Cisco Secure Network Analytics

Failover Configuration Guide 7.4.2

Table of Contents

Introduction

Use the failover configuration to establish a failover relationship between two Cisco Secure Network Analytics Managers (formerly Stealthwatch Management Consoles or SMCs) so that one of them serves as a backup to the other.

If the primary Manager fails, you can manually set the secondary Manager to become the primary Manager to continue monitoring the system.

> ⚠ If your primary Manager goes offline, please note that the Managers do not swap roles automatically. Make sure you change the Manager roles in the order shown in this guide.

Before you Begin

Before you start the failover configuration, install your Cisco Secure Network Analytics (formerly Stealthwatch) appliances and complete the system configuration. For instructions, refer to your Cisco Secure Network Analytics installation guides and the Cisco Secure Network Analytics System Configuration Guide.

Also, review the details and instructions in this guide, so you are prepared for the failover configuration requirements and implementation.

Data Store Deployments

If you are using a Data Store deployment with your Secure Network Analytics system, we recommend that you configure Failover before initializing the Data Store. If you have a Data Store that you have already initialized, refer to **Configuring Failover Following Data Store Initialization**.

Security Analytics and Logging (OnPrem)

If Cisco Security Analytics and Logging (On Premises) is enabled on one Manager, make sure it is enabled on the other Manager before you start the failover configuration.

To enable Security Analytics and Logging (OnPrem) on both Managers, refer to the Cisco Security Analytics and Logging (On Premises): Firepower Event Integration Guide.

Appliance Status

Before you start any configuration changes in Secure Network Analytics, make sure the appliance status is shown as Connected. We include instructions to review the status in this guide.

> ⚠ Do not change any other configurations or add or remove appliances from Central Management until you have finished the failover configuration.

Configuration Requirements

This guide includes details that are critical for a successful configuration, including:

Admin User

To configure failover, log in to your Managers as the admin user.

Back up Configuration Files and Databases

Plan time to back up each Manager configuration and database. You will need the backup files if there is a problem with the failover configuration, and you need both backups to restore an Manager completely. For instructions, refer to **2. Back up Manager Configuration and Databases**.

Certificates

Make sure you save the correct certificates to the required appliance Trust Stores before you configure failover. This procedure sets up trust between appliances, so they can communicate. For instructions, refer to **3. Add Certificates to Trust Stores**.

Failover Roles

When you save the failover configuration, your primary Manager will actively monitor and manage your appliances, and your secondary Manager becomes read-only. To plan which Manager will be configured in the primary or secondary failover role, refer to **Saving the Failover Configuration** and **1. Plan Failover Roles**.

If your secondary Manager is managing appliances in Central Management, move them to your primary Manager (or another Manager) before you start the failover configuration. Refer to the Cisco Secure Network Analytics System Configuration Guide for instructions.

> ⚠ If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the Manager Trust Store before you add the appliance to Central Management.

Configuration Order

Configure the secondary Manager before the primary Manager. Refer to **4. Configure the Failover Pair** for instructions.

> ⚠ Make sure you configure your secondary Manager for failover before you configure your primary Manager. When you save the failover configuration, the

> ⚠ secondary Manager domain configuration is deleted, so make sure you follow the instructions in order.

Configuration Changes

Do not change any other configurations or add or remove appliances from Central Management until you have finished the failover configuration.

Software Version

Ensure that the Secure Network Analytics v7.4.2 is installed on your Managers before you proceed to the instructions in this guide.

Saving the Failover Configuration

When you save the failover configuration, a trusted relationship and configuration channel is established between the primary and secondary Manager. Also, the following system changes occur:

Primary Manager

The primary Manager pushes its domain configuration, user settings, and policies to the secondary Manager.

Secondary Manager (Read-Only)

The secondary Manager domain configuration is deleted. It will become read-only for all users and synchronize with the primary Manager.

Passwords

The primary Manager pushes its local users and password credentials to the secondary Manager, so they are synchronized. This means you will use the same password to log in to your primary Manager and secondary Manager. To change the password on the secondary Manager, log in to your primary Manager.

Domain Changes

The primary Manager automatically shares any domain configuration changes with the secondary Manager, such as host groups, users, and policies.

If you change the domain configuration on the primary Manager while the communication channel to the secondary Manager is down (Config Channel Down), the primary Manager will send a full configuration push as soon as the secondary Manager communication channel is restored.

Flow Collectors

The Flow Collectors automatically send their data to both Managers.

External Services

If an external service is configured on the primary Manager, make sure you configure it on the secondary Manager. For example, if you enable the Threat Feed on the primary Manager, enable it on the secondary Manager.

Changing Roles

If you need to promote your secondary Manager to the primary failover role, make sure you change the roles in order. The order is critical, and they do not swap roles automatically.

- If your primary Manager is offline, refer to **Troubleshooting** for more information.
- To change failover roles, refer to **Changing Failover Roles**.

Certificates

When your Managers are configured for failover, the Trust Stores are updated automatically as follows:

- The secondary Manager identity certificate and chain (if applicable) are added to the Trust Stores of all managed appliances.
- The identity certificates and chain (if applicable) of all managed appliances are added to the secondary Manager Trust Store when they are added to the primary Manager Central Management.

Restoring the Primary Manager

If you restore a primary Manager that is configured for failover, the secondary Manager will synchronize to the primary Manager after the restoration is completed.

Rebooting the Primary Manager

If your primary Manager goes offline because you rebooted it, it will resume the primary failover role when the appliance status returns to Connected and it detects the secondary Manager.

- If the primary Manager role changes to secondary and does not resolve itself, refer to **Troubleshooting**.
- To change failover roles, refer to **Changing Failover Roles**.

Changing Network Interfaces

If your Managers are configured for failover, delete the failover relationship before you change your Manager network interfaces, host name, or network domain name. For details, refer to **Changing Network Interfaces**.

Failover Configuration Overview

To configure failover, make sure you complete the following procedures:

1. **Plan Failover Roles**
2. **Back up Manager Configuration and Databases**
3. **Add Certificates to Trust Stores**
4. **Configure the Failover Pair**
5. **Confirm the Failover Configuration**

1. Plan Failover Roles

Before you start the failover configuration, plan which Manager will be configured in the primary or secondary failover role.

- **IP Address:** Make sure you have the IP address of each Manager.
- **Secondary Manager:** If your secondary Manager is managing appliances in Central Management, move them to your primary Manager (or another Manager) before you start the failover configuration. Refer to the Cisco Secure Network Analytics System Configuration Guide for instructions.

> ⚠ If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the Manager Trust Store before you add the appliance to Central Management.

> ⚠ Before you start the failover configuration, make sure Security Analytics and Logging (OnPrem) is enabled on both Managers. To enable Security Analytics and Logging (OnPrem) on both Managers, refer to the Cisco Security Analytics and Logging (On Premises): Firepower Event Integration Guide.

- **Saving the Failover Configuration:** When you save the failover configuration, your primary Manager actively monitors and manages your appliances, and your secondary Manager becomes read-only. For details, refer to **Saving the Failover Configuration**.

Planned Failover Role	Summary	IP Address
Primary Manager	Actively monitors and manages Secure Network Analytics	
Secondary Manager	Read-only	

2. Back up Manager Configuration and Databases

Before you configure your Managers for failover, back up each appliance configuration and database. You need both backups to restore the Managers completely.

New Installations: If your Managers are new installations and you do not need to restore the configuration in the future, you can skip this procedure. Go to **3. Add Certificates to Trust Stores**.

> ⚠ Without a backup, you will not be able to recover your files if a problem occurs during the failover configuration. For assistance, please contact Cisco Support.

1. Create a Backup Configuration File

Complete these steps to create a backup configuration file for each Manager. If your Manager also manages appliances as a Central Manager, it creates a Manager backup configuration file and a Central Management backup configuration file.

1. Log in to your **secondary** Manager.
2. From the main menu, select **Configure** > **GLOBAL Central Management**.
3. Click the ••• (**Ellipsis**) icon for the Manager.
4. Select **Support**.
5. Select the **Configuration Files** tab.
6. Click the **Backup Actions** drop-down menu.
7. Select **Create Backup**.
8. Click **Download**. Save the file to a secure location.
9. Log in to your primary Manager. Repeat steps 2 through 8 to save the backup configuration file for your primary Manager.

2. Back up the Manager Databases

To back up the Manager database to a remote file system, you will use Central Management and the Appliance Admin interface.

> ⚠ Make sure you complete the procedures to back up the database on your primary Manager and secondary Manager.

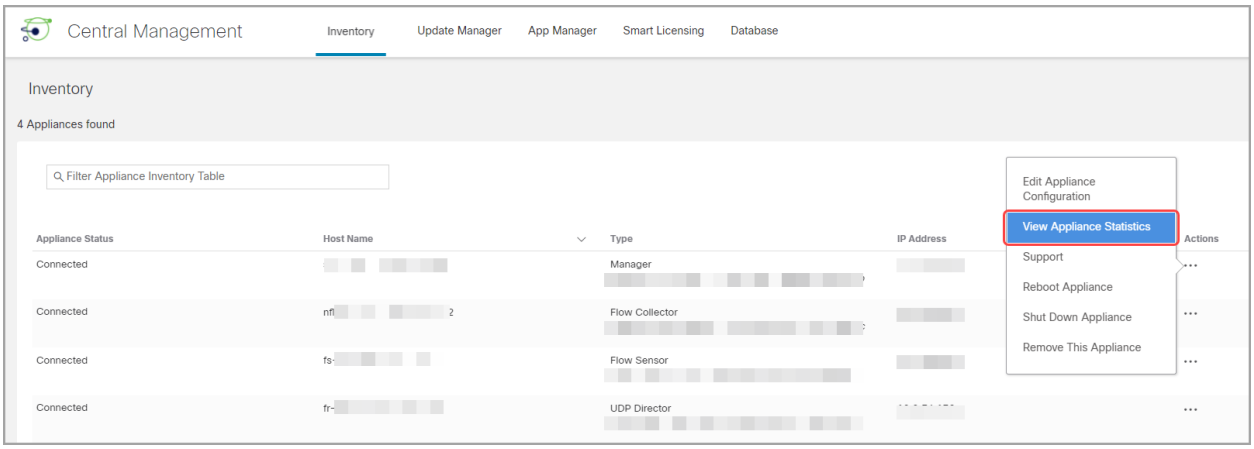
1. Back up the Databases

Use the following instructions to back up your Manager database. Also, review the following:

- **Space:** Make sure the remote file system has enough space to store the database backup.
- **Time:** After you back up the database once, subsequent backups will be quicker because the process backs up only what has changed since the last backup. This process backs up approximately 0.5 GB to 2 GB of data per minute.

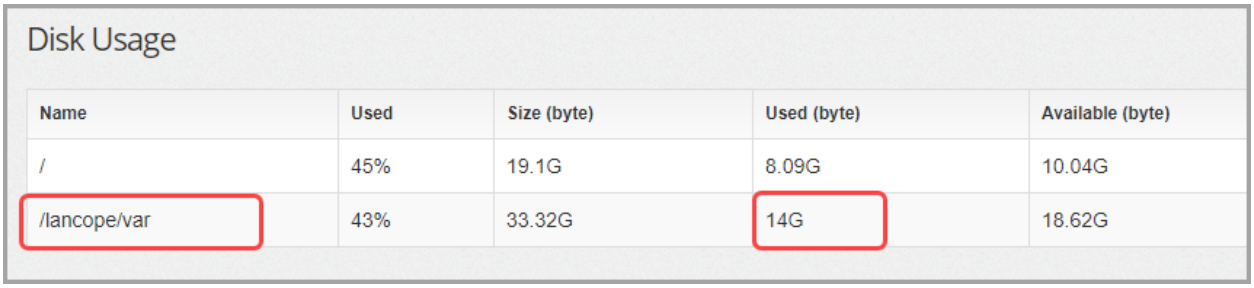
1. Log in to your Manager Appliance Admin interface.

   In Central Management, click the Manager ••• (**Ellipsis**) icon > **View Appliance Statistics**.



2. Determine how much space you will need on the remote file system to store the database backup as follows:

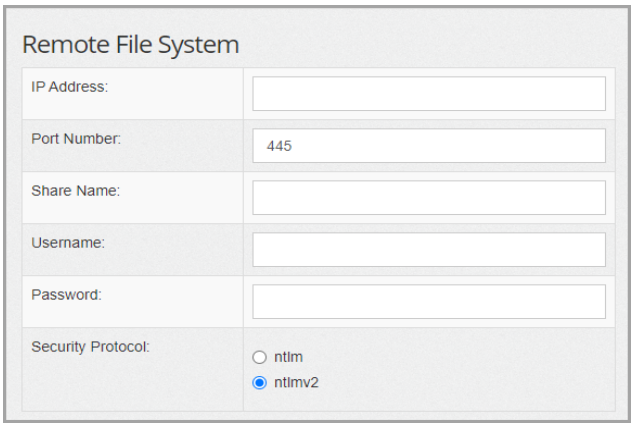
   - Click **Home**.
   - Locate the **Disk Usage** section.
   - Review the **Used (byte)** column for the **/lancope/var** file system. You will need at least this much space plus 15% more on the remote file system to store the database backup.



Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	45%	19.1G	8.09G	10.04G
/lancope/var	43%	33.32G	14G	18.62G

3. Click **Configuration** > **Remote File System**.



4. Complete the fields using the settings for the remote file system where you want to store the backup files.

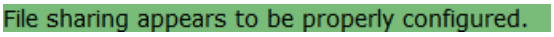
   The Secure Network Analytics file share uses the CIFS (Common Internet File System) protocol, also known as SMB (Server Message Block).

5. Click **Apply** to place the settings in the configuration file.

   If the Apply button is not enabled after you enter the password, click once in a blank area on the Remote File System page to enable it.

6. Click **Test** to verify that the Secure Network Analytics appliance and the remote file system can communicate with each other.

   Confirm you see the following message at the bottom of the Remote File System page when the test is complete.

7. Click **Support** > **Backup/Restore Database**.
8. Click **Create Backup**. This process may take a long time.

   - After the backup process starts, you can mouse away from the page without interrupting the process. However, if you click **Cancel** while the backup is in progress, you may not be able to resume the backup without restarting the appliance.
   - Follow the on-screen prompts until the backup is completed.
   - To view details of the backup process, click **View Log**.

9. Click **Close** to close the progress window.

> If you cancel the backup before it finishes, make sure you delete the database snapshots. Refer to **4. Delete the Database Snapshots** for instructions.

2. Delete the Database Snapshots

Before you create backup files, make sure you delete any saved snapshots on the Manager and Flow Collector databases using the following instructions.

> Make sure you delete the Manager and Flow Collector database snapshots. This step is critical for a successful backup.

1. Log in to the Manager and Flow Collector appliance database console as **admin**.
2. **Check for Snapshots:** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from database_snapshots;"
   ```

3. Confirm Database Backup

Repeat the procedures in **2. Back up the Manager Databases** and confirm you've saved the database backup for each Manager.

4. Delete the Database Snapshots

After you have saved the backup files, use the following instructions to delete the snapshots on the Manager and Flow Collector databases.

> ⚠ Make sure you delete the Manager and Flow Collector database snapshots. This step is critical for a successful update.

1. Log in to the Manager or Flow Collector appliance database console as **admin**.
2. **Check for Snapshots:** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from database_snapshots;"
   ```

3. **Delete Snapshots (if they exist):** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot('StealthWatchSnap1');"
   ```

4. **Wait until the snapshot folder is removed:** Check:

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   If the results are not empty, continue to wait. You may need to wait several minutes until the folder is removed, depending on the size of the database.

5. Repeat steps 1 through 4 to delete all saved Manager and Flow Collector database snapshots.

3. Add Certificates to Trust Stores

Use the following instructions to save the required appliance identity certificates and chains to the Trust Stores.

Trust Store Requirements

The instructions will guide you through the following requirements:

- Adding the secondary Manager certificates to the primary Manager Trust Store.
- Adding the primary Manager certificates to the secondary Manager Trust Store.

Certificate Chain

If your appliance identity certificate includes a certificate chain, make sure you add the certificate chain (root and intermediate) to the Trust Stores.

Uploading Certificates to the Trust Store

Upload each file individually.

1. Download the Appliance Identity Certificates

Use the following instructions to download and save your appliance identity certificates. The steps vary based on the browser you are using.

If your certificates are already saved, you can skip this procedure. Go to **2. Add Certificates to the Manager Trust Stores**.

> You can also click the lock/security icon in your browser. Follow the on-screen prompts to download your certificates. The steps vary based on the browser you are using.

1. In the browser address bar, replace the path after the IP address with the following: **/secrets/v1/server-identity**

   For example: https://<IPaddress>/secrets/v1/server-identity

2. Follow the on-screen prompts to save the certificate.

   Open: To view the file, select a text file format.

Troubleshooting: If you do not see the prompt to download the certificate, check your Downloads folder in case it was downloaded automatically, or try a different browser.

3. Repeat steps 1 and 2 on each Manager.

2. Add Certificates to the Manager Trust Stores

Use the following instructions to save your secondary Manager appliance identity certificate and chain (if applicable) to the primary Manager Trust Store.

1. Log in to your Manager.
2. From the main menu, select **Configure** > **GLOBAL Central Management**.
3. Confirm the Appliance Status is shown as Connected.
4. Click the ••• (**Ellipsis**) icon in the **Actions** column for the Manager.
5. Select **Edit Appliance Configuration**.
6. Click the **General** tab, locate the **Trust Store** section.
7. Click **Add New**.

> ⚠ Make sure you upload each appliance identity certificate and chain (root and intermediate) certificate individually.

8. In the **Friendly Name** field, enter a name for the certificate.
9. Click **Choose File**. Select the certificate.
10. Click **Add Certificate**. Confirm the certificate is shown in the Trust Store list.
11. Repeat steps 6 through 9 to add any other required certificates to the Trust Store.

    - If you are logged in to the secondary Manager, add the primary Manager certificates.
    - If you are logged in to the primary Manager, add the secondary Manager certificates.

12. Click **Apply Settings**. Follow the on-screen prompts.
13. **Connected:** On the Central Management Inventory page, confirm the Appliance Status returns to Connected.
14. Repeat steps 1 through 13 on the other Manager.

Configuring Failover Following Data Store Initialization

If you've deployed Secure Network Analytics with a Data Store, make sure you configure Failover before you initialize the Data Store. If you configure Failover after you've initialized the Data Store, follow the instructions in the section below to configure the secondary Manager for secure communication with the Data Store.

The process for configuring failover following Data Store initialization is summarized below.

1. Configure your failover pair.
2. Add a secondary Manager.

Configuring Your Failover Pair

Configure your failover pair by following the instructions in the **4. Configure the Failover Pair** section of this guide. Once this process is complete, you will see a "Data Store Not Configured" message in the Central Management Inventory for the secondary Manager. Follow the **Adding a Manager after the Data Store is Initialized** to configure the secondary Manager.

Adding a Manager after the Data Store is Initialized

Use the following instructions to add a Manager to your Data Store if you've already initialized the Data Store.

If you have existing Managers or Flow Collectors that you configured for use without a Data Store, you need to reset each appliance to factory defaults (RFD) before you can configure them for use with a Data Store and add them to your deployment.

1. **RFD:** Follow the instructions in the Resetting Factory Defaults section of the Secure Network Analytics System Configuration Guide.

> You can choose to keep or discard your current network settings. If you discard them, you must reconfigure these network settings.

2. Follow the instructions in 1. Configuring Your Environment using First Time Setup and 2. Configuring the Managed System in the Secure Network Analytics System Configuration Guide to configure the appliance and add it to Central Management. Configure the appliance in First Time Setup.
3. Log in to the Primary Manager appliance console as root.

4. Type `SystemConfig` and press Enter.
5. Select **Data Store**.
6. Select **SSH**. Wait while SSH is enabled across your appliances.
7. From the **Data Store** menu, select **New Appliances**. Follow the on-screen prompts.
8. Exit SystemConfig.

> When you exit the Data Store menu, the system restores your previous SSH settings.

9. Check Central Management to ensure that the appliance status is Connected.

4. Configure the Failover Pair

Use the following instructions to configure your Managers for failover. When you save the failover configuration, the secondary Manager domain configuration is deleted. It will become read-only and synchronize with the primary Manager. For details, refer to **Saving the Failover Configuration**.

Before you Begin

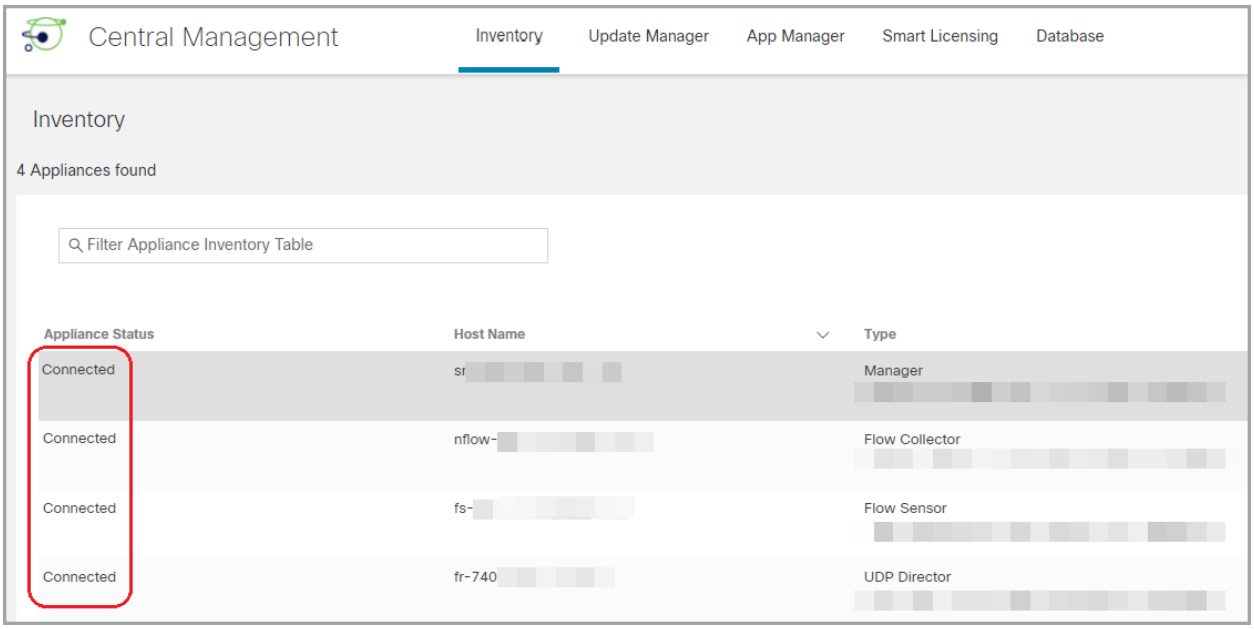
Make sure you complete the following procedures before you start these instructions:

1. **Plan Failover Roles**
2. **Back up Manager Configuration and Databases**
3. **Add Certificates to Trust Stores**

> ⚠ Make sure you configure your secondary Manager for failover before you configure your primary Manager. When you save the failover configuration, the secondary Manager domain configuration is deleted, so make sure you follow the instructions in order.

1. Confirm Manager Appliance Status

1. Log in to your **primary** Manager.
2. From the main menu, select **Configure** > **GLOBAL Central Management**.
3. Confirm the Appliance Status for each appliance is shown as **Connected**.

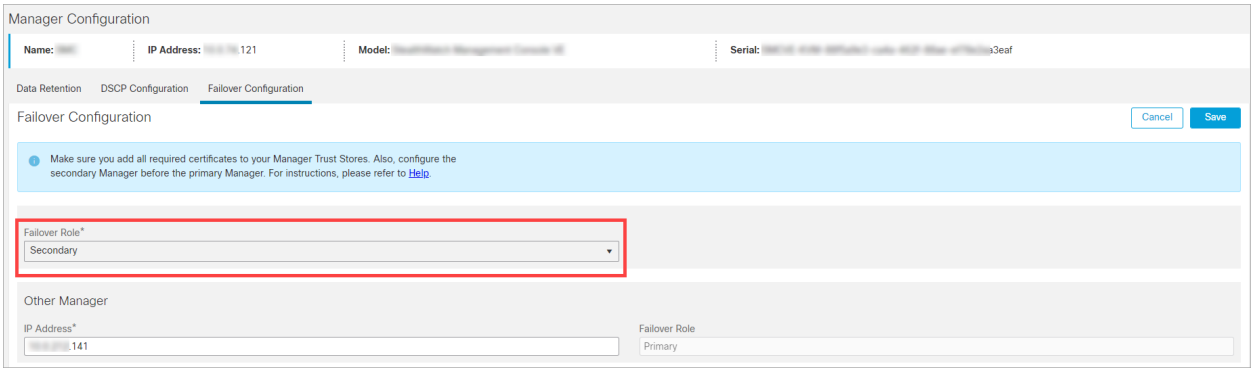


4. Log in to your **secondary** Manager.
5. From the main menu, select **Configure** > **GLOBAL Central Management**.
6. Confirm the Appliance Status is shown as **Connected**.
7. Stay logged in to both Managers, and go to the next procedure.

2. Configure the Secondary Manager

When you save the failover configuration, the secondary Manager domain configuration is deleted. It will become read-only and synchronize with the primary Manager. For details, refer to **Saving the Failover Configuration**.

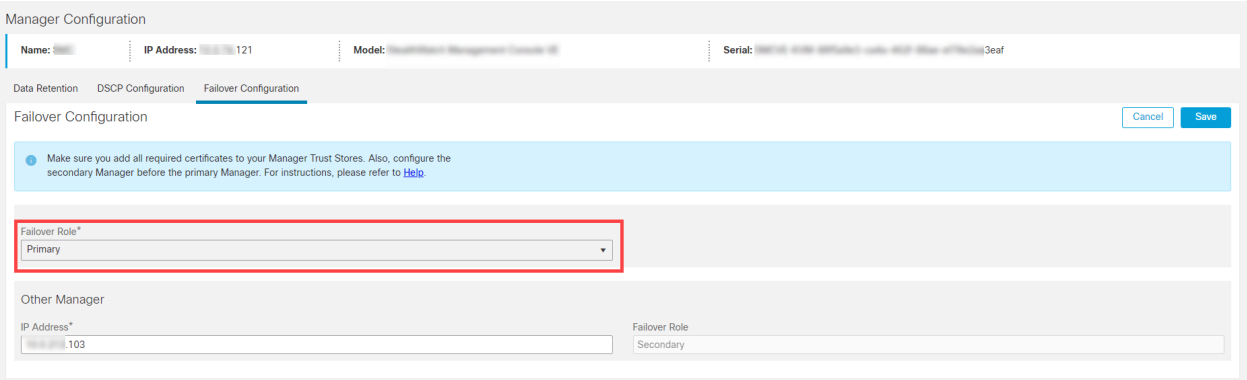
1. In the **secondary** Manager, click the **Security Insight dashboard** tab.
2. From the main menu, select **Configure** > **GLOBAL Manager**.
3. Click the **Failover Configuration** tab.
4. Click the **Failover Role** drop-down menu. Select **Secondary**.



5. In the **IP Address** field, enter the IP address of your other Manager. This will be your primary Manager.
6. Click **Save**.
7. Follow the on-screen prompts to save your changes.

3. Configure the Primary Manager

1. In the **primary** Manager, click the **Security Insight dashboard** tab.
2. From the main menu, select **Configure** > **GLOBAL Manager**.
3. Click the **Failover** tab.
4. Click the **Failover Role** drop-down menu. Select **Primary**.



5. In the **IP Address** field, enter the IP address of your secondary Manager.
6. Click **Save**.
7. Follow the on-screen prompts to save your changes.

5. Confirm the Failover Configuration

Use the following instructions to confirm your Managers are configured for failover and communicating.

1. Confirm Configuration Changes

Confirm your primary Manager shows the failover configuration changes. Also, confirm the appliance status for each appliance is shown as Connected.

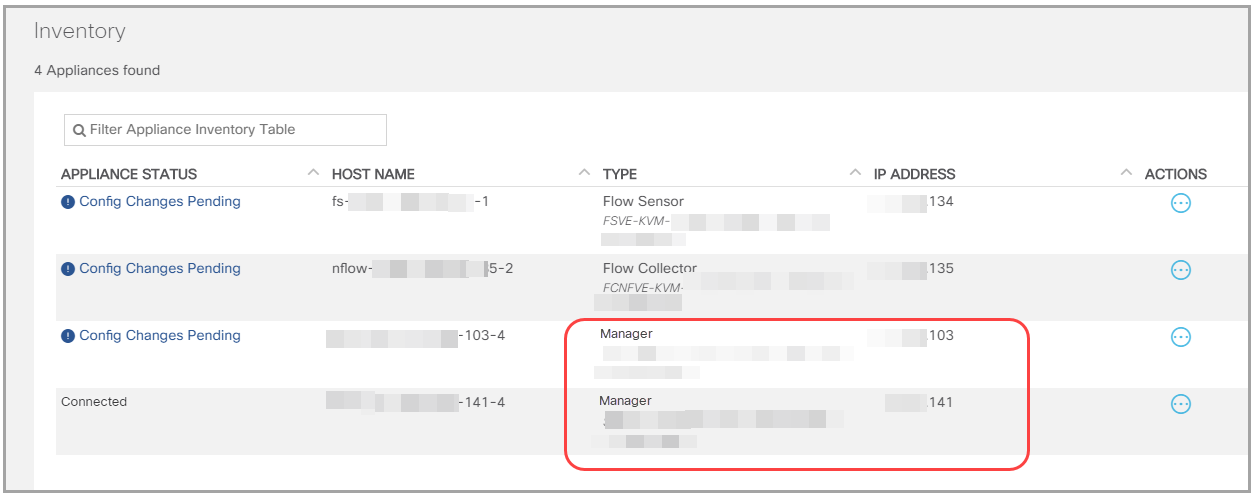
1. In the primary Manager, open Central Management.

   Select **Configure** > **GLOBAL Central Management**.

2. Confirm the following:

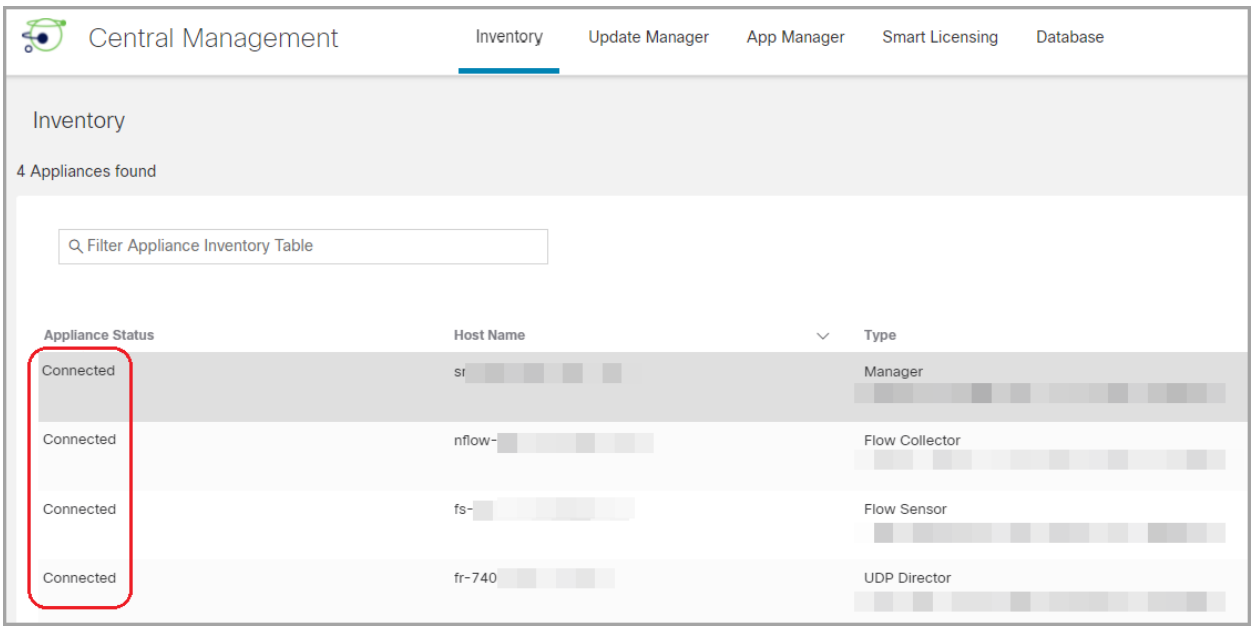
   - The secondary Manager is shown in the inventory.
   - The Appliance Status for each appliance is shown as Connected.

Confirming the Primary and Secondary Manager are Shown



> Wait while Central Management updates. The appliance status for your appliances will show **Config Changes Pending**.

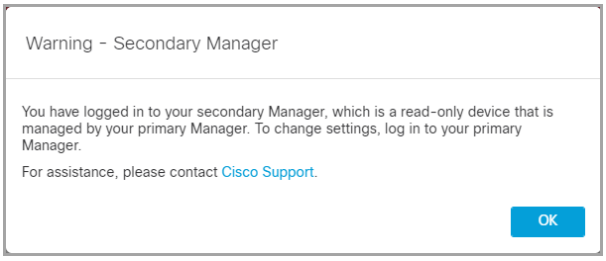
Confirming All Appliances are Connected



2. Confirm Flow Collection

Use the following instructions to confirm the secondary Manager is operating as read-only and is receiving flows.

1. Log in to your **secondary Manager**.
2. You should see a notification that your Manager is read-only. If your secondary Manager has not changed to read-only, check your failover configuration.



3. On the Security Insight dashboard, review the Flow Collection Trend.

4. **If flow collection is in progress,** no further action is required. You are finished with the failover configuration.

   If flow collection stopped, use Central Management to reboot your Flow Collectors and secondary Manager in the following order (or refer to **Troubleshooting**):

   - Log in to your primary Manager.
   - From the main menu, select **Configure** > **GLOBAL Central Management**.
   - Locate the Flow Collector.
   - Click the ••• (**Ellipsis**) icon in the **Actions** column.
   - Select **Reboot Appliance**. Follow the on-screen prompts.
   - **Flow Collectors:** Repeat these steps to reboot every Flow Collector in Central Management.
   - **Secondary Manager:** Repeat these steps to reboot your secondary Manager.

> ⚠ If your primary Manager goes offline because you rebooted it, it will resume the primary failover role when the appliance status returns to Connected and it detects the secondary Manager. If the primary Manager role changes to secondary and does not resolve itself, refer to **Troubleshooting**.

Changing Failover Roles

Use the following instructions to change the primary and secondary Manager roles. Please note that they do not swap roles automatically.

> ⚠ When you change the failover configuration, the secondary Manager domain configuration is deleted, so make sure you follow the instructions in order.

Time

When you promote a secondary Manager to primary, it may take at least 1 hour for all appliances to change from **Config Channel Down** to **Connected**. Monitor the status in Central Management. Refer to **5. Confirm the Failover Configuration** for details.

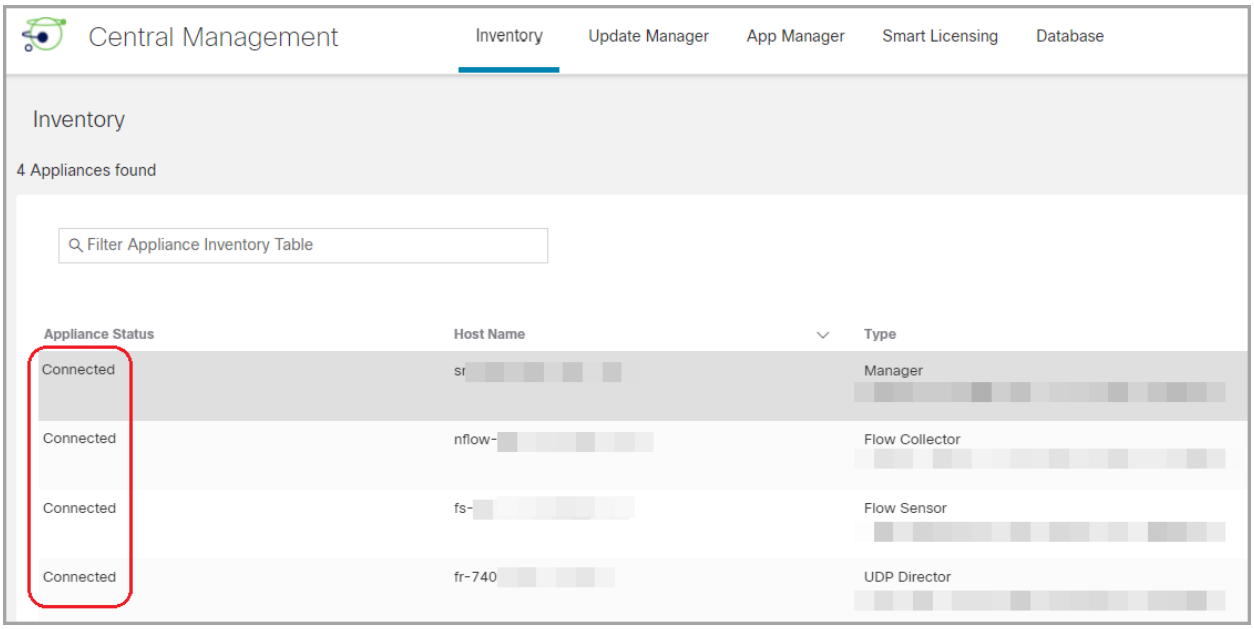
1. Back up the Primary Manager

Before you change the failover roles, back up the primary Manager in case you need to restore the configuration in the future. Refer to **2. Back up Manager Configuration and Databases** for details.

2. Confirm the Appliance Status

1. Log in to your primary Manager.
2. From the main menu, select **Configure** > **GLOBAL Central Management**.
3. Confirm the Appliance Status for each appliance is shown as **Connected**.

    - **Managers:** If the appliance status for the primary or secondary Manager is shown as Config Channel Down, check your communication settings and refer to **Troubleshooting**.
    - **Other Appliances:** If the appliance status for the Flow Collectors, Data Nodes, Flow Sensors, or UDP Directors is shown as Config Channel Down, check your configuration settings and use Central Management to reboot the appliance (••• (**Ellipsis**) icon > **Reboot Appliance**). For additional troubleshooting, refer to the Cisco Secure Network Analytics System Configuration Guide.



3. Change the Failover Configuration

Use the following instructions to change your primary Manager to secondary and promote your secondary Manager to primary.

In this configuration, your primary Manager becomes the secondary Manager, and its domain configuration is deleted. It will become read-only and synchronize with the newly- promoted primary Manager. For details, refer to **Saving the Failover Configuration**.

> ⚠ Do not add or remove appliances from Central Management until you've finished the failover configuration changes.

1. Change the Primary Manager to Secondary

1. In the current **primary** Manager, click the **Security Insight dashboard** tab.
2. From the main menu, select **Configure** > **GLOBAL Manager**.
3. Click the **Failover Configuration** tab.
4. Confirm the **Failover Role** is shown as **Primary**.

   If your primary Manager is shown as Secondary, refer to **Troubleshooting**.

5. Click the **Failover Role** drop-down menu. Select **Secondary**.
6. Click **Save**.
7. Follow the on-screen prompts to save your changes.

2. Change the Secondary Manager to Primary

1. Log in to your **secondary** Manager.
2. From the main menu, select **Configure** > **GLOBAL Manager**.
3. Click the **Failover Configuration** tab.
4. Confirm the **Failover Role** is shown as **Secondary**.
5. Click the **Failover Role** drop-down menu. Select **Primary**.
6. Click **Save**.
7. Follow the on-screen prompts to save your changes.

4. Confirm your Configuration Changes

To confirm your failover configuration changes, go to **5. Confirm the Failover Configuration** and follow the instructions.

Changing Network Interfaces

If your Managers are configured for failover, delete the failover relationship before you change any appliance network interfaces, host name, or network domain name. The overall steps are as follows:

> ⚠ If you delete the failover configuration, all domain configuration data will be deleted from the secondary Manager. Make sure you follow all instructions in order.

1. Delete the Failover Configuration

For instructions, refer to **Deleting the Failover Configuration**.

2. Change Manager Network Interfaces

Follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide.

As part of the procedure, you will remove the appliance from Central Management temporarily, and the appliance identity certificate is replaced automatically.

> The appliance identity certificate is replaced automatically as part of this procedure.
>
> ⚠ **If your appliance uses a custom certificate,** please contact Cisco Support to change these settings. Do not use the instructions shown here. Make sure you have a copy of the custom certificate and private key.

3. Configure Manager Failover

Follow the instructions in this guide to configure failover. Make sure you back up your Managers and add any new certificates to the Manager Trust Stores.

Deleting the Failover Configuration

Before you delete the failover configuration, confirm the status of both Managers and follow the instructions in order.

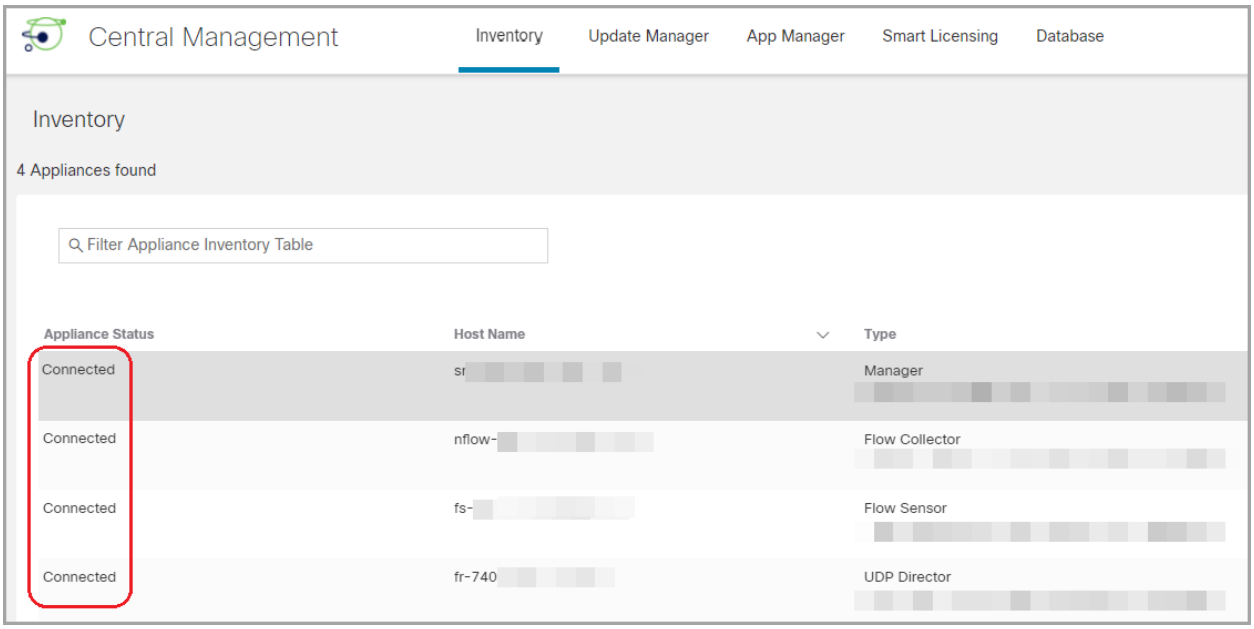
> ⚠ If you delete the failover configuration, all domain configuration data will be deleted from the secondary Manager.

1. Confirm Appliance Status

Before you start, confirm the primary Manager shows the secondary Manager as a managed appliance, and confirm both Managers are shown as Connected.

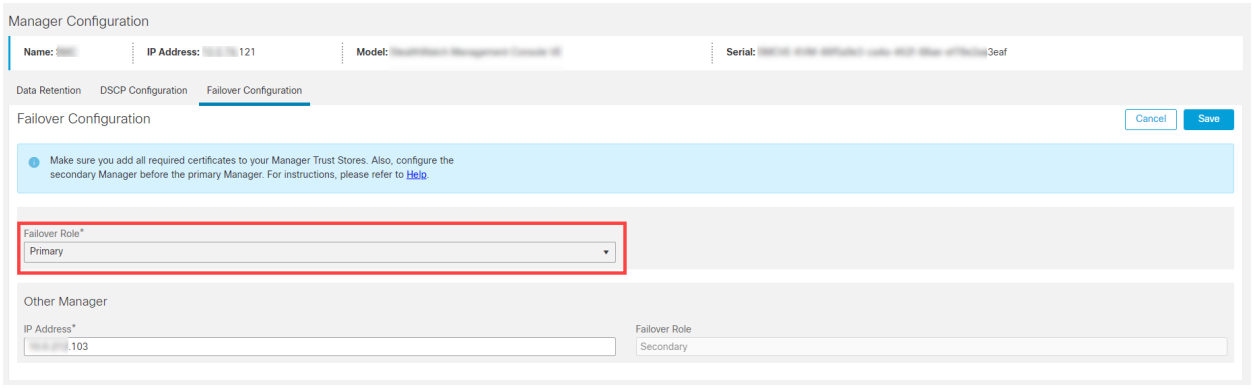
1. Log in to your **primary** Manager.
2. Select **Configure** > **GLOBAL Central Management**.
3. Confirm the Appliance Status for each appliance is shown as **Connected**.

    - **Managers:** If the appliance status for the primary or secondary Manager is shown as Config Channel Down, check your communication settings and refer to **Troubleshooting**.
    - **Other Appliances:** If the appliance status for the Flow Collectors, Flow Sensors, or UDP Directors is shown as Config Channel Down, check your configuration settings and use Central Management to reboot the appliance (••• **(Ellipsis) icon** > **Reboot Appliance**). For additional troubleshooting, refer to the Cisco Secure Network Analytics System Configuration Guide.



2. Review the Failover Roles

1. In the **primary** Manager, click the **Security Insight dashboard** tab.
2. From the main menu, select **Configure** > **GLOBAL Manager**.
3. Click the **Failover Configuration** tab.
4. Confirm the **Failover Role** is shown as **Primary**.



5. Log in to your **secondary** Manager. Follow steps 1 through 4 to confirm the **Failover Role** is shown as **Secondary**.

    - If the failover roles are correct for each Manager, keep the Failover Configuration tabs open on both Managers, and go to **3. Delete the Failover Configuration**.

- If both Managers are shown as secondary, update the failover configuration so you have one primary Manager and one secondary Manager before you proceed with deleting. For instructions, refer to **Changing Failover Roles**.

> ⚠ Make sure you follow the configuration order and instructions in **Changing Failover Roles**. For assistance, please contact Cisco Support.

3. Delete the Failover Configuration

Use the following instructions to delete failover configuration. Make sure you follow these instructions in order.

> ⚠ If you delete the failover configuration, all domain configuration data will be deleted from the secondary Manager.

1. Go to the **Failover Configuration** tab on the **primary** Manager.
2. Click **Delete**.
3. Follow the on-screen prompts to delete the failover configuration.

> ⚠ If you delete the failover configuration, all domain configuration data will be deleted from the secondary Manager.

4. Go to the **Failover Configuration** tab on the **secondary** Manager.
5. Click **Delete**.
6. Follow the on-screen prompts to delete the failover configuration.

4. Remove the Secondary Manager from Central Management

1. In the **primary** Manager, open Central Management.

   Select **Configure** > **GLOBAL Central Management**.

2. Locate the **secondary** Manager.

> ⚠ Confirm the IP address of the secondary Manager before you remove it.

3. Click the ••• (**Ellipsis**) icon. Select **Remove This Appliance**.
4. Follow the on-screen prompts to remove the secondary Manager from Central Management.

5. Delete the Secondary Manager Certificates

Use the following instructions to delete the secondary Manager certificates from the other appliance Trust Stores.

> ⚠ Confirm the IP address of the secondary Manager before you delete the certificates.

1. Return to Central Management in the primary Manager. Confirm the following:
   - The secondary Manager is no longer shown in inventory.
   - The Appliance Status for each appliance returns to Connected.
2. Click the ••• (**Ellipsis**) icon for the an appliance.
3. Select **Edit Appliance Configuration**.
4. Click the **General** tab. Locate the **Trust Store** section.
5. Locate the secondary Manager certificates.
6. Click **Delete** to remove each secondary Manager certificate from the Trust Store.
7. Repeat steps 2 though 6 on each appliance in Central Management.

6. Reset the Secondary Manager to Factory Defaults

To use the secondary Manager, reset the factory defaults. Follow the instructions in the Cisco Secure Network Analytics System Configuration Guide.

The procedure includes completing the following steps:

- Resetting the appliance to factory defaults.
- Configuring the IP address.
- Configuring the Manager using the Appliance Setup Tool.

Troubleshooting

Manager is Offline or Fails

Your primary Manager may go offline if the network is down, if you shut down the Manager and reboot it, or for other various reasons.

If your primary Manager goes offline because you rebooted it, it will resume the primary failover role when the appliance status returns to Connected and it detects the secondary Manager.

If the primary Manager role changes to secondary and does not resolve itself, review the following scenarios to determine what you need to do.

> For assistance, please contact Cisco Support.

If...	And...	Then...
The primary Manager fails or is shut down and rebooted,	You have manually promoted an existing secondary Manager to primary, and it is online,	The new primary Manager maintains its role as primary. When it reboots, the original primary Manager automatically assumes its new role as secondary.
The primary Manager fails or is shut down and rebooted,	You have not manually promoted an existing secondary Manager to primary, so there is no primary Manager online,	When you reboot the original primary Manager, both it and the original secondary Manager are in the secondary role. Promote one of them to be the primary Manager. For instructions, refer to **Changing Failover Roles**.
The network goes down and is restored,	You have manually promoted an existing secondary Manager to primary, and it is online,	The new primary Manager maintains its role as primary. When rebooted, the original primary Manager automatically assumes its new role as secondary.

If...	And...	Then...
The network goes down and is restored,	You have not manually promoted an existing secondary Manager to primary, so there is no primary Manager online,	The original primary Manager automatically resumes its role as primary, and the original secondary Manager automatically resumes its role as secondary Manager.

Trust Errors

If you receive an error that your Manager is not trusted, check the certificates in the Trust Store. Refer to **3. Add Certificates to Trust Stores** for instructions.

Flows Do Not Display on Secondary Manager

If the secondary Manager doesn't display flows, make sure the secondary Manager certificates are saved to the Flow Collector Trust Store. Refer to **3. Add Certificates to Trust Stores** for instructions.

Password Expiration

When the failover configuration is saved, the primary Manager pushes its local users and password credentials to the secondary Manager, so they are synchronized. This means you will use the same password to log in to your primary Manager and secondary Manager. To change the password on the secondary Manager, log in to your primary Manager.

If your primary Manager is down and the password expires, you cannot change your password using the secondary Manager. In this case, wait until the primary Manager appliance status returns to Connected so you can change your password.

- To reset your passwords to the default, refer to the Cisco Secure Network Analytics System Configuration Guide.
- If you need to reset factory defaults on your primary Manager, process a return merchandise authorization, or re-deploy it, you also need to reset factory defaults on your secondary Manager and then reconfigure the failover relationship. To reset factory defaults, refer to the Cisco Secure Network Analytics System Configuration Guide. For assistance, please contact Cisco Support.

Analytics jobs are lagging

In both of the following instances, the "Analytics performance has degraded" system alarm will be triggered.

The secondary Manager has been promoted to primary Manager

When you change the role of the primary Manager to that of the secondary Manager, and more than 5 hours has passed before the original primary Manager has been recovered and re-assigned to the primary role, the "Analytics performance has degraded" system alarm will be triggered. Analytics will recover and run the jobs that occurred during the last 6 hours, while the original primary Manager was down. Job performance will continue to lag until your system has processed all jobs from the last 6 hours and begins to process jobs in real time.

An appliance went down due to degradation

If your system is experiencing degradation (which is usually due to insufficient resources such as CPU or memory), jobs will begin to lag. If this lag exceeds 5 hours, then the "Analytics performance has degraded" system alarm will be triggered. At this point, results will be incomplete and unreliable.

A possible cause for this failure is that you have increased the flows per second beyond what is supported in your setup. To resolve this, either reduce the flows per second or increase the resources on the Manager, the Data Store, or both. If you cannot resolve the issue, contact Cisco Support.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	March 2, 2023	Initial Version.
1_1	December 20, 2023	Corrected cross reference for Configuring Your Failover Pair section.

Copyright Information