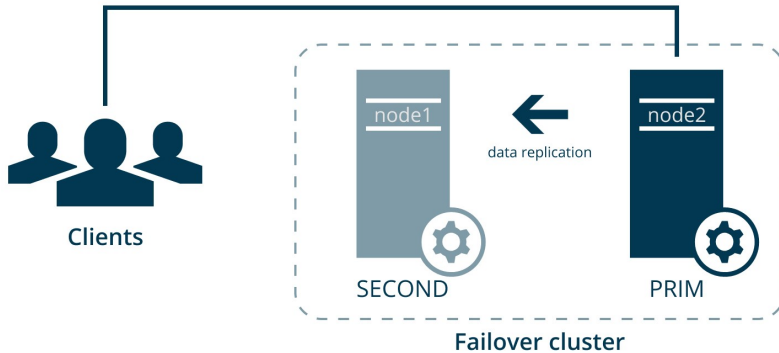
- II. If the management server on node1 becomes unavailable for 30 seconds, node2 takes over.

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



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

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



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

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

## System architecture and XProtect Management Server Failover

Depending on the size of your VMS installation and resources, you can configure XProtect Management Server Failover in the following different ways. To learn more about the standard configuration, see [Failover steps on page 6](#).

### The failover cluster with external SQL Server

If you have a large VMS installation and want to use SQL Server on a separate computer, you can exclude SQL Server from the failover cluster.

In this scenario, the XProtect Management Server Failover solution does not monitor the SQL Server databases. Milestone recommends regular backups of the SQL Server databases as a disaster recovery measure.

See [Prerequisites for using external SQL Server on page 20](#).

### The failover cluster and a recording server

The failover cluster can work with a recording server installed on the primary or secondary computer. You can install a recording server on the primary, secondary, or both computers.

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

See [Prerequisites for installing a recording server on the primary or secondary computer on page 21](#).



### **The failover cluster and a failover recording server**

You can install a failover recording server on the primary or secondary computer in a domain environment.

If you have limited resources, you can use the primary and secondary computers 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 the secondary computer and using the recording server failover on the primary computer.



If you configure a failover recording server on the primary or secondary computer, you must use it in a Hot standby setup.

## Licensing

### XProtect Management Server Failover licenses

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

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



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

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

You can add the license during the failover cluster configuration or afterward. See [Add a license for XProtect Management Server Failover on page 34](#).

## Requirements and considerations

### Before you configure

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

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

#### Network and computer prerequisites

Prerequisite	Description
Operating system	Install two identical operating systems on the primary and secondary computers. To see a list of supported operating systems, go to <a href="https://www.milestonesys.com/systemrequirements/">https://www.milestonesys.com/systemrequirements/</a> .
IP addresses	Assign static IPv4 addresses to the primary and secondary computers. Both computers must belong to the same subnet.
IPv6	XProtect Management Server Failover does not support IPv6 addresses. Do not assign IPv6 addresses to the management server and external SQL Server computers.
Virtual IP	The virtual IP allows the remote servers to connect seamlessly to the running management server. Reserve an unused IPv4 address on the subnet of the primary and secondary computers.
Environment	Configure the failover cluster in an Active Directory (AD) domain or workgroup environment.  <b>Domain</b> Use the same AD domain for the primary and secondary computers.  <b>Workgroup</b> See <a href="#">Prerequisites for configuring the failover cluster in a workgroup environment on page 19</a> .
Time	Synchronize the time and the time zones between the computers.

Prerequisite	Description
ICMP traffic	Allow inbound ICMP traffic through Windows Defender Firewall.
PowerShell execution policy	Set your PowerShell execution policy to <b>Unrestricted</b> . This allows the configuration wizard to run PowerShell scripts on both computers. See <a href="#">about_Execution_Policies</a> .
Windows Defender Advanced Thread Protection Service	You must disable Windows Defender Advanced Thread Protection Service. See <a href="#">Disable Windows Defender Advanced Thread Protection Service on page 16</a> .
IP address and host name resolution	To ensure your computers resolve the IP addresses and host names, you must perform forward and reverse DNS lookup queries in PowerShell. See <a href="#">DNS lookups on page 17</a> .

### SQL Server prerequisites

#### SQL Server is part of the failover cluster

If you want XProtect Management Server Failover to replicate the SQL Server databases and provide failover for SQL Server, you must have SQL Server on the primary and secondary computers.

Prerequisite	Description
SQL Server installation	You need to have one SQL Server on the primary and secondary computers. The installations must be identical.  To see a list of supported SQL Server editions for your VMS product, go to <a href="https://www.milestonesys.com/systemrequirements/">https://www.milestonesys.com/systemrequirements/</a> .
Database backup	Back up any existing databases to avoid loss of data.  During the failover cluster configuration, the wizard replicates the SQL Server databases on the primary computer to the SQL Server databases on the secondary computer. All data on the secondary computer's SQL Server databases is overwritten.

Prerequisite	Description
SQL Server service account	The SQL Server service must run under the same AD user account as the XProtect services. To change a service account for the XProtect VMS, see <a href="#">Changing the service account that runs a VMS service on page 22</a>
Databases	Place the <b>DATA</b> and <b>Log</b> databases in the same folder. See <a href="#">View or Change the Default Locations for Data and Log Files</a> .
Instance name	Verify that the instance name of your SQL Server is <b>MSSQLSERVER</b> . See <a href="#">View the instance name of the SQL Server on page 18</a> .

### You have external SQL Server in your network

You can exclude the SQL Server databases from data replication and use your own SQL Server installation.

You must always have only one running management server that communicates with SQL Server. To avoid potential database conflicts, there are additional steps, see [Prerequisites for using external SQL Server on page 20](#).



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

### VMS prerequisites

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

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.

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

- XProtect Management Server
- XProtect Event Server
- XProtect Log Server
- XProtect Management Server Failover
- XProtect Recording Server (optional), see [Prerequisites for installing a recording server on the primary or secondary computer on page 21](#).



Milestone recommends that you install all other server components not mentioned above on different computers.

Depending on your system configuration, consider the following:

Prerequisite	Description
Encryption	To encrypt the connection to and from the running management server, you must install the CA certificate and an SSL certificate on the primary and secondary computers. See <a href="#">Encrypting the connection to the failover cluster on page 14</a> .
System configuration password	To assign a system configuration password, use the same password for the VMS installations on the primary and secondary computers.
External IDP	To use an external IDP, you must set up data protection. For more information, see <a href="#">Install in a cluster</a> .
API Gateway	To use API Gateway, you must install the component on both computers.

## Encrypting the connection to the failover cluster

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



To learn how to generate and install certificates, see the [XProtect VMS certificates guide](#).

To enable encryption between the management servers and the remote servers, you must install on the primary and secondary computers:

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



Do not enable encryption on the management server if you have already configured the failover cluster.

If you want 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 all client computers.
3. Create an SSL certificate for the failover cluster.
4. Install the SSL certificate for the failover cluster on the primary and secondary computers.
5. Enable encryption for the Management Server service on the primary and secondary computers.
6. Create and install certificates on the remote servers.
7. Enable encryption on the remote servers.

## The 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 on page 37](#).

The wizard downloads a server certificate from a local web service while configuring the failover cluster.

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.



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 on page 33](#).

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, see [Download the server certificate to access the failover web console on page 34](#).

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.

## 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 on page 37](#).

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

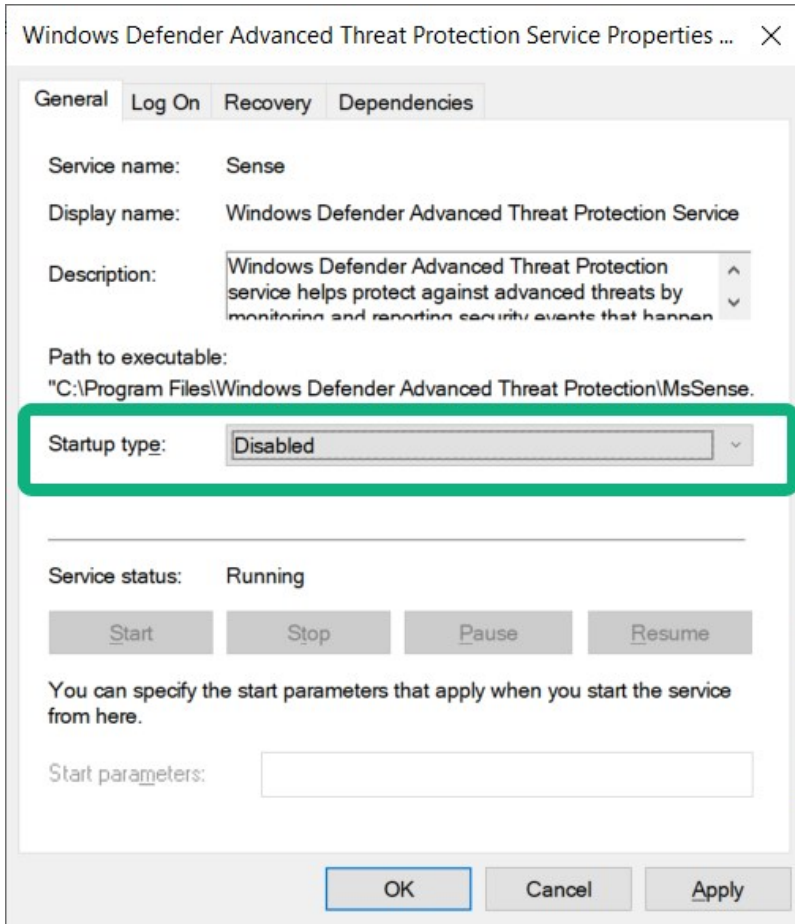
- Network, firewall, and proxy configuration must allow access to the administration network of all the servers that are administered with the web console.
- JavaScript must be available and enabled in the web browser.
- To avoid security popups in Internet Explorer, you may add the addresses of the 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**.

## Disable Windows Defender Advanced Thread Protection Service

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



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



## DNS lookups

For successful failover cluster configuration, Milestone recommends that you run DNS queries in Windows PowerShell:

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

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

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

## View the instance name of the SQL Server

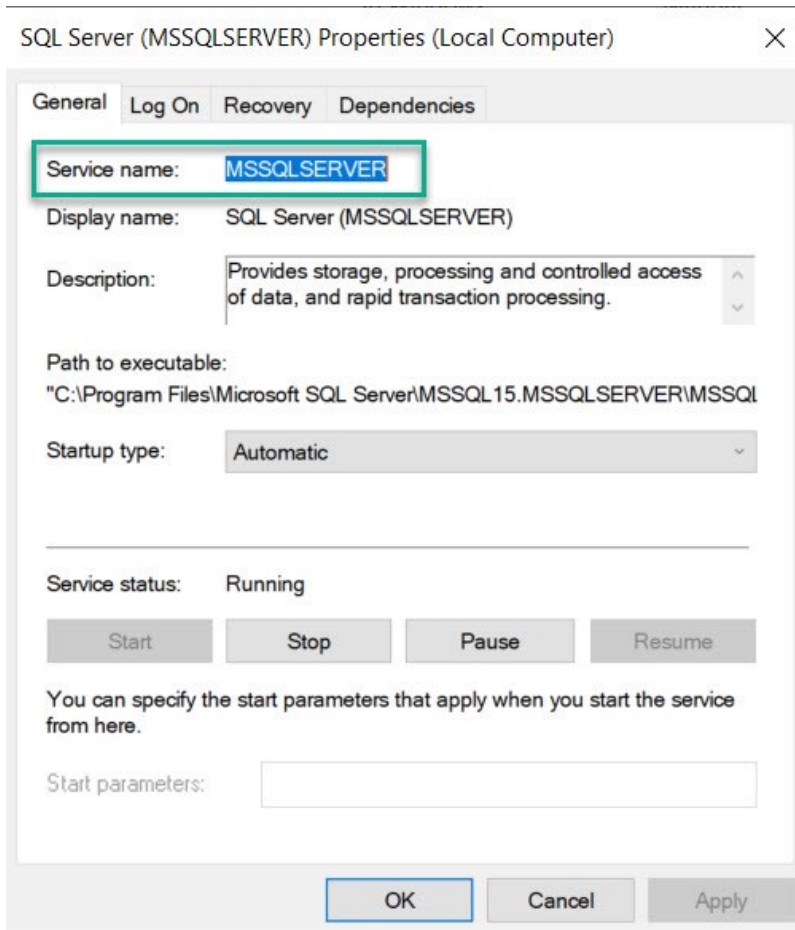
Milestone recommends that you check the SQL Server instance name before you start the configuration of the failover cluster.

XProtect Management Server Failover uses a hardcoded name for the SQL Server instance name **MSSQLSERVER** when the SQL Server is part of the failover cluster.



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

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



If the instance name is not **MSSQLSERVER**, see <https://supportcommunity.milestonesys.com/s/article/Management-Server-Failover-Configuration-fails-if-SQL-is-installed-separately-troubleshooting>.

## Prerequisites for advanced configurations

### Prerequisites for configuring the failover cluster in a workgroup environment

The configuration of the failover cluster in a workgroup environment requires some additional steps. To learn about the general prerequisites for the failover cluster configuration, see [Before you configure on page 11](#).

Prerequisite	Description
Workgroup	Add the primary and secondary computers to the same workgroup.
Host names	(When without DNS server) Map the host names of the primary and secondary computers to IP addresses. See <a href="#">Map the host names of the primary and secondary computers on page 24</a> .
Windows group	You must add a new Windows group in XProtect Management Client on the primary and secondary computers.  Go to <b>Roles</b> and add the BUILTIN/Administrators Windows group to the <b>Administrators</b> 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 the primary and secondary computers.  Go to <b>Roles</b> and add an existing basic user or create a new one.


## Prerequisites for using external SQL Server

The configuration of the failover cluster with external SQL Server requires some additional steps. To learn about the general prerequisites for the failover cluster configuration, see [Before you configure on page 11](#).



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 <b>public</b> role and map the user to the <b>db_owner</b> database role for the following databases: <ul style="list-style-type: none"> <li>• <b>Surveillance: Management and event server</b></li> <li>• <b>Surveillance_IDP: IDP</b></li> <li>• <b>Surveillance_IM: Incident Manager</b></li> </ul>

Prerequisite	Description
	<ul style="list-style-type: none"> <li>• <b>LogserverV2: LogServer</b></li> </ul>
<p>Connection to the SQL Server</p>	<p>Make sure that the VMS installations on the primary and secondary computers are connected to external SQL Server.</p> <p>If you want to change the SQL Server address after installing the VMS, you can do that from Windows registry. For more information, see the Maintenance section in the <a href="#">XProtect VMS administrator manual</a>.</p>
<p>Service account</p>	<p>Make sure that the Management Server service on the primary and secondary computers is running under the Windows user you added on the SQL Server computer.</p> <p>If your SQL Server runs under a different user, you can change the account that runs the Management Server service. See <a href="#">Changing the service account that runs a VMS service on page 22</a>.</p>
<p>Database conflicts</p>	<p>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 conflicts, before you configure the failover cluster, on the primary computer:</p> <ul style="list-style-type: none"> <li>• Stop all VMS services. See <a href="#">Start or stop a VMS service on page 23</a>.</li> <li>• Stop all Internet Information Services (IIS) application pools for the VMS. See <a href="#">Start or stop an Internet Information Services (IIS) application pool on page 23</a>.</li> </ul> <div style="border: 1px solid #ccc; background-color: #fff9e6; padding: 10px; margin-top: 10px;">  <p>You must manually start the XProtect Management Server service and IIS application pools before you start the failover cluster configuration on the primary computer.</p> </div>

## Prerequisites for installing a recording server on the primary or secondary computer

The installation of the recording server on the primary or secondary computer requires additional steps. To learn about the general prerequisites for the failover cluster configuration, see [Before you configure on page 11](#).

You can have a recording server or failover recording server on the primary or secondary computer, or on both.



If you configure a failover recording server on the primary or secondary computer, you must use it in a Hot standby setup.



XProtect Management Server Failover can work with failover recording server in a domain environment only.

To learn more about the configuration of the failover recording server, see the [XProtect VMS administrator manual](#).

Prerequisite	Description
VMS components	<p>Install the XProtect Recording Server component on the primary or secondary computer.</p> <p>You can install the component as part of a new VMS installation or install the component only.</p>
(For encrypted connections only) Certificates	<p>To encrypt the connection between the VMS components, you must install the SSL certificate for the recording server on the recording server computer. Then, enable encryption for the recording server from the recording server's Server Configurator.</p>
(For encrypted connection only) Services	<p>Before you configure the failover cluster, stop the Milestone XProtect Recording Server service. See <a href="#">Start or stop a VMS service on page 23</a>.</p> <p>Once you have configured the failover cluster, start the Recording Server service.</p>

## 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. You must 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: Management and event server**
  - **Surveillance\_IDP: IDP**
  - **Surveillance\_IM: Incident Manager**
  - **LogserverV2: LogServer**
3. Stop the VMS services, see [Start or stop a VMS service on page 23](#).
4. Stop the IIS application pools for the VMS, see [Start or stop an Internet Information Services \(IIS\) application pool on page 23](#).
5. Change the identity of an IIS application pool, see [Change the identity of an IIS application pool for XProtect on page 24](#).
6. Change the service accounts for the VMS, see [Change the service account for a Windows service on page 25](#).
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 on page 23](#).

## 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 **inetmgr** 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 primary and secondary computers

If you do not have a DNS server to resolve the host names of the primary and secondary computers, you must map their IP address to host names manually.

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

 You must run the text editor as administrator.

2. Under the section `localhost` name resolution is handled within DNS itself, specify the IP address of the primary computer and its host name. On a new line, add the IP address of the secondary computer 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
192.168.1.2 PRIMARY-COMPUTER
192.168.1.3 SECONDARY-COMPUTER
```

Repeat the same steps on the secondary computer.

## 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 **inetmgr** 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 **MilestoneXProtectManagement Server** service
  - The **MilestoneXProtectLog Server** service
  - The **MilestoneXProtectEvent Server** service
  - The **MilestoneXProtectData 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.

## Installation

### Install XProtect Management Server Failover on a computer

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



To set up a failover cluster, you must install the XProtect Management Server Failover component on two separate computers.

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

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

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

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

To continue with the cluster configuration, see [Configure the failover cluster on page 27](#)

## Configuration

### Configure failover management server (wizard)

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

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

To learn more about the supported products, see [Compatibility on page 6](#).

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

Make sure that you have installed the XProtect Management Server Failover component on the computer, see [Install XProtect Management Server Failover on a computer on page 26](#).

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

You have started the configuration process, see [Configure the failover cluster on page 27](#).

#### **Manage your configuration**

From this page you can:

- **Apply failover license**, see [Add a license for XProtect Management Server Failover on page 34](#)
- **Download server certificate on your computer**, see [Download the server certificate to access the failover web console on page 34](#)
- **Change current password for authentication**, see [Change the password for authentication on page 36](#)
- **Remove existing configuration**, see [Remove the existing failover cluster configuration on page 35](#)

### Configure the failover cluster

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



If you want the wizard to replicate the SQL Server databases, you must select your current management server as the primary computer. The wizard will replicate the databases from the primary to the secondary computer and overwrite the databases on the secondary computer.

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

- I. [Start the configuration on the secondary computer](#). Once you prepare the secondary computer, move to the primary computer.
- II. [Continue the configuration on the primary computer](#). Once done, move to the secondary computer.
- III. [Finish the configuration on the secondary computer](#).

### Start the configuration on the secondary computer

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



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

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

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



(For HTTPS only) Save the security code. To establish a secure connection between the primary and secondary computers, you must specify the security code on the primary computer.

You are now ready to continue on the primary computer.

### When using external SQL Server

Make sure that the Management Server and the IIS application pools for the VMS on the primary computer are running. See [Start or stop a VMS service on page 23](#) and [Start or stop an Internet Information Services \(IIS\) application pool on page 23](#).

### Continue the configuration on the primary computer

1. In the notification area, right-click the Management Server Manager tray icon and select **Configure failover management server**.
2. In the **Failover management server** wizard, select **Configure the primary computer**.

If you want to exclude the SQL Server from the failover cluster, select **Use an external SQL Server**.





If you select this option, 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.

Then, select **Continue**.

3. If you have prepared the primary computer, select **Confirm** to continue.
4. On the **Select connection protocol** page, select the same connection protocol you selected on the secondary computer. Select **Continue**.

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

Name	Description
<b>Secondary computer's FQDN (recommended), host name, or IPv4 address</b>	Specify the address of the secondary computer. <ul style="list-style-type: none"> <li>• When in an AD domain, you must specify the Fully Qualified Domain Name (FQDN) of the secondary computer.</li> <li>• If it is a workgroup environment, specify the host name (recommended) or IP address of the secondary computer.</li> </ul>
<b>Failover license</b>	If you have purchased an XProtect Management Server Failover license, you can add it now on this computer. If you leave the field blank and continue, you can still configure the failover cluster using a demo license and add a license later. <div data-bbox="549 846 1386 976" style="border: 1px solid #ccc; background-color: #fff9e6; padding: 10px; margin-top: 10px;">  If you do not add a license, the Management Server service will stop after three days.                     </div> <div data-bbox="549 1025 1386 1196" style="border: 1px solid #ccc; background-color: #fff9e6; padding: 10px; margin-top: 10px;">  You must add the same XProtect Management Server Failover license on the primary and secondary computers.                     </div>
<b>Virtual IPv4 address</b>	The remote servers will communicate with this IPv4 address. Specify an available IPv4 address in your network to replace the actual address of the management server.
<b>Security code (for HTTPS only)</b>	Specify the security code from the secondary computer to establish a secure connection between the primary and secondary computers.

Then, select **Continue**. A message informs you that the management server becomes unavailable after three days when using a demo license.

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

The wizard configures the failover cluster. It may take 5 to 10 minutes, depending on the system load and connection speed.

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 certificate is exported to C:\Users\{user}\Documents.

Select **Continue**. The wizard saves the certificate to the selected folder.

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

### Finish the configuration on the secondary computer

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



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

3. When the configuration is successful, the failover web console opens automatically on the secondary computer. The primary computer (node1) comes into the PRIM state, and the secondary computer (node2) comes into the SECOND state.

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

To finish the setup, you must register the remote servers. See [Register remote servers on page 31](#).

#### **If you have selected an HTTPS connection**

Install the server certificate. See [Install the server certificate on a computer on page 33](#).

#### **When using external SQL Server**

Start the XProtect Management Server service and IIS application pools on the primary computer.

#### **If you have installed a recording server on the primary or secondary computer**

Start the Recording Server services on the computer that hosts the recording server.

If the configuration fails, you can remove the current configuration and start the process again, see [Remove the existing failover cluster configuration on page 35](#).

## Register remote servers

A remote server is any server that is not installed on the primary and secondary computers. The virtual IP address reroutes the data packets from the remote servers to the computer that runs the Management Server service, Event Server service, and Log Server service.

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



If you have not registered the remote servers with the virtual IP address of the failover cluster, the communication with the running management server will fail if failover occurs.

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

- [Recording Server service](#)
- [Mobile Server service](#)
- [DLNA Server service](#)
- [Milestone Open Network Bridge](#)
- API Gateway

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

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

There is no host name that is associated with the virtual IP address.

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

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

If the change is successful, a confirmation window appears.

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

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

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



### Change the management server address on the DLNA server

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

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

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

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

If the change is successful, a confirmation window appears.

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

Select **Next** to continue.

4. Select **Place all certificates in the following store** and specify a folder.
5. Select **Browse**, and then **Trusted Root Certification Authorities**.
6. Select **OK** and **Next**.
7. On the **Completing the Certificate Import Wizard** dialog, select **Finish**.

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

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

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

## Maintenance

### Add a license for XProtect Management Server Failover

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

You have the option for when to add the license:

- During the failover cluster configuration (see [Configure failover management server \(wizard\) on page 27](#)).
- After the failover cluster configuration, from the **Manage your configuration** page on the primary and the secondary computer.

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

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

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

### 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 [The server certificate for the failover web console on page 15](#).

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



You can only download the server certificate from the primary computer.

If you have a running recording server on the primary computer, you must stop the XProtect Recording Server service on that computer until you have completed the steps. Then, you must manually start the service. See [Start or stop a VMS service on page 23](#).

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 on page 33](#)

## 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 the SQL database.
- Change the system configuration password.

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



To keep the connection to the management server, replace the virtual IP address with the address of the running management server on all clients and remote servers before you remove the failover cluster configuration.



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

If you use external SQL Server and want to remove your configuration, see [Removing the existing configuration when the failover cluster is connected to external SQL Server on page 36](#).

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

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

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

5. (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.

## Removing the existing configuration when the failover cluster is connected to external SQL Server

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 the PRIM and SECOND nodes from the failover web console. See [Start or stop a node on page 43](#)
3. Remove the existing failover cluster configuration from the secondary computer. See [Remove the existing failover cluster configuration on page 35](#).
4. Stop the VMS services on the secondary computer or change the address of SQL Server. See [Start or stop a VMS service on page 23](#).
5. Remove the existing failover cluster configuration from the primary computer. See [Remove the existing failover cluster configuration on page 35](#).

## Change the password for authentication

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

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

To change the password for authentication on a computer:

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

## Uninstall XProtect Management Server Failover



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

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

## The failover web console

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

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

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

To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).

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

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

- [View the status of the nodes on page 42](#)
- [Swap the state of the nodes on page 43](#)
- [Start or stop a node on page 43](#)
- [Identify the host name of a node on page 44](#)

- [Change the behavior of a node after restart on page 44](#)
- See your license information
- View logs entries

## User interface details

The failover web console consists of two main tabs:

### Control

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

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

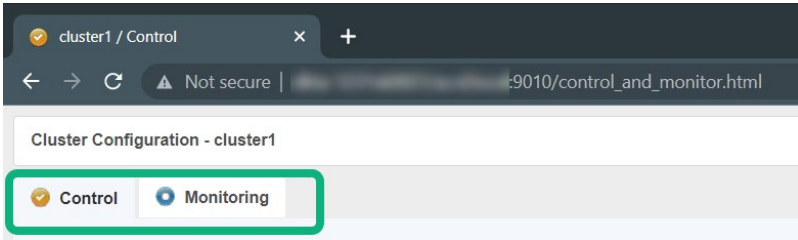


On the **Module Log**, **Application Log**, and **Commands Log** tabs, click on the refresh button to get the last messages or on the save button to save the log locally.

### 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.



### Cluster options

From the left-hand panel, you can:

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

The control panel consists of four columns:



- Node actions menu **1** shows the options to change the state of a node.
- Node1 and node2 **2**: node1 corresponds to the computer you selected as the primary computer, while node2 corresponds to the computer you selected as the secondary computer.
- Node state **3** column shows the current state of a node.
- The node data synchronization status **4** column shows the current data synchronization status of a node. The column is not available when the failover cluster is connected to external SQL Server.

### Node actions

Option	Description
Start	Start a node.

Option	Description
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.

**Node states**

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



### State colors

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

### Node data synchronization statuses

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

## Open the failover web console

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

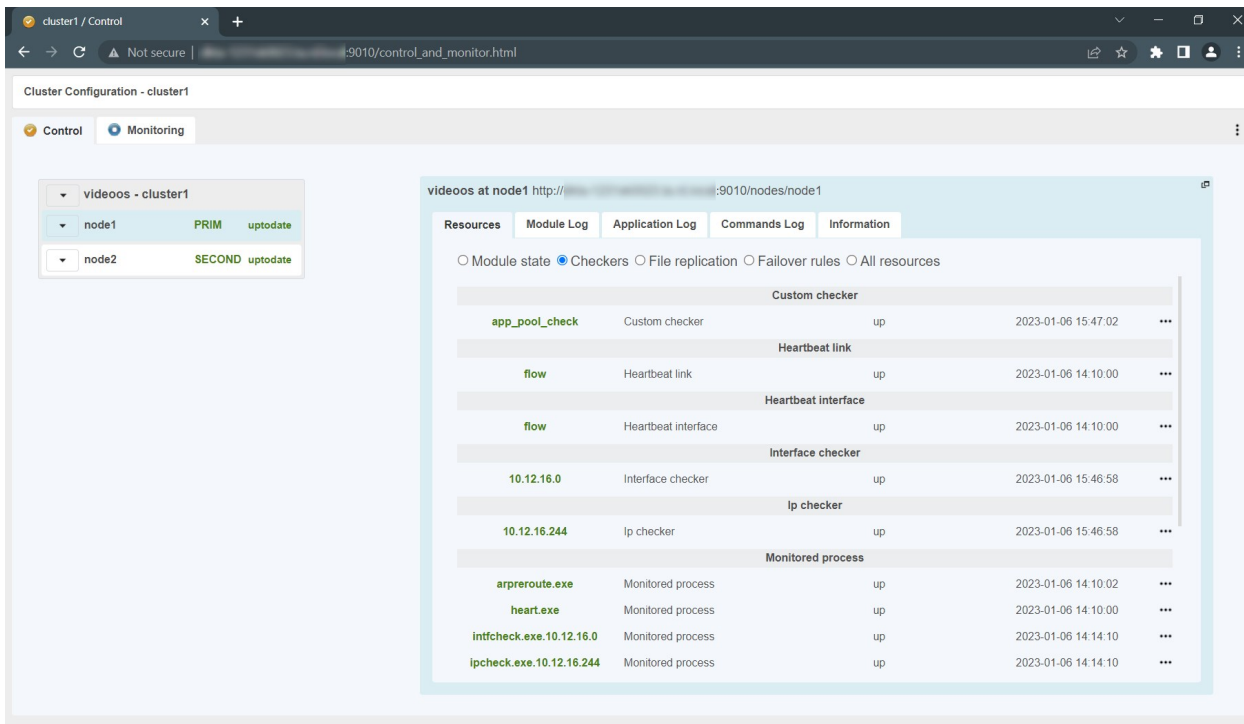
The [computername.domainname] is the FQDN of the primary or the secondary computer.



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).


The failover web console opens:



## View the status of the nodes

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

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



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).
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 on page 38](#).

## Start or stop a node

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

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



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).
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 **videeos-cluster1** to trigger an action on both nodes.

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

## Swap the state of the nodes

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

To swap the state of the nodes:

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

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



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).

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

## Identify the host name of a node

The failover web console represents the primary computer as node1 and the secondary computer as node2. To see the host name that corresponds to a node:

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

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



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).
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 the primary or the secondary computer.



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).
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 the primary or the secondary computer.



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

2. To log in to the failover web console, you must authenticate with the user name **admin** and the password you set during the configuration of the failover cluster. If you do not remember your password, see [Change the password for authentication on page 36](#).
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.
safewebsserver	Local and remote TCP access on port 9010 for the HTTP web console or port 9453 for the HTTPS web console	The safewebsserver service is a standard Apache web service that is mandatory for running the web console, the distributed command-line interface, and the <module> checkers.
safecaserv (optional)	Local and remote access on TCP port 9001	The safecaserv service is a web service for securing the web console with the SafeKit PKI.
safeagent (optional)	Local and remote access on UDP port 3600	The safeagent service for SNMP v2.

### Failover cluster modules

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

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

# Upgrade

## 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 on page 35](#).

After you upgrade your XProtect VMS, Milestone recommends that you restart the primary and secondary computers.

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.



## FAQ

### XProtect Management Server Failover FAQ

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

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

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

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

#### **How can I determine if the primary node has failed?**

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

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

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

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

XProtect Management Server Failover supports all editions of SQL Server.

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

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

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

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

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

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

#### **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 the primary and secondary computers 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 the primary and secondary computers. 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 the 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.



[helpfeedback@milestone.dk](mailto:helpfeedback@milestone.dk)

#### About Milestone

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

