Synology®
White Paper

CMS Failover White Paper

Surveillance Station 8.0.0 and above

Table of Contents

Find your information

Synology publishes a wide range of supporting documentation.

In **Knowledge Base**, you will find useful **Help** and **FAQ** articles, as well as **video tutorials** breaking up processes into handy steps.

In **Synology Documentation**, you can find **User's Guides**, **Solution Guides**, brochures, and **White Papers**. Experienced users and administrators will find answers and guidance in technical **Administrator's Guides** and **Developer Guides**.

Got a problem and unable to find the solution in our official documentation? Search hundreds of answers by users and support staff in **Synology Community** or reach **Synology Support** through the web form, email or telephone.

Introduction

Overview

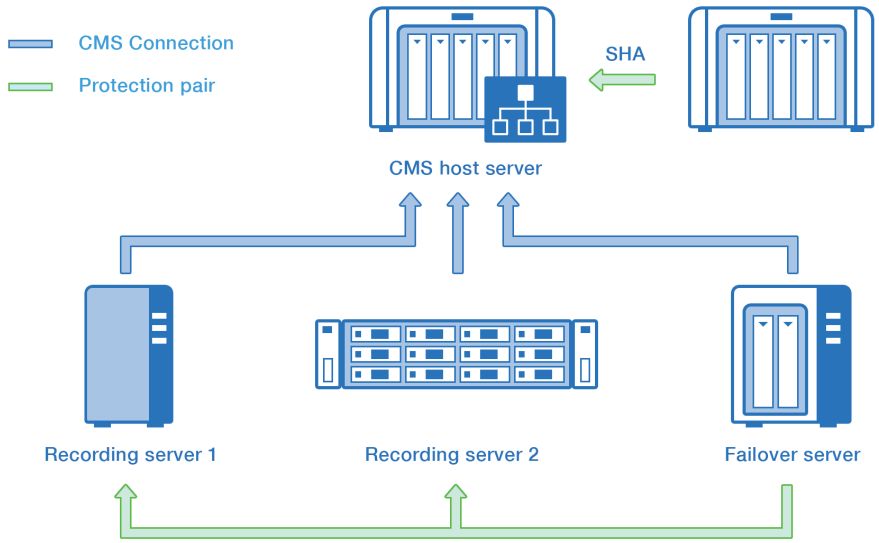
Businesses require 24/7 uninterrupted video surveillance. However, in real situations, unexpected accidents such as equipment or power supply failure or storage device malfunction can still occur and result in the shutdown of surveillance services. To ensure continuous and uninterrupted surveillance service, instant failover protection is essential for any surveillance system.

Surveillance Station provides flexible failover options that allow for automatic or manual transfer of services to the backup system during unexpected situations, reducing the risk of data loss or other damages caused by service downtime. Please find the key features below:

- Many-to-many failover framework maximizes data protection while minimizing hardware costs.
- Provides proactive server abnormality detection with the option to failover automatically or manually. Conditions for triggering the failover can also be customized based on individual needs.
- Detects an extensive range of abnormal status including connection status, storage space status, and package status.
- After failover is activated, servers with normal status can be chosen to replace the original server in the case that the original server is damaged and cannot be repaired.
- The recordings and snapshots taken during the failover period will be synced back to the recording server after it is repaired and running again.

Failover framework

Surveillance Station integrates the role of the failover server into its CMS framework. The purpose is to offer failover service while waiting for the host server to allocate resources and take over the non-functioning recording servers. During the waiting period, the sole purpose of failover servers is to provide failover protection and therefore will not offer any other functions from Surveillance Station.



The failover server setup in the CMS architecture is similar to that of the recording server in which both are added to and managed by the CMS host server. Users can set up pairing relationships between recording servers and failover servers.

Multiple recording servers can be paired with the same failover server, however when failover is required, the recording servers cannot simultaneously transfer services to the same failover server within the same time period. In order to avoid situations where no failover servers are available to take over surveillance services in the event of disaster, it is recommended to increase the number of failover servers that are to be paired with the recording servers. The failover server will be chosen among all other paired failover servers for failover when the supported maximum number of cameras of that failover server matches closest with the number of cameras on the recording server. The flexibility of the failover architecture allows for a balance between installation cost and security.

The CMS host server plays a crucial role and must not depend on a failover server for data protection since the failover will still result in a short period of downtime. However, the host server can still be protected by Synology High Availability (SHA), which offers a one-to-one protection with minimal downtime.

Flexible failover settings

Users can define trigger conditions for the failover server to take over surveillance services upon detecting abnormal behaviors on the CMS host server. The supported trigger conditions include exceeding the tolerated time for connection loss, detecting abnormal status (uninstalling or disabling Surveillance Station) for the Surveillance Station package installed on the recording server, and detecting damaged storage space of the recording server.

In addition to the automatic failover function, users have the flexibility to determine whether or not to manually terminate the failover status once the system detects that the failed recording server has been recovered.

Migration of device licenses

Failover servers within the failover framework do not require purchasing extra licenses. Device license keys can be migrated from the original server to the failover server when executing failover or replacing the original server. Furthermore, the failover function does not require additional expense.

Downtime

During the failover process when services are transferred to the failover server, there will be a short period of downtime. The duration of this period is determined by the number of devices or cameras that need to be transferred and the computing power of the failover server's CPU. If the failover is triggered automatically, additional server disconnection time may occur in order to allow sufficient time for the system to analyze and confirm the abnormal status of the server.

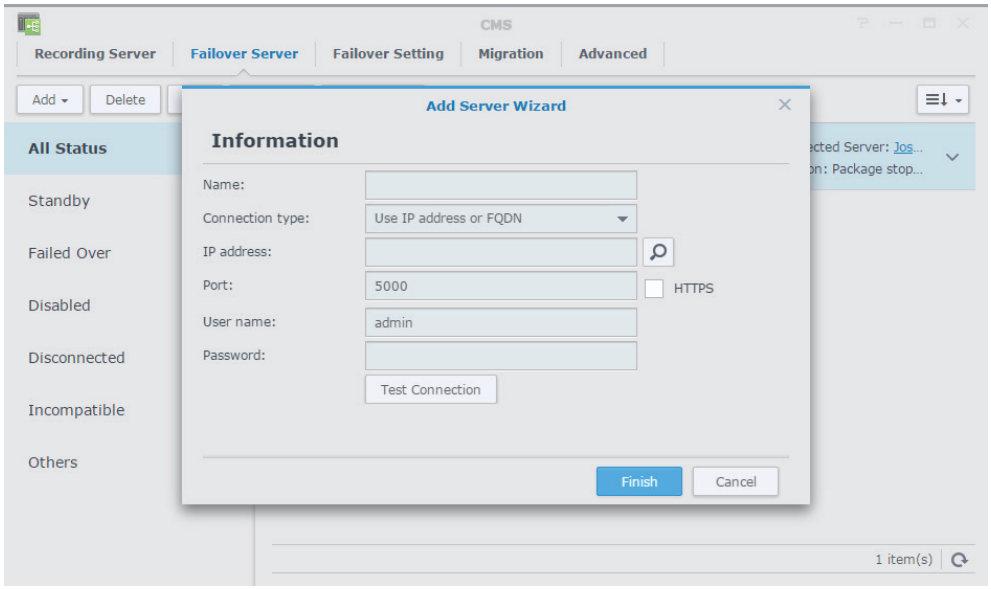
When conducting our experiment, we found that the actual downtime requires about 8.7 seconds, starting from manually activating the failover to the failover server actually taking over. In this experiment, the recording server used is connected with 90 cameras, and DS3018xs (CPU: Intel Xeon D-1508, Memory: 8GB), running DSM 6.1.1-15067, is the NAS model used for the failover server.

Failover setup

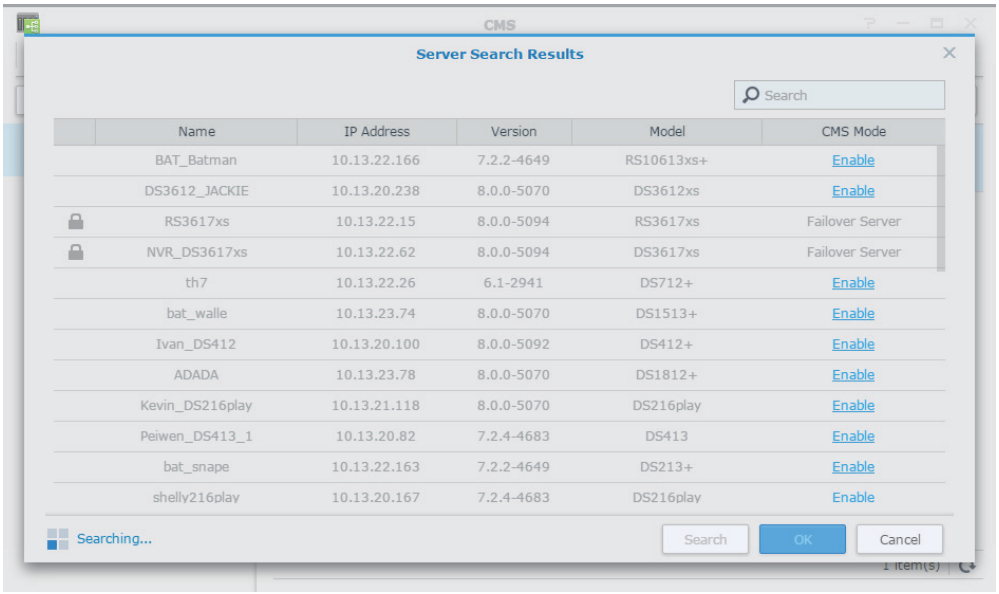
This section explains how to set up failover protection and customize failover settings based on individual demands in a CMS environment.

Adding failover servers

CMS is a Surveillance Station add-on. Go to **Add-ons** and enable the **CMS** add-on for further configuration. A failover server can only be added through a host server, therefore before adding a failover server, launch the **CMS** add-on, and select **Host server mode** under **Pairing Settings** in the **Advanced** tab, then switch to the **Failover Server** tab and click **Add** to add a failover server. Enter the information for the failover server on the wizard. The process of adding failover servers is similar to that of the recording servers, the connection type **QuickConnect** is also supported.



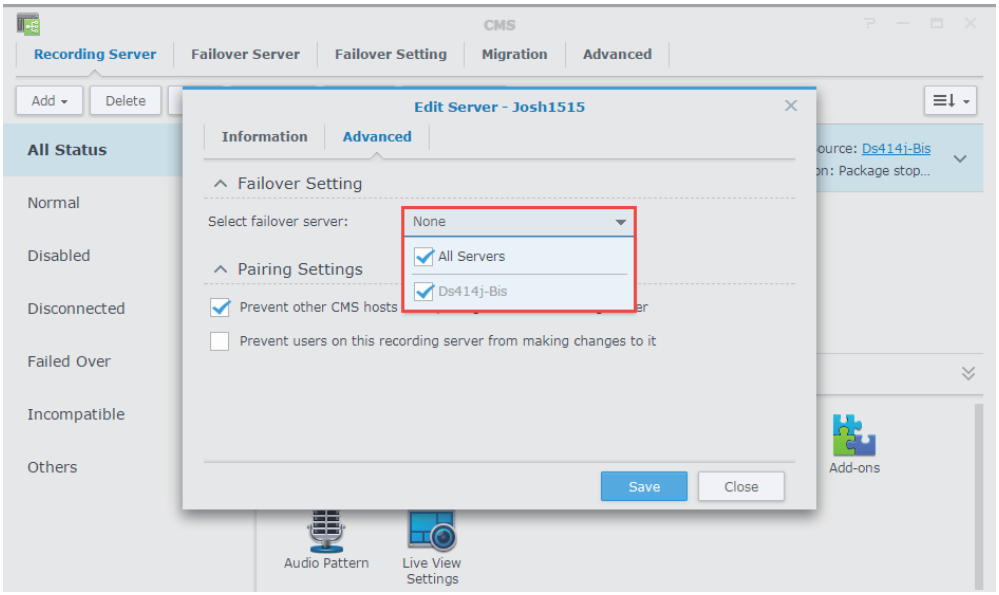
Click the search icon next to **IP address** to search and select an available server. If the CMS service of a server has not been activated, an **Enable** button will be displayed in the corresponding **CMS mode** column. Click the **Enable** button to activate the CMS service of the selected server, assigning it as a failover server. Once assigning a server as a failover server, a warning message will appear to inform users that all data will be erased. Click the button to confirm.



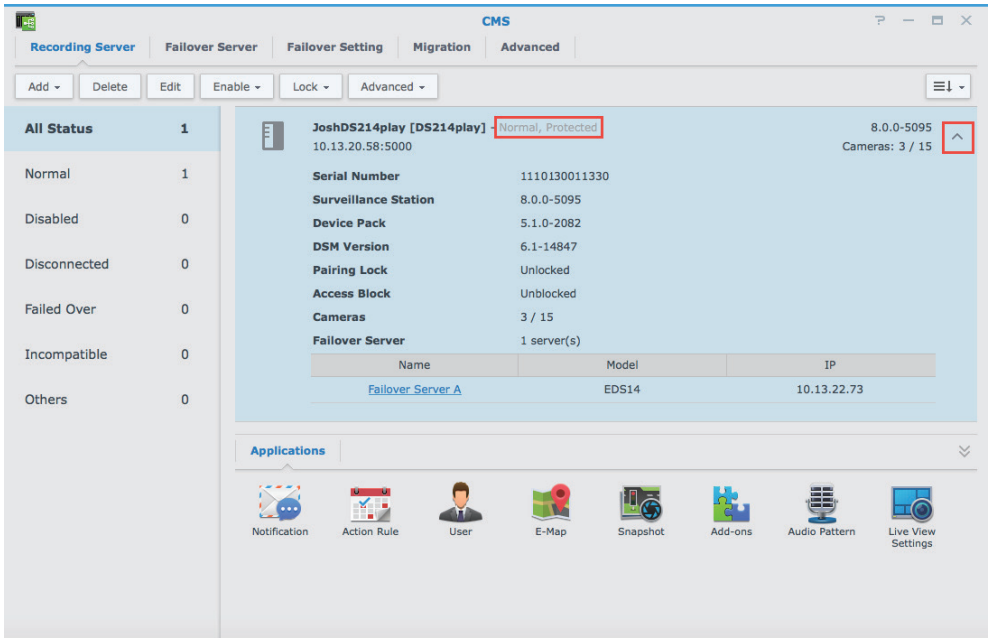
Pairing failover servers with recording servers

After adding the failover server, go to the **Recording Server** tab, select a recording server, and click **Edit**. From the **Select failover server** drop-down menu, choose a failover server for the recording server to be paired with, and click **Save** to complete the pairing process.

To pair all newly added and existing failover servers with the recording server, check the box for **All Servers** in the **Select failover server** drop-down menu, and click **Save**. By checking this box, all failover servers that are added in the future will be automatically paired with this recording server.

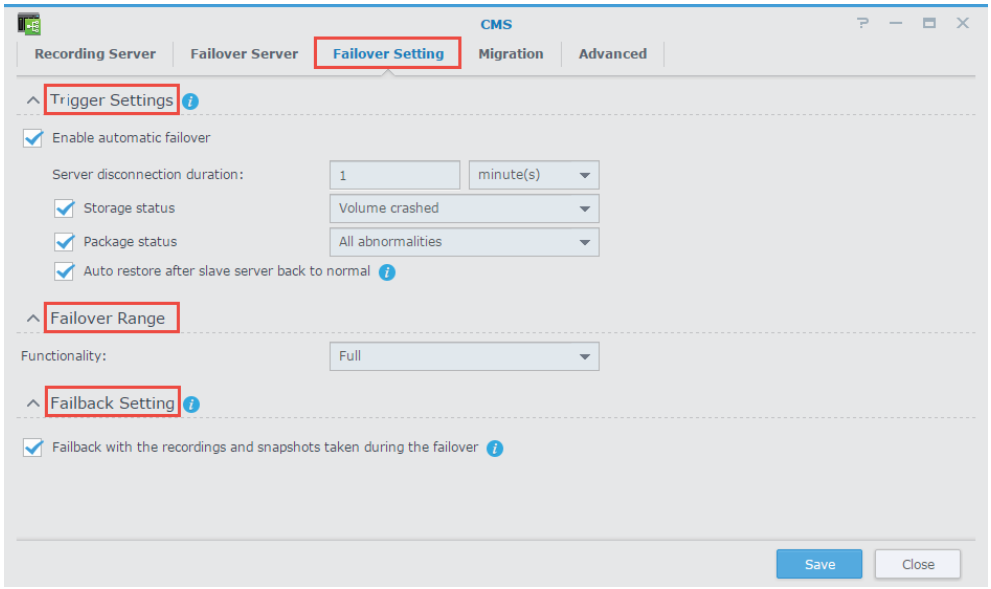


To find more information on the recording server, including which failover server it is paired with, click the expand icon to the right of the recording server in the **Recording Server** tab. Also, there will be a **Protected** label next to the name of the recording server with paired failover server(s).



Failover settings

After adding the failover server and pairing it with the corresponding recording servers, users can define **Trigger Settings**, **Failover Range**, and **Failback Setting** in the **Failover Setting** tab.



Trigger settings

The failover server can be activated manually or automatically. Users can manually activate the failover server in the **Recording Server** tab. In the **Failover Setting** tab, users can enable automatic failover, define trigger conditions, and modify other failover settings. Currently, in **Trigger Settings**, users can determine three different trigger conditions to activate automatic failover:

- **Server disconnection duration**: This condition is enabled by default. Failover will be automatically activated once the host server detects that the time of connection loss of the recording server has exceeded the specified duration (1-60 minutes).
- **Storage status**: When enabling this trigger condition, failover will be automatically activated when the storage space of the recording server has been damaged or degraded to avoid losing important recordings.
- **Package status**: When enabling this trigger condition, failover will be automatically activated when the status of Surveillance Station on the recording server is abnormal (e.g., uninstalling or disabling).

In addition to the three trigger conditions, users can choose to stop failover automatically once the recording server has been recovered. If this option is not enabled, the failover server will continue to take over the services of the recording server even after the recording server has been recovered from its abnormal status. The recording server will remain on standby until the failover service has been manually canceled.

Failover range

In the **Functionality** drop-down menu, users can choose between **Full** and **Full (except recording)** modes. Users who only require live view streaming and do not wish to store recordings on the failover server due to bandwidth limitations or other constraints can choose the **Full (except recording)** mode.

Failback setting

After the recording server is repaired, the settings of the recording server will be restored to the original settings before the malfunction took place. Therefore, any changes made on the failover server during the failover period will not be saved. However, users can choose whether or not to save the recordings or snapshots produced during the failover period and restore them back to the recording server.

Failover operating process

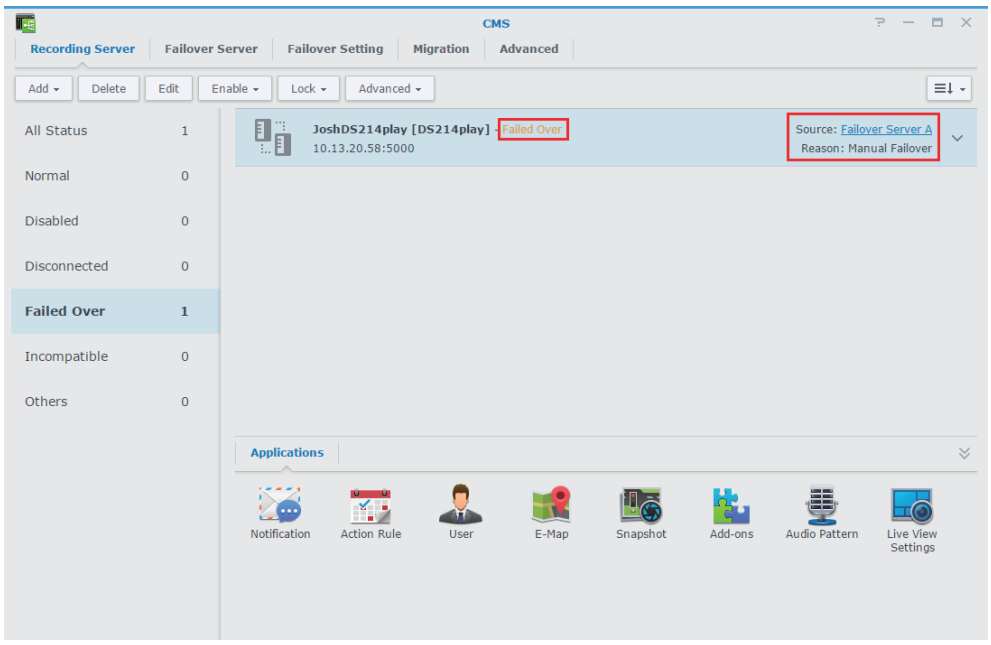
Starting the failover

Failover can be set automatically or manually. Automatic failover will be activated upon the trigger conditions defined in **Failover Setting**. In some circumstances, users may want to manually activate the failover. In the **Recording Server** tab, users can activate failover manually by clicking **Manual Failover** in **Advanced**.

Once failover has been activated, the CMS host server will assign an available failover server from the list of paired failover servers to take over the services of the recording server and start the failover process. Once failover starts, the failover server will apply most of the settings from the original recording server to ensure the failover server operates the same way as the original recording server. Settings from the recording server that will be applied include the following: IP Camera, I/O Module, Axis Door Controller, VisualStation, E-map, Action Rule, Layout Settings (Live view and Timeline), Notification, Audio Pattern, and License.

For more convenience, after the failover server has been activated, the device licenses of the original recording server will be migrated to the failover server to ensure a smooth takeover during the failover period. However, if the number of cameras that require failover exceeds the maximum number of IP cameras the failover server can support, the surplus cameras from the original recording server will be disabled.

When failover occurs, the CMS host server will update the status of all servers immediately. As shown in the figure below, a yellow **Failed Over** status will appear next to the name of the recording server to show that this server is no longer operating. The name of the corresponding failover server will be shown on the right and will be hyperlinked to the setting page of this failover server. The reason for activating failover will also be displayed below the failover server, providing a quick overview of the server's condition.



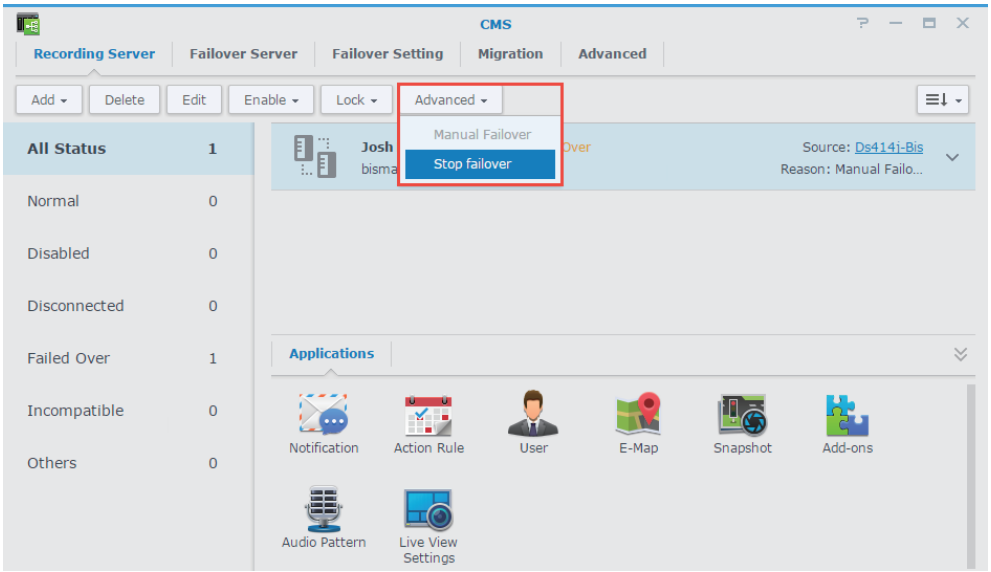
When a failover server takes over, operating the failover server within the host server is no different than that of the original recording server. The failover server and the devices installed on the failover server uses the original name of the recording server and its devices. Users can modify settings (e.g. adding, editing, and deleting cameras), however, changes made on these settings can only take effect during the failover period. After ending the failover, all settings will restore to the original settings before the occurrence of hardware failure.

During the failover period, users can log in to Surveillance Station and manage the failover server using the same applications used for the original recording server.

Ending the failover

There are different methods to end failover, depending on the failover type (automatic or manual).

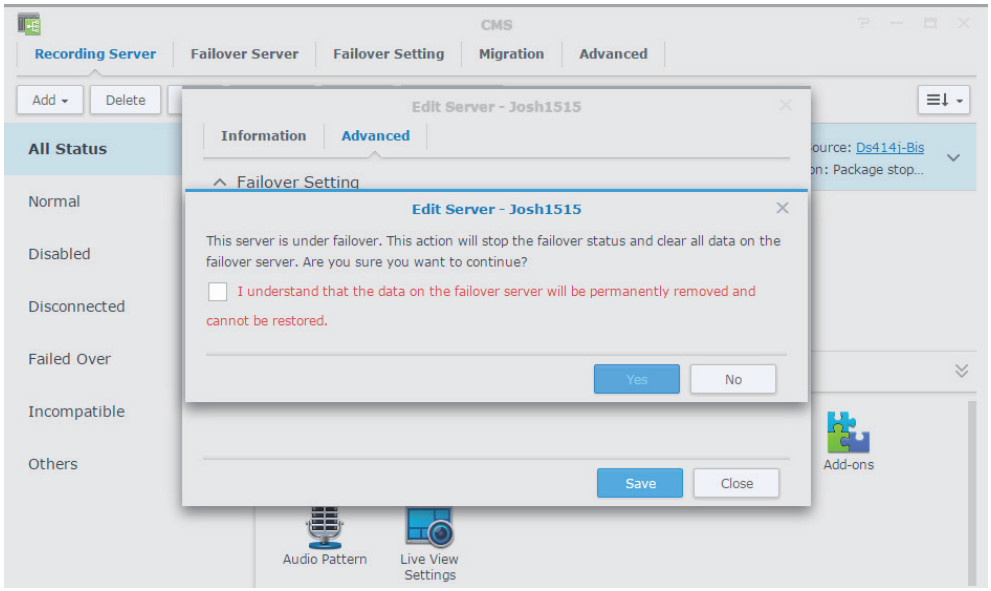
To end an automatic failover, the failover reason shown on the right side of the recording server must be cleared. To end a manual failover, go to the **Recording Server** tab and click **Stop failover** in **Advanced**.

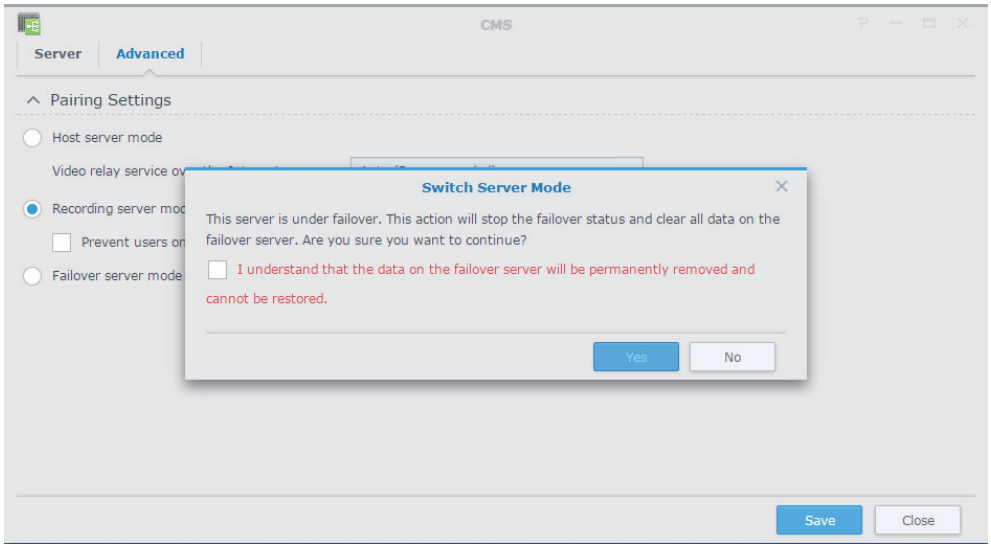


If the option to save the recordings and snapshots produced in the failover period have been selected in **Failback Setting**, upon terminating the failover in which the two servers in the failover pairing enter failback mode, the failover server will start transferring recordings and snapshots produced during the failover period to the recording server. In the circumstances where the failed over recording server cannot be fixed, in the **Failover Server** tab, users can click **CMS construction in LAN** in **Advanced** to permanently replace the recording server with the currently paired failover server or with another available recording server.

If the server is currently undergoing failover, executing the actions listed below will trigger a warning message reminding users that failover is currently taking place and that executing this action will interrupt the failover service and clear all data stored on the failover server, as shown in the figures below.

- Editing failover settings of the recording server
- Disabling/deleting the server
- Switching the CMS mode of the server



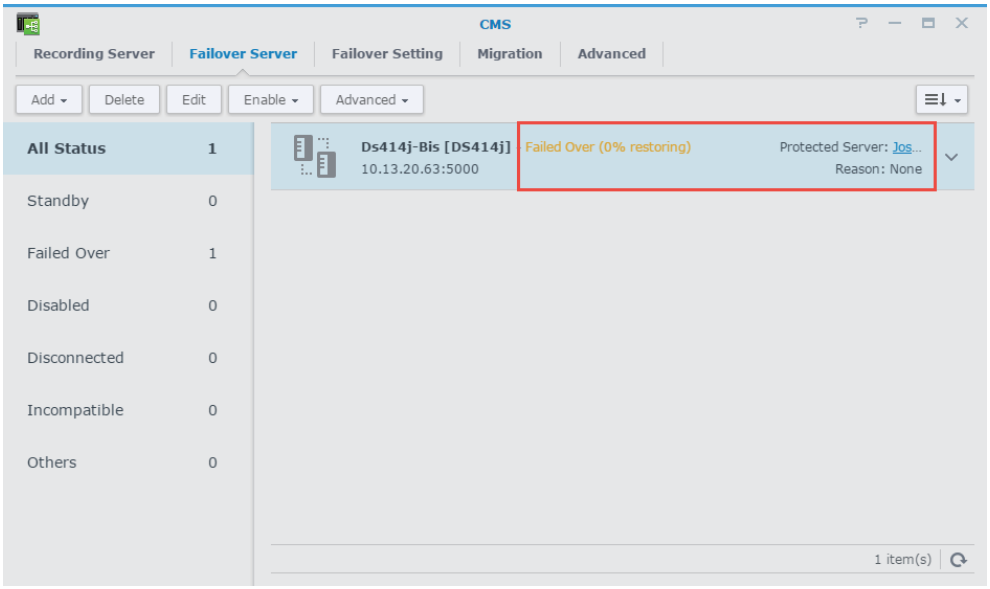


Failback process

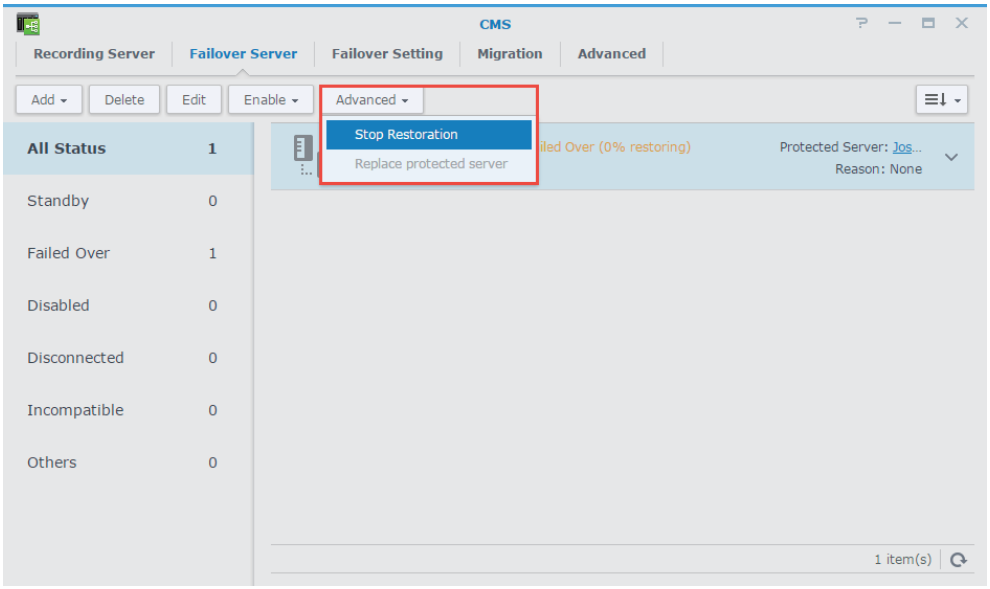
When failover is over, depending on the failover settings made by users, recordings and snapshots produced during the failover period will be synchronized back to the recording server or removed directly from the failover server.

If the system synchronizes data back to the recording server after failover ends, the failover server will not be able to take over other recording servers during the synchronization process. After completing or manually stopping the synchronization process, files will be automatically removed from the failover server as it reverts back to standby mode, ready to take over an abnormal recording server again.

When a server enters failback mode, the failover reason on the right side of the server name will be cleared, the server status will be changed to **Failed Over**, and the percentage completion will be displayed to show failback progress.

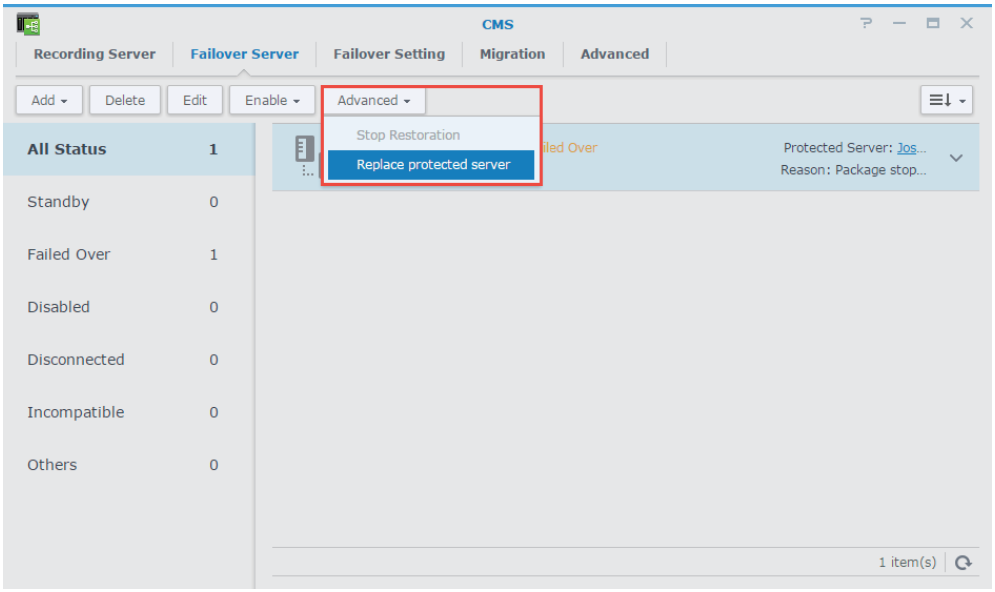


Due to bandwidth or hardware constraints, users can go to the **Failover Server** tab and click **Stop Restoration** in **Advanced** to stop the failback. After failback has been stopped, all recordings and snapshots that are not transferred completely will be directly removed.

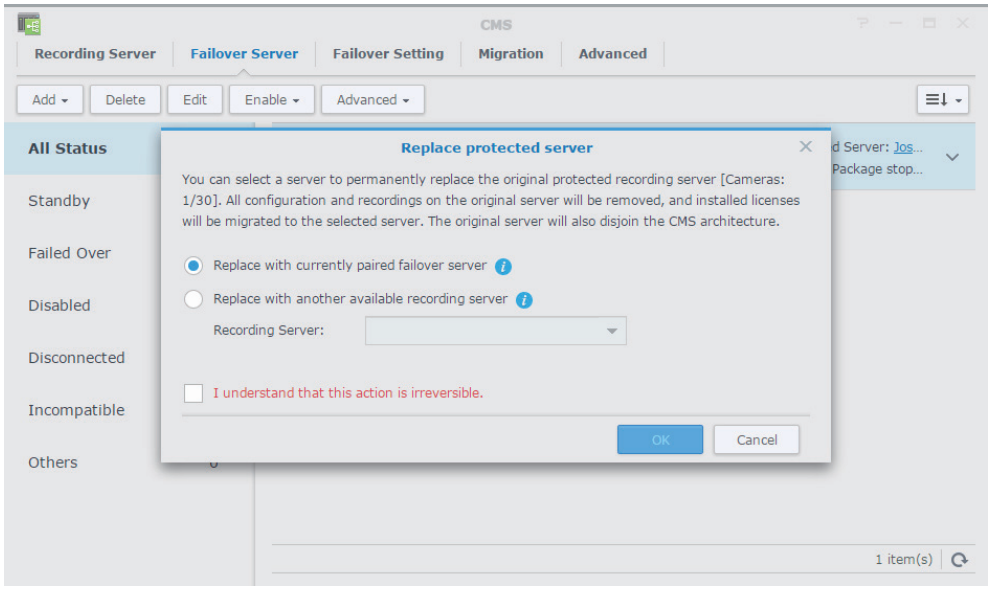


Permanently replacing protected servers

To permanently replace protected servers, go to the **Failover Server** tab and click **Replace protected server** in **Advanced**.



A pop-up window will appear to provide users the option to choose between replacing the original server with the current failover server or with another recording server.



If users choose to permanently replace the original server with another recording server, the settings of the original recording server will be applied to the newly selected recording server. Depending on the failover settings, recordings and snapshots produced during the failover period will be synchronized to the new recording server or removed from the failover server. The device licenses will also be automatically migrated to the new recording server permanently.

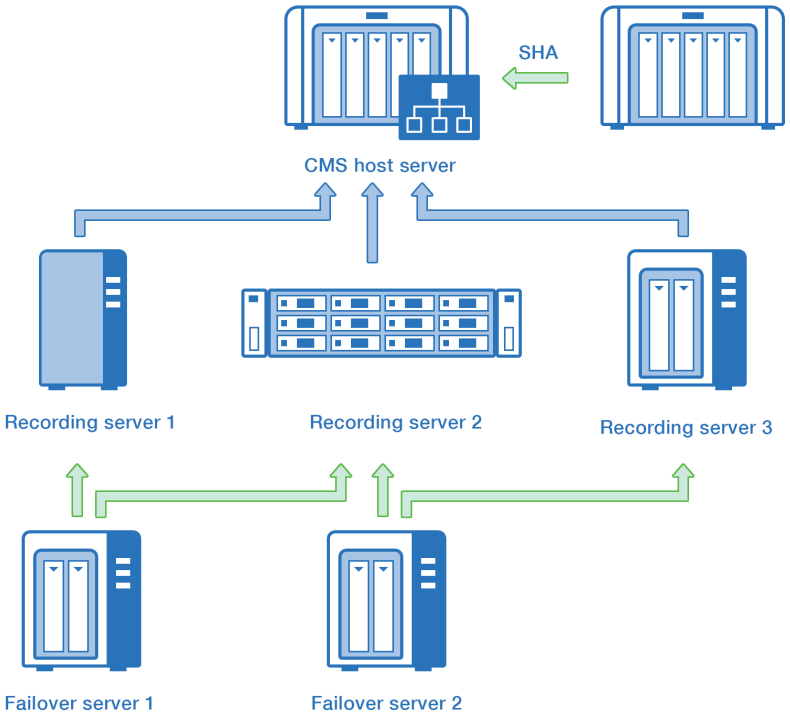
After replacing the protected server with a new recording server, the original recording server will be deleted, and the new recording server will use the same name and settings as the original recording server. The numbers in the bracket next to the server name represent the current number of cameras and the maximum number of cameras.

CMS construction examples

Two construction examples are shown below for user reference.

CMS construction in LAN

The purpose of this example is to explain the basic construction behavior of the failover architecture. Under the premise that each recording server is of different importance, different failover policies and settings should be applied to each server. This example is based on the assumption that all servers are in the same domain.



As shown in the figure above, the CMS host server, three recording servers, and all other devices are in the same domain. The following construction plan provided is based on the assumption that **Recording Server 2** is of higher importance than other servers:

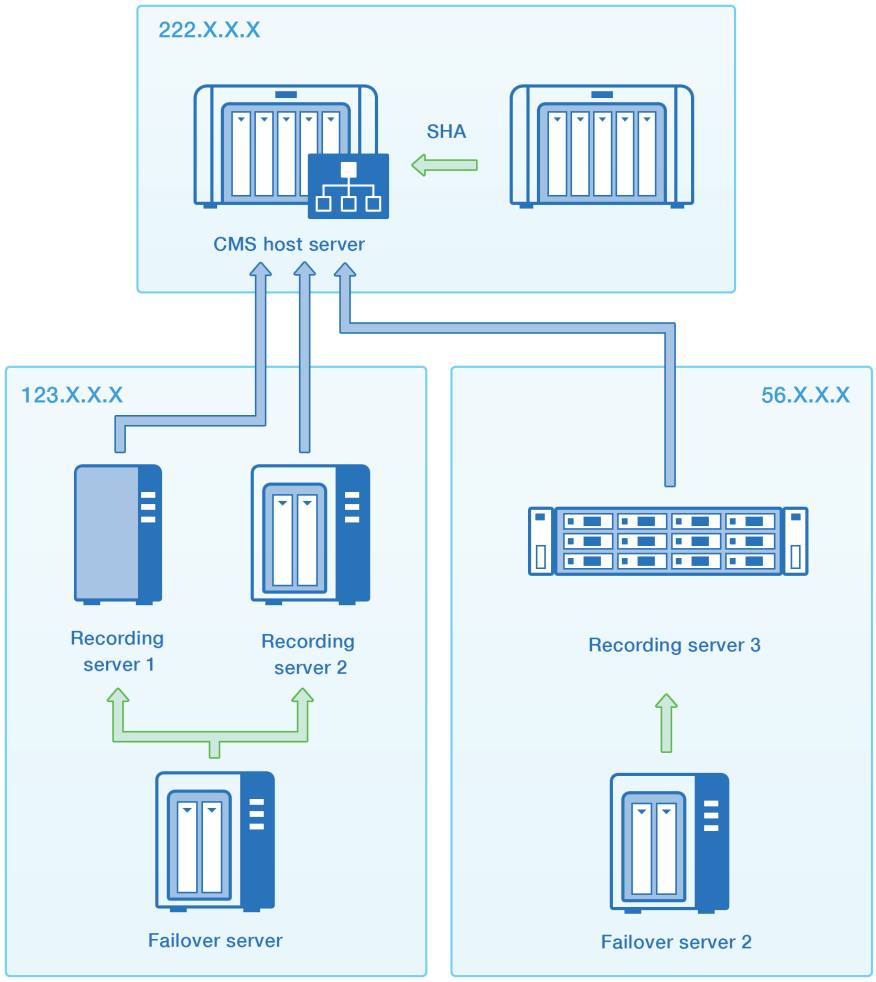
Since the CMS host server is the central and most significant component of the failover architecture, it is recommended for users to utilize Synology High Availability (SHA) to provide one-to-one protection for the CMS host server. This ensures a shorter halt time while settings (e.g., IP address) remain the same.

Unlike the CMS host, the recording servers will operate under the failover solution from Surveillance Station. Two failover servers are available in this example, as shown in the figure above. Since this construction plan is based on the assumption that **Recording Server 2** is of higher importance, it is recommended to pair **Recording Server 1** and **Recording Server 3** with **Failover Server 1** and **Failover Server 2** respectively, while pairing **Recording Server 2**, the server of higher importance, with both failover servers (**Failover Server 1** and **Failover Server 2**).

In this configuration, it is expected that all the recording servers can be protected by the failover mechanism, and **Recording Server 2** can have more complete protection. In other words, the number of failover servers and their configuration can be adjusted based on the different levels of importance of each server.

CMS construction with cross-domain servers

The purpose of this example is to recommend a failover architecture that applies to a CMS framework involving cross-domain servers.



In this example, the CMS setup crosses three domains (222.x.x.x, 123.x.x.x, 56.x.x.x), as shown in the figure above. Among the three domains, one CMS host server is allocated to the domain 222.x.x.x, two recording servers are allocated to the domain 123.x.x.x, and one recording server is allocated to the domain 56.x.x.x. Based on these assumptions, the construction plan for this example is provided below:

Since the CMS host server is the central and most significant component of the failover architecture, it is recommended for users to utilize Synology High Availability (SHA) to provide one-to-one protection for the CMS host server. This ensures a shorter halt time while settings (e.g. IP address) remain the same. Unlike the CMS host, the recording servers will operate under the failover solution from Surveillance Station.

It is recommended that one failover server should be allocated to each domain. This ensures that all devices (e.g. cameras, door controllers) will remain within the same domain after failover occurs. Operating within the same domain also guarantees that the recordings and snapshots produced during the failover period can be successfully synchronized back to the original server after the failover is over.

SYNOLOGY INC.

9F, No. 1, Yuan Dong Rd.
Banqiao, New Taipei 220632
Taiwan
Tel: +886 2 2955 1814

SYNOLOGY AMERICA CORP.

3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
Tel: +1 425 818 1587

SYNOLOGY UK LTD.

Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL,
United Kingdom
Tel.: +44 (0)1908048029

SYNOLOGY FRANCE SARL

102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
Tel: +33 147 176288

SYNOLOGY GMBH

Grafenberger Allee 295
40237 Düsseldorf
Deutschland
Tel: +49 211 9666 9666

SYNOLOGY SHANGHAI

200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

SYNOLOGY JAPAN CO., LTD.

4F, No. 3-1-2, Higashikanda
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®

synology.com