# Cisco Secure Network Analytics

SSL/TLS Certificates for Managed Appliances 7.4.1

# Table of Contents

# Introduction

Use this guide to change SSL/TLS certificate-related configurations on your Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.1 appliances:

- Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console)
- Cisco Secure Network Analytics Flow Collector
- Cisco Secure Network Analytics Flow Sensor
- Cisco Secure Network Analytics UDP Director

For details, refer to **Overview**.

## Data Store

This guide does not include Cisco Secure Network Analytics Data Store information. Please contact Cisco Support for assistance.

## DoDIN and Common Criteria Compliance

To configure Secure Network Analytics for the Department of Defense Information Network (DoDIN) or Common Criteria (CC) compliance, follow the instructions in the *DoDIN Military Unique Deployment Guide* or the *Common Criteria Administrative Guide*.

## Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for installing and configuring Secure Network Analytics products. We assume you have familiarity with SSL/TLS certificates. For assistance, please contact Cisco Support.

## Terminology

This guide uses the term “**appliance**” for any Secure Network Analytics product, including virtual products such as the Flow Sensor Virtual Edition (VE).

A "**cluster**" is your group of Secure Network Analytics appliances that are managed by the Manager).

## Planning Time

It is important to configure Secure Network Analytics at a time that will cause the least amount of disruption. The procedures in this guide may include installing certificates, changing configuration settings, and rebooting. During these changes, the system will be unavailable and you may experience network connection problems. For assistance, please contact Cisco Support.

## Best Practices

- **Review Procedures:** Before you get started, review the procedures to make sure you understand the requirements and instructions. Also, make sure you follow the instructions in order.
- **Rebooting:** Do not force the appliance to reboot while it is restarting or making configuration changes.
- **One at a Time:** Configure one appliance at a time. Make sure the Appliance Status is shown as **Connected** before you start the next appliance configuration.
- **Friendly Names:** If you are replacing the appliance identity certificates, adding client identity certificates, or adding certificates to the trust stores, make sure each friendly name is unique. Do not duplicate any friendly names.
- **Removing/Adding Appliances:** Many procedures in this guide include removing your appliances from Central Management temporarily. Make sure you follow the order and instructions for removing appliances from Central Management and adding them back to Central Management (using the Appliance Setup Tool).

  **Managers:** If you are changing the host information or appliance identity certificates on the Manager, you will need to remove all appliances from Central Management (in the order shown), and then rebuild your cluster after you've made changes.

  **Non-Manager Appliances:** If you are changing the host information or appliance identity certificate for an individual, non-Manager appliance (Flow Collectors, Flow Sensors, or UDP Directors), you will only need to remove the individual appliance from Central Management and then add it back to Central Management after you've made your changes.

# Appliance Identity Certificates

Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate.

## Authentication

The communication of the appliances in your Secure Network Analytics cluster is authenticated using x.509v3 certificates.

## Certificate Requirements

You can replace a Secure Network Analytics default appliance identity certificate with an appliance identity certificate from a Certificate Authority.

- Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.
- You can choose to generate a Certificate Signing Request (CSR) in Central Management or skip the CSR if you already have certificates from a Certificate Authority. If you generate the CSR in Central Management, the listed requirements are included in the CSR.

| **Requirements** | **Generate CSR<br>in Central Management** | **Skip CSR<br>in Central Management** |
|---|---|---|
| Format | PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks)<br>If you use PEM, refer to **PEM Chain File Requirements**. | PKCS#12 (.p12, .pfx, .pks) |
| RSA Key Length | 4096 bits or 8192 bits | 2048 bits (not recommended) or more |
| Authentication<br>(Extended Key Usage) | The CSR requests server (serverAuth) and client (clientAuth) authentication. | Server (serverAuth) and client (clientAuth) authentication are required for appliance identity certificates. |
| Date Range | Make sure the certificate dates are current and not expired. | Make sure the certificate dates are current and not expired. |

## Appliance Setup Tool

When you add an appliance to Central Management using the Appliance Setup Tool, the appliance identity certificate is replaced automatically with a Secure Network Analytics default appliance identity certificate.

⚠ If your appliance uses custom certificates, make sure they are saved so you can replace the default appliance identity with your custom certificate after you add it to Central Management. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

## Manager Failover

If your Managers are configured as a failover pair, you may need to delete the failover relationship and reconfigure it, depending on the certificates procedure. Make sure you review the instructions for the procedure you choose.

# Client Identity Certificates

The client identity is used for communication between external services. Refer to **Adding SSL/TLS Client Identities** for instructions.

## Certificate Requirements

If you add a client identity certificate to the Manager, make sure you have certificates from a Certificate Authority.

- Refer to **Adding SSL/TLS Client Identities** for instructions.
- You can choose to generate a Certificate Signing Request (CSR) in Central Management or skip the CSR if you already have certificates from a Certificate Authority. Refer to the table to confirm your certificates meet the requirements. If you generate the CSR in Central Management, the listed requirements are included in the CSR.

| Requirements | Generate CSR in Central Management | Skip CSR in Central Management |
|---|---|---|
| Format | PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks)<br>If you use PEM, refer to **PEM Chain File Requirements**. | PKCS#12 (.p12, .pfx, .pks) |
| RSA Key Length | 2048 bits (not recommended), 4096 bits, or 8192 bits | 2048 bits (not recommended) or more |
| Authentication<br>(Extended Key Usage) | The CSR requests server (serverAuth) and client (clientAuth) authentication. | Client (clientAuth) authentication is required for client identity certificates. |
| Date Range | Make sure the certificate dates are current and not expired. | Make sure the certificate dates are current and not expired. |

## PEM Chain File Requirements

If you replace the appliance identity certificate or add a client identity certificate to the Manager using Certificate Authority (CA) certificates with PEM format, we recommend uploading the CA certificate chain file as part of the instructions. Your chain file includes the root and intermediate certificates.

Make sure your chain file meets the following requirements:

- **Contents:** Make sure the chain file includes all signing certificates and the Certificate Authority certificate. Do not include the identity certificate in the chain file upload.
- **Order:** If you build the certificate chain manually, build the certificates in descending order, so the last intermediate certificate is first in the file, followed by the remaining intermediate certificates in descending order. Your root certificate is last in the file order.

  For example:

  – BEGIN CERTIFICATE –

  Intermediate Certificate #3

  – END CERTIFICATE –

  – BEGIN CERTIFICATE –

  Intermediate Certificate #2

  – END CERTIFICATE –

  – BEGIN CERTIFICATE –

  Intermediate Certificate #1

  – END CERTIFICATE –

  – BEGIN CERTIFICATE –

  **Root CA Certificate**

  – END CERTIFICATE –

> When you upload the chain file to replace the appliance identity, you will upload the chain as one file. When you upload the chain file to the trust stores, you will upload each part of the chain individually. Make sure you follow the instructions in the procedure you choose.

# Trust Store Requirements

Many procedures in this guide require adding or deleting certificates in the appliance trust stores in a specific order. These steps are critical for system communication. When you save a certificate to the appliance trust store, the appliance trusts the identity and allows communication with it. The certificates and requirements are determined by the Certificate Authority.

When you upload appliance identity certificates and client identity certificates to the trust stores, make sure you upload the following certificates:

- identity
- chain (root and intermediate certificates)

**If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one file.

**Friendly Names:** If you are adding certificates to the trust stores, make sure each friendly name is unique. Do not duplicate any friendly names.

## Wild Card Certificates (Client Identity Only)

If you updated the appliance to 7.x and have a client identity wild card certificate installed in the trust store from an earlier version of Secure Network Analytics (formerly Stealthwatch), the wild card certificate can be used until it expires. New wild card certificates are only supported if you skip the CSR step in Central Management.

# Additional Certificate Configurations

This guide covers appliance identity and client identity configurations. There may be additional configurations in Secure Network Analytics that involve certificates and requirements for server identity verification. Make sure you follow the instructions in the help or guide for the feature.

- **Audit Log Destination:** Follow the instructions in the Help. Select 👤 (**User**) icon and search "Audit Log Destination."
- **Cisco ISE or Cisco ISE-Pic:** Follow the instructions in the ISE and ISE-PIC Configuration Guide.
- **LDAP:** Follow the instructions in the Help. Select ⚙ (**Global Settings**) icon and search "LDAP."

- **Packet Analyzer:** Follow the instructions in the Help. Select ⚙ (**Global Settings**) icon and search "Packet Analyzer."
- **SAML SSO:** Follow the instructions in the System Configuration Guide.
- **SMTP Configuration for Response Management:** Follow the instructions in the Help. Select 👤 (**User**) icon and search "SMTP Configuration."

> ℹ For additional configuration guides, refer to Configuration Guides.

## Opening Central Management

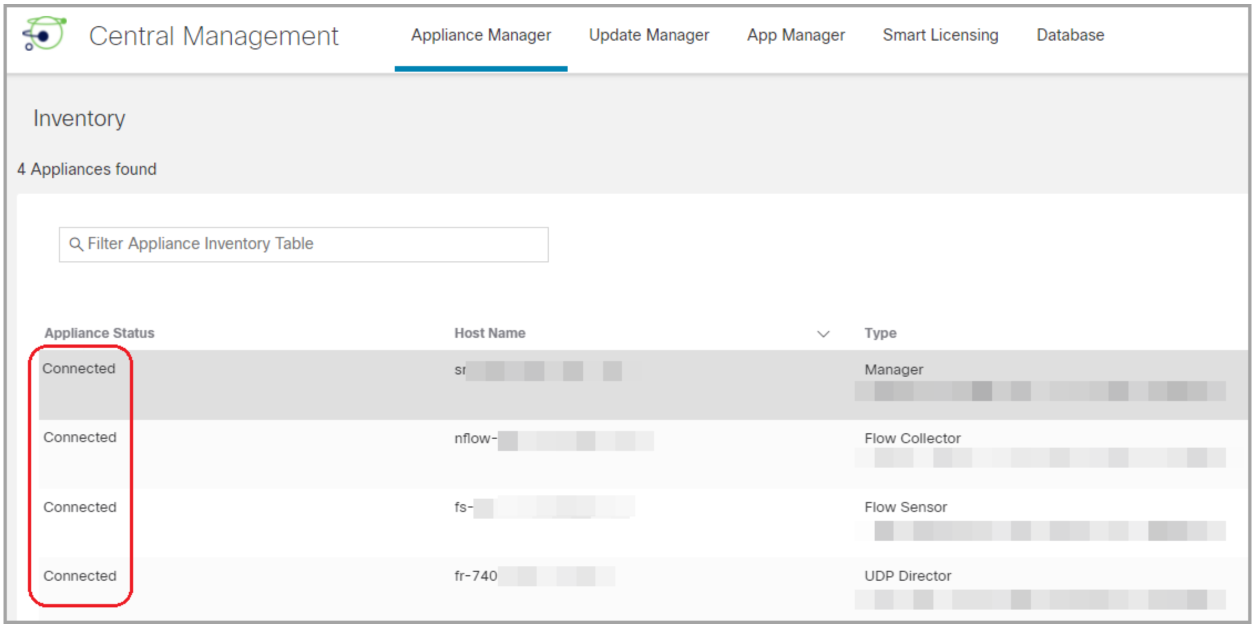
You will primarily use Central Management in this guide.

1. Log in to the appliance as admin: https://<IPAddress>
2. Click the ⚙ (**Global Settings**) icon.
3. Choose **Central Management**.

## Confirming the Appliance Status is Connected

Configure one appliance at a time. As you add appliances to Central Management or make configuration changes, the appliance status changes from **Initializing** or **Config Channel Pending** to **Connected**.

Check the **Appliance Status** column. Make sure the appliance status for all appliances in Central Management is shown as Connected before you proceed with any other changes.



Inventory

4 Appliances found

| Appliance Status | Host Name | Type |
|---|---|---|
| Connected | sr[redacted] | Manager<br>[redacted] |
| Connected | nflow-[redacted] | Flow Collector<br>[redacted] |
| Connected | fs-[redacted] | Flow Sensor<br>[redacted] |
| Connected | fr-740[redacted] | UDP Director<br>[redacted] |

# Overview

Certificates are involved with several configuration changes in Secure Network Analytics. When you choose a procedure, review it to understand the certificates requirements and instructions before you start.

⚠ Your certificates are critical for your system’s security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss.

| Tasks | Notes |
|---|---|
| Reviewing Certificates | Review the appliance identity certificate or client identity certificates installed on the selected appliance. |
| Saving Certificates | Save the appliance identity certificate. |
| Downloading Cisco Bundles | |
| Changing the Certificate Validity Period | If you have Secure Network Analytics v7.4 installed on your appliances, you can update the validity period on expired or unexpired Cisco default appliance identity certificates, and the appliance host information (IP address, host name, domain name) will be preserved.<br>If your appliances use custom certificates from a Certificate Authority, refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions. |
| Replacing the Appliance Identity Certificate | Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate. Follow the instructions to |

| | |
|---|---|
| | replace the appliance identity certificate with a certificate from a Certificate Authority. |
| Changing the Host Name | Change the appliance host name on appliances that use Cisco default certificates.<br>If your appliance uses a custom certificate, please contact Cisco Support to change these settings. |
| Changing the Network Domain Name | Change the network domain name on appliances that use Cisco default certificates.<br>If your appliance uses a custom certificate, please contact Cisco Support to change these settings. |
| Changing the IP address (eth0) | Change the IP address (eth0 network interface) on appliances that use Cisco default certificates. This section also includes instructions to change eth1 or eth2, etc. in Central Management.<br>If your appliance uses a custom certificate, please contact Cisco Support to change these settings. |
| Client Identity Certificates | The client identity is used for communication between external services. If your Secure Network Analytics appliance uses an external service, follow the instructions to add the required client identity certificates. |
| Troubleshooting | |

# Reviewing Certificates

Use the following instructions to review the appliance identity certificate or client identity certificates for the selected appliance.

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. Choose the **Appliance** tab.
5. **To review the appliance identity certificate,** go to the SSL/TLS Appliance Identity section.

   **To review the client identity certificates,** go to the Additional SSL/TLS Client Identities section.

# Saving Certificates

Use the following instructions to save your current appliance identity certificate. It is helpful to save the certificate before making any changes in case you need to restore defaults.

> ⓘ 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. Log in to the appliance.
2. 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

3. 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 or method.

# Downloading Cisco Bundles

Cisco periodically releases bundles of pre-validated digital certificates of a select number of root certificate authorities (CAs). We release these bundles as common appliance patch SWU files that apply to all Secure Network Analytics appliances (v7.3.1 and later).

Each patch includes a core certificate bundle and an external certificate bundle, which are used for connecting to Cisco services and to non-Cisco services. We also provide a readme file with the patch that provides information on the contents of each bundle.

You can download these bundles and readme files on Software Central at https://software.cisco.com.

- You are required to have the latest Cisco Bundle patch installed on all your appliances.
- If you RefreshImage for an appliance, the Cisco Bundle patches are not reapplied, and the certificate bundles will be reverted to the certificate bundles that were shipped with the release. You will need to update to the latest bundle.

## Certificate Check in Updates

When you upgrade Secure Network Analytics, it includes a certificate check to verify the Cisco Bundles upgrade will not cause issues with your environment. If only the end-entity certificate is present in the trust store, the upgrade will fail. Make sure the Central Management trust store has the full chain of certificates. For more information and instructions, refer to the System Update Guide.

⚠ If you do not have the full chain of certificates added to the Central Manager trust store, the system update will fail. Refer to the System Update Guide for more information.

# Changing the Certificate Validity Period (Overview)

Choose the a method to update your certificate validity period depending on the type of certificates your appliances use and if they are already expired.

| Certificates | Instructions |
|---|---|
| Unexpired Cisco Default Certificates | Refer to **Replacing Unexpired Cisco Default Certificates** for instructions.<br>If you need to change the host information in addition to the validity period, use the instructions in **Changing Network Interfaces** or **Changing the Host Name or Network Domain Name**. |
| Expired Cisco Default Certificates | Refer to **Replacing Expired Cisco Default Certificates** for instructions.<br>If you need to change the host information in addition to the validity period, use the instructions in **Changing Network Interfaces** or **Changing the Host Name or Network Domain Name**. |
| Custom SSL/TLS Certificates | If your appliances use custom certificates from a Certificate Authority, refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions. |

ⓘ We do not support regenerating certificates if you have custom SSL/TLS certificates installed on your appliances. However, you can replace custom certificates using **Replacing the SSL/TLS Appliance Identity Certificate**.

# Replacing Unexpired Cisco Default Certificates

Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate. Use the following instructions to change the validity period on your **unexpired** appliance identity certificates.

- **Host Information:** The appliance host information (IP address, host name, domain name) is preserved. If you need to change the host information in addition to the validity period, use the instructions in **Changing Network Interfaces** or **Changing the Host Name or Network Domain Name** (instead of the instructions in this section).
- **Custom Certificates:** We do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

> If your certificates have expired, refer to **Replacing Expired Cisco Default Certificates**. If your appliances use custom certificates from a Certificate Authority, refer to **Replacing the SSL/TLS Appliance Identity Certificate**.

## Requirements

Before you get started, review the **Best Practices** in the Introduction, and confirm the following requirements:

- **Users:** You need **admin** and **sysadmin** user access.
- **Manager Failover:** If you are updating your Manager certificates and your Managers are configured as a failover pair, delete the failover relationship before you start these procedures. For instructions, refer to the Failover Configuration Guide. When you delete the failover pair, the secondary Manager is removed from the cluster. The instructions include resetting the secondary Manager to factory defaults.

## Select the Procedure for your Appliance

- **Manager and Managed Appliances:** Use **Manager and Managed Appliances** to change the certificate validity period for the Manager and other managed appliances in your cluster. As part of the procedure, you will remove all appliances from Central Management (in the order shown), and then rebuild your cluster after you've made your changes.

- **Individual, Non- Manager Appliance:** Use **Individual, Non-Manager Appliances** to change the certificate validity period for an individual, non-Manager appliance (Flow Collectors, Flow Sensors, or UDP Directors). In this procedure, you will only remove the individual appliance from Central Management and then add it back to Central Management after you've made your changes.

# Manager and Managed Appliances

Use these instructions to change the certificate validity period for the Manager and other managed appliances in your cluster. Make sure you remove appliances from Central Management and add them back in the specified order.

**Manager Failover:** If your Managers are configured as a failover pair, delete the failover relationship before you start these procedures. For instructions, refer to the Failover Configuration Guide. When you delete the failover pair, the secondary Manager is removed from the cluster. The instructions include resetting the secondary Manager to factory defaults.

> ⚠ The appliance identity certificate is replaced automatically as part of this procedure.
>
> **If your appliance uses a custom certificate,** we do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

## Overview

The overall steps are as follows:

1. **Review the Appliance Status**
2. **Remove Appliances using Central Management**
3. **Remove Appliances using System Configuration**
4. **Regenerate the Certificates**
5. **Register your Manager in Central Management**
6. **Add Appliances to Central Management**
7. **Delete Outdated Certificates from the Trust Stores**
8. **Configure the Manager Failover Pair**

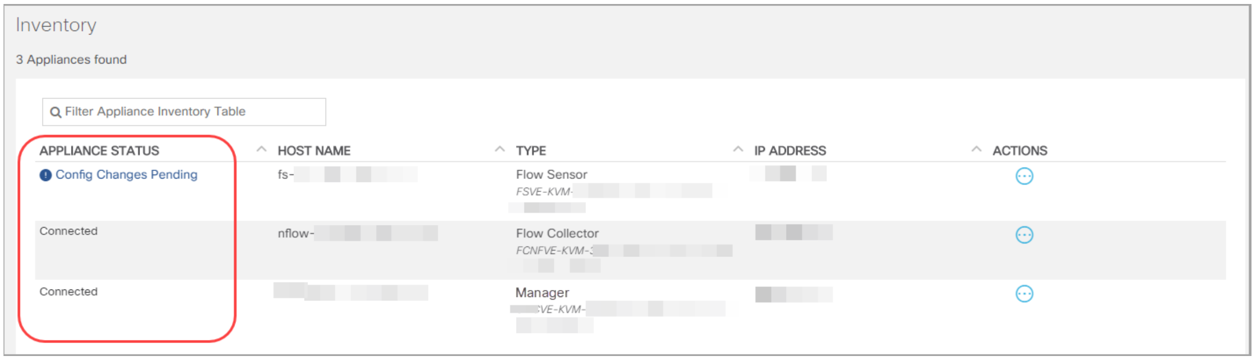
> ⓘ If you only need to change the Manager, you still need to remove all appliances from Central Management. If you only need to change an individual, non-Manager appliance, refer to **Individual, Non-Manager Appliances**.

## 1. Review the Appliance Status

Make sure all appliances are shown as Connected before you remove them from Central Management.

1. Log in to your primary Manager.
2. Click the ⚙ (**Global Settings**) icon.
3. Choose **Central Management**.
4. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.

   If an appliance status is shown as **Config Channel Down** or **Config Changes Pending**, wait a few minutes until it returns to Connected. If it does not resolve, you will remove the appliance from Central Management using **2. Remove Appliances using Central Management**. Then, complete the procedure in **3. Remove Appliances using System Configuration**.



Inventory

3 Appliances found

Filter Appliance Inventory Table

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Config Changes Pending | fs-[redacted] | Flow Sensor<br>FSVE-KVM-[redacted] | [redacted] | ⋯ |
| Connected | nflow-[redacted] | Flow Collector<br>FCNFVE-KVM-[redacted] | [redacted] | ⋯ |
| Connected | [redacted] | Manager<br>[redacted]VE-KVM-[redacted] | [redacted] | ⋯ |

## 2. Remove Appliances using Central Management

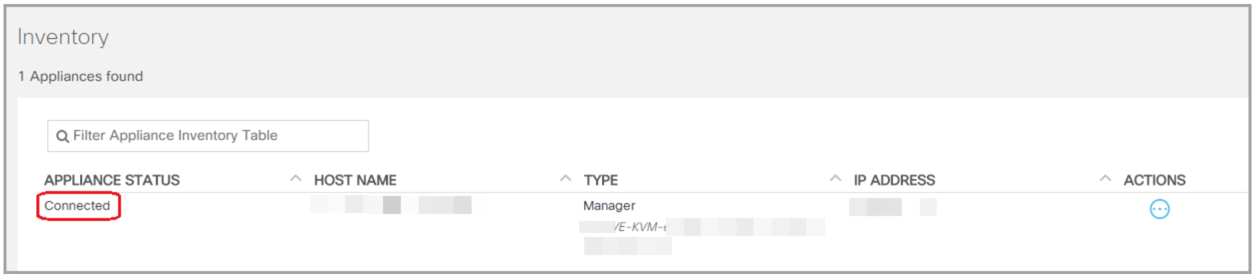
Use the following instructions to remove your appliances from Central Management. Make sure you remove all appliances from Central Management in the specified order.

Remove the Manager from Central Management last.

1. Remove every appliance **(except the primary Manager)** from Central Management:
   - Click the ⋯ (**Ellipsis**) icon for an appliance.
   - Choose **Remove This Appliance**.

When you remove an appliance from Central Management, the Manager appliance status transitions from Config Changes Pending to Connected.

2. Confirm the Manager appliance status is shown as **Connected** and that there are no other appliances in Central Management.



Inventory

1 Appliances found

Filter Appliance Inventory Table

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

3. Remove the primary Manager from Central Management.
   - Click the ••• (**Ellipsis**) icon
   - Choose **Remove This Appliance**.

## 3. Remove Appliances using System Configuration

If an appliance was shown as **Config Channel Down** or **Config Changes Pending** in Central Management and does not resolve, make sure you complete this procedure.

**Requirements:** sysadmin user

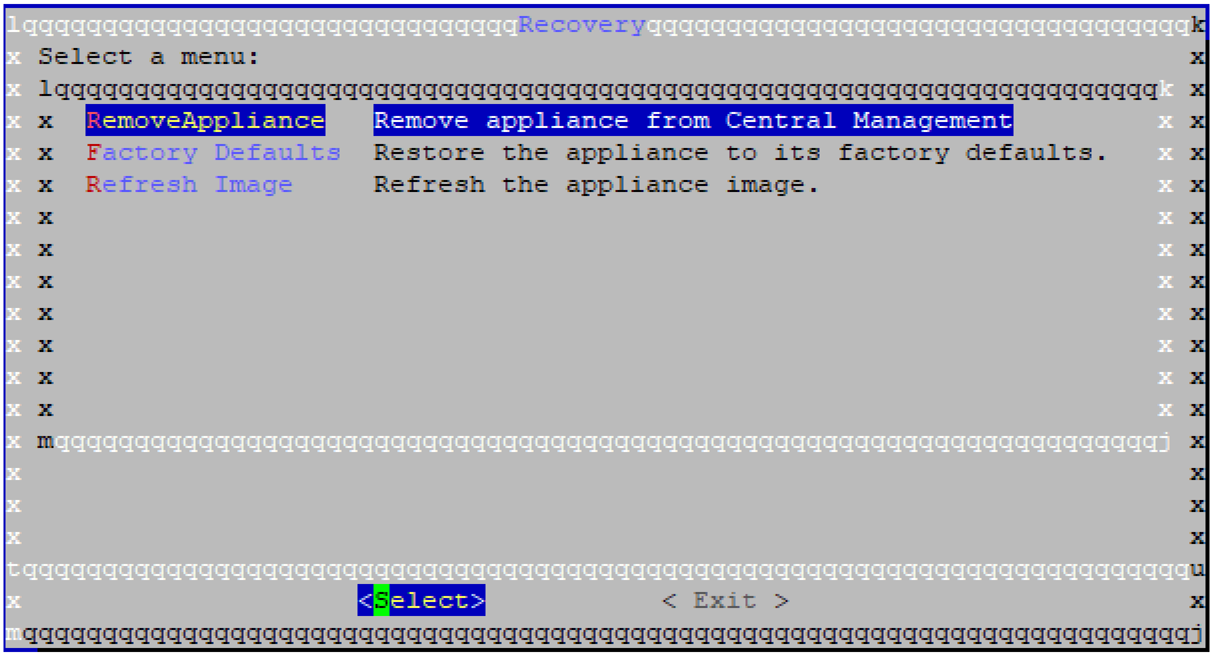
If the appliance status was shown as Connected when you removed it from Central Management, you can skip this procedure. Go to **4. Regenerate the Certificates**.

1. Log in to the appliance console as sysadmin.
   - **First:** Log in to your Flow Collectors, Flow Sensors, and UDP Directors first.
   - **Last:** Log in to the Manager last (after you have completed steps 1 though 5 on all other appliances as needed).

Remove the Manager from Central Management last.

2. Type **SystemConfig**. Press Enter.
3. From the main menu, select **Recovery**.
4. Select **RemoveAppliance**.

   If the menu is not shown, the appliance is already removed from Central Management.



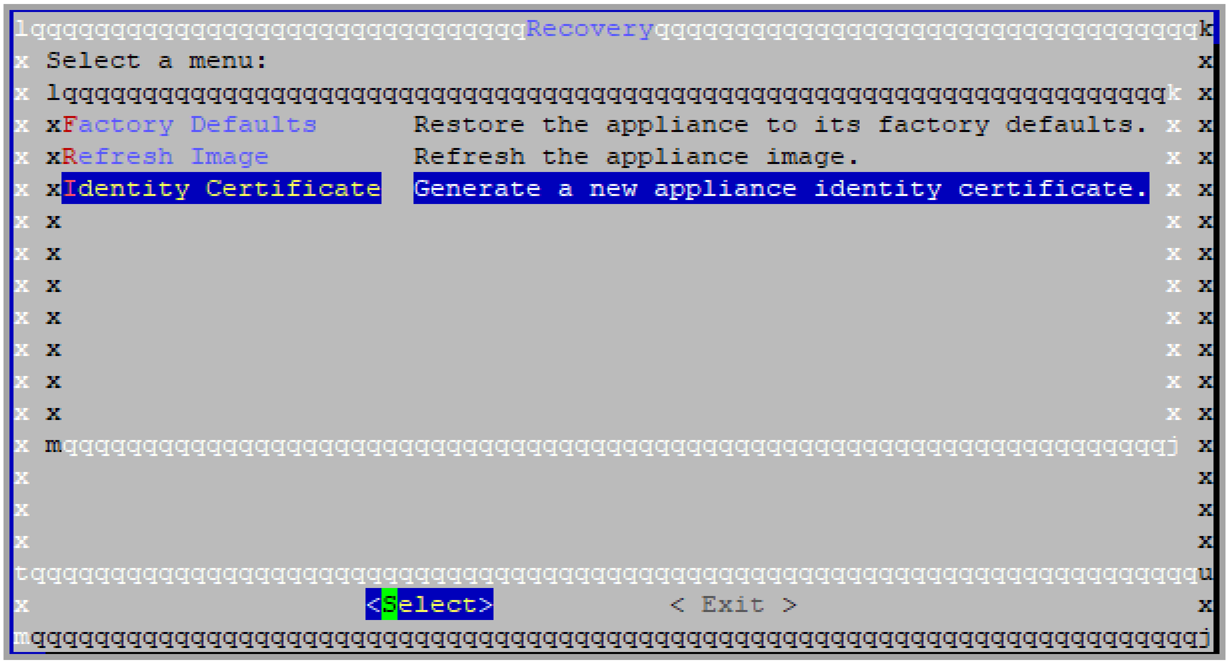
```
                                Recovery
  Select a menu:

     RemoveAppliance     Remove appliance from Central Management
     Factory Defaults    Restore the appliance to its factory defaults.
     Refresh Image       Refresh the appliance image.

                      <Select>              < Exit >
```

5. Follow the on-screen prompts to remove the appliance.
6. Repeat steps 1 through 5 on each appliance to remove it from Central Management.

## 4. Regenerate the Certificates

Use the following instructions to enter a new validity period and regenerate the certificate on each appliance.

1. Log in to the appliance console as sysadmin.
2. Type **SystemConfig**. Press Enter.
3. From the main menu, select **Recovery**.
4. Select **Identity Certificate**. Follow the on-screen prompts to confirm.

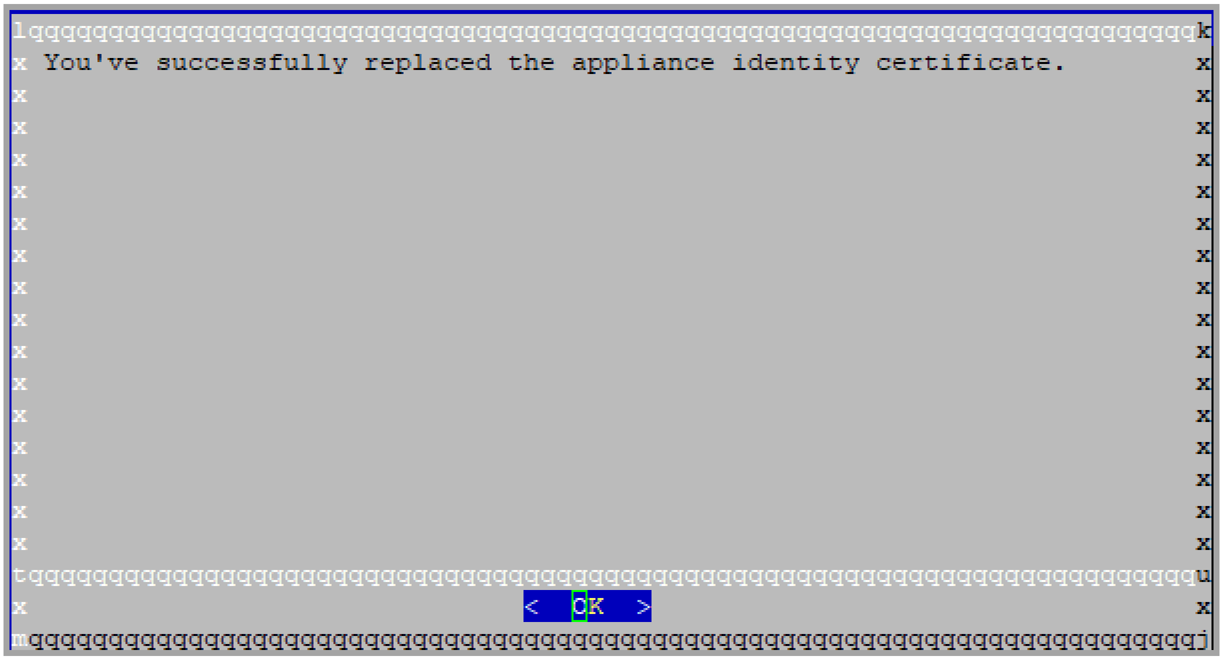


```
Recovery
 Select a menu:
 Factory Defaults       Restore the appliance to its factory defaults.
 Refresh Image          Refresh the appliance image.
 Identity Certificate   Generate a new appliance identity certificate.

                    <Select>          < Exit >
```

If the Identity Certificate menu is not shown, remove the appliance from Central Management. Refer to **2. Remove Appliances using Central Management** and **3. Remove Appliances using System Configuration**.

5. Enter a validity period between 1 and 5 years.
6. Click **OK**.

   Wait until you see the confirmation that you've successfully replaced the certificate. Click **OK** and close the console.



```
You've successfully replaced the appliance identity certificate.
```

7. Repeat steps 1 through 6 on each appliance.

## 5. Register your Manager in Central Management

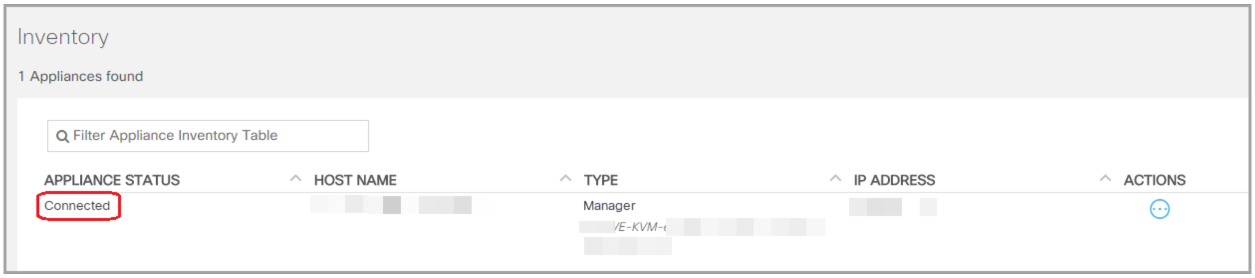
Use the following instructions to register your Manager using the Appliance Setup Tool. Note that your appliance configuration for IP address, host name, etc. have been preserved.

**Manager Failover:** If you have two Managers, you only need to complete this procedure on the primary Manager. You will register the secondary Manager in **6. Add Appliances to Central Management**.

> ⚠ We do not recommend changing your host information (IP address, host name, or domain name) as part of this procedure. Refer to Host Information for details.

1. Log in to the Manager as admin: https://<IPAddress>.
2. Click **Continue/Next** and scroll to the **Register Your Appliance** tab.
3. Click **Restart and Proceed**. Follow the on-screen prompts to restart the Manager.
4. Log in to the Manager again.
5. On the **Register Your Appliance** tab, review the IP address and click **Save**.
   - This installs Central Management on the Manager.
   - The Manager IP address is detected automatically and cannot be changed.

6. When the appliance setup is completed, review the inventory in Central Management. Confirm the Manager appliance status is shown as **Connected**.



Inventory

1 Appliances found

Filter Appliance Inventory Table

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

## 6. Add Appliances to Central Management

Use the Appliance Setup Tool to add your other appliances to Central Management.

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Connected** before you start configuring the next appliance in your cluster.
- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** Follow the appliance configuration order.
- **Access:** You need admin privileges to access Central Management.

### Appliance Configuration Order

Configure your appliances in the following order, and note the details for each appliance:

| Order | Appliance | Details |
|---|---|---|
| 1. | UDP Directors (also known as FlowReplicators) | |
| 2. | Flow Collector 5000 Series Database | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine configuration. |
| 3. | Flow Collector 5000 Series Engine | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine |

| | | |
|---|---|---|
| | | configuration. |
| 4. | All Other Flow Collectors (NetFlow and sFlow) | |
| 5. | Flow Sensors | Make sure your Flow Collector is shown as Connected before you start the Flow Sensor configuration. |
| 6. | Secondary Manager (if used) | Make sure the primary Manager is shown as Connected before you start the secondary Manager configuration.<br>The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to **8. Configure the Manager Failover Pair**. |

Use the following instructions to configure each appliance using the Appliance Setup Tool. Note that your appliance configuration for IP address, host name, etc. have been preserved.

⚠ We do not recommend changing your host information (IP address, host name, or domain name) as part of this procedure. Refer to Host Information for details.

1. In the address field of your browser, type **https://** followed by the IP address of the appliance.

   - **Connected:** Confirm each appliance is Connected before you add the next appliance to Central Management.
   - **Order:** Make sure you configure your appliances in order so they communicate correctly.

2. **Secondary Manager:** Enter the following credentials to log in:
   - **User Name:** admin
   - **Password:** lan411cope

**All Other Appliances:** Skip to step 4.

3. **Secondary Manager:** Enter new passwords for admin, root, and sysadmin. Click **Next** to scroll to each user.

   Use the following criteria:

   - **Length:** 8 to 256 characters
   - **Change:** Make sure the new password is different from the default password by at least 4 characters.

| User | Default Password |
|---|---|
| admin | lan411cope |
| root | lan1cope |
| sysadmin | lan1cope |

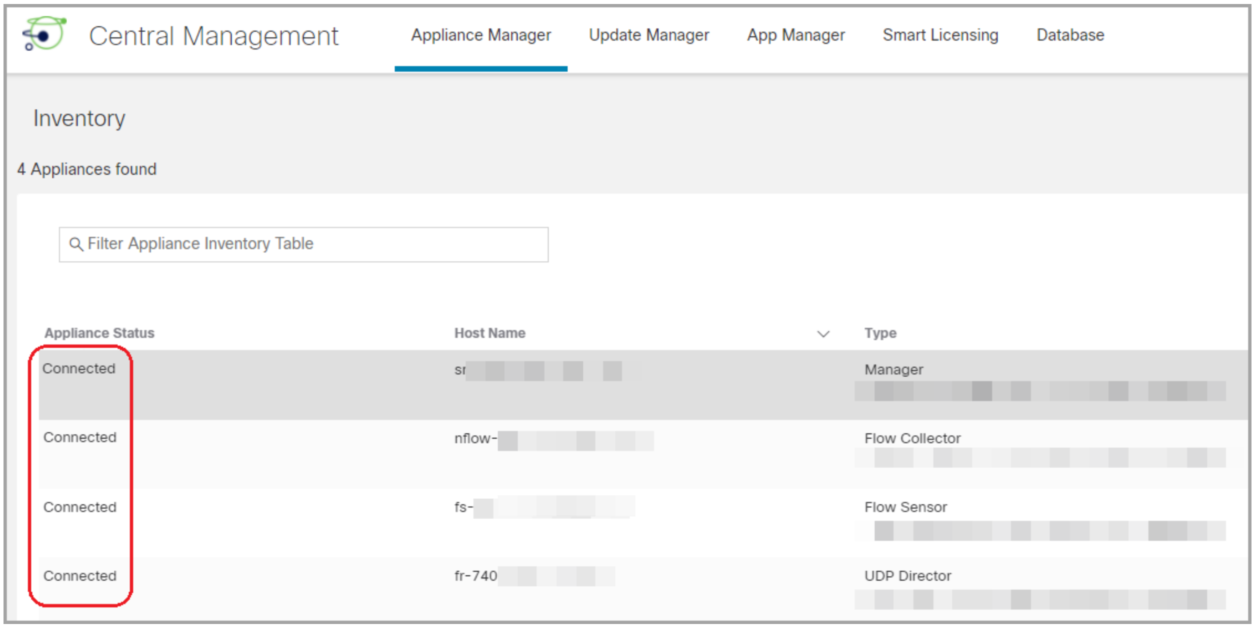
4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).
5. Add the appliance to Central Management as follows:

   - **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **8. Configure the Manager Failover Pair**.
   - **All Other Appliances:** Enter the IP address of your primary Manager. Click **Save**. Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manager admin user name and password. Select the Secure Network Analytics domain and complete any other required info.

> The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, select a Flow Collector.

6. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. Make sure the primary Manager and each appliance is shown as Connected before you add the next appliance to Central Management using the configuration order and details.



Inventory

4 Appliances found

Filter Appliance Inventory Table

| Appliance Status | Host Name | Type |
|---|---|---|
| Connected | sr[redacted] | Manager<br>[redacted] |
| Connected | nflow-[redacted] | Flow Collector<br>[redacted] |
| Connected | fs-[redacted] | Flow Sensor<br>[redacted] |
| Connected | fr-740[redacted] | UDP Director<br>[redacted] |

7. Repeat steps 1 through 6 to add each appliance to Central Management.

## 7. Delete Outdated Certificates from the Trust Stores

Delete the expired/outdated certificates from each appliance trust store. For details about where each appliance identity certificate is saved, refer to **Trust Store Location**.

Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Click the ••• (**Ellipsis**) icon for the appliance
2. Choose **Edit Appliance Configuration**.
3. Choose the **General** tab.
4. Review the **Trust Store** list. Locate all expired certificates (identity, root, and intermediate certificates) from the appliance, Manager, and other appliances.
5. Click **Delete** to delete each old certificate.
6. Click **Apply Settings**. Follow the on-screen prompts.

7. On the Central Management inventory, confirm the appliance and Manager appliance status returns to Connected.
8. Repeat steps 1 through 7 on each Flow Collector, Flow Sensor, and UDP Director.

## 8. Configure the Manager Failover Pair

To reconfigure your Managers as a failover pair, follow the instructions in the Failover Configuration Guide.

## Individual, Non-Manager Appliances

Use this procedure to change the certificate validity period for an individual, non-Manager appliance (Flow Collectors, Flow Sensors, and UDP Directors). In this procedure, you will only remove the individual appliance from Central Management and then add it back to Central Management after you've made your changes.

> ⚠ The appliance identity certificate is replaced automatically as part of this procedure.
>
> **If your appliance uses a custom certificate,** we do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

### Overview

The overall steps are as follows:

**1. Remove the Appliance from Central Management**

**2. Regenerate the Certificate**

**3. Delete Outdated Certificates from the Manager Trust Store**

**4. Add the Appliance to Central Management**

> ⓘ If you need to change the Manager certificate validity period, refer to **Manager and Managed Appliances**.

### 1. Remove the Appliance from Central Management

Use the following instructions to remove your appliance from Central Management.

1. Open Central Management.
2. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.
    - If the appliance you are changing is not shown as Connected, you will address it in a later step.
    - If the Manager status is not shown as Connected, wait a few minutes until it resolves.

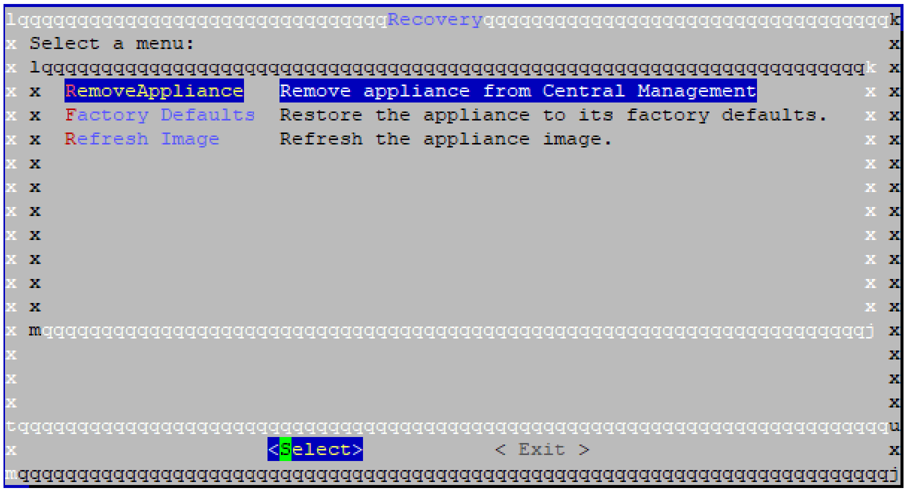
3. Remove the appliance from Central Management:

- Click the ••• (**Ellipsis**) icon for an appliance.
- Choose **Remove This Appliance**.

> When you remove an appliance from Central Management, the Manager appliance status transitions from Config Changes Pending to Connected.

4. Confirm the Manager appliance status is shown as **Connected**.
5. Log in to the appliance console as sysadmin.
6. Type **SystemConfig**. Press Enter.
7. From the main menu, select **Recovery**.
8. Select **RemoveAppliance**. Follow the on-screen prompts to remove the appliance.

   If the menu is not shown, the appliance is already removed from Central Management.



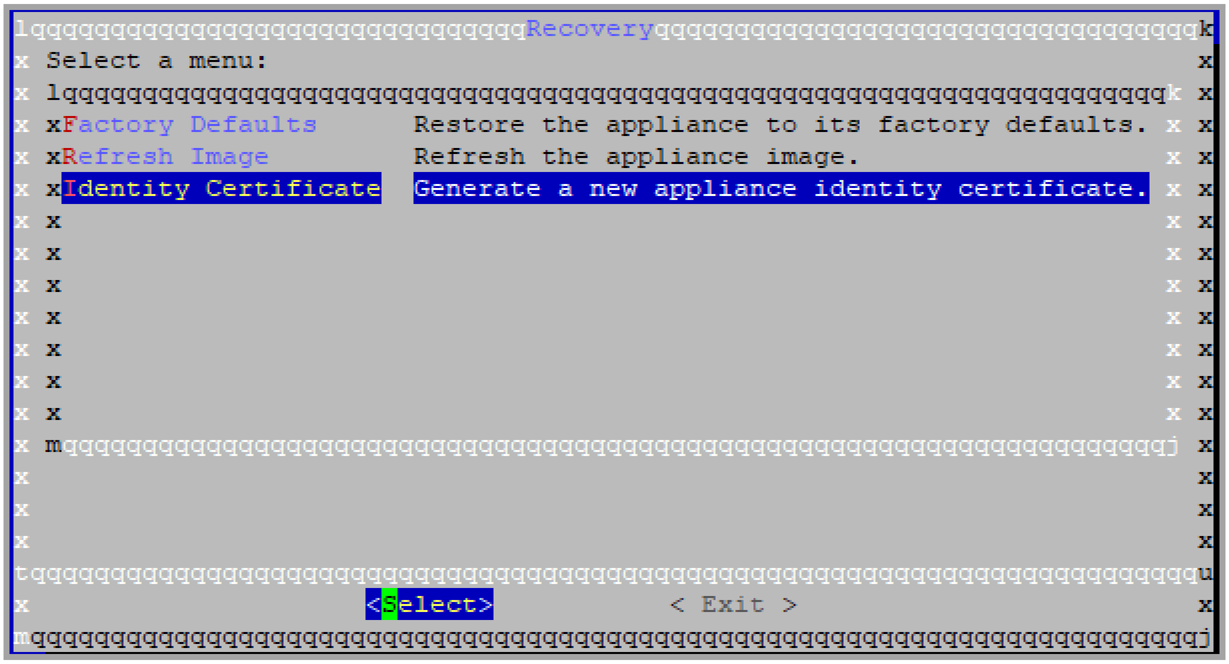
```
Recovery
Select a menu:
   RemoveAppliance    Remove appliance from Central Management
   Factory Defaults   Restore the appliance to its factory defaults.
   Refresh Image      Refresh the appliance image.

                     <Select>          < Exit >
```

> You will continue with System Config in the next procedure.

## 2. Regenerate the Certificate

Use the following instructions to enter a new validity period and regenerate the certificate.

1. From the main menu in System Config, select **Recovery**.
2. Select **Identity Certificate**. Follow the on-screen prompts to confirm.

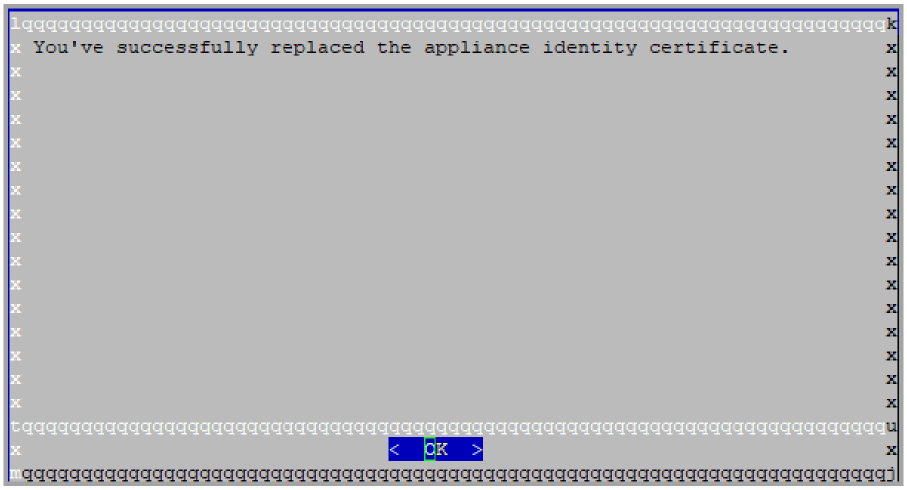


```
Recovery
Select a menu:
Factory Defaults        Restore the appliance to its factory defaults.
Refresh Image           Refresh the appliance image.
Identity Certificate    Generate a new appliance identity certificate.

            <Select>            < Exit >
```

If the Identity Certificate menu is not shown, remove the appliance from Central Management. Refer to **1. Remove the Appliance from Central Management**.

3. Enter a validity period between 1 and 5 years.
4. Click **OK**.

   Wait until you see the confirmation that you've successfully replaced the certificate. Click **OK** and close the console.



```
You've successfully replaced the appliance identity certificate.

                      <  OK  >
```

## 3. Delete Outdated Certificates from the Manager Trust Store

Use the following procedure to delete the expired/outdated appliance certificates from the Manager trust store.

> ⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Log in to the Manager as admin: https://<IPAddress>
2. Open Central Management.
3. Confirm the Manager appliance status is shown as Connected.
4. Click the ••• (**Ellipsis**) icon for the Manager.
5. Choose **Edit Appliance Configuration**.
6. Choose the **General** tab.
7. Review the **Trust Store** list. Locate the expired certificates (identity, root, and intermediate certificates).
8. Click **Delete** to delete each old certificate.
9. Click **Apply Settings**. Follow the on-screen prompts.
10. On the Central Management inventory, confirm the Manager appliance status returns to Connected.

## 4. Add the Appliance to Central Management

Use the Appliance Setup Tool to add your appliance to Central Management. Note that your appliance configuration for IP address, host name, etc. have been preserved.

> ⚠ We do not recommend changing your host information (IP address, host name, or domain name) as part of this procedure. Refer to Host Information for details.

- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** If you need to add more than one appliance to Central Management, follow the appliance configuration order.
- **Access:** You need admin privileges to access Central Management.

1. In the address field of your browser, type **https://** followed by the IP address of the appliance.
2. Click **Next** and scroll to the **Central Management** tab.

3. Add the appliance to Central Management as follows:
   - Enter the IP address of your primary Manager. Click **Save**.
   - Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manager admin user name and password.
   - Select the Secure Network Analytics domain and complete any other required info.

> ⓘ The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, select a Flow Collector.

4. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

> ⚠ The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. If the appliance does not change to Connected, you may have outdated or duplicated certificates in your trust stores. Refer to **Troubleshooting** and **Deleting Certificates from the Trust Stores** for details.

# Replacing Expired Cisco Default Certificates

Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate. Use the following instructions to change the validity period on your **expired** appliance identity certificates.

- **Host Information:** The appliance host information (IP address, host name, domain name) is preserved. If you need to change the host information in addition to the validity period, use the instructions in **Changing Network Interfaces** or **Changing the Host Name or Network Domain Name** (instead of the instructions in this section).
- **Custom Certificates:** We do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

> ⓘ If your certificates have not yet expired, refer to **Replacing Unexpired Cisco Default Certificates**. If your appliances use custom certificates from a Certificate Authority, refer to **Replacing the SSL/TLS Appliance Identity Certificate**.

## Requirements

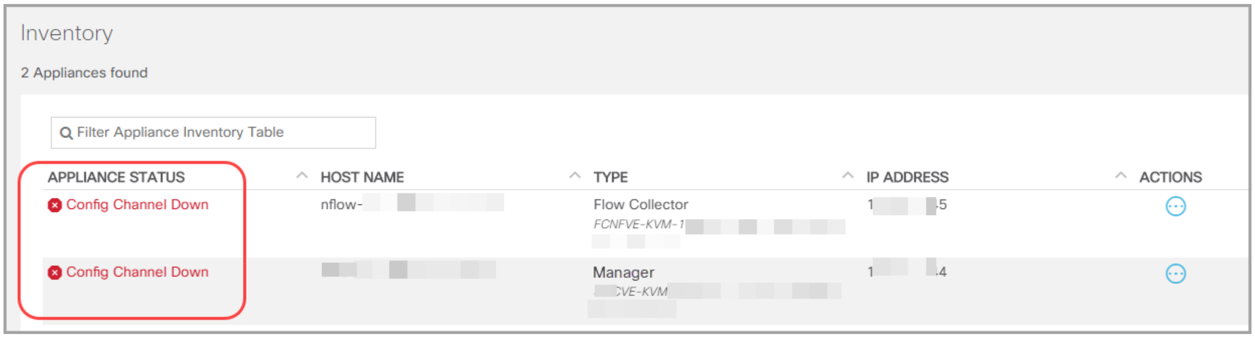
Before you get started, review the **Best Practices** in the Introduction, and confirm the following requirements:

- **Users:** You need **admin** and **sysadmin** user access.
- **Manager Failover:** If you are updating your Manager certificates and your Managers are configured as a failover pair, delete the failover relationship before you start these procedures. For instructions, refer to the Failover Configuration Guide. When you delete the failover pair, the secondary Manager is removed from the cluster. The instructions include resetting the secondary Manager to factory defaults.

## 1. Review the Appliance Status

1. Log in to your primary Manager.
2. Click the ⚙ (**Global Settings**) icon.

3. Choose **Central Management**.
4. Review the Appliance Status column. If the appliance status is shown as **Config Channel Down**, your certificates have expired.



Inventory

2 Appliances found

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| ✗ Config Channel Down | nflow-[redacted] | Flow Collector<br>*FCNFVE-KVM-1*[redacted] | 1[redacted]5 | ⋯ |
| ✗ Config Channel Down | [redacted] | Manager<br>[redacted]*CVE-KVM*[redacted] | 1[redacted]4 | ⋯ |

## 2. Select the Procedure for your Appliance

- **Manager and Managed Appliances:** Use **Manager and Managed Appliances** to change the certificate validity period for the Manager and other managed appliances in your cluster. As part of the procedure, you will remove all appliances from Central Management (in the order shown), and then rebuild your cluster after you've made your changes.
- **Individual, Non-Manager Appliance:** Use **Individual, Non-Manager Appliances** to change the certificate validity period for an individual, non-Manager appliance (Flow Collectors, Flow Sensors, and UDP Directors). In this procedure, you will only remove the individual appliance from Central Management and then add it back to Central Management after you've made your changes.

## Manager and Managed Appliances

Follow these instructions to change the certificate validity period for the Manager and other managed appliances in your cluster. As part of the procedure, you will remove all appliances from Central Management (in the order shown), and then rebuild your cluster after you've made your changes.

**Manager Failover:** If your Managers are configured as a failover pair, delete the failover relationship before you start these procedures. For instructions, refer to the Failover Configuration Guide. When you delete the failover pair, the secondary Manager is removed from the cluster. The instructions include resetting the secondary Manager to factory defaults.

⚠ The appliance identity certificate is replaced automatically as part of this procedure.

⚠ **If your appliance uses a custom certificate,** we do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

## Overview

The overall steps are as follows:

1. **Remove Appliances and Regenerate Certificates**
2. **Register your Manager in Central Management**
3. **Delete Expired Certificates from the Manager Trust Store**
4. **Add Appliances to Central Management**
5. **Delete Expired Certificates from the Trust Stores**
6. **Configure the Manager Failover Pair**

## 1. Remove Appliances and Regenerate Certificates

Use these instructions to change the certificate validity period for the Manager and other managed appliances in your cluster. Make sure you remove all appliances from Central Management in the specified order.

ⓘ If you only need to change the Manager, you still need to remove all appliances from Central Management. If you only need to change an individual, non-Manager appliance, refer to **Individual, Non-Manager Appliances**.

- **First:** Complete these instructions on all Flow Collectors, Flow Sensors, and UDP Directors.
- **Last:** Complete these instructions on the Manager last.
- **Default Validity Period:** The regenerated certificate defaults to 5 years. However, you can change this period in a later procedure.

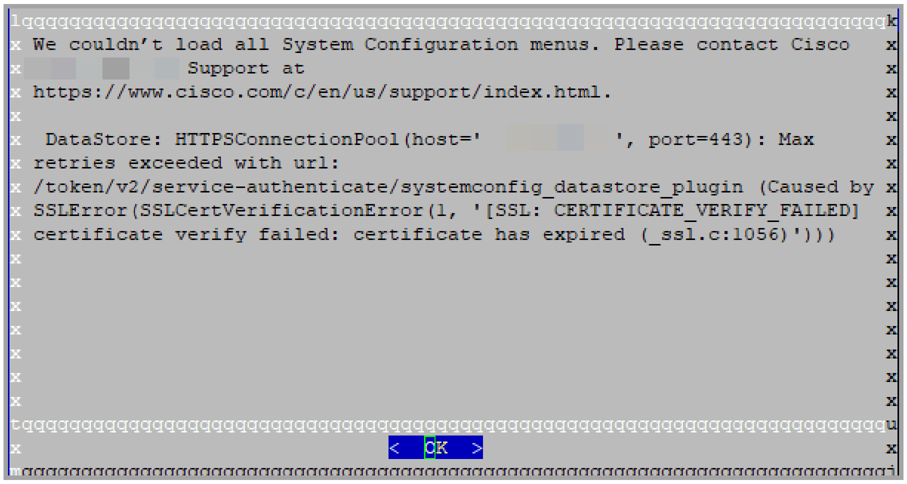
⚠ Remove the Manager from Central Management last.

1. **Remove the Appliance from Central Management:** Click the ••• (**Ellipsis**) icon for an appliance. Choose **Remove This Appliance**.

- **First:** Remove your Flow Collectors, Flow Sensors, and UDP Directors first.
- **Last:** Remove your primary Manager after you have completed steps 1 through 9 on all other appliances.

2. Log in to the appliance console as sysadmin.
   - **First:** Log in to your Flow Collectors, Flow Sensors, and UDP Directors first.
   - **Last:** Log in to your primary Manager after you have completed steps 1 though 9 on all other appliances.
3. Type **SystemConfig**. Press Enter.

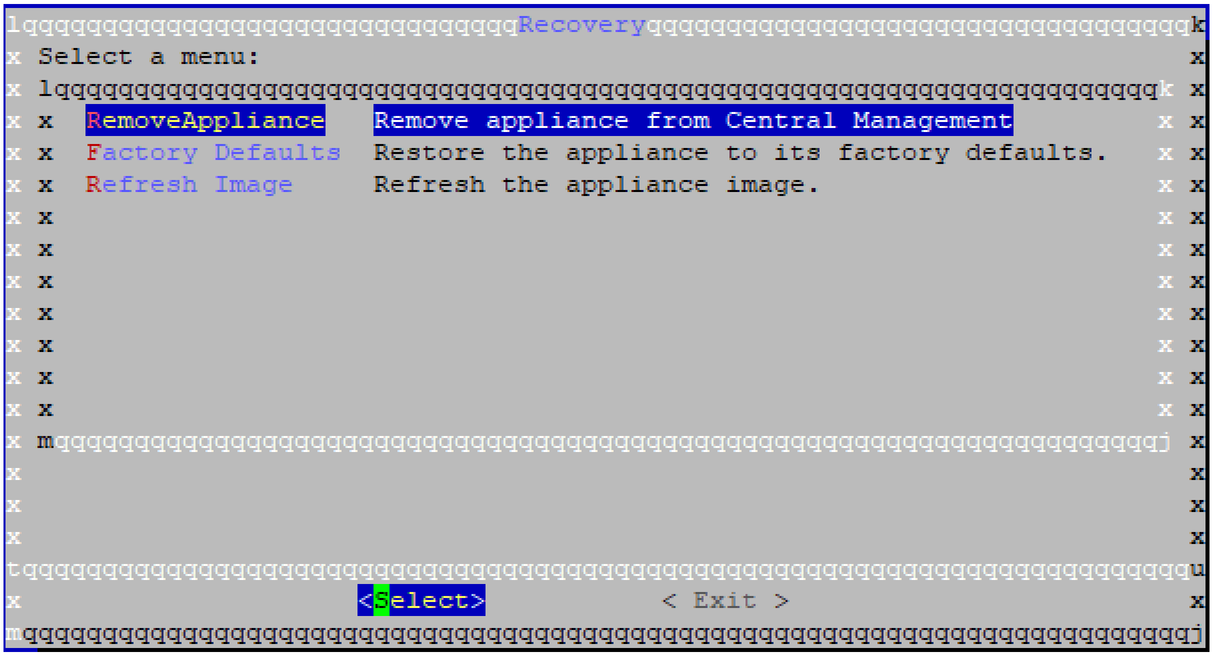
   **Managers:** If you log in to the Manager and receive an error that we couldn't load all System Configuration menus, click OK.



```
We couldn't load all System Configuration menus. Please contact Cisco
[redacted] Support at
https://www.cisco.com/c/en/us/support/index.html.

 DataStore: HTTPSConnectionPool(host='[redacted]', port=443): Max
retries exceeded with url:
/token/v2/service-authenticate/systemconfig_datastore_plugin (Caused by
SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED]
certificate verify failed: certificate has expired (_ssl.c:1056)')))
```

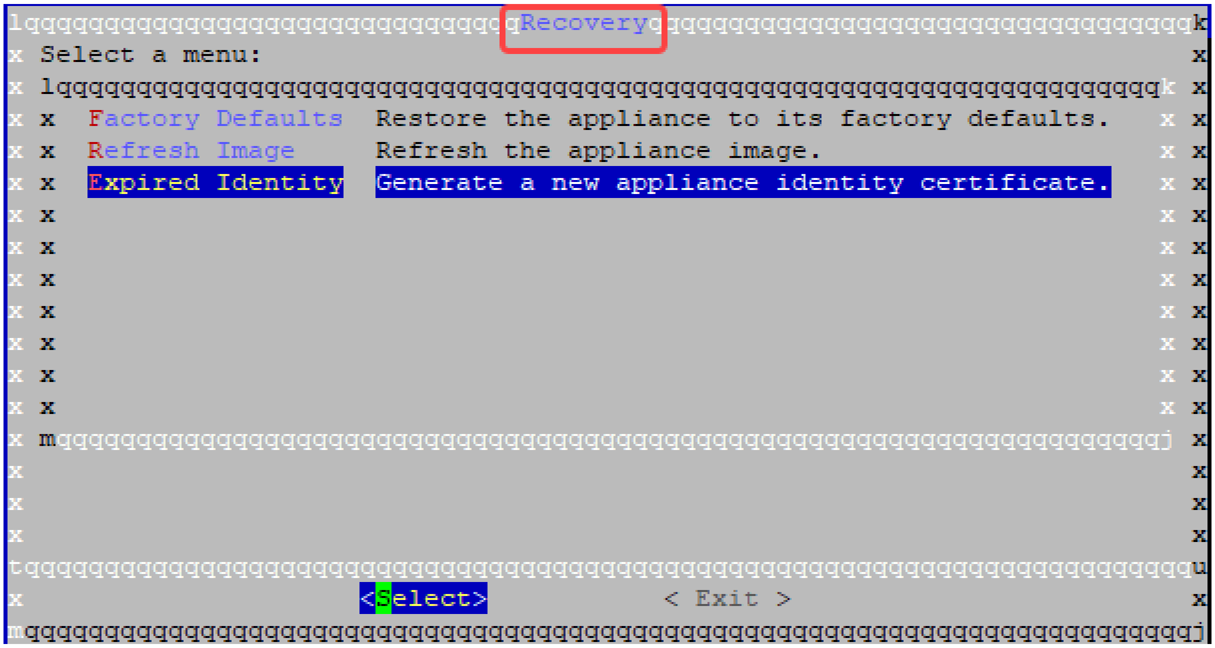
4. From the main menu, select **Recovery**.
5. Select **RemoveAppliance**.

   If the menu is not shown, the appliance is already removed from Central Management.



```
Recovery
Select a menu:
  RemoveAppliance     Remove appliance from Central Management
  Factory Defaults    Restore the appliance to its factory defaults.
  Refresh Image       Refresh the appliance image.

                  <Select>              < Exit >
```

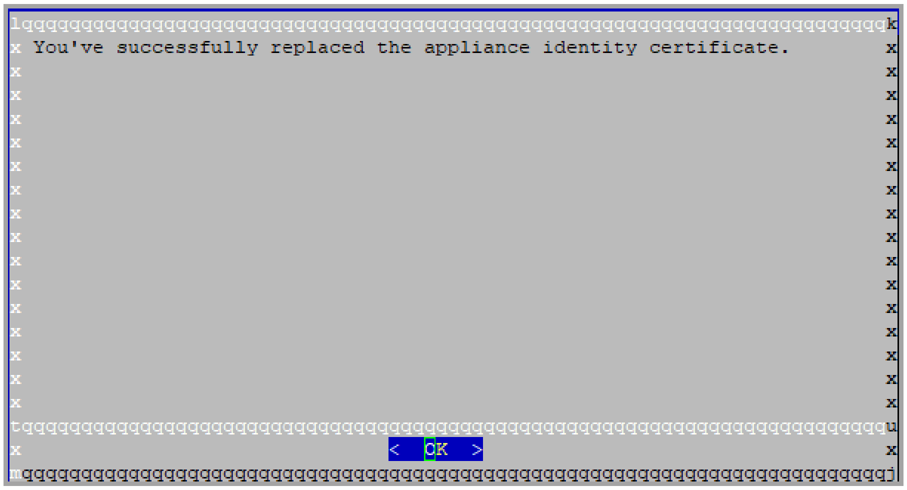
6. Follow the on-screen prompts to remove the appliance.
7. From the Recovery menu, select **Expired Identity**. Follow the on-screen prompts to confirm.



```
Recovery
Select a menu:
  Factory Defaults    Restore the appliance to its factory defaults.
  Refresh Image       Refresh the appliance image.
  Expired Identity    Generate a new appliance identity certificate.

                  <Select>              < Exit >
```

8. Wait until you see the confirmation that you've successfully replaced the certificate.

- **Exit:** Click **OK** and close the console.
- **Change Certificate Validity Period (optional):** The certificate validity period defaults to 5 years. To change the validity period, click **OK** and return to the **Recovery** menu. Select **Identity Certificate**, and follow the on-screen prompts to enter a validity period between 1 and 5 years. Wait until you see the confirmation that you've successfully replaced the certificate.



```
You've successfully replaced the appliance identity certificate.
```

9. Repeat steps 1 through 8 on each appliance.

## 2. Register your Manager in Central Management

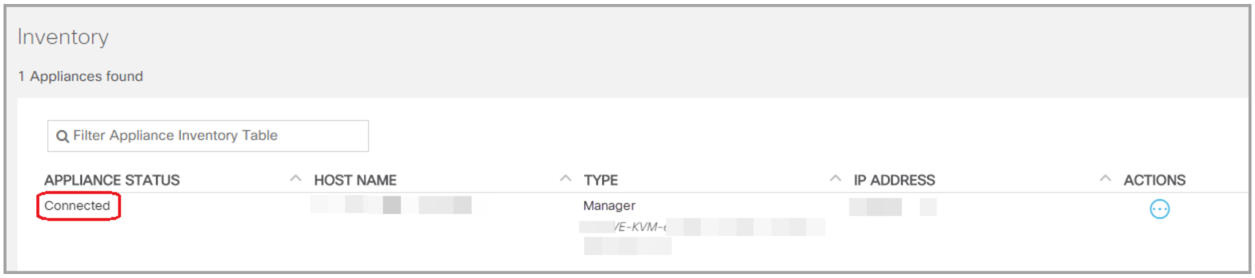
Use the following instructions to register your Manager using the Appliance Setup Tool. Note that your appliance configuration for IP address, host name, etc. have been preserved.

**Manager Failover:** If you have two Managers, you only need to complete this procedure on the primary Manager. You will register the secondary Manager in **4. Add Appliances to Central Management**.

⚠ We do not recommend changing your host information (IP address, host name, or domain name) as part of this procedure. Refer to Host Information for details.

1. Log in to the Manager as admin: https://<IPAddress>
2. Click **Continue/Next** and scroll to the **Register Your Appliance** tab.
3. Click **Restart and Proceed**. Follow the on-screen prompts to restart the Manager.
4. Log in to the Manager again.

5. On the **Register Your Appliance** tab, review the IP address and click **Save**.
    - This installs Central Management on the Manager.
    - The Manager IP address is detected automatically and cannot be changed.
6. When the appliance setup is completed, review the inventory in Central Management. Confirm the Manager appliance status is shown as **Connected**.



Inventory

1 Appliances found

Filter Appliance Inventory Table

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

## 3. Delete Expired Certificates from the Manager Trust Store

If you have two Managers, you only need to complete this procedure on the primary Manager (because the secondary Manager was reset to factory defaults).

> ⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Click the ••• (**Ellipsis**) icon for the Manager.
2. Choose **Edit Appliance Configuration**.
3. Choose the **General** tab.
4. Review the **Trust Store** list. Locate all expired certificates from the Manager and other non-Manager appliances (identity, root, and intermediate certificates).
5. Click **Delete** to delete each old certificate.
6. Click **Apply Settings**. Follow the on-screen prompts.
7. On the Central Management inventory, confirm the Manager appliance status returns to Connected.

## 4. Add Appliances to Central Management

Use the Appliance Setup Tool to add your other appliances to Central Management.

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Connected** before you start configuring the next appliance in your cluster.

- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** Follow the appliance configuration order.
- **Access:** You need admin privileges to access Central Management.

## Appliance Configuration Order

Configure your appliances in the following order, and note the details for each appliance:

| | Appliance | Details |
|---|---|---|
| 1. | UDP Directors (also known as FlowReplicators) | |
| 2. | Flow Collector 5000 Series Database | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine configuration. |
| 3. | Flow Collector 5000 Series Engine | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine configuration. |
| 4. | All Other Flow Collectors (NetFlow and sFlow) | |
| 5. | Flow Sensors | Make sure your Flow Collector is shown as Connected before you start the Flow Sensor configuration. |
| 6. | Secondary Manager (if used) | Make sure the primary Manager is shown as Connected before you start the secondary Manager configuration.<br>The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to **6. Configure the Manager Failover Pair**. |

Use the following instructions to configure each appliance using the Appliance Setup Tool. Note that your appliance configuration for IP address, host name, etc. have been preserved.

> ⚠ We do not recommend changing your host information (IP address, host name, or domain name) as part of this procedure. Refer to Host Information for details.

1. In the address field of your browser, type **https://** followed by the IP address of the appliance.

   - **Connected:** Confirm each appliance is Connected before you add the next appliance to Central Management.
   - **Order:** Make sure you configure your appliances in order so they communicate correctly.

2. **Secondary Manager:** Enter the following credentials to log in:

   - **User Name:** admin
   - **Password:** lan411cope

   **All Other Appliances:** Skip to step 4.

3. **Secondary Manager:** Enter new passwords for admin, root, and sysadmin. Click **Next** to scroll to each user.

   Use the following criteria:

   - **Length:** 8 to 256 characters
   - **Change:** Make sure the new password is different from the default password by at least 4 characters.

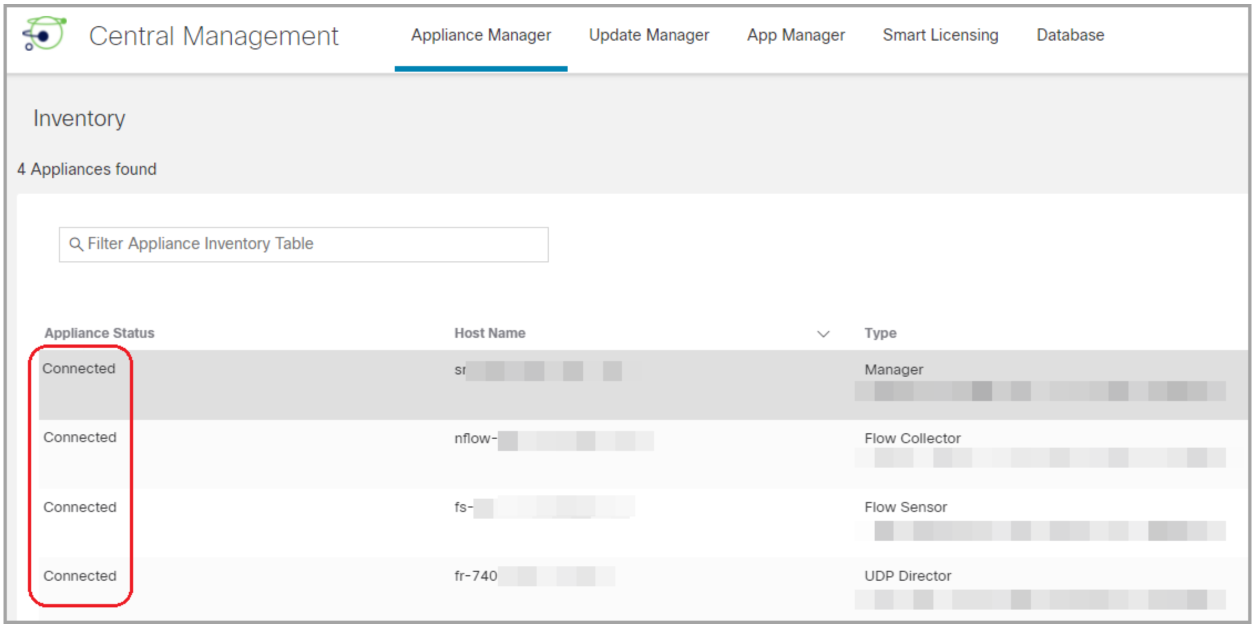
| User | Default Password |
|---|---|
| admin | lan411cope |
| root | lan1cope |
| sysadmin | lan1cope |

4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).
5. Add the appliance to Central Management as follows:
   - **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **6. Configure the Manager Failover Pair**.
   - **All Other Appliances:** Enter the IP address of your primary Manager. Click **Save**. Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manager admin user name and password. Select the Secure Network Analytics domain and complete any other required info.

ℹ The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, select a Flow Collector.

6. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

⚠ The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. Make sure the primary Manager and each appliance is shown as Connected before you add the next appliance to Central Management using the configuration order and details.



Inventory

4 Appliances found

| Appliance Status | Host Name | Type |
|---|---|---|
| Connected | sr[redacted] | Manager<br>[redacted] |
| Connected | nflow-[redacted] | Flow Collector<br>[redacted] |
| Connected | fs-[redacted] | Flow Sensor<br>[redacted] |
| Connected | fr-740[redacted] | UDP Director<br>[redacted] |

7. Repeat steps 1 through 6 to add each appliance to Central Management.

## 5. Delete Expired Certificates from the Trust Stores

Delete the expired/outdated certificates from each appliance trust store. For details about where each appliance identity certificate is saved, refer to **Trust Store Location**.

⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Click the ••• (**Ellipsis**) icon for the appliance.
2. Choose **Edit Appliance Configuration**.
3. Choose the **General** tab.
4. Review the **Trust Store** list. Locate all expired certificates (identity, root, and intermediate certificates) from the appliance, Manager, and other appliances.
5. Click **Delete** to delete each old certificate.
6. Click **Apply Settings.** Follow the on-screen prompts.
7. On the Central Management inventory, confirm the appliance and Manager appliance status returns to Connected.
8. Repeat steps 1 through 7 on each Flow Collector, Flow Sensor, and UDP Director.

## 6. Configure the Manager Failover Pair

To reconfigure your Managers as a failover pair, follow the instructions in the Failover Configuration Guide.

## Individual, Non-Manager Appliances

Follow these instructions to change the certificate validity period for an individual, non-Manager appliance (Flow Collectors, Flow Sensors, or UDP Directors). In this procedure, you will only remove the individual appliance from Central Management and then add it back to Central Management after you've made your changes.

**Default Validity Period:** The regenerated certificate defaults to 5 years. However, you can change this period in a later procedure.

> ⚠ The appliance identity certificate is replaced automatically as part of this procedure.
>
> **If your appliance uses a custom certificate,** we do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

### Overview

The overall steps are as follows:

**1. Remove the Appliance and Regenerate Certificates**

**2. Delete Expired Certificates from the Manager Trust Store**

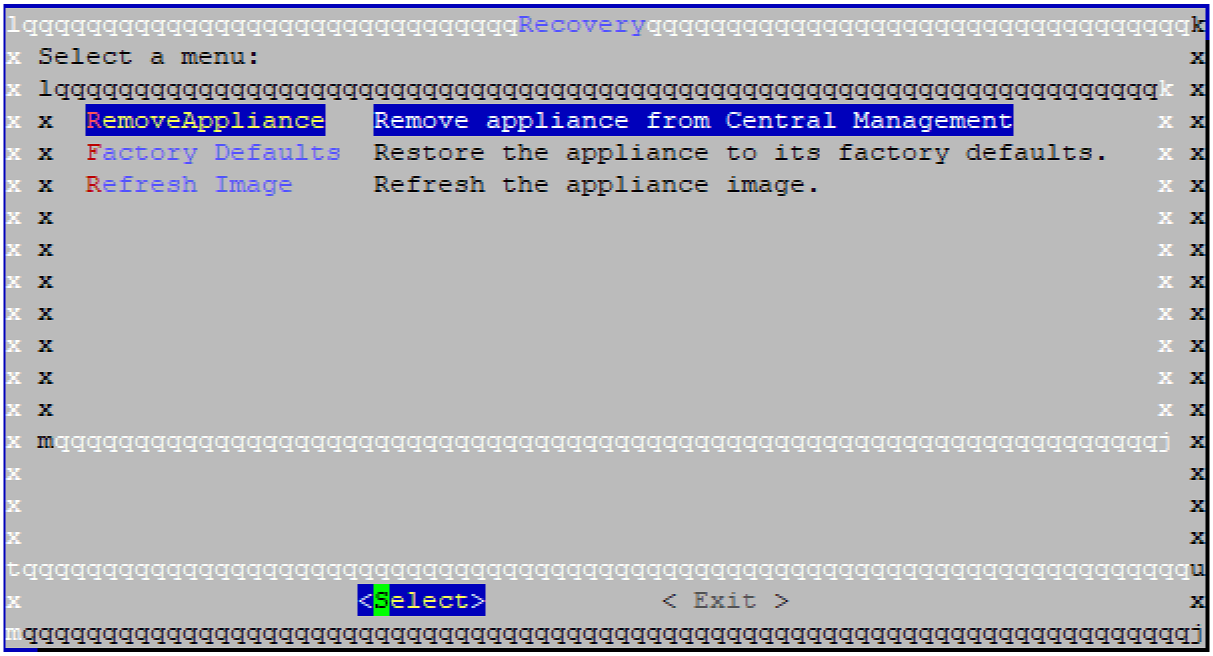
**3. Add the Appliance to Central Management**

> ⓘ If you need to change the Manager certificate validity period, refer to **Manager and Managed Appliances**.

### 1. Remove the Appliance and Regenerate Certificates

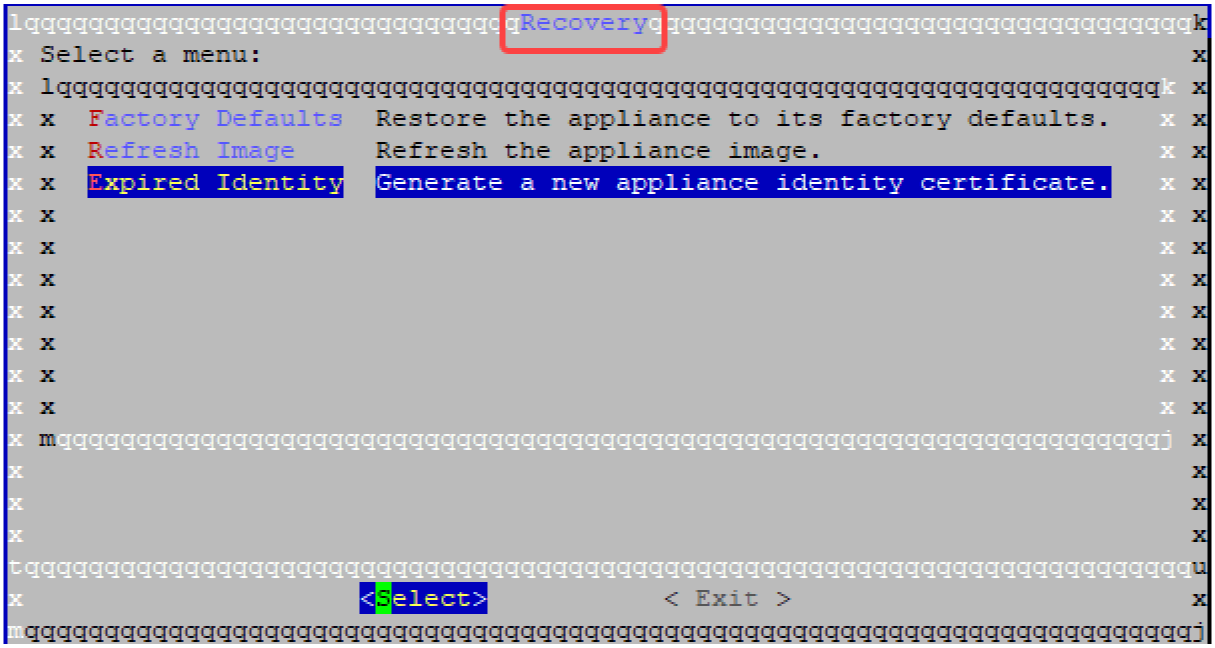
1. **Remove the Appliance from Central Management:** Click the ••• (**Ellipsis**) icon for an appliance. Choose **Remove This Appliance**.
2. Log in to the appliance console as sysadmin.
3. Type **SystemConfig**. Press Enter.
4. From the main menu, select **Recovery**.
5. Select **RemoveAppliance**.

   If the menu is not shown, the appliance is already removed from Central Management.



```
Recovery
Select a menu:
   RemoveAppliance     Remove appliance from Central Management
   Factory Defaults    Restore the appliance to its factory defaults.
   Refresh Image       Refresh the appliance image.

                  <Select>            < Exit >
```

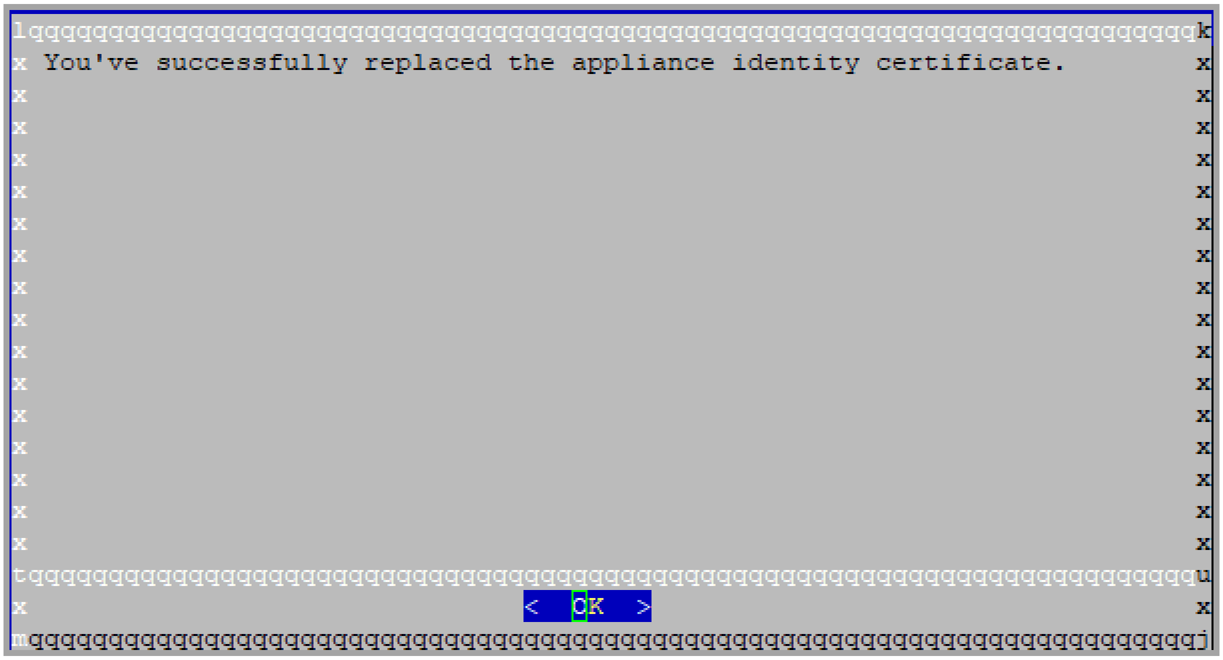
6. Follow the on-screen prompts to remove the appliance.
7. From the Recovery menu, select **Expired Identity**. Follow the on-screen prompts to confirm.



```
Recovery
Select a menu:
   Factory Defaults    Restore the appliance to its factory defaults.
   Refresh Image       Refresh the appliance image.
   Expired Identity    Generate a new appliance identity certificate.

                  <Select>            < Exit >
```

8. Wait until you see the confirmation that you've successfully replaced the certificate.

- **Exit:** Click **OK** and close the console.
- **Change Certificate Validity Period (optional):** The certificate validity period defaults to 5 years. To change the validity period, click **OK** and return to the **Recovery** menu. Select **Identity Certificate**, and follow the on-screen prompts to enter a validity period between 1 and 5 years. Wait until you see the confirmation that you've successfully replaced the certificate.



```
You've successfully replaced the appliance identity certificate.
```

9. Repeat steps 1 through 8 on each appliance.

## 2. Delete Expired Certificates from the Manager Trust Store

Use the following procedure to delete the expired appliance certificates from the Manager trust store.

> ⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Log in to the Manager as admin: https://<IPAddress>
2. Confirm the Manager appliance status is shown as Connected.
3. Click the ••• (**Ellipsis**) icon for the Manager.
4. Choose **Edit Appliance Configuration**.
5. Choose the **General** tab.

6. Review the **Trust Store** list. Locate the expired certificates (identity, root, and intermediate certificates).
7. Click **Delete** to delete each old certificate.
8. Click **Apply Settings**. Follow the on-screen prompts.
9. On the Central Management inventory, confirm the Manager appliance status returns to Connected.

## 3. Add the Appliance to Central Management

Use the Appliance Setup Tool to add your appliance to Central Management. Note that your appliance configuration for IP address, host name, etc. have been preserved.

> ⚠ We do not recommend changing your host information (IP address, host name, or domain name) as part of this procedure. Refer to Host Information for details.

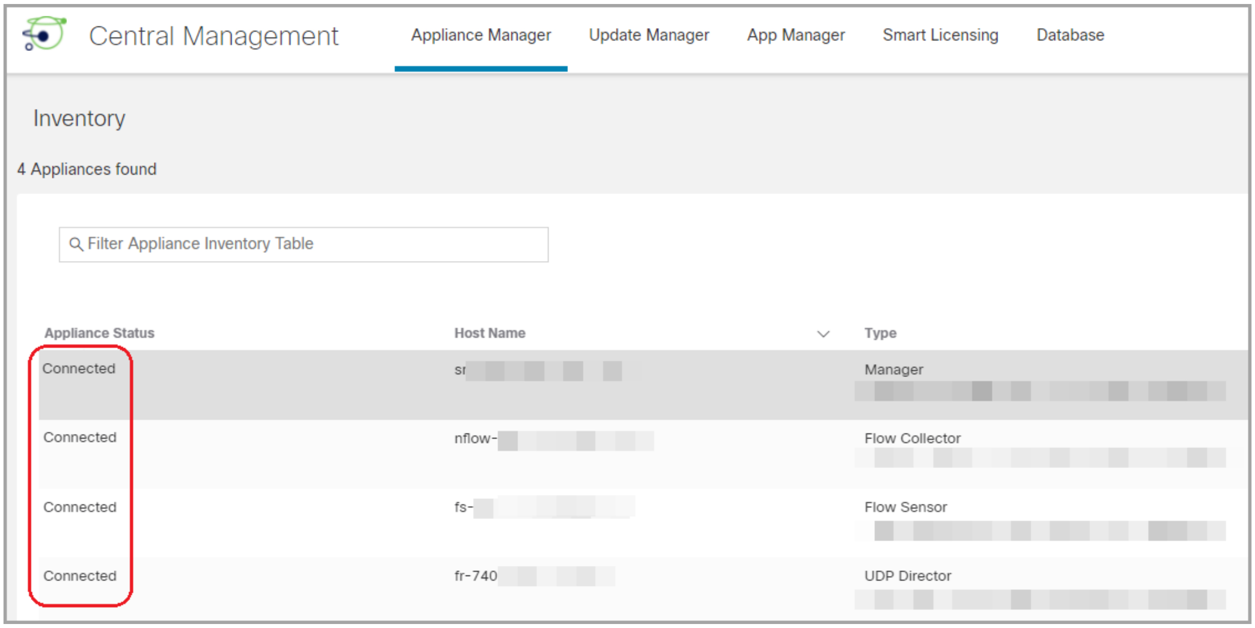
- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** If you need to add more than one appliance to Central Management, follow the appliance configuration order.
- **Access:** You need admin privileges to access Central Management.

1. In the address field of your browser, type **https://** followed by the IP address of the appliance.
2. Click **Next** and scroll to the **Central Management** tab.
3. Add the appliance to Central Management as follows:
   - Enter the IP address of your primary Manager. Click **Save**.
   - Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manager admin user name and password.
   - Select the Secure Network Analytics domain and complete any other required info.

> ℹ The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, select a Flow Collector.

4. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

⚠ The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. If the appliance does not change to Connected, you may have outdated or duplicated certificates in your trust stores. Refer to **Troubleshooting** and **Deleting Certificates from the Trust Stores** for details.



Inventory

4 Appliances found

| Appliance Status | Host Name | Type |
|---|---|---|
| Connected | sr[redacted] | Manager<br>[redacted] |
| Connected | nflow-[redacted] | Flow Collector<br>[redacted] |
| Connected | fs-[redacted] | Flow Sensor<br>[redacted] |
| Connected | fr-740[redacted] | UDP Director<br>[redacted] |

# Replacing the SSL/TLS Appliance Identity Certificate

Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate. You can replace the default certificate with an appliance identity certificate from a Certificate Authority.

> ⚠ Your certificates are critical for your system's security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss.

## Certificate Requirements

If you replace the appliance identity certificate, make sure you have certificates from a Certificate Authority. For best practices and certificate requirements, refer to **Appliance Identity Certificates** in the Introduction.

## Select the Procedure for your Environment

You can choose to generate a **Certificate Signing Request (CSR)** in Central Management or skip the CSR if you already have certificates from a Certificate Authority.

- To generate a Certificate Signing Request, go to **Generating the CSR in Central Management**.
- To skip the Certificate Signing Request, go to **Skipping the CSR in Central Management**.

## Generating the CSR in Central Management

Use the following instructions to generate a CSR in Central Management and replace the appliance identity certificate with a custom identity certificate.

### Overview

The overall steps are as follows:

1. **Generate a Certificate Signing Request**
2. **Add Certificates to the Trust Stores**
3. **Replace the Appliance Identity Certificate**

**4. Trust the Certificate in the Desktop Client**

## 1. Generate a Certificate Signing Request

Use the following instructions to prepare the Certificate Signing Request (CSR).

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. Locate the **SSL/TLS Appliance Identity** section.
5. Click **Update Identity**.
6. Do you need to generate a CSR (Certificate Signing Request)? Choose **Yes**. Click **Next**.

> ⓘ If you do not need to generate a CSR, go to **Skipping the CSR in Central Management**.

7. Select an **RSA Key Length** that is supported by your Certificate Authority.
8. Complete the fields (optional) in the **Generate a CSR** section.
9. Click **Generate a CSR**. The generation process may take several minutes.

   **Cancel:** If you click **Cancel** after you generate a CSR, or anytime while you're waiting for the CA certificate, the canceled CSR will be invalid. Generate a new CSR in this case.
10. Click **Download CSR**.

    **Multiple Appliances:** If you are updating the identity on all appliances in your cluster, repeat steps 1 through 10 on every appliance to generate the CSR.

    **Cancel:** If Cancel is clicked anytime after you generate the CSR, the CSR will be invalid, and you will not be able to use it to update the appliance identity. Generate a new CSR in this case.
11. Submit the downloaded CSRs to a Certificate Authority.

    **Multiple CSRs:** Submit all CSRs to the same Certificate Authority.

## 2. Add Certificates to the Trust Stores

Before you update the appliance identity, add the Certificate Authority (CA) certificates to the required trust stores.

**Friendly Names:** If you are naming new certificates or adding them to the trust stores, make sure each friendly name is unique. Do not duplicate any friendly names.

**If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one certificate.

Make sure you upload the following certificates:

- identity
- chain (root and intermediate certificates)

> ⚠ When you add a certificate to your appliance trust store, your appliance trusts that identity and allows communication with it.

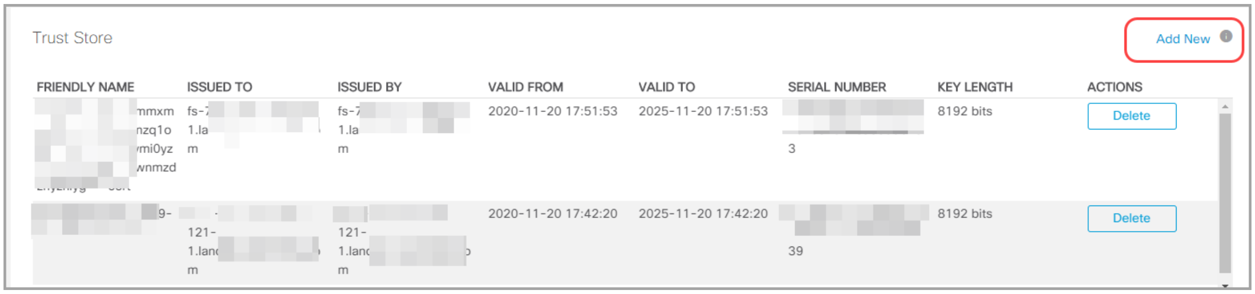
1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the appliance.

   **Order:** Select your appliances in the following order:

   - Flow Collectors
   - Flow Sensors
   - UDP Directors
   - Managers

> ⚠ Make sure you follow the selection order to update the trust stores of your appliances before you update the Manager trust store.

3. Choose **Edit Appliance Configuration**.
4. On the **General** tab, locate the Trust Store section.
5. Click **Add New**.



Trust Store

| FRIENDLY NAME | ISSUED TO | ISSUED BY | VALID FROM | VALID TO | SERIAL NUMBER | KEY LENGTH | ACTIONS |
|---|---|---|---|---|---|---|---|
| [redacted] mmxm nzq1o ymi0yz wnmzd | fs-7[redacted] 1.la m | fs-7[redacted] 1.la m | 2020-11-20 17:51:53 | 2025-11-20 17:51:53 | [redacted] 3 | 8192 bits | Delete |
| [redacted] 9- | [redacted] 121- 1.lanc[redacted] m | [redacted] 121- 1.lanc[redacted] m | 2020-11-20 17:42:20 | 2025-11-20 17:42:20 | [redacted] 39 | 8192 bits | Delete |

6. In the **Friendly Name** field, enter a unique name for the certificate.
7. Click **Choose File**. Select the new certificate.

8. Click **Add Certificate**. Confirm the new certificate is shown in the Trust Store list.
    - **If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain.
    - Make sure you add the appliance identity certificate and certificate chain (if applicable) to the appliance trust store (its own trust store) and the trust stores shown in the **Trust Store Requirements** table.
9. Repeat steps 1 though 9 on each appliance trust store.

## Trust Store Requirements

Use this table to add the **appliance identity** and **certificate chain** (if applicable) to the appliance trust stores. If your file chain includes more than one certificate (root and intermediate certificates), upload each certificate individually to the trust store. Do not upload an entire chain as one certificate.

To confirm where to add the identity and chain certificates, refer to the **Add to Trust Stores** column.

| Appliance Identity Certificates | Details | Add to Trust Stores |
|---|---|---|
| Manager/ Central Manager | Add the Manager certificates to the Manager trust store and the trust store of every appliance in Central Management. | • Primary Manager<br>• Flow Collectors<br>• Flow Collector Databases (5000 series only)<br>• Flow Sensors<br>• UDP Directors<br>• Secondary Manager (Failover only) |
| Secondary Manager<br>(Failover Only) | If your Managers are configured for failover, and you are replacing the secondary Manager identity certificate, add the new secondary Manager | • Flow Collectors<br>• Flow Collector Databases (5000 series only)<br>• Flow Sensors |

| | | |
|---|---|---|
| | certificates to the secondary Manager trust store, the primary Manager trust store, and the trust store of every appliance in Central Management.<br>If you have not yet configured the failover pair, finish replacing the appliance identity, and then configure failover using the Failover Configuration Guide. | • UDP Directors<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| Flow Collector | Add the Flow Collector certificates to the Flow Collector trust store and the Manager trust store.<br>**5000 Series Only:**<br>• Add the Flow Collector engine certificates to the Flow Collector database trust store.<br>• Add the Flow Collector database certificates to the Flow Collector engine trust store. | • Flow Collector<br>• Flow Collector Databases (5000 series only)<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| Flow Sensor | Add the Flow Sensor certificates to the Flow Sensor trust store and the Manager trust store. | • Flow Sensor<br>• Secondary Manager (Failover only)<br>• Primary Manager |

| | | |
|---|---|---|
| UDP Director | Add the UDP Director certificates to the UDP Director trust store and the Manager trust store. | • UDP Director<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| UDP Director in High Availability Pair | • Add the secondary UDP Director certificates to the primary UDP Director trust store.<br>• Add the primary UDP Director certificates to the secondary UDP Director trust store. | • Secondary UDP Director (High Availability only)<br>• Primary UDP Director (High Availability only)<br>• Secondary Manager (Failover only)<br>• Primary Manager |

## 3. Replace the Appliance Identity Certificate

**Preparation:** Each appliance reboots automatically as part of this process, so plan to replace certificates at a time when your appliances will be experiencing relatively low volumes of traffic.

1. Open Central Management.
2. On the Appliance Manager page, click the ⋯ (**Ellipsis**) icon for the appliance.

   **Multiple Appliances:** Start with the Flow Collector, Flow Sensor, or UDP Director.
3. Return to the **Appliance** tab > **SSL/TLS Appliance Identity**.
4. In the **Friendly Name** field, enter a unique name for the certificate.
5. Click **Choose File**. Select the new certificate.

   Also, complete these steps for your certificate file format:

   - **PKCS#12:** In the Bundle Password field, enter the password required to decrypt the file. The password is not stored.
   - **PEM:** In the Certificate Chain File field, upload the Certificate Authority (CA) chain file separately (click Choose File). Make sure the chain file is in the correct order and meets the requirements. Refer to **PEM Chain File Requirements** in the Introduction for details.

⚠ Do not include the appliance identity certificate in the chain file.

6. Click **Replace Identity**.
7. Click **Apply Settings**.
8. Follow the on-screen prompts. The appliance reboots automatically.
9. Review the inventory in **Central Management** > **Appliance Manager**. Confirm the Appliance Status is shown as Connected.
10. Review the SSL/TLS Appliance Identity list. Confirm the new certificate is shown.

    **Multiple Appliances:** If you are updating the identity on all appliances in your cluster, repeat steps 1 through 11 on every appliance. Make sure each appliance finishes the configuration changes and returns to Connected before proceeding to the next appliance.

## 4. Trust the Certificate in the Desktop Client

The Desktop Client trusts only certificates saved in the default trust store installed on the local computer.

1. Log in to the Manager as admin: https://<IPAddress>
2. Click the ⤓ (**Download**) icon.
3. Follow the on-screen prompts to review the new certificate and trust it.

# Skipping the CSR in Central Management

If you already have certificates from a Certificate Authority that meet the **Appliance Identity Certificates** requirements, use the following instructions to replace the appliance identity certificate with a custom identity certificate.

## Overview

The overall steps are as follows:

1. **Add Certificates to the Trust Stores**
2. **Replace the Appliance Identity Certificate**
3. **Trust the Certificate in the Desktop Client**

## 1. Add Certificates to the Trust Stores

Before you update the appliance identity, add the Certificate Authority (CA) certificates to the required trust stores.

**Friendly Names:** If you are naming new certificates or adding them to the trust stores, make sure each friendly name is unique. Do not duplicate any friendly names.

**If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one certificate.

Make sure you upload the following certificates:

- identity
- chain (root and intermediate certificates)

> ⚠ When you add a certificate to your appliance trust store, your appliance trusts that identity and allows communication with it.

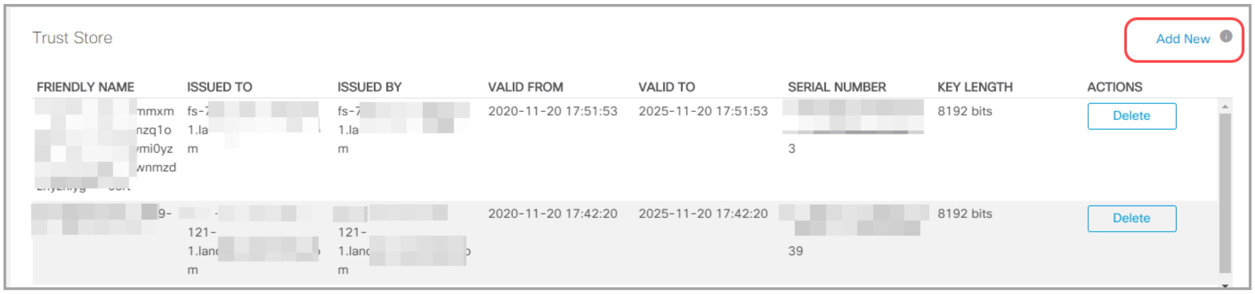
1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the appliance.

   **Order:** Select your appliances in the following order:

   - Flow Collectors
   - Flow Sensors
   - UDP Directors
   - Managers

> ⚠ Make sure you follow the selection order to update the trust stores of your appliances before you update the Manager trust store.

3. Choose **Edit Appliance Configuration**.
4. On the **General** tab, locate the Trust Store section.
5. Click **Add New**.



Trust Store

| FRIENDLY NAME | ISSUED TO | ISSUED BY | VALID FROM | VALID TO | SERIAL NUMBER | KEY LENGTH | ACTIONS |
|---|---|---|---|---|---|---|---|
| [redacted] mmxm<br>nzq1o<br>mi0yz<br>wnmzd | fs-[redacted]<br>1.la<br>m | fs-[redacted]<br>1.la<br>m | 2020-11-20 17:51:53 | 2025-11-20 17:51:53 | [redacted]<br>3 | 8192 bits | Delete |
| [redacted]9- | [redacted]<br>121-<br>1.lan[redacted]<br>m | [redacted]<br>121-<br>1.lan[redacted]<br>m | 2020-11-20 17:42:20 | 2025-11-20 17:42:20 | [redacted]<br>39 | 8192 bits | Delete |

6. In the **Friendly Name** field, enter a unique name for the certificate.
7. Click **Choose File**. Select the new certificate.
8. Click **Add Certificate**. Confirm the new certificate is shown in the Trust Store list.
    - **If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain.
    - Make sure you add the appliance identity certificate and certificate chain (if applicable) to the appliance trust store (its own trust store) and the trust stores shown in the **Trust Store Requirements** table.
9. Repeat steps 1 though 9 on each appliance trust store.

## Trust Store Requirements

Use this table to add the **appliance identity** and **certificate chain** (if applicable) to the appliance trust stores. If your file chain includes more than one certificate (root and intermediate certificates), upload each certificate individually to the trust store. Do not upload an entire chain as one certificate.

To confirm where to add the identity and chain certificates, refer to the **Add to Trust Stores** column.

| Appliance Identity Certificates | Details | Add to Trust Stores |
|---|---|---|
| Manager<br>Central Manager | Add the Manager certificates to the Manager trust store and the trust store of every appliance in Central Management. | • Primary Manager<br>• Flow Collectors<br>• Flow Collector Databases (5000 series only)<br>• Flow Sensors<br>• UDP Directors<br>• Secondary Manager (Failover only) |
| Secondary Manager<br>(Failover Only) | If your Managers are configured for failover, and you are replacing the secondary Manager identity certificate, add the new secondary Manager certificates to the secondary Manager trust store, the primary Manager trust store, and the trust store of every appliance in Central Management.<br>If you have not yet configured the failover pair, | • Flow Collectors<br>• Flow Collector Databases (5000 series only)<br>• Flow Sensors<br>• UDP Directors<br>• Secondary Manager (Failover only)<br>• Primary Manager |

| | | |
|---|---|---|
| | finish replacing the appliance identity, and then configure failover using the Failover Configuration Guide. | |
| Flow Collector | Add the Flow Collector certificates to the Flow Collector trust store and the Manager trust store.<br>**5000 Series Only:**<br>• Add the Flow Collector engine certificates to the Flow Collector database trust store.<br>• Add the Flow Collector database certificates to the Flow Collector engine trust store. | • Flow Collector<br>• Flow Collector Databases (5000 series only)<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| Flow Sensor | Add the Flow Sensor certificates to the Flow Sensor trust store and the Manager trust store. | • Flow Sensor<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| UDP Director | Add the UDP Director certificates to the UDP Director trust store and the Manager trust store. | • UDP Director<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| UDP Director in High Availability Pair | • Add the secondary UDP Director certificates to the | • Secondary UDP Director (High Availability only) |

| | | |
|---|---|---|
| | primary UDP Director trust store.<br>• Add the primary UDP Director certificates to the secondary UDP Director trust store. | • Primary UDP Director (High Availability only)<br>• Secondary Manager (Failover only)<br>• Primary Manager |

## 2. Replace the Appliance Identity Certificate

**Preparation:** Each appliance reboots automatically as part of this process, so plan to update certificates at a time when your appliances will be experiencing relatively low volumes of traffic.

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the appliance.

   **Multiple Appliances:** Start with the Flow Collector, Flow Sensor, or UDP Director. Update your Manager last.
3. Choose **Edit Appliance Configuration**.
4. Locate the **SSL/TLS Appliance Identity** section.
5. Click **Update Identity**.
6. Do you need to generate a CSR (Certificate Signing Request)? Choose **No**. click **Next**.
7. In the **Friendly Name** field, enter a unique name for the certificate.
8. Click **Choose File**. Choose the new certificate.
   - **Format:** PKCS#12 (.p12). For details, refer to **Appliance Identity Certificates** in the Introduction.
   - **Password:** In the Bundle Password field, enter the password required to decrypt the file. The password is not stored.
9. Click **Replace Identity**.
10. Click **Apply Settings**.
11. Follow the on-screen prompts. The appliance reboots automatically.
12. Review the inventory in **Central Management** > **Appliance Manager**. Confirm the Appliance Status is shown as Connected.
13. Review the SSL/TLS Appliance Identity list. Confirm the new certificate is shown.

**Multiple Appliances:** If you are updating the identity on all appliances in your cluster, repeat steps 1 through 13 on every appliance. Make sure each appliance finishes the configuration changes and returns to Connected before proceeding to the next appliance.

## 3. Trust the Certificate in the Desktop Client

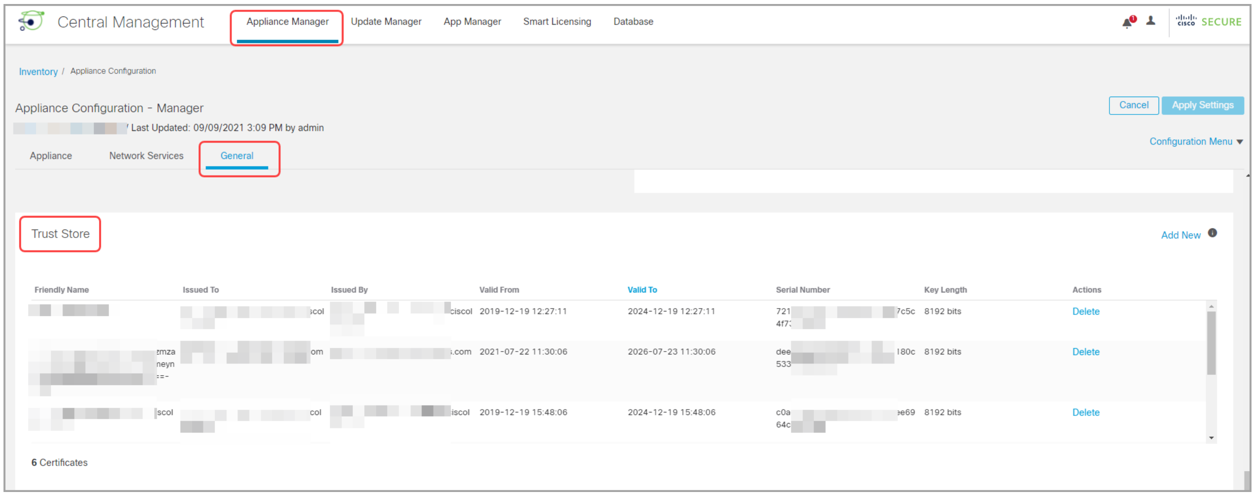
The Desktop Client trusts only certificates saved in the default trust store installed on the local computer.

1. Log in to the Manager as admin: https://<IPAddress>
2. Click the ⤓ (**Download**) icon.
3. Follow the on-screen prompts to review the new certificate and trust it.

# Reviewing Trust Store Certificates

Use the following instructions to review the certificates saved to the selected appliance trust store.

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. Choose the **General** tab.
5. Review the **Trust Store** list.



Appliance Configuration - Manager

[redacted] Last Updated: 09/09/2021 3:09 PM by admin

| Friendly Name | Issued To | Issued By | Valid From | Valid To | Serial Number | Key Length | Actions |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | 2019-12-19 12:27:11 | 2024-12-19 12:27:11 | [redacted] | 8192 bits | Delete |
| [redacted] | [redacted] | [redacted] | 2021-07-22 11:30:06 | 2026-07-23 11:30:06 | [redacted] | 8192 bits | Delete |
| [redacted] | [redacted] | [redacted] | 2019-12-19 15:48:06 | 2024-12-19 15:48:06 | [redacted] | 8192 bits | Delete |

**6** Certificates

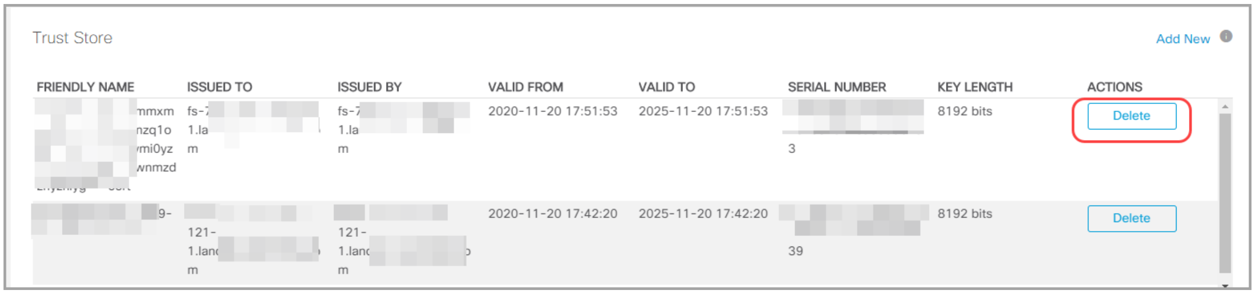
## Deleting Certificates from the Trust Stores

Use the following instructions to delete certificates from the appliance trust stores. Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

> ⚠ If you replace the appliance identity, do not delete the outdated certificates until you've added the new certificates (identity and chain) and fully completed the **Replacing the SSL/TLS Appliance Identity Certificate** instructions.

1. On the Trust Store list, locate the certificates you want to delete (identity, intermediate, or root).
2. Click **Delete**.

> ⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.



Trust Store

| FRIENDLY NAME | ISSUED TO | ISSUED BY | VALID FROM | VALID TO | SERIAL NUMBER | KEY LENGTH | ACTIONS |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | 2020-11-20 17:51:53 | 2025-11-20 17:51:53 | [redacted] | 8192 bits | Delete |
| [redacted] | [redacted] | [redacted] | 2020-11-20 17:42:20 | 2025-11-20 17:42:20 | [redacted] | 8192 bits | Delete |

3. Click **Apply Settings**. Follow the on-screen prompts.
4. On the Central Management inventory, confirm the appliance status returns to Connected.

## Trust Store Location

Refer to the Trust Stores column to confirm where appliance identity certificates (identity and chain) are saved. If the chain file was uploaded to the trust stores, the root and intermediate certificate files are listed individually.

| Appliance Identity Certificates | Trust Stores |
|---|---|
| Manager<br>Central Manager | • Primary Manager<br>• Flow Collectors<br>• Flow Collector Databases (5000 series only)<br>• Flow Sensors<br>• UDP Directors<br>• Secondary Manager (Failover only) |
| Secondary Manager<br>(Failover Only) | • Flow Collectors<br>• Flow Collector Databases (5000 series only)<br>• Flow Sensors<br>• UDP Directors<br>• Secondary Manager (Failover only)<br>• Primary Manager<br>**Manager Failover:**<br>If you delete an Manager failover relationship, delete the secondary Manager certificates from the trust stores of all appliances. Refer to the Failover Configuration Guide for details and instructions. |
| Flow Collector | • Flow Collector<br>• Secondary Manager (Failover only)<br>• Primary Manager |

| | |
|---|---|
| | **5000 Series Only:**<br>• The Flow Collector engine certificates are saved to the Flow Collector database trust store.<br>• The Flow Collector database certificates are saved to the Flow Collector engine trust store. |
| Flow Sensor | • Flow Sensor<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| UDP Director | • UDP Director<br>• Secondary Manager (Failover only)<br>• Primary Manager |
| UDP Director in High Availability Pair | • Secondary UDP Director (High Availability only)<br>• Primary UDP Director (High Availability only)<br>• Secondary Manager (Failover only)<br>• Primary Manager |

# Changing the Host Name or Network Domain Name

The appliance host name and network domain name are configured as part of the installation process using the Appliance Setup Tool. The Host Naming section of Central Management shows this information as read-only.

> ⓘ To change the appliance IP address, refer to **Changing Network Interfaces**.

## Reviewing the Current Configuration

Use the following instructions to review the host name and network domain name for a selected appliance.

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. Choose the **Appliance** tab.

## Changing the Host Name or Network Domain Name

Use the following instructions to change the appliance host name or network domain name. As part of this 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.

### Requirements

Before you change an appliance host name or network domain name, review the **Best Practices** in the Introduction, and review the following requirements:

- A unique host name and a fully qualified domain name are required for each appliance.

- **Manager Failover:** If your Managers are configured as a failover pair, delete the failover relationship before you change your Manager host name or network domain name. Follow the instructions in the Failover Configuration Guide.

## Select the Procedure for your Appliance

- **Manager**: **Manager**
- **Flow Collector, Flow Sensor, or UDP Director: Non-Manager Appliances**

⚠ If you are changing the host name or network domain name on the Manager and another appliance (such as the Flow Collector), complete the Manager procedure first.

# Manager

Use the following instructions to change the Managerhost name or network domain name. The procedure includes removing your appliances from Central Management temporarily. Make sure you follow the specified order. If you have several appliances, this procedure may take a significant amount of time. For assistance, please contact Cisco Support.

**Manager Failover:** If your Managers are configured as a failover pair, delete the failover relationship before you change these settings. Follow the instructions in the Failover Configuration Guide.

> ⚠ 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.

## Overview

The overall steps are as follows:

**1. Remove Appliances from Central Management**

**2. Change the Manager Host Name or Network Domain Name**

**3. Add Appliances to Central Management**

**4. Delete Outdated Manager Certificates from the Trust Stores**

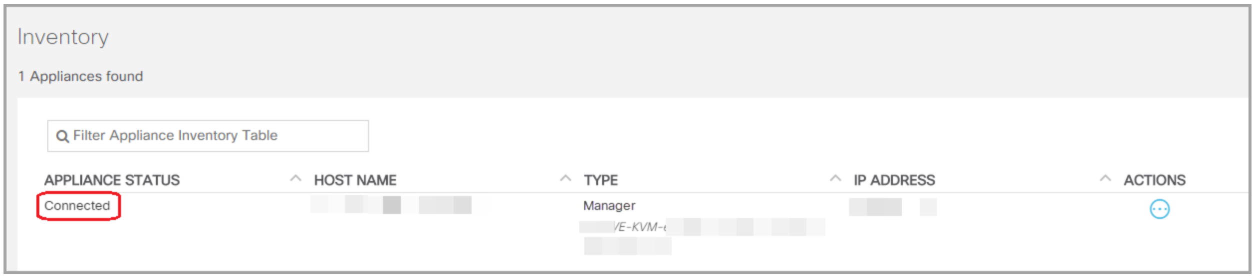
**5. Configure the Manager Failover Pair**

## 1. Remove Appliances from Central Management

1. Open Central Management.
2. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.
3. Remove every appliance **(except the primary Manager)** from Central Management.
   - On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the appliance.

- Choose **Remove This Appliance**.
- **Config Channel Down:** If the appliance status is shown as Config Channel Down, log in to the appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

4. Confirm the Manager appliance status is shown as Connected.



Inventory

1 Appliances found

Filter Appliance Inventory Table

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

5. Remove the primary Manager from Central Management.
    - On the Appliance Manager page, click the ⋯ (**Ellipsis**) icon for the primary Manager.
    - Choose **Remove This Appliance**.
    - **Config Channel Down:** If the appliance status is shown as Config Channel Down, log in to the Manager appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

## 2. Change the Manager Host Name or Network Domain Name

Use the following instructions to change the Manager host name or network domain name (and register the appliance in Central Management) using the Appliance Setup Tool.

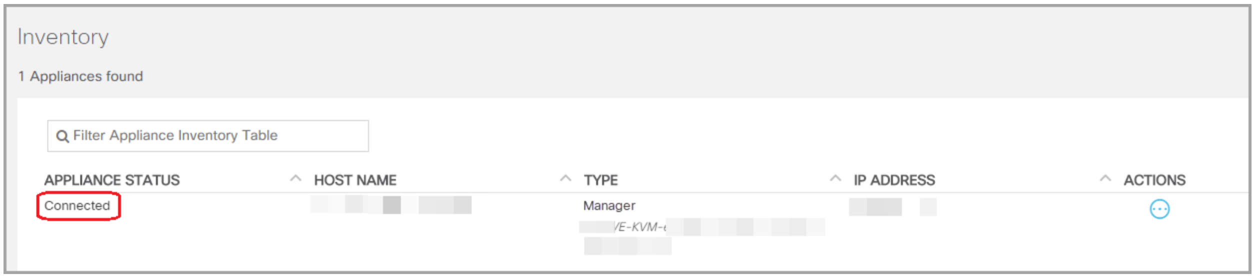
**Manager Failover:** If you have two Managers, you only need to complete this procedure on the primary Manager. You will register the secondary Manager in **3. Add Appliances to Central Management**.

1. Log in to the Manager as admin: https://<IPAddress>

    **Appliance Setup Tool:** If the Appliance Setup Tool does not open automatically, log in to the Manager appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

2. Click **Continue/Next** and scroll to the **Host Name and Domains** tab.
3. Enter the new host name or network domain name in the fields.
4. Click **Next** until the **Review and Restart** dialog opens.

5. Confirm your new configuration is correct. Click **Restart and Proceed**. Follow the on-screen prompts to restart the Manager.
6. Log in to the Manageragain.
7. On the **Register Your Appliance** tab, review the IP address and click **Save**.
    - This installs Central Management on the Manager.
    - The Manager IP address is detected automatically and cannot be changed.
8. When the appliance setup is completed, review the inventory in Central Management. Confirm the Manager appliance status is shown as **Connected**.



Inventory

1 Appliances found

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

## 3. Add Appliances to Central Management

Use the Appliance Setup Tool to add your other appliances to Central Management.

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Connected** before you start configuring the next appliance in your cluster.
- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** Follow the appliance configuration order.
- **Access:** You need admin privileges to access Central Management.

### Appliance Configuration Order

Configure your appliances in the following order, and note the details for each appliance:

| Order | Appliance | Details |
|---|---|---|
| 1. | UDP Directors (also known as FlowReplicators) | |
| 2. | Flow Collector 5000 | Make sure the Flow Collector 5000 |

| | | |
|---|---|---|
| | Series Database | series database is shown as Connected before you start the engine configuration. |
| 3. | Flow Collector 5000 Series Engine | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine configuration. |
| 4. | All Other Flow Collectors (NetFlow and sFlow) | |
| 5. | Flow Sensors | Make sure your Flow Collector is shown as Connected before you start the Flow Sensor configuration. |
| 6. | Secondary Manager (if used) | Make sure the primary Manager is shown as Connected before you start the secondary Manager configuration.<br>The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to **5. Configure the Manager Failover Pair**. |

1. In the address field of your browser, type **https://** followed by the IP address of the appliance.
    - **Connected:** Confirm each appliance is Connected before you add the next appliance to Central Management.
    - **Order:** Make sure you configure your appliances in order so they communicate correctly.
2. **Secondary Manager:** Enter the following credentials to log in:
    - **User Name:** admin
    - **Password:** lan411cope

**All Other Appliances:** Skip to step 4.

3. **Secondary Manager:** Enter new passwords for admin, root, and sysadmin. Click **Next** to scroll to each user.

   Use the following criteria:

   - **Length:** 8 to 256 characters
   - **Change:** Make sure the new password is different from the default password by at least 4 characters.

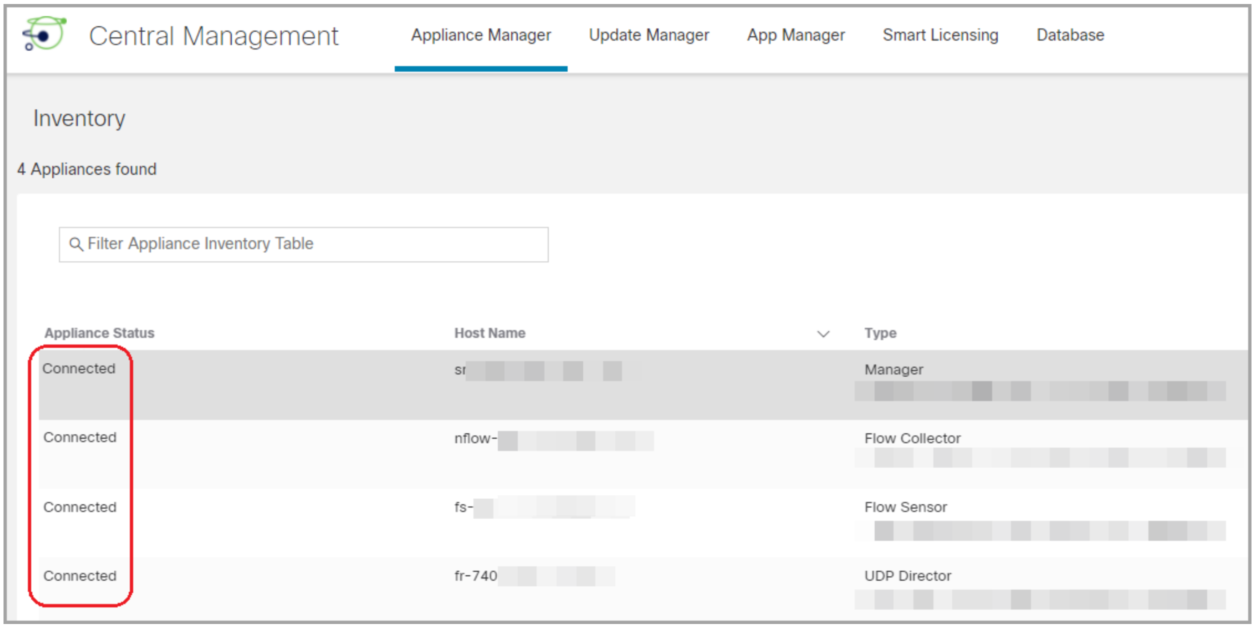
| User | Default Password |
|---|---|
| admin | lan411cope |
| root | lan1cope |
| sysadmin | lan1cope |

4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).
5. Add the appliance to Central Management as follows:
   - **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **5. Configure the Manager Failover Pair**.
   - **All Other Appliances:** Enter the IP address of your primary Manager. Click **Save**. Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manageradmin user name and password. Select the Secure Network Analytics domain and complete any other required info.

> ⓘ The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, select a Flow Collector.

6. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

> ⚠ The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. Make sure the primary Manager and each appliance is shown as Connected before you add the next appliance to Central Management using the [configuration order and details.]()



Inventory

4 Appliances found

| Appliance Status | Host Name | Type |
|---|---|---|
| Connected | sr[redacted] | Manager<br>[redacted] |
| Connected | nflow-[redacted] | Flow Collector<br>[redacted] |
| Connected | fs-[redacted] | Flow Sensor<br>[redacted] |
| Connected | fr-740[redacted] | UDP Director<br>[redacted] |

7. Repeat steps 1 through 6 to add each appliance to Central Management.

## 4. Delete Outdated Manager Certificates from the Trust Stores

Check each non-Manager trust store and delete the outdated Manager certificates. For details about where each appliance identity certificate is saved, refer to **Trust Store Location**.

> ⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Click the ••• (**Ellipsis**) icon for the appliance
2. Choose **Edit Appliance Configuration**.
3. Choose the **General** tab.
4. Review the **Trust Store** list. Locate all outdated Manager certificates (identity, intermediates, and root).
5. Click **Delete** to delete each outdated certificate.
6. Click **Apply Settings**. Follow the on-screen prompts.

7. On the Central Management inventory, confirm the appliance and Manager appliance status returns to Connected.
8. Repeat steps 1 through 7 on each Flow Collector, Flow Sensor, and UDP Director.

## 5. Configure the Manager Failover Pair

To reconfigure your Managers as a failover pair, follow the instructions in the Failover Configuration Guide.

# Non-Manager Appliances

Use the following instructions to change the host name or network domain name on non-Manager appliances (Flow Collector, Flow Sensor, and UDP Director).

> ⚠ 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.

## Overview

The overall steps are as follows:

**1. Remove the Appliance from Central Management**

**2. Change the Appliance Host Name or Network Domain Name**

> ℹ To change the Manager host name or network domain name, use the **Manager** instructions.

## 1. Remove the Appliance from Central Management

1. Open Central Management.
2. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.
3. Locate the appliance you are going to change. Click the ••• (**Ellipsis**) icon.
4. Choose **Remove This Appliance**.

   **Config Channel Down:** If the appliance status is shown as Config Channel Down, log in to the appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

## 2. Change the Appliance Host Name or Network Domain Name

You will use the Appliance Setup Tool to make configuration changes and add the appliance back to Central Management.

1. Log in to the appliance as admin: https://<IPAddress>

**Appliance Setup Tool:** If the Appliance Setup Tool does not open automatically, log in to the appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

2. Click **Continue/Next** and scroll to the **Host Name and Domains** tab.
3. Enter the new host name or network domain name in the fields.
4. Click **Next** until the **Review and Restart** dialog opens.
5. Review your settings. Click **Restart and Proceed**.
6. The appliance restarts.
7. Log in to the appliance.
8. Click **Continue/Next** to scroll to the **Central Management** tab in the Appliance Setup Tool.
    - Enter the IP address of your primary Manager/Central Manager. Click **Save**.
    - Follow the on-screen prompts to finish the changes in the Central Management tab.
9. Log in to the primary Manager/Central Manager.
    - Confirm the appliance is shown in the Appliance Manager inventory.
    - Confirm the Appliance Status is shown as **Connected**.

⚠ The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. If the appliance does not change to Connected, you may have outdated or duplicated certificates in your trust stores. Refer to **Troubleshooting** and **Deleting Certificates from the Trust Stores** for details.

# Changing Network Interfaces

The appliance network interfaces are configured as part of the installation process using the Appliance Setup Tool. You can change selected network interfaces in Central Management, or you can change the IP address (eth0 network interface) using the Appliance Setup Tool.

- **IP Address:** To change the appliance IP address, refer to **Changing the Appliance IP Address**.
- **Host Name or Domain Name:** To change the appliance host name or domain name, refer to **Changing the Host Name or Network Domain Name**.

## Reviewing the Current Configuration

Use the following instructions to review Network Interfaces for a selected appliance.

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. Choose the **Appliance** tab.

## Changing Network Interfaces in Central Management

Use the following instructions to add or change **eth1 or eth2 network interfaces** in Central Management.

The following interfaces cannot be changed in Central Management:

- **eth0:** To change the appliance IP address, refer to **Changing the Appliance IP Address**.
- **eth2 (Flow Collectors 5000 series only)** network interfaces
- Flow Sensor network interfaces
- UDP Director network interfaces

1. In the Network Interfaces section, locate the interface (eth1, eth2, etc.) you want to add or change.
2. Click the arrow.
3. Enter the required information in the following fields:

- IPV4 Address
- Subnet Mask
- Default Gateway
- Broadcast

4. Click **Save**.
5. Click **Apply Settings**.
6. Follow the on-screen prompts. The appliance reboots automatically.

## Changing the Appliance IP Address

Use the following instructions to change the **eth0 network interface**, which includes the appliance **IP address**. As part of this 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.

### Requirements

Before you change the appliance IP address (eth0 network interface), review the **Best Practices** in the Introduction, and review the following:

- **Record:** Before you make any changes, record your current network settings. Also, when you enter the new eth0 values, make sure the values are correct. If you enter incorrect values for eth0, you will lose connectivity and will need root access to fix it.

- **Manager Failover:** If your Managers are configured as a failover pair, delete the failover relationship before you change your Manager IP address. Follow the instructions in the Failover Configuration Guide.

## Select the Procedure for your Appliance

- **Manager: Manager**
- **Flow Collector, Flow Sensor, or UDP Director Non-Manager Appliances**

> ⚠ If you are changing the IP address on the Manager and another appliance (such as the Flow Collector), complete the Manager procedure first.

# Manager

Use the following instructions to change the Manager IP address (eth0 network interface). The procedure includes removing your appliances from Central Management temporarily. Make sure you follow the specified order. If you have several appliances, this procedure may take a significant amount of time. For assistance, please contact Cisco Support.

**Manager Failover:** If your Managers are configured as a failover pair, delete the failover relationship before you change these settings. Follow the instructions in the Failover Configuration Guide.

> ⚠ 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.

## Overview

The overall steps are as follows:

**1. Remove Appliances from Central Management**

**2. Change the Manager IP Address**

**3. Add Appliances to Central Management**

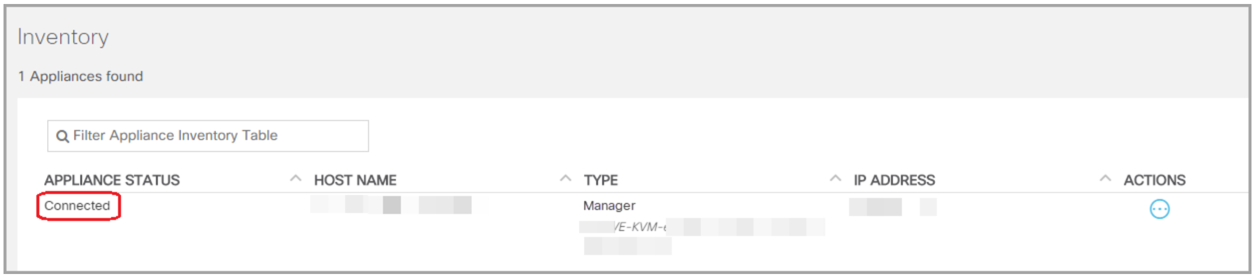
**4. Delete Outdated Manager Certificates from the Trust Stores**

**5. Configure the Manager Failover Pair**

## 1. Remove Appliances from Central Management

1. Open Central Management.
2. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.

3. Remove every appliance **(except the primary Manager)** from Central Management.
    - On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the appliance.
    - Choose **Remove This Appliance**.
    - **Config Channel Down:** If the appliance status is shown as Config Channel Down, log in to the appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.
4. Confirm the Manager appliance status is shown as Connected.



Inventory

1 Appliances found

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

5. Remove the primary Manager from Central Management.
    - On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the primary Manager.
    - Choose **Remove This Appliance**.
    - **Config Channel Down:** If the appliance status is shown as Config Channel Down, log in to the Manager appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

## 2. Change the Manager IP Address

Use the following instructions to change the Manager IP address and register it in Central Management using the Appliance Setup Tool.

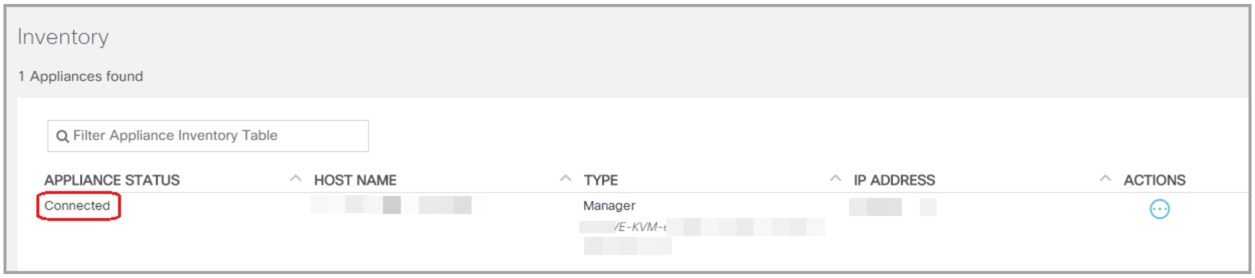
**Manager Failover:** If you have two Managers, you only need to complete this procedure on the primary Manager. You will register the secondary Manager in **3. Add Appliances to Central Management**.

1. Log in to the Manager as admin: https://<IP address>

    **Appliance Setup Tool:** If the Appliance Setup Tool does not open automatically, log in to the Manager. From the main menu, select **Recovery** > **RemoveAppliance**.

2. Click **Continue/Next** and scroll to the **Management Network Interface** tab.
3. Enter the new IP address in the field.

   When you change the IP address or Subnet Mask, the **Gateway and Broadcast Address** revert to their default settings. Make sure these fields are correct for your network before you proceed to the next step.
4. Click **Next** until the **Review and Restart** dialog opens.
5. Confirm your new configuration is correct. Click **Restart and Proceed**. Follow the on-screen prompts to restart the Manager.
6. Log in to the Manager (using the new IP address).
7. On the **Register Your Appliance** tab, review the IP address and click **Save**.
    - This installs Central Management on the Manager.
    - The Manager IP address is detected automatically and cannot be changed.
8. When the appliance setup is completed, review the inventory in Central Management. Confirm the Manager appliance status is shown as **Connected**.



Inventory

1 Appliances found

| APPLIANCE STATUS | HOST NAME | TYPE | IP ADDRESS | ACTIONS |
|---|---|---|---|---|
| Connected | [redacted] | Manager<br>[redacted] | [redacted] | ⋯ |

## 3. Add Appliances to Central Management

Use the Appliance Setup Tool to add your other appliances to Central Management.

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Connected** before you start configuring the next appliance in your cluster.
- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** Follow the appliance configuration order.
- **Access:** You need admin privileges to access Central Management.

## Appliance Configuration Order

Configure your appliances in the following order, and note the details for each appliance:

| Order | Appliance | Details |
|---|---|---|
| 1. | UDP Directors (also known as FlowReplicators) | |
| 2. | Flow Collector 5000 Series Database | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine configuration. |
| 3. | Flow Collector 5000 Series Engine | Make sure the Flow Collector 5000 series database is shown as Connected before you start the engine configuration. |
| 4. | All Other Flow Collectors (NetFlow and sFlow) | |
| 5. | Flow Sensors | Make sure your Flow Collector is shown as Connected before you start the Flow Sensor configuration. |
| 6. | Secondary Manager (if used) | Make sure the primary Manager is shown as Connected before you start the secondary Manager configuration.<br>The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to **5. Configure the Manager Failover Pair**. |

1. In the address field of your browser, type **https://** followed by the IP address of the appliance.

- **Connected:** Confirm each appliance is Connected before you add the next appliance to Central Management.
- **Order:** Make sure you configure your appliances in order so they communicate correctly.

2. **Secondary Manager:** Enter the following credentials to log in:
    - **User Name:** admin
    - **Password:** lan411cope

    **All Other Appliances:** Skip to step 4.

3. **Secondary Manager:** Enter new passwords for admin, root, and sysadmin. Click **Next** to scroll to each user.

    Use the following criteria:

    - **Length:** 8 to 256 characters
    - **Change:** Make sure the new password is different from the default password by at least 4 characters.

| User | Default Password |
|---|---|
| admin | lan411cope |
| root | lan1cope |
| sysadmin | lan1cope |

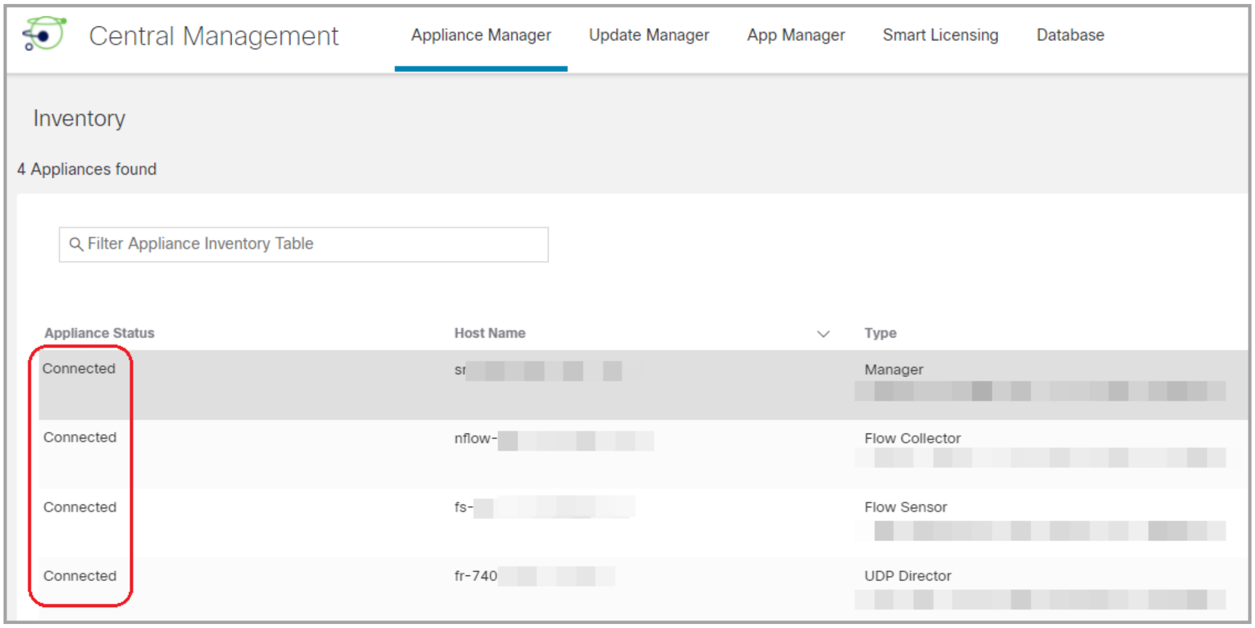
4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).
5. Add the appliance to Central Management as follows:
    - **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **5. Configure the Manager Failover Pair**.
    - **All Other Appliances:** Enter the IP address of your primary Manager. Click **Save**. Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manager admin user name and password.

Select the Secure Network Analytics domain and complete any other required info.

> The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, select a Flow Collector.

6. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

> The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. Make sure the primary Manager and each appliance is shown as Connected before you add the next appliance to Central Management using the configuration order and details.



Inventory

4 Appliances found

| Appliance Status | Host Name | Type |
|---|---|---|
| Connected | sr[redacted] | Manager<br>[redacted] |
| Connected | nflow-[redacted] | Flow Collector<br>[redacted] |
| Connected | fs-[redacted] | Flow Sensor<br>[redacted] |
| Connected | fr-740[redacted] | UDP Director<br>[redacted] |

7. Repeat steps 1 through 6 to add each appliance to Central Management.

## 4. Delete Outdated Manager Certificates from the Trust Stores

Check each non-Manager trust store and delete the outdated Manager certificates. For details about where each appliance identity certificate is saved, refer to **Trust Store Location**.

> Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

1. Click the ••• (**Ellipsis**) icon for the appliance.
2. Choose **Edit Appliance Configuration**.
3. Choose the **General** tab.
4. Review the **Trust Store** list. Locate all outdated Manager certificates (identity, intermediates, and root).
5. Click **Delete** to delete each outdated certificate.
6. Click **Apply Settings**. Follow the on-screen prompts.
7. On the Central Management inventory, confirm the appliance and Manager appliance status returns to Connected.
8. Repeat steps 1 through 7 on each Flow Collector, Flow Sensor, and UDP Director.

## 5. Configure the Manager Failover Pair

To reconfigure your Managers as a failover pair, follow the instructions in the Failover Configuration Guide.

## Non-Manager Appliances

Use the following instructions to change the IP address on your non-Manager appliances (Flow Collector, Flow Sensor, and UDP Director).

> ⚠ 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.

### Overview

The overall steps are as follows:

**1. Remove the Appliance from Central Management**

**2. Change the Appliance IP Address**

> ⓘ To change the Manager IP address, use the **Manager** instructions.

### 1. Remove the Appliance from Central Management

1. Open Central Management.
2. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.
3. Locate the appliance you are going to change. Click the ••• (**Ellipsis**) icon.
4. Choose **Remove This Appliance**.

   **Config Channel Down:** If the appliance status is shown as Config Channel Down, log in to the appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

### 2. Change the Appliance IP Address

You will use the Appliance Setup Tool to make configuration changes and add the appliance back to Central Management.

1. Log in to the appliance as admin: https://<IPAddress>

**Appliance Setup Tool:** If the Appliance Setup Tool does not open automatically, log in to the appliance console. From the main menu, select **Recovery** > **RemoveAppliance**.

2. Click **Continue/Next** and scroll to the **Management Network Interface** tab.
3. Enter the new IP address in the field.

   When you change the IP address or Subnet Mask, the **Gateway and Broadcast Address** revert to their default settings. Make sure these fields are correct for your network before you proceed to the next step.
4. Click **Next** until the **Review and Restart** dialog opens.
5. Review your settings. Click **Restart and Proceed**.
6. The appliance restarts.
7. Log in to the appliance (using the new IP address).
8. Click **Continue/Next** to scroll to the **Central Management** tab in the Appliance Setup Tool.
   - Enter the IP address of your primary Manager/Central Manager. Click **Save**.
   - Follow the on-screen prompts to finish the changes in the Central Management tab.
9. Log in to the primary Manager/Central Manager.
   - Confirm the appliance is shown in the Appliance Manager inventory.
   - Confirm the Appliance Status is shown as **Connected**.

⚠ The appliance status changes from **Initializing** or **Config Changes Pending** to **Connected**. If the appliance does not change to Connected, you may have outdated or duplicated certificates in your trust stores. Refer to **Troubleshooting** and **Deleting Certificates from the Trust Stores** for details.

# Adding SSL/TLS Client Identities

The client identity is used for communication between external services. If your Manager uses an external service, use this procedure to add a client identity certificate as required.

> Your certificates are critical for your system's security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss.

## Additional Certificate Configurations

This guide covers appliance identity and client identity configurations. There may be additional configurations in Secure Network Analytics that involve certificates and requirements for server identity verification. Make sure you follow the instructions in the help or guide for the feature.

- **Audit Log Destination:** Follow the instructions in the Help. Select 👤 (**User**) icon and search "Audit Log Destination."
- **Cisco ISE or Cisco ISE-Pic:** Follow the instructions in the ISE and ISE-PIC Configuration Guide.
- **LDAP:** Follow the instructions in the Help. Select ⚙ (**Global Settings**) icon and search "LDAP."
- **Packet Analyzer:** Follow the instructions in the Help. Select ⚙ (**Global Settings**) icon and search "Packet Analyzer."
- **SAML SSO:** Follow the instructions in the System Configuration Guide.
- **SMTP Configuration for Response Management:** Follow the instructions in the Help. Select 👤 (**User**) icon and search "SMTP Configuration."

> For additional configuration guides, refer to Configuration Guides.

## Certificate Requirements

If you add a client identity certificate, make sure you have certificates from a Certificate Authority. For certificate and trust store requirements, refer to **Client Identity Certificates** in the Introduction.

# Select the Procedure for your Environment

You can choose to generate a **Certificate Signing Request (CSR)** in Central Management or skip the CSR if you already have certificates from a Certificate Authority.

- To generate a Certificate Signing Request, go to **Generating the CSR in Central Management**.
- To skip the Certificate Signing Request, go to **Skipping the CSR in Central Management**.

# Generating the CSR in Central Management

Use the following instructions to generate a CSR in Central Management and add client identity certificates to your Manager.

## Overview

The overall steps are as follows:

**1. Generate a Certificate Signing Request**

**2. Add Certificates to the Trust Stores**

**3. Add the Client Identity Certificate**

## 1. Generate a Certificate Signing Request

Use the following instructions to prepare the Certificate Signing Request (CSR).

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the Manager.
3. Choose **Edit Appliance Configuration**.
4. Locate the **Additional SSL/TLS Client Identities** section.
5. Click **Add New**.
6. Do you need to generate a CSR (Certificate Signing Request)? Choose **Yes.** Click **Next**.

> ℹ If you do not need to generate a CSR, go to **Skipping the CSR in Central Management**.

7. Choose an **RSA Key Length** that is supported by your Certificate Authority.

> Choose the longest key length possible. We do not recommend using 2048 bits. Use 2048 bits only if it is required by the external service.

8. Complete the fields (optional) in the **Generate a CSR** section.
9. Click **Generate a CSR**. The generation process may take several minutes.

   **Cancel:** If you click **Cancel** after you generate a CSR, or anytime while you're waiting for the CA certificate, the canceled CSR will be invalid. Generate a new CSR in this case.
10. Click **Download CSR**.
11. Submit the downloaded CSRs to a Certificate Authority.

## 2. Add Certificates to the Trust Stores

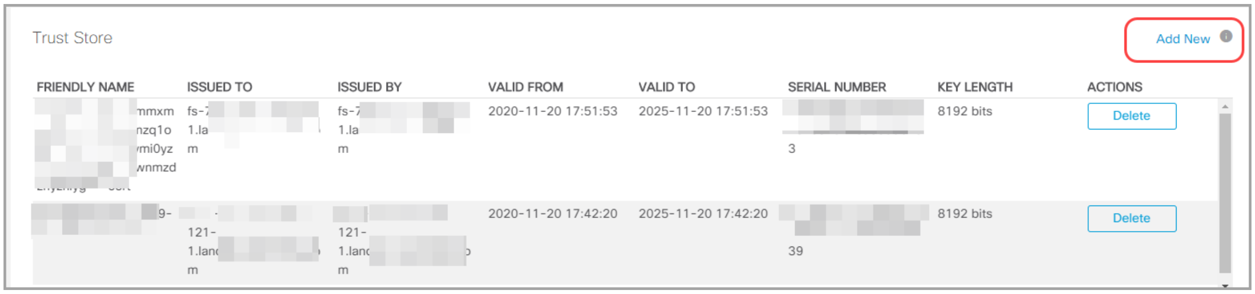
When you receive certificates from the Certificate Authority (CA), add them to the required trust stores.

**Friendly Names:** If you are naming new certificates or adding them to the trust stores, make sure each friendly name is unique. Do not duplicate any friendly names.

**If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one file.

> ⚠ When you add a certificate to your appliance trust store, your appliance trusts that identity and allows communication with it.

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the Manager.
3. Choose **Edit Appliance Configuration**.
4. On the **General** tab, locate the Trust Store section.
5. Click **Add New**.



Trust Store

| FRIENDLY NAME | ISSUED TO | ISSUED BY | VALID FROM | VALID TO | SERIAL NUMBER | KEY LENGTH | ACTIONS |
|---|---|---|---|---|---|---|---|
| [redacted] mmxm nzq1o mi0yz wnmzd | fs-[redacted] 1.la[redacted] m | fs-[redacted] 1.la[redacted] m | 2020-11-20 17:51:53 | 2025-11-20 17:51:53 | [redacted] 3 | 8192 bits | Delete |
| [redacted] 9- | [redacted] 121- 1.lan[redacted] m | [redacted] 121- 1.lan[redacted] m | 2020-11-20 17:42:20 | 2025-11-20 17:42:20 | [redacted] 39 | 8192 bits | Delete |

6. In the **Friendly Name** field, enter a unique name for the certificate.
7. Click **Choose File**. Select the new certificate.
8. Click **Add Certificate.** Confirm the new certificate is shown in the Trust Store list.

   **If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one file.

## 3. Add the Client Identity Certificate

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the Manager.
3. Choose **Edit Appliance Configuration**.
4. Return to the Appliance tab > Additional SSL/TLS Client Identities.
5. In the **Friendly Name** field, enter a name for the certificate.
6. Click **Choose File**. Select the new certificate.

   Also, complete these steps for your certificate file format:

   - **PKCS#12:** In the Bundle Password field, enter the password required to decrypt the file. The password is not stored.
   - **PEM:** In the Certificate Chain File field, upload the Certificate Authority (CA) chain file separately (click Choose File). Make sure the chain file is in the correct order and meets the requirements. Refer to **PEM Chain File Requirements** in the Introduction for details.

⚠ Do not include the client identity certificate in the chain file.

7. Click **Add Client Identity**.
8. Click **Apply Settings.**
9. Review the Additional SSL/TLS Client Identities list. Confirm the new certificate is shown.

# Skipping the CSR in Central Management

If you already have certificates from a Certificate Authority that meet the **Client Identity Certificates** requirements, follow the instructions to add them to your Manager.

## Overview

The overall steps are as follows:

**1. Add Certificates to the Trust Stores**

**2. Add the Client Identity Certificate**

## 1. Add Certificates to the Trust Stores

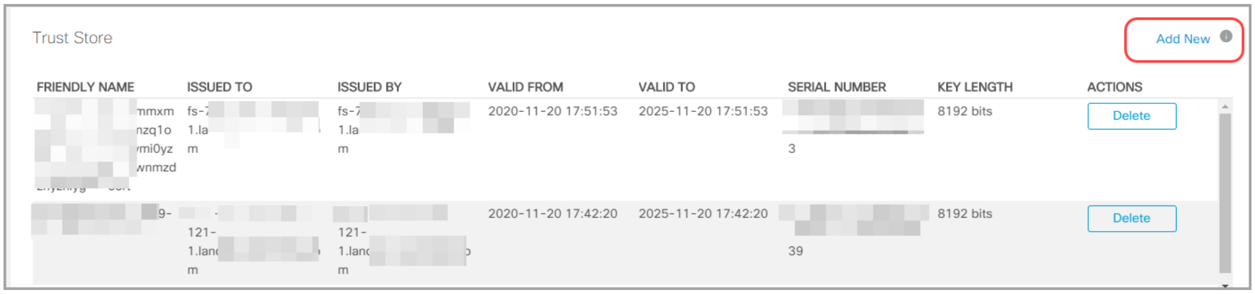
Add the Certificate Authority (CA) certificates to the required trust stores.

**Friendly Names:** If you are naming new certificates or adding them to the trust stores, make sure each friendly name is unique. Do not duplicate any friendly names.

**If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one certificate.

⚠ When you add a certificate to your appliance trust store, your appliance trusts that identity and allows communication with it.

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the Manager.
3. Choose **Edit Appliance Configuration**.
4. On the **General** tab, locate the Trust Store section.
5. Click **Add New**.



Trust Store

| FRIENDLY NAME | ISSUED TO | ISSUED BY | VALID FROM | VALID TO | SERIAL NUMBER | KEY LENGTH | ACTIONS |
|---|---|---|---|---|---|---|---|
| [redacted] mmxm nzq1o mi0yz wnmzd | fs-[redacted] 1.la[redacted] m | fs-[redacted] 1.la[redacted] m | 2020-11-20 17:51:53 | 2025-11-20 17:51:53 | [redacted] 3 | 8192 bits | Delete |
| [redacted] 9- | [redacted] 121- 1.lanc[redacted] m | [redacted] 121- 1.lanc[redacted] m | 2020-11-20 17:42:20 | 2025-11-20 17:42:20 | [redacted] 39 | 8192 bits | Delete |

6. In the **Friendly Name** field, enter a unique name for the certificate.
7. Click **Choose File**. Select the new certificate.

8. Click **Add Certificate**. Confirm the new certificate is shown in the Trust Store list.

   **If your file includes more than one certificate,** upload each certificate individually to the trust store. Do not upload an entire chain as one file.

## 2. Add the Client Identity Certificate

1. Open Central Management.
2. On the Appliance Manager page, click the ••• (**Ellipsis**) icon for the Manager.
3. Choose **Edit Appliance Configuration**.
4. Locate the **Additional SSL/TLS Client Identities** section.
5. Click **Add New**.
6. Do you need to generate a CSR (Certificate Signing Request)? Choose **No**. click **Next**.

> ℹ If you need to generate a CSR, go to **Generating the CSR in Central Management**.

7. In the **Friendly Name** field, enter a name for the certificate.
8. Click **Choose File**. Select the new certificate.
   - **Format:** PKCS#12. For details, refer to **Certificate Requirements**.
   - **Password:** In the Bundle Password field, enter the password required to decrypt the file. The password is not stored.
9. Click **Add Client Identity**.
10. Click **Apply Settings**.
11. Review the Additional SSL/TLS Client Identities list. Confirm the new certificate is shown.

# Deleting a Client Identity Certificate

1. Open Central Management.
2. Click the ••• (**Ellipsis**) icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. Choose the **Appliance** tab.
5. On the **Additional SSL/TLS Client Identities** list, locate the certificate you want to delete.
6. Click **Delete**.

# Troubleshooting

We've included some troubleshooting information here for your review. For assistance, please contact Cisco Support.

⚠ Your certificates are critical for your system’s security. Improperly modifying your certificates can stop Secure Network Analytics appliance communications and cause data loss.

## Do I have to select a certificate before I log in?

When you open the landing page for your Manager, you may be prompted to select a certificate before you can log in. This dialog does not affect whether or not you can log in to Secure Network Analytics. You may see this prompt if you have a certificate saved to your computer that contains the same Certificate Authority as your appliance identity certificate.

⚠ Check your company policy before you proceed.

## Why is my appliance identity certificate invalid?

If you replaced the appliance identity certificate with a custom certificate from a Certificate Authority, confirm it meets the requirements.

Also, make sure the new appliance identity certificates are saved to the required trust stores.

Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

## I removed the appliance from Central Management, but it is still managed.

If you removed your appliance from Central Management, but the system indicates it is still managed, remove the appliance from System Configuration:

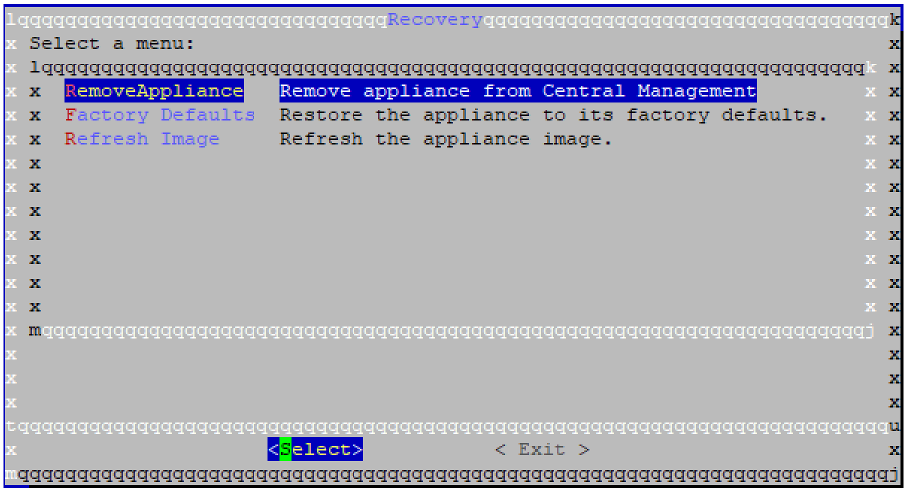
1. Log in to the appliance console as sysadmin.
    - **First:** If you are removing more than one appliance, log in to your Flow Collectors, Flow Sensors, and UDP Directors first.
    - **Last:** If you are removing more than one appliance, log in to the Manager last

(after you have completed steps 1 though 5 on all other appliances as needed).

⚠ Remove the Manager from Central Management last.

2. Type **SystemConfig**. Press Enter.
3. From the main menu, select **Recovery**.
4. Select **RemoveAppliance**.

   If the menu is not shown, the appliance is already removed from Central Management.



```
                                Recovery
 Select a menu:

   RemoveAppliance    Remove appliance from Central Management
   Factory Defaults   Restore the appliance to its factory defaults.
   Refresh Image      Refresh the appliance image.


                      <Select>          < Exit >
```

5. Follow the on-screen prompts to remove the appliance.

## The Appliance Status shows Initializing instead of Connected

If the appliance status is shown as **Initializing** or **Config Channel Down** and does not return to Connected, check the Manager trust store and the appliance trust store. Confirm you do not have duplicated certificates in the trust store. For example, if you have outdated certificates and new certificates in a trust store for the same appliance, there will be a conflict. Refer to the original procedure you used and refer to **Deleting Certificates from the Trust Stores** for details.

⚠ Make sure you only delete outdated certificates that are no longer valid. If you delete current certificates, it will break communication with your system.

# 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

# Copyright Information