Cisco Stealthwatch

Failover Configuration Guide 7.3

Table of Contents

Introduction

Use the failover configuration to establish a failover relationship between two Stealthwatch Management Consoles (SMCs) so that one of them serves as a backup console to the other. If the primary SMC fails, you can manually set the secondary SMC to become the primary SMC to continue monitoring the system.

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

Before you Begin

Before you start the failover configuration, install your Stealthwatch appliances and complete the system configuration. For instructions, refer to your Stealthwatch installation guides and the Stealthwatch System Configuration Guide.

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

Security Analytics and Logging (On Premises)

If Security Analytics and Logging (On Prem) is enabled on one Stealthwatch Management Console (SMC), make sure it is enabled on the other SMC before you start the failover configuration.

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

Appliance Status

Before you start any configuration changes in Stealthwatch, make sure the appliance status is shown as Up. 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 the SMCs as the admin user.

Back up Configuration Files and Databases

Plan time to back up each SMC 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 SMC completely. For instructions, refer to **2. Back up SMC 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 SMC will actively monitor and manage your appliances, and your secondary SMC becomes read-only. To plan which SMC will be configured in the primary or secondary failover role, refer to **Saving the Failover Configuration** and **1. Plan Failover Roles**.

If your secondary SMC is managing appliances in Central Management, move them to your primary SMC (or another SMC) before you start the failover configuration. Refer to the Stealthwatch 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 SMC Trust Store before you add the appliance to Central Management.

Configuration Order

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

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

Saving the Failover Configuration

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

Primary SMC

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

Secondary SMC (Read-Only)

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

Passwords

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

Domain Changes

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

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

Flow Collectors

The Flow Collectors automatically send their data to both SMCs.

External Services

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

Changing Roles

If you need to promote your secondary SMC 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 SMC is offline, refer to **Troubleshooting** for more information.
- To change failover roles, refer to **Changing Failover Roles**.

Certificates

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

- The secondary SMC 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 SMC Trust Store when they are added to the primary SMC Central Management.

Restoring the Primary SMC

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

Rebooting the Primary SMC

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

- If the primary SMC 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 SMCs are configured for failover, delete the failover relationship before you change your SMC 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 SMC 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 SMC will be configured in the primary or secondary failover role.

- **IP Address:** Make sure you have the IP address of each SMC.
- **Secondary SMC:** If your secondary SMC is managing appliances in Central Management, move them to your primary SMC (or another SMC) before you start the failover configuration. Refer to the Stealthwatch 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 SMC Trust Store before you add the appliance to Central Management.

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

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

Planned Failover Role	Summary	IP Address
Primary SMC	Actively monitors and manages Stealthwatch	
Secondary SMC	Read-only	

2. Back up SMC Configuration and Databases

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

New Installations: If your SMCs 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 Stealthwatch Support.

1. Create a Backup Configuration File

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

1. Log in to your **secondary** SMC.
2. Click the **Global Settings** icon. Select **Central Management**.
3. Click the **Actions** menu for the SMC.
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 SMC. Repeat steps 2 through 8 to save the backup configuration file for your primary SMC.

2. Back up the SMC Databases

To back up the SMC database to a remote file system, you will use the Appliance Admin interface and the Desktop Client. You can switch between both interfaces as you complete the following procedures:

1. **Delete the Database Snapshots**
2. **Back up the Databases**
3. **Delete the Database Snapshots**
4. **Confirm Database Backup**

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

1. Delete the Database Snapshots

Before you create backup files, make sure you delete any saved snapshots on the SMC database using the following instructions.

> ⚠ Make sure you delete the SMC database snapshots. This step is critical for a successful backup.

1. Log in to the SMC appliance 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 SMC database snapshots.

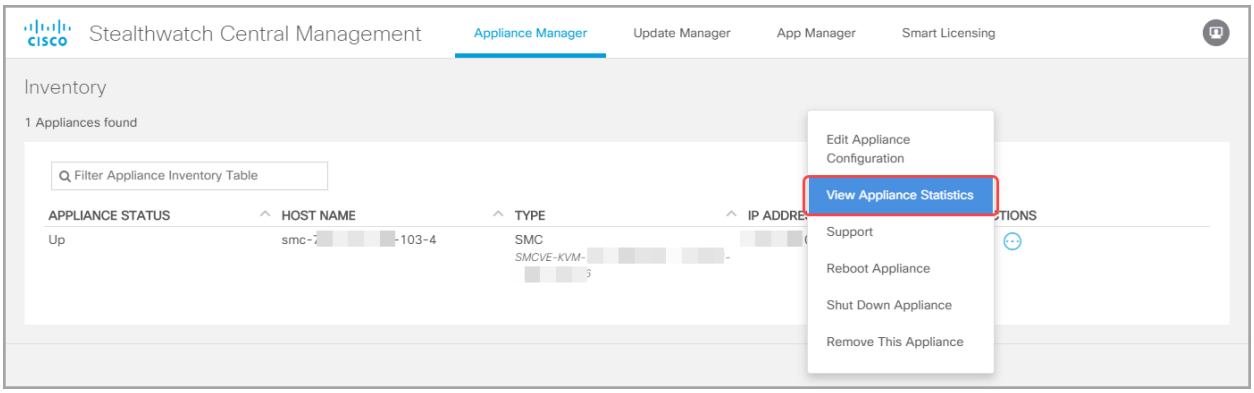
2. Back up the Databases

Use the following instructions to back up your SMC 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 the SMC Appliance Admin interface (but do not close the Desktop Client).

   In Central Management, click the SMC **Actions** menu > **View Appliance Statistics**.



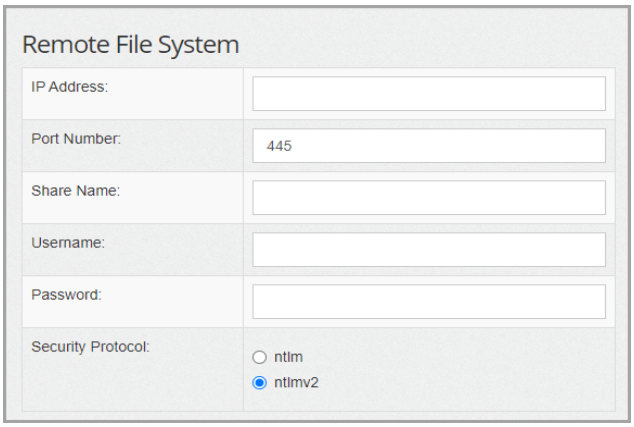
2. Determine how much space you will need on the remote file system to store the database backup as follows:

   - 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 Stealthwatch 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 Stealthwatch 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.

   File sharing appears to be properly configured.

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 **3. Delete the Database Snapshots** for instructions.

3. Delete the Database Snapshots

After you have saved the backup files, use the following instructions to delete the snapshots on the SMC database.

> Make sure you delete the SMC database snapshots.

1. Log in to the SMC appliance 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 SMC database snapshots.

4. Confirm Database Backup

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

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

2. Add Certificates to the SMC Trust Stores

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

1. Log in to the SMC.
2. Click the **Global Settings** icon. Select **Central Management**.
3. Confirm the Appliance Status is shown as Up.
4. Click the **Actions** menu for the SMC.
5. Select **Edit Appliance Configuration**.
6. On the **Appliance Manager** > **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 SMC, add the primary SMC certificates.
    - If you are logged in to the primary SMC, add the secondary SMC certificates.
12. Click **Apply Settings**. Follow the on-screen prompts.
13. **Up:** On the Appliance Manager page, confirm the Appliance Status returns to Up.
14. Repeat steps 1 through 13 on the other SMC.

4. Configure the Failover Pair

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

Before you Begin

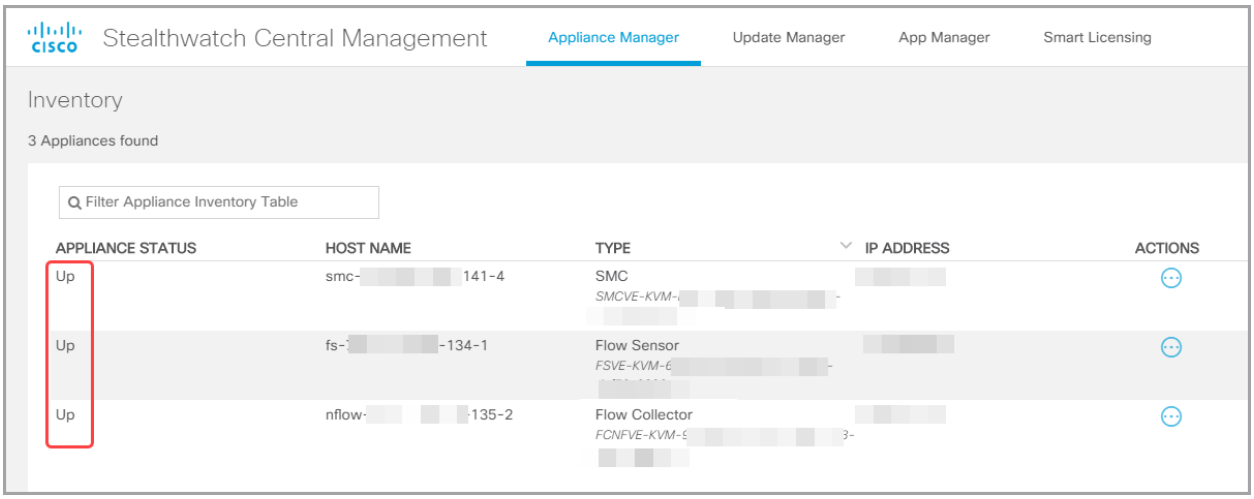
Make sure you complete the following procedures before you start these instructions:

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

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

1. Confirm SMC Appliance Status

1. Log in to the **primary** SMC.
2. Click the **Global Settings** icon. Select **Central Management**.
3. Confirm the Appliance Status for each appliance is shown as **Up**.

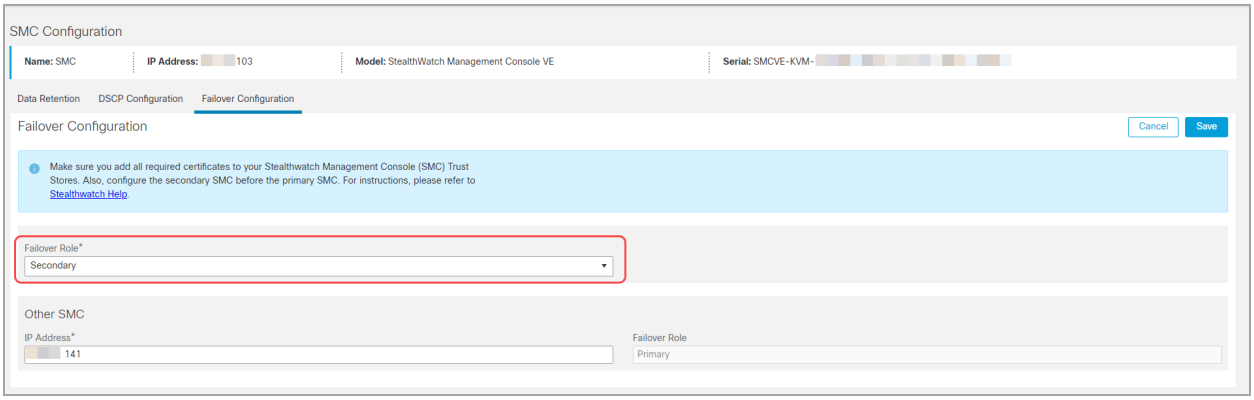


4. Log in to the **secondary** SMC.
5. Click the **Global Settings** icon. Select **Central Management**.
6. Confirm the Appliance Status is shown as **Up**.
7. Stay logged in to both SMCs, and go to the next procedure.

2. Configure the Secondary SMC

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

1. In the **secondary** SMC, click the **Security Insight Dashboard** tab.
2. Click the **Global Settings** icon.
3. Select **SMC Configuration**.
4. Click the **Failover Configuration** tab.
5. Click the **Failover Role** drop-down menu. Select **Secondary**.

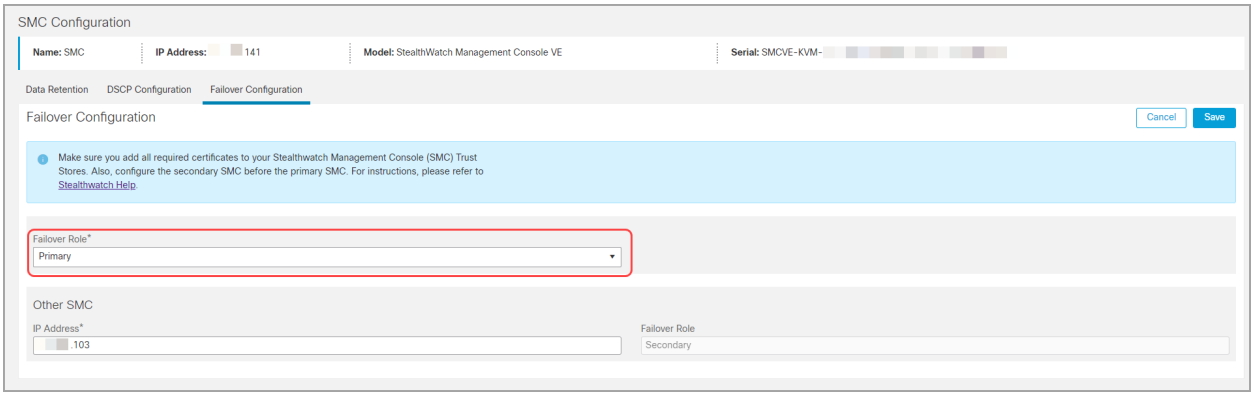


6. In the **IP Address** field, enter the IP address of your other SMC. This will be your primary SMC.
7. Click **Save**.
8. Follow the on-screen prompts to save your changes.

3. Configure the Primary SMC

1. In the **primary** SMC, click the **Security Insight Dashboard** tab.
2. Click the **Global Settings** icon.
3. Select **SMC Configuration**.

4. Click the **Failover** tab.
5. Click the **Failover Role** drop-down menu. Select **Primary**.



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

5. Confirm the Failover Configuration

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

1. Confirm Configuration Changes

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

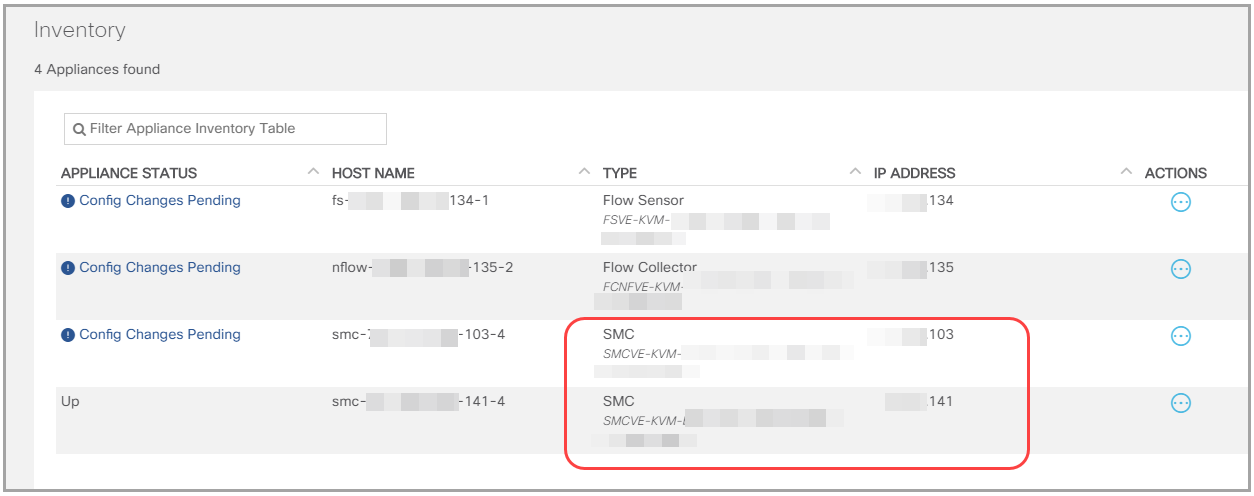
1. In the primary SMC, open Central Management.

   Click the **Global Settings** icon. Select **Central Management**.

2. Confirm the following:

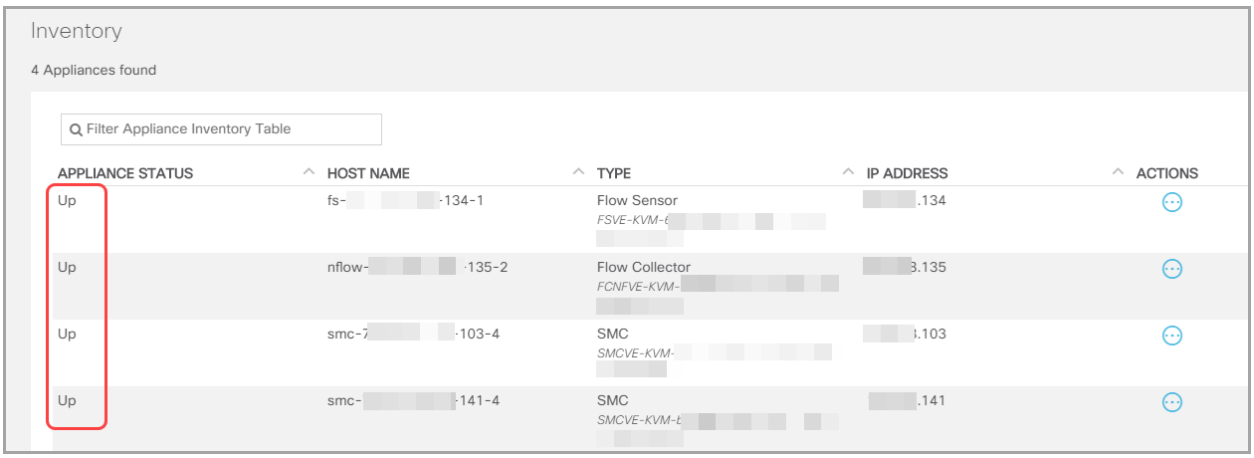
   - The secondary SMC is shown in the inventory.
   - The Appliance Status for each appliance is shown as Up.

Confirming the Primary and Secondary SMC are Shown



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

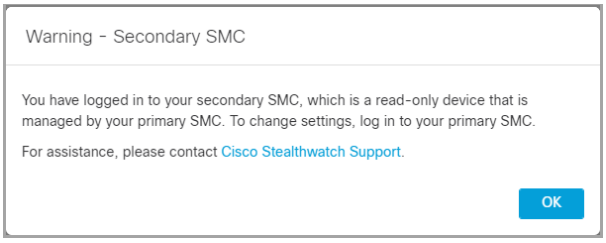
Confirming All Appliances are Up



2. Confirm Flow Collection

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

1. Log in to the **secondary SMC**.
2. You should see a notification that your SMC is read-only. If your secondary SMC 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 SMC in the following order (or refer to **Troubleshooting**):

   - Log in to the primary SMC.
   - Click the **Global Settings** icon. Select **Central Management**.
   - Locate the Flow Collector.
   - Click the **Actions** menu.
   - Select **Reboot Appliance**. Follow the on-screen prompts.
   - **Flow Collectors:** Repeat these steps to reboot every Flow Collector in Central Management.
   - **Secondary SMC:** Repeat these steps to reboot your secondary SMC.

> ⚠ If your primary SMC goes offline because you rebooted it, it will resume the primary failover role when the appliance status returns to Up and it detects the secondary SMC. If the primary SMC 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 SMC roles. Please note that they do not swap roles automatically.

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

Time

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

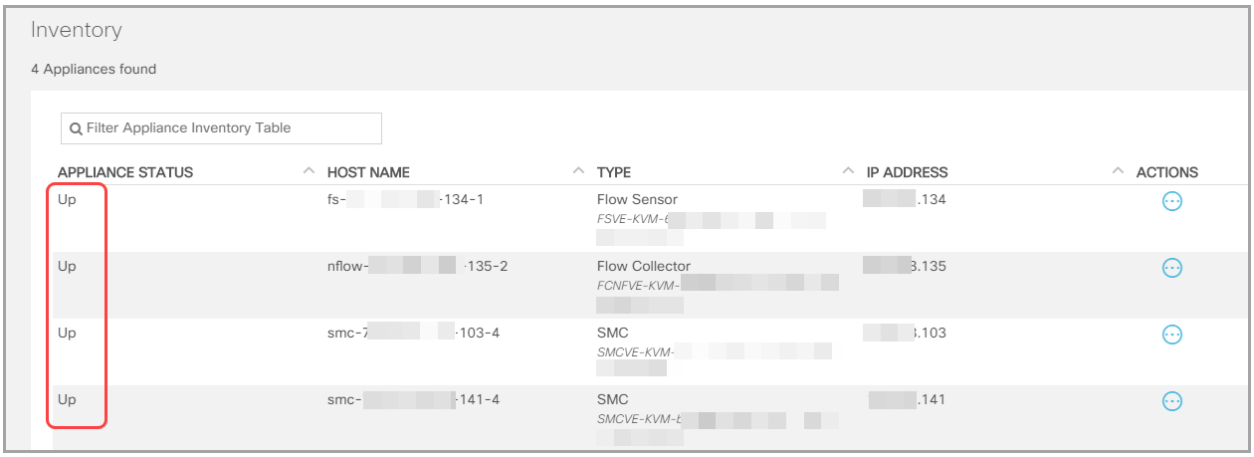
1. Back up the Primary SMC

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

2. Confirm the Appliance Status

1. Log in to the primary SMC.
2. Click the ⚙ **Global Settings** icon. Select **Central Management**.
3. Confirm the Appliance Status for each appliance is shown as **Up**.

    - **SMCs:** If the appliance status for the primary or secondary SMC 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, UDP Directors, or Endpoint Concentrators is shown as Config Channel Down, check your configuration settings and use Central Management to reboot the appliance (**Actions** menu > **Reboot Appliance**) . For additional troubleshooting, refer to the Stealthwatch System Configuration Guide.



3. Change the Failover Configuration

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

In this configuration, your primary SMC becomes the secondary SMC, and its domain configuration is deleted. It will become read-only and synchronize with the newly-promoted primary SMC. 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 SMC to Secondary

1. In the current **primary** SMC, click the **Security Insight Dashboard** tab.
2. Click the **Global Settings** icon.
3. Select **SMC Configuration**.
4. Click the **Failover Configuration** tab.
5. Confirm the **Failover Role** is shown as **Primary**.

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

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

2. Change the Secondary SMC to Primary

1. Log in to the **secondary** SMC.
2. Click the **Global Settings** icon.
3. Select **SMC Configuration**.
4. Click the **Failover Configuration** tab.
5. Confirm the **Failover Role** is shown as **Secondary**.
6. Click the **Failover Role** drop-down menu. Select **Primary**.
7. Click **Save**.
8. 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 SMCs 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 SMC. Make sure you follow all instructions in order.

1. Delete the Failover Configuration

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

2. Change SMC 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 Stealthwatch 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 SMC Failover

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

Deleting the Failover Configuration

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

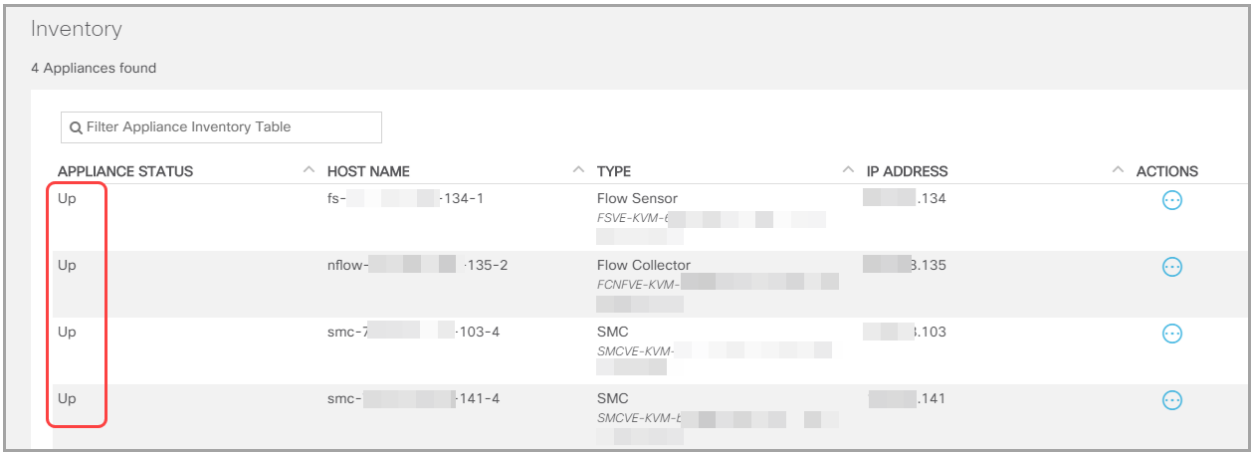
> ⚠ If you delete the failover configuration, all domain configuration data will be deleted from the secondary SMC.

1. Confirm Appliance Status

Before you start, confirm the primary SMC shows the secondary SMC as a managed appliance, and confirm both SMCs are shown as Up.

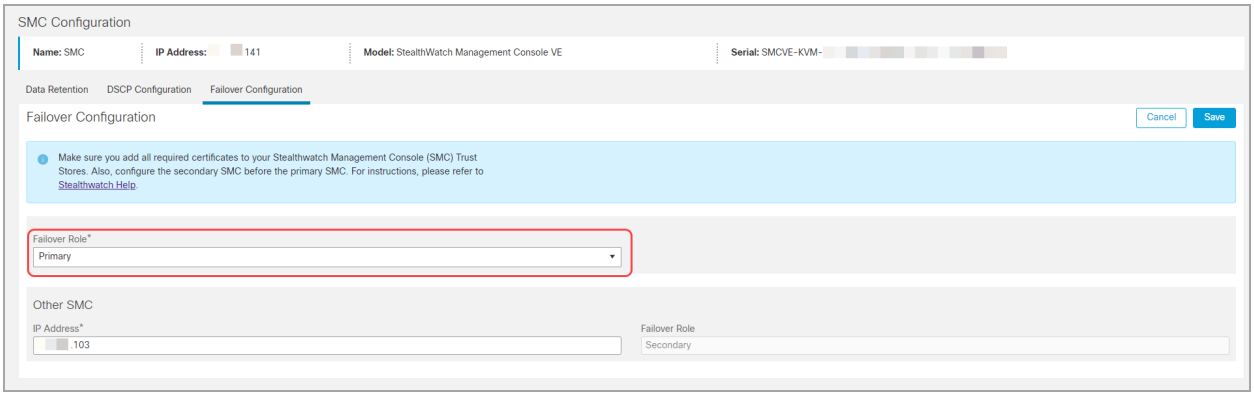
1. Log in to the **primary** SMC.
2. Click the **Global Settings** icon. Select **Central Management**.
3. Confirm the Appliance Status for each appliance is shown as **Up**.

   - **SMCs:** If the appliance status for the primary or secondary SMC 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, UDP Directors, or Endpoint Concentrators is shown as Config Channel Down, check your configuration settings and use Central Management to reboot the appliance (**Actions** menu > **Reboot Appliance**) . For additional troubleshooting, refer to the Stealthwatch System Configuration Guide.



2. Review the Failover Roles

1. In the **primary** SMC, click the **Security Insight Dashboard** tab.
2. Click the **Global Settings** icon. Select **SMC Configuration**.
3. Click the **Failover Configuration** tab.
4. Confirm the **Failover Role** is shown as **Primary**.



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

   - If the failover roles are correct for each SMC, keep the Failover Configuration tabs open on both SMCs, and go to **3. Delete the Failover Configuration**.
   - If both SMCs are shown as secondary, update the failover configuration so you have one primary SMC and one secondary SMC 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 Stealthwatch 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 SMC.

1. Go to the **Failover Configuration** tab on the **primary** SMC.
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 SMC.

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

4. Remove the Secondary SMC from Central Management

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

   Click the **Global Settings** icon. Select **Central Management**.

2. Locate the **secondary** SMC.

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

3. Click the **Actions** menu. Select **Remove This Appliance**.
4. Follow the on-screen prompts to remove the secondary SMC from Central Management.

5. Delete the Secondary SMC Certificates

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

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

1. Return to Central Management in the primary SMC. Confirm the following:

   - The secondary SMC is no longer shown in inventory.
   - The Appliance Status for each appliance returns to Up.

2. Click the **Actions** menu for the an appliance.
3. Select **Edit Appliance Configuration**.

4. Click the **General** tab. Locate the **Trust Store** section.
5. Locate the secondary SMC certificates.
6. Click **Delete** to remove each secondary SMC certificate from the Trust Store.
7. Repeat steps 2 though 6 on each appliance in Central Management.

6. Reset the Secondary SMC to Factory Defaults

To use the secondary SMC, reset the factory defaults. Follow the instructions in the Stealthwatch System Configuration Guide.

The procedure includes completing the following steps:

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

Troubleshooting

SMC is Offline or Fails

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

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

If the primary SMC 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 Stealthwatch Support.

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

If...	And...	Then...
and is restored,	promoted an existing secondary SMC to primary, so there is no primary SMC online,	automatically resumes its role as primary, and the original secondary SMC automatically resumes its role as secondary SMC.

Trust Errors

If you receive an error that your SMC 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 SMC

If the secondary SMC doesn't display flows, make sure the secondary SMC 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 SMC pushes its local users and password credentials to the secondary SMC, so they are synchronized. This means you will use the same password to log in to the primary SMC and secondary SMC. To change the password on the secondary SMC, log in to the primary SMC.

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

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

Contacting Support

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

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch 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

Copyright Information