



Cisco Secure Network Analytics

SSL/TLS Certificates for Managed Appliances 7.5.0



Table of Contents

Introduction	8
DoDIN and Common Criteria Compliance	8
Audience	8
Terminology	8
Planning Time	8
Best Practices	9
Replacing Your Certificates Before They Expire	10
Changing Network Settings	10
Manager Failover	10
Appliance Identity Certificates	11
Authentication	11
Certificate Requirements	11
Subject Alternative Name (SAN)	13
Testing Certificates	13
Self-Signed Certificates	14
Certificate Signed by a Certificate Authority (chain length = 2)	14
Certificate Signed by a Certificate Authority (chain length > 2)	14
Client Identity Certificates	15
Certificate Requirements	15
PEM Chain File Requirements	17
Trust Store Requirements	18
Wild Card Certificates (Client Identity Only)	18
Additional Certificate Configurations	18
Opening Central Management	19
Confirming the Appliance Status is Connected	19
Overview	20
Changing the TLS Version	22
Reviewing Certificates	23

Saving Certificates	24
Downloading Cisco Bundles	25
Receiving Notifications for Expiring Certificates	26
System Alarms	26
Email Notifications	26
Previously Enabled Email Notifications	26
Newly Enabled Email Notifications	27
Creating a Custom Email Notification	27
1. Create the Action	27
2. Create the Rule	29
Disabling an Email Notification	31
Enabling an Email Notification	32
Replacing Unexpired or Expired Certificates (Overview)	33
Replacing Unexpired Cisco Default Certificates (Certificate Refresh)	34
Requirements	34
Refreshing Certificates on All or Selected Appliances	35
Overview	35
1. Review the Appliance Status	35
2. Generate Certificates	36
3. Review Central Management	40
4. Review the Trust Stores	40
Replacing Expired Cisco Default Certificates	42
Requirements	42
1. Review the Appliance Status	42
2. Select the Procedure for your Appliance	43
Manager and Managed Appliances	43
Overview	44
1. Stop the Data Store Database	44
2. Remove Appliances from Central Management	45
3. Regenerate the Appliance Identity Certificate	45

4. Register your Manager in Central Management	48
5. Delete Expired Certificates from the Manager Trust Store	49
6. Add Appliances to Central Management	49
Appliance Configuration Order	49
7. Start the Data Store Database	52
8. Delete Expired Certificates from the Trust Stores	52
9. Configure the Manager Failover Pair	52
Individual, Non-Manager Appliances	53
Overview	53
1. Stop the Data Store Database	53
2. Remove the Appliance and Regenerate Certificates	54
3. Delete Expired Certificates from the Manager Trust Store	56
4. Add the Appliance to Central Management	57
5. Start the Data Store Database	57
Replacing the SSL/TLS Appliance Identity Certificate	59
Certificate Requirements	59
Select the Procedure for your Environment	59
Generating the CSR in Central Management	59
Overview	59
1. Generate a Certificate Signing Request	60
2. Add the Root CA Certificate to the Trust Stores	60
Trust Store Requirements	61
3. Stop the Data Store Database	63
4. Replace the Appliance Identity Certificate	64
5. Trust the Certificate in the Desktop Client	64
Skipping the CSR in Central Management	66
Overview	66
1. Add the Required Certificate to the Trust Stores	66
Trust Store Requirements	67
2. Stop the Data Store Database	69

3. Replace the Appliance Identity Certificate	69
4. Trust the Certificate in the Desktop Client	70
Reviewing Trust Store Certificates	71
Deleting Certificates from the Trust Stores	71
Trust Store Location	72
Changing the Host Name or Network Domain Name	75
Reviewing the Current Configuration	75
Changing the Host Name or Network Domain Name	75
Requirements	76
Select the Procedure for your Appliance	76
Manager	77
Overview	77
1. Stop the Data Store Database	77
2. Remove Appliances from Central Management	78
3. Change the Manager Host Name or Network Domain Name	78
4. Register the Manager in Central Management	79
5. Add Appliances to Central Management	79
Appliance Configuration Order	80
6. Start the Data Store Database	82
7. Delete Outdated Manager Certificates from the Trust Stores	82
8. Configure the Manager Failover Pair	83
Non-Manager Appliances	84
Overview	84
1. Stop the Data Store Database	84
2. Remove the Appliance from Central Management	85
3. Change the Appliance Host Name or Network Domain Name	85
4. Add the Appliance to Central Management	85
5. Start the Data Store Database	86
Changing Network Interfaces	87
Reviewing the Current Configuration	87

Changing Network Interfaces in Central Management	87
Changing the Appliance IP Address	88
Requirements	88
Select the Procedure for your Appliance	89
Manager	89
Overview	89
1. Remove Appliances from Central Management	90
2. Change the Manager IP Address	90
3. Register the Manager in Central Management	91
4. Add Appliances to Central Management	91
Appliance Configuration Order	91
5. Delete Outdated Manager Certificates from the Trust Stores	93
6. Configure the Manager Failover Pair	94
Non-Manager Appliances	95
Overview	95
1. Remove the Appliance from Central Management	95
2. Change the Appliance IP Address	96
3. Add the Appliance to Central Management	96
Adding SSL/TLS Client Identities	97
Additional Certificate Configurations	97
Certificate Requirements	97
Select the Procedure for your Environment	97
Generating the CSR in Central Management	98
Overview	98
1. Generate a Certificate Signing Request	98
2. Add Certificates to the Trust Stores	99
3. Add the Client Identity Certificate	100
Skipping the CSR in Central Management	101
Overview	101
1. Add Certificates to the Trust Stores	101

2. Add the Client Identity Certificate	102
Deleting a Client Identity Certificate	103
Troubleshooting	104
Do I have to select a certificate before I log in?	104
Why is my appliance identity certificate invalid?	104
I removed the appliance from Central Management, but it is still managed.	104
The Appliance Status shows Initializing instead of Connected	105
Contacting Support	106
Change History	107

Introduction

Use this guide to change SSL/TLS certificate-related configurations on your Cisco Secure Network Analytics (formerly Stealthwatch) v7.5.0 appliances:

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

For details, refer to [Overview](#).

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).

The appliance identity certificate is a leaf certificate.

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.

Managers: For example, if you are replacing an expired appliance identity certificate with a new Cisco self-signed appliance identity certificate 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: For example, if you are replacing an expired appliance identity certificate with a new Cisco self-signed appliance identity certificate on an individual, non-Manager appliance (Flow Collectors, Flow Sensors, UDP Directors, or Data Nodes), 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.

- **Data Store:** Many procedures in this guide require stopping the Data Store database. If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.

Replacing Your Certificates Before They Expire

-  Make sure you replace your appliance identity certificates before they expire. To check expiration dates, follow the instructions in [Reviewing Certificates](#).


You can replace your unexpired appliance identity certificates as follows:


- **Cisco Certificates (Certificate Refresh):** To generate new Cisco self-signed appliance identity certificates on all or selected appliances, refer to [Replacing Unexpired Cisco Default Certificates \(Certificate Refresh\)](#) for instructions. The appliance host information (IP address, host name, domain name) is preserved.
- **Custom Certificates:** To replace your appliance identity certificates with custom certificates, refer to [Appliance Identity Certificates](#) for requirements and [Replacing the SSL/TLS Appliance Identity Certificate](#) for instructions.

If your certificates have already expired, refer to [Replacing Expired Cisco Default Certificates](#) for instructions, or replace them with custom certificates.

Changing Network Settings

If you change a network setting ([host name](#), [network domain name](#), or [eth0 IP address](#)), you may be prompted to generate a new appliance identity certificate. Make sure you follow the on-screen prompts and review if regenerating the certificate is required or if you can choose to preserve it.

-  **If you are using custom certificates**, save your certificates before you change your network settings (host name, network domain name, or eth0 IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

-  **Do not change the eth0 network interface on Data Nodes using this guide.** To change the eth0 IP address on any Data Nodes, contact [Cisco Support](#) for professional assistance.

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.

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

Use the following guidelines to replace a Secure Network Analytics appliance identity certificate with a custom certificate.

- Refer to [Replacing the SSL/TLS Appliance Identity Certificate](#) for instructions.
- **Generate CSR in Central Management:** If you generate the CSR in Central Management, the listed requirements designated with (*) are included in the CSR (refer to the [Generate the CSR in Central Management](#) column).
- **Skip the CSR in Central Management:** If you generate the CSR outside of Central Management, confirm the CSR includes the requirements in this table (refer to the [Skip CSR in Central Management](#) column).
- **Verifying and Testing Certificate Requirements:** Whether you generate the CSR in Central Management or skip the CSR, confirm your certificates meet the requirements in this table before you use them to replace your appliance identity certificates. Also, refer to [Testing Certificates](#) to test your certificates.

Requirements	Generate CSR in Central Management	Skip CSR in Central Management
File Format*	PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks) If you use PEM, refer to PEM Chain File Requirements .	PKCS#12 (.p12, .pfx, .pks)
Keys*	RSA Key Lengths Available: 2048 bits (not recommended), 4096 bits, or 8192 bits	RSA Key Lengths Required: 2048 bits (not recommended) or more or ECDSA Key Curves Required: NIST P-256, P-384, or P-521

Requirements	Generate CSR in Central Management	Skip CSR in Central Management
	ECDSA Curves: Not available	
Common Name or Subject Alternative Name*	The CSR requests the Common Name and/or Subject Alternative Name matches the FQDN.	Confirm the Common Name and/or Subject Alternative Name matches the FQDN.
Signed by	Confirm the appliance identity certificate is self-signed or signed by a Certificate Authority.	Confirm the appliance identity certificate is self-signed or signed by a Certificate Authority.
Authentication (Extended Key Usage)*	The CSR requests server (serverAuth) and client (clientAuth) authentication.	Server (serverAuth) and client (clientAuth) authentication are required for appliance identity certificates.
Unique Identification (Self-Signed Only)	Confirm the self-signed appliance identity certificate uses: <ul style="list-style-type: none"> • A unique Subject Name (date, identifier, string, etc.) compared to other certificates in the trust store or <ul style="list-style-type: none"> • An Authority Key Identifier and a Subject Key Identifier. If you use these key identifiers, 	Confirm the self-signed appliance identity certificate uses: <ul style="list-style-type: none"> • A unique Subject Name (date, identifier, string, etc.) or <ul style="list-style-type: none"> • A unique Authority Key Identifier and a Subject Key Identifier. If you use these key identifiers, confirm the certificate you are replacing

Requirements	Generate CSR in Central Management	Skip CSR in Central Management
	confirm the certificate you are replacing includes key identifiers. We do not include these key identifiers in our default appliance identity certificates.	includes key identifiers. We do not include these key identifiers in our default appliance identity certificates.
Date Range	Confirm the certificate dates are current and not expired.	Confirm the certificate dates are current and not expired.

**If you generate the CSR in Central Management, the listed requirements designated with (*) are included in the CSR.*

Subject Alternative Name (SAN)

Your appliance Network IP Mode setting determines the SAN in the Cisco self-signed certificate and when [generating a CSR](#) as follows:

- **IPv4:** IPv4 SAN
- **IPv6:** IP SAN not available
- **Dual Stack:** IPv4 SAN

For more information about the Network IP Mode, refer to the [System Configuration Guide](#).

Testing Certificates

Before you use replace your appliance identity certificates, test your certificates to confirm they meet the system requirements.

Test the new identity certificate with your intermediate CA certificates and root CA certificate organized into separate files.

- **PEM (.cer, .crt, .pem) Files:** If you're using openssl to generate your .cer, .crt, or .pem file to upload certificates to Central Management, combine the CA certificates into one certificate chain file after you finish testing your certificates. For more information, refer to [PEM Chain File Requirements](#).
- **PKCS#12 (.p12, .pfx, .pks) Files:** If you're using openssl to generate your .p12, .pfx, or .pks file to upload certificates to Central Management, combine the CA

certificates into one file (specified by the `-certfile` argument) after you finish testing your certificates.

Self-Signed Certificates

Run the following command on a laptop or any server with openSSL where your self-signed certificates are saved:

```
openssl verify -CAfile <identity-cert-file> <identity-cert-file>
```

Certificate Signed by a Certificate Authority (chain length = 2)

Run the following command on a laptop or any server with openSSL where your CA-signed certificates are saved:

```
openssl verify -CAfile <root-ca-cert-file> <identity-cert-file>
```

Certificate Signed by a Certificate Authority (chain length > 2)

Run the following command on a laptop or any server with openSSL where your CA-signed certificates are saved:

```
openssl verify -CAfile <root-ca-cert-file> -untrusted <intermediate-ca-certs-file> <identity-cert-file>
```

Client Identity Certificates

The client identity is used for communication between external services. Refer to [Adding SSL/TLS Client Identities](#) for instructions.

Certificate Requirements

Use the following guidelines to add a client identity certificate to the Manager.

- Refer to [Adding SSL/TLS Client Identities](#) for instructions.
- **Generate CSR in Central Management:** If you generate the CSR in Central Management, the listed requirements designated with (*) are included in the CSR (refer to the **Generate the CSR in Central Management** column).
- **Skip the CSR in Central Management:** If you generate the CSR outside of Central Management, confirm the CSR includes the requirements in this table (refer to the **Skip CSR in Central Management** column).
- **Verifying Certificate Requirements:** Whether you generate the CSR in Central Management or skip the CSR, confirm your certificates meet the requirements in this table before you add them to your Manager.

Requirements	Generate CSR in Central Management	Skip CSR in Central Management
File Format*	PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks) If you use PEM, refer to PEM Chain File Requirements .	PKCS#12 (.p12, .pfx, .pks)
Keys*	RSA Key Lengths Available: 2048 bits (not recommended), 4096 bits, or 8192 bits ECDSA Curves: Not available	RSA Key Lengths Required: 2048 bits (not recommended) or more or ECDSA Key Curves Required: NIST P-256, P-384, or P-521
Signed By	Confirm the client identity	Confirm the client identity

Requirements	Generate CSR in Central Management	Skip CSR in Central Management
	certificate is self-signed or signed by a Certificate Authority.	certificate is self-signed or signed by a Certificate Authority.
Authentication (Extended Key Usage)*	The CSR requests client (clientAuth) authentication.	Client (clientAuth) authentication is required for client identity certificates.
Date Range	Confirm the certificate dates are current and not expired.	Confirm the certificate dates are current and not expired.

**If you generate the CSR in Central Management, the listed requirements designated with (*) are included in the CSR.*

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, you will upload 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 –
```



Do not include the identity certificate in the chain file.

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.





- **Custom Certificates:** If you replace the appliance identity certificate with a custom certificate, you need to upload the required certificate to the required trust stores. Refer to [Replacing the SSL/TLS Appliance Identity Certificate](#) for instructions.
- **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. Click the  (**Help**) icon. Choose **Help**. 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. Click the  (**Help**) icon. Choose **Help**. Search "LDAP."
- **Packet Analyzer:** Follow the instructions in the Help. Click the  (**Help**) icon. Choose **Help**. Search "Packet Analyzer."
- **SAML SSO:** Follow the instructions in the [System Configuration Guide](#).
- **SMTP Configuration for Response Management:** Follow the instructions in the Help. Click the  (**Help**) icon. Choose **Help**. Search "SMTP Configuration."

 For additional configuration guides, refer to [Configuration Guides](#).

Opening Central Management

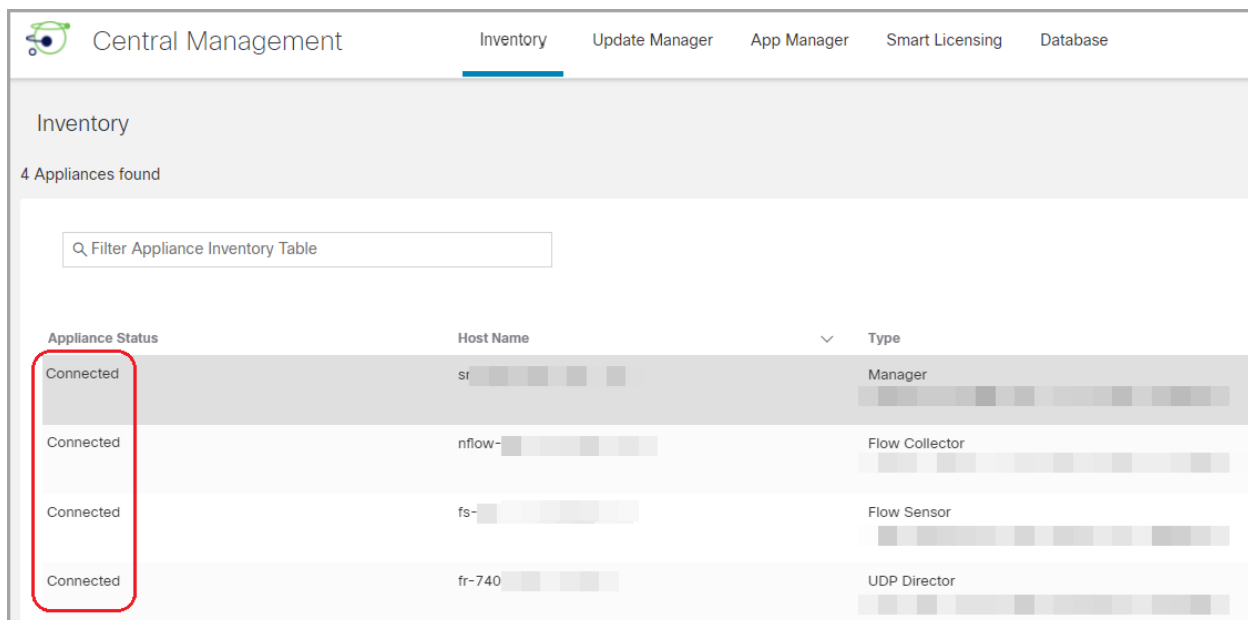
You will primarily use Central Management in this guide.

1. Log in to the Manager as admin: `https://<IPAddress>`
2. From the main menu, select **Configure > GLOBAL 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.



The screenshot shows the 'Central Management' interface with the 'Inventory' tab selected. It displays a table of 4 appliances. The 'Appliance Status' column for all entries is 'Connected', which is highlighted with a red box. The table includes columns for 'Appliance Status', 'Host Name', and 'Type'.

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

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	Review Cisco Bundles information.
Receiving Notifications for Expiring Certificates	Configure email notifications for certificates that are about to expire.
Replacing Unexpired or Expired Certificates	<p>To generate new Cisco self-signed appliance identity certificates when your existing certificates have not expired (and preserve the appliance host information), refer to Replacing Unexpired Cisco Default Certificates (Certificate Refresh).</p> <p>To review additional options for replacing your unexpired or expired certificates, review Replacing Unexpired or Expired Certificates (Overview).</p>
Replacing the Appliance Identity Certificate	Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate.

	<p>Follow the instructions to replace the appliance identity certificate with a custom certificate from a Certificate Authority.</p>
<p>Changing the Host Name</p>	<p>Change the appliance host name on appliances that use Cisco default certificates.</p> <p>If your appliance uses a custom certificate, please contact Cisco Support to change these settings.</p>
<p>Changing the Network Domain Name</p>	<p>Change the network domain name on appliances that use Cisco default certificates.</p> <p>If your appliance uses a custom certificate, please contact Cisco Support to change these settings.</p>
<p>Changing the IP address (eth0)</p>	<p>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.</p> <p>If your appliance uses a custom certificate, please contact Cisco Support to change these settings.</p>
<p>Client Identity Certificates</p>	<p>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.</p>
<p>Troubleshooting</p>	


Changing the TLS Version

Use the following instructions to choose the TLS version support for your appliances. You can choose different modes within your system. We support the following:

- TLS 1.2 and 1.3 (default)
- TLS 1.3 only (not supported for Data Store)

To change the TLS version on an appliance, complete the following steps:

1. Log in to the appliance console (SystemConfig) as sysadmin.
2. Select **Security**.
3. Select **TLS Version**.
4. To choose the TLS version, select it and click it (or press the space key on your keyboard). [*] indicates the selected version.

 Do not use **TLS v1.3 only** if you have a Data Store deployed.

5. Click **OK**. The appliance restarts.
6. Open [Central Management](#). Confirm all appliances are shown as Connected.

Reviewing Certificates

Use the following instructions to review the appliance identity certificate or client identity certificates for the selected appliance. You can review details such as the friendly name, issued information, and expiration date.

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.
6. **Expiration Date:** Review the **Valid To** column.

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 or host name 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.

Receiving Notifications for Expiring Certificates

We provide **System Alarms** on your dashboard when appliance identify certificates are about to expire. Additionally, you have the option to also receive **Email Notifications**.

System Alarms

When you have appliance identity certificates expiring, the following system alarms will begin displaying on your dashboard:

- Appliance Certificate Expiration less than 90 days
- Appliance Certificate Expiration less than 60 days
- Appliance Certificate Expiration less than 30 days
- Appliance Certificate Expiration less than 14 days
- Appliance Certificate Expiration less than 3 days
- Appliance Certificate has expired

These system alarms are enabled by default and will continue to display until you've replaced the required appliance identity certificates. See **Replacing Expired Cisco Default Certificates** for details about replacing appliance identity certificates.

Email Notifications

Email notifications are set up through Response Management. For more information about email notifications, go to the *Response Management: Action Types* Help topic.

Previously Enabled Email Notifications

If email notifications have already been enabled for Manager System Alarms, you'll begin receiving **all** of the appliance identity certificate expiration email notifications by default in addition to email notifications for other system alarms.



When email notifications for Manager System Alarms have already been set up by another user or for another purpose, we suggest **Creating a Custom Email Notification** to avoid undoing the email notifications already configured.

To limit the email notifications you receive, you have the following options:

- Set up email notifications specifically for expiring appliance identify certificates. See [Creating a Custom Email Notification](#).
- Disable email notifications you don't want to receive. See [Disabling an Email Notification](#).

Newly Enabled Email Notifications

If you newly enable email notifications for Manager System Alarms, make sure to specify which email notifications you'd like to receive. We suggest [Creating a Custom Email Notification](#) so you'll receive only the email notifications you'd like to receive.

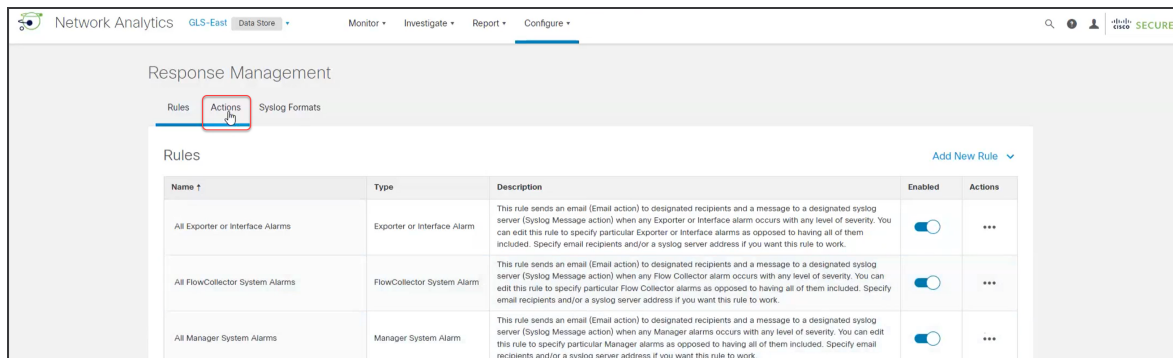
Creating a Custom Email Notification

Start with **1. Create the Action** to create a new action; and then go to **2. Create the Rule** to assign the rule to the action you've created.

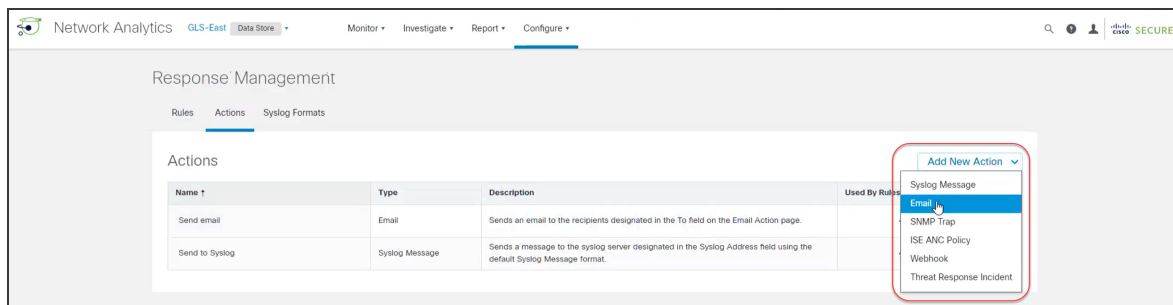
1. Create the Action

Use the following instructions to create a new action for certificate expiration email notifications:

1. From the main menu, select **Configure > DETECTION Response Management**.
2. Click the **Actions** tab.



3. In the Actions area, select **Email** from the **Add New Actions** menu.



- In the **Name** field, type a name; "Send Cert Expiration Email" for example. You may also want to add a description in the **Description** field.

Response Management

Rules Actions Syslog Formats

Email Action Cancel Save

Warning: You must configure SMTP before using an Email action. To do this, from the toolbar in the upper right corner of the page, select Configure > GLOBAL Central Management. From the Actions menu for the Manager, select Edit Appliance Configuration. Click the General tab and scroll down to the SMTP Configuration section.

Name: Description:

Enabled Disabled actions are not performed for any associated rules.

To:

i Make sure the **Enabled** button is toggled on.

- In the **To** field, type the email address (and/or list alias) for anyone who should be notified when appliance identity certificates are expiring.

To:

Subject:

Body:

+ Alarm Variables Preview

- Make sure your selection is added to the **To** field by clicking on it.

To:

ame@Company.com

Name@Company.com +

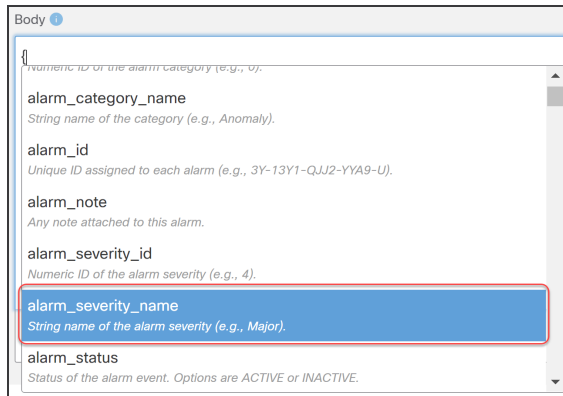
- It displays highlighted in green after it is added.

To:

Name@Company.com X

6. Click **+Alarm Variable** at the bottom of the **Body** area, then select each variable you'd find helpful in managing your email notifications. For example:

- alarm_severity_name
- alarm_status
- alarm_category_name



7. Copy your selections, then paste them in the **Subject** field.

8. Click **Preview** to see a sample of how your email notifications will appear.

- Click **Test Action** to send a test email notification.
- Click **Edit** to make any changes, if needed.

i To dismiss the preview, click **Edit** or anywhere in the **Body** area.

9. Click **Save**.

2. Create the Rule

Use the following instructions to create a new rule to assign the action you created.

1. Click the **Rules** tab.
2. Locate the **All Manager System Alarms** row of the Rules table, then click the **(Ellipsis)** icon in the Actions column.
3. Select **Duplicate**.

4. Locate the **Associated Actions** area, then toggle on the Assigned column for the action you just created in both the **active** and **inactive** tables.

Associated Actions

Execute the following actions when the alarm becomes *active*:

Name ↑	Type	Description	Used By Rules	Assigned
Send Cert Expiration Email	Email		0	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>

Execute the following actions when the alarm becomes *inactive*:

Name ↑	Type	Description	Used By Rules	Assigned
Send Cert Expiration Email	Email		0	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>

5. Toggle on the Assigned column for the action you just created in both the **active** and **inactive** tables.
6. Locate the **Name** field in the **Rules | Manager System Alarm** area, then type a name; "Cert Exp Rule" for example. You may also want to add a description in the **Description** field.

Network Analytics swbeta - Monitor - Investigate - Report - Configure - Apps -

Response Management

Rules | Manager System Alarm

Name: Cert Exp Rule

Description:

Enabled Disabled rules are not triggered even when associated conditions are met.

Rule is triggered if:

ANY of the following is true:

- Type is Appliance Certificate Expiration less than 90 days
- Type is Appliance Certificate Expiration less than 60 days
- Type is Appliance Certificate Expiration less than 30 days
- Type is Appliance Certificate Expiration less than 14 days
- Type is Appliance Certificate Expiration less than 3 days
- Type is Appliance Certificate has expired

i Make sure the **Enabled** button is toggled on.

- In the **Rule is triggered if:** area, select **ANY**.

- Select **Type**, then scroll through the list to select each email notifications you'd like to receive.
- Click the **+** (Plus) icon to add a type; click the **-** (Minus) icon to remove a type.
- Click **Save**.

Disabling an Email Notification

Use the following instructions to disable one or more email notifications:

- From the main menu, select **Configure > DETECTION Response Management**.
- Locate the **All Manager System Alarms** row of the Rules table, then click the **(Ellipsis)** icon in the Actions column.
- Select **Edit**.

Name ↑	Type	Description	Enabled	Actions
All Exporter or Interface Alarms	Exporter or Interface Alarm	This rule sends an email (Email action) to designated recipients and a message to a designated syslog server (Syslog Message action) when any Exporter or Interface alarm occurs with any level of severity. You can edit this rule to specify particular Exporter or Interface alarms as opposed to having all of them included. Specify email recipients and/or a syslog server address if you want this rule to work.	<input checked="" type="checkbox"/>	...
All FlowCollector System Alarms	FlowCollector System Alarm	This rule sends an email (Email action) to designated recipients and a message to a designated syslog server (Syslog Message action) when any Flow Collector alarm occurs with any level of severity. You can edit this rule to specify particular Flow Collector alarms as opposed to having all of them included. Specify email recipients and/or a syslog server address if you want this rule to work.	<input checked="" type="checkbox"/>	...
All Manager System Alarms	Manager System Alarm	This rule sends an email (Email action) to designated recipients and a message to a designated syslog server (Syslog Message action) when any Manager alarms occurs with any level of severity. You can edit this rule to specify particular Manager alarms as opposed to having all of them included. Specify email recipients and/or a syslog server address if you want this rule to work.	<input checked="" type="checkbox"/>	... Edit Duplicate Delete
All UDP Director Alarms	UDP Director Alarm	This rule sends an email (Email action) to designated recipients and a message to a designated syslog server (Syslog Message action) when any UDP Director alarm occurs with any level of severity. You can edit this rule to specify particular UDP Director alarms as opposed to having all of them included. Specify email recipients and/or a syslog server address if you want this rule to work.	<input checked="" type="checkbox"/>	...
Inside Hosts as the Source of alarm	Host Alarm	Notify when a Worm Propagation or Bot Infected Host - Successful C&C Activity alarm is triggered by an Inside host. This rule was created as an example. If you want to use it, assign an action and then enable both the action and the rule.	<input type="checkbox"/>	...

The page displays as follows.

4. In the **Rule is triggered if:** area, select **NONE**.
5. Select **Type**, then scroll through the list to select the email notification you'd like to disable.
6. Click the **+** (Plus) icon and repeat step 5 to disable an additional email notification.
7. Click **Save**.

Enabling an Email Notification

Use the following instructions to enable an email notification:

1. From the main menu, select **Configure > DETECTION Response Management**.
2. Locate the **In the All Manager System Alarms** row of the Rules table, then click the **(Ellipsis)** icon in the Actions column.
3. Select **Edit**.
4. In the **Rule is triggered if:** area, select the email notification you'd like to enable again.

5. Click the **-** (Minus) icon to remove the disabled email notification.
6. Click **Save**.

Replacing Unexpired or Expired Certificates (Overview)


Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate. Choose a method to replace your appliance identity certificates.

Certificates	Instructions
Unexpired Cisco Default Certificates	<p>Refer to Replacing Unexpired Cisco Default Certificates (Certificate Refresh) for instructions.</p> <p>If you need to change the host information in addition to the certificate, use the instructions in Changing Network Interfaces or Changing the Host Name or Network Domain Name.</p>
Expired Cisco Default Certificates	<p>Refer to Replacing Expired Cisco Default Certificates for instructions.</p> <p>If you need to change the host information in addition to the certificate, use the instructions in Changing Network Interfaces or Changing the Host Name or Network Domain Name.</p>
Custom SSL/TLS Certificates	<p>To replace your current certificates with custom certificates from a Certificate Authority, refer to Replacing the SSL/TLS Appliance Identity Certificate for instructions.</p>

Replacing Unexpired Cisco Default Certificates (Certificate Refresh)

Each Secure Network Analytics appliance is installed with a unique, Cisco self-signed appliance identity certificate. Use the following instructions to generate new Cisco self-signed appliance identity certificates when your existing certificates have not expired.

- **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:** The appliance identity certificate is replaced automatically with a Cisco self-signed appliance identity certificate in this certificate refresh procedure. To replace your existing certificates 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 review the following:

- **Users:** You need sysadmin access for the Manager appliance console (System Configuration) and administrator access for the Manager web login.
- **Central Management:** Do not change your configurations or add/remove appliances in Central Management during this process.
- **Data Collection:** We will restart your appliances and databases, and they will stop collecting data temporarily.
- **Failover:** The Certificate Refresh menu is not available on the secondary Manager. If your Managers are configured as a failover pair, log in to your primary Manager to refresh the secondary Manager certificate.

Refreshing Certificates on All or Selected Appliances

Follow these instructions to generate new Cisco self-signed appliance identity certificates for the Manager and other managed appliances in your inventory. You can generate certificates for all appliances in the list (default) or for selected, individual appliances.

This process may take a long time if you select many appliances because the certificates are generated in sequential order.

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



To replace your existing certificates 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. [Generate Certificates](#)
3. [Review Central Management](#)
4. [Review the Trust Stores](#)



Do not restart the appliance while configuration changes are pending or if the configuration channel is down.

1. Review the Appliance Status

Make sure all appliances are shown as **Connected** before you generate new certificates.

1. Log in to your primary Manager.
2. From the main menu, select **Configure > GLOBAL Central Management**.
3. 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**.



We cannot generate certificates for any appliances if your Manager is not shown as Connected. If an appliance status is not shown as Connected, we cannot generate a new certificate for it.

Inventory

3 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	fs-	Flow Sensor FSVE-KVM-		
Connected	nflow-	Flow Collector FCNFVE-KVM-		
Connected		Manager -VE-KVM-		

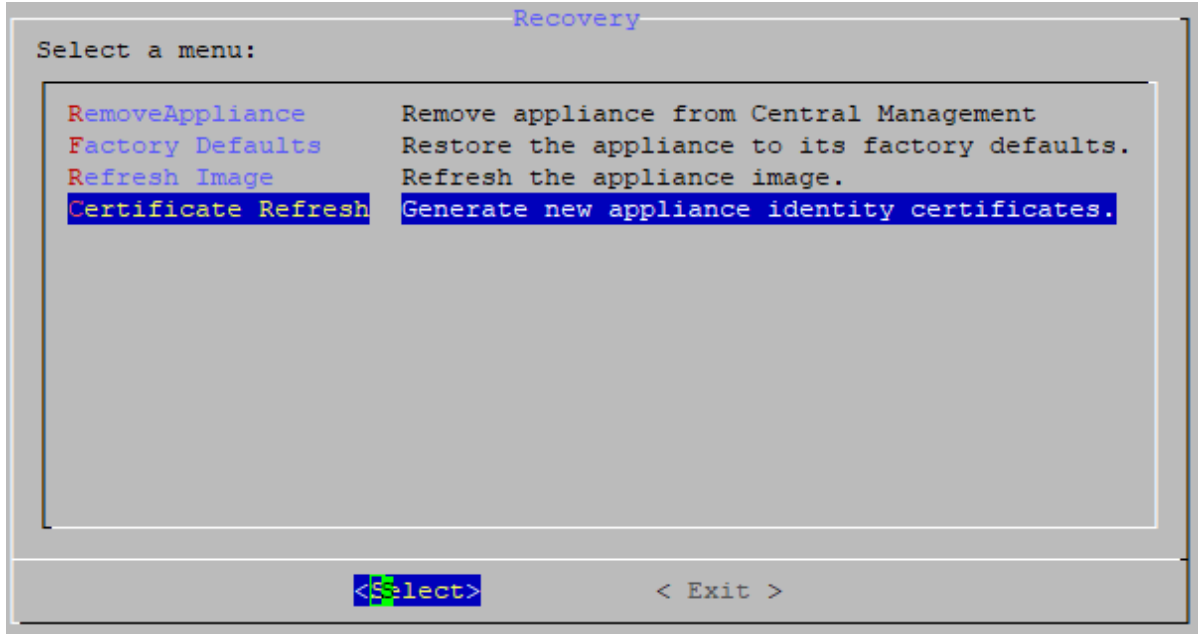
2. Generate Certificates

Use the following instructions to generate new Cisco self-signed appliance identity certificates.

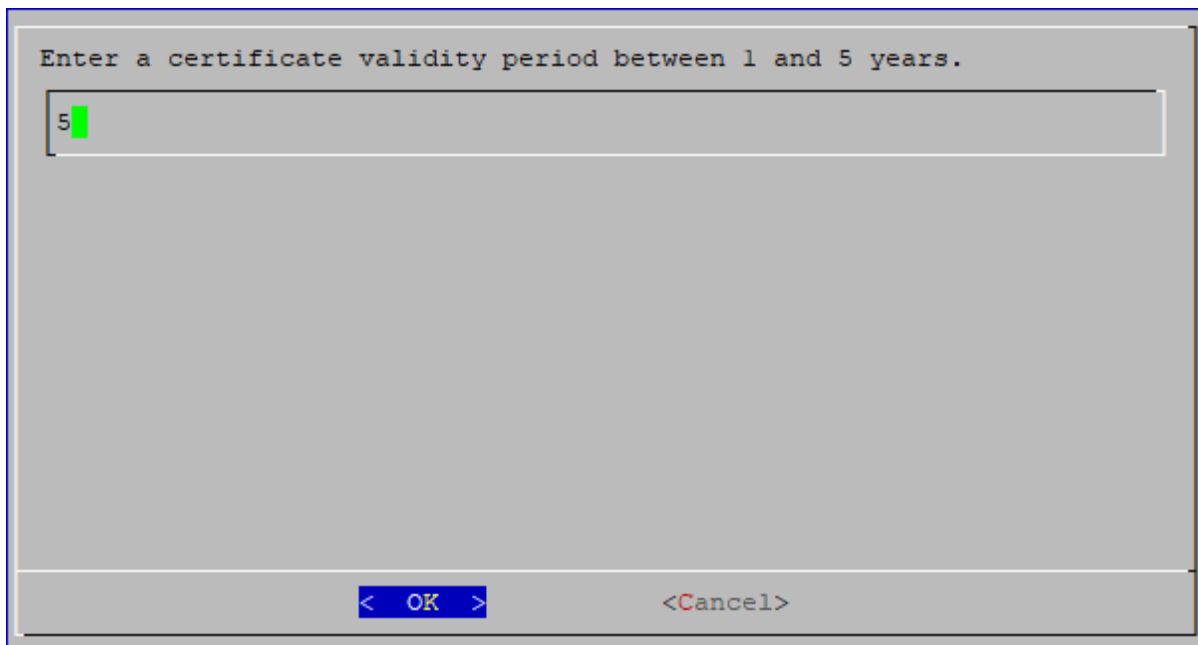


Do not change your configurations or add/remove appliances in Central Management during this process. We will restart your appliances and databases, and they will stop collecting data temporarily.

1. Log in to your primary Manager appliance console as sysadmin.
2. System Configuration opens.
3. From the main menu, select **Recovery**.
4. Select **Certificate Refresh**. Follow the on-screen prompts.

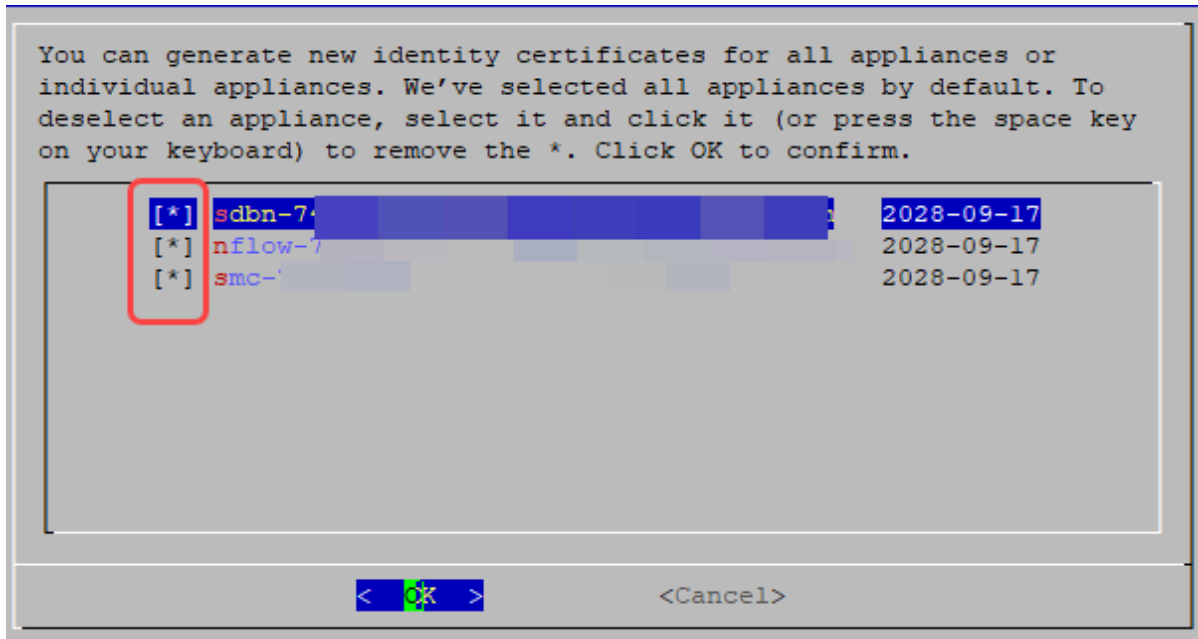


5. Enter a validity period between 1 and 5 years. Click **OK**.



6. Review the appliance list and certificate expiration dates. You can generate certificates for all appliances in the list or for selected, individual appliances.
- [*] indicates that the appliance is selected. We've selected all appliances by default.

- To deselect an appliance, select it and click it (or press the space key on your keyboard) to remove the *.
- Click OK to generate certificates for the selected appliances.



7. Follow the on-screen prompts.
8. To review the progress of the certificate refresh, review the statistics (failed, skipped, completed, and selected).

System Config Log: For more information, review system_config.log at one of the following locations:

- /lancope/var/logs/system_config.log
- Log in to the Appliance Admin. Select **Support > Browse Files > logs > system_config.log**.

```
We are generating new appliance identity certificates:
```

```
sdbn-7 [REDACTED] : COMPLETED  
nflow [REDACTED] : RUNNING  
smc- [REDACTED] : WAITING
```

```
Failed: 0 | Skipped: 0 | Completed: 1 | Selected: 3  
For details, review the system_config.log.
```

After this process is completed, review your Central Management inventory, and confirm all appliances are shown as Connected.

Also, check each appliance trust store, confirm the new appliance identity certificates are shown, and delete the old certificates.

9. Leave System Configuration open until all appliances are shown as completed and the success message is shown.

- SSH will close, and the selected appliances will restart.
- If the certificate refresh process fails, review the error message and check the [System Config Log](#) for more information.

```
You've successfully completed the certificate refresh process for all  
selected appliances. We are waiting for this appliance to restart.
```

After this process is completed, review your Central Management inventory, and confirm all appliances are shown as Connected.

Also, check each appliance trust store, confirm the new appliance identity certificates are shown, and delete the old certificates.

3. Review Central Management

1. Log in to your primary Manager.
2. From the main menu, select **Configure > GLOBAL Central Management**.
3. 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**.

Central Management Inventory

3 Appliances found

Q, Filter Appliance Inventory Table

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow-...-0-1	Flow Collector FCNFVE-...	10.0... 1	...
Connected	sdbn-7...-1	Data Node DNODEVE-K1	10... 2	...
Connected	smc-...-1	Manager SMCVE-...	10... 0	...

4. Review the Trust Stores

1. In the Central Management inventory, click the **...** (**Ellipsis**) icon for the Manager.
2. Choose **Edit Appliance Configuration**.
3. Choose the **General** tab.
4. Review the **Trust Store** list, making sure to scroll through the entire list.
 - Confirm the new certificates are shown.
 - Delete the old certificates.



Do not delete any new certificates.

Trust Store Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
...	smc-...	smc-...	2023-09-15 16:12:21	2028-09-15 16:12:21	...	8192 bits	Delete
nflow-742	nflow-...	nflow-74...	2023-09-15 16:13:23	2028-09-15 16:13:23	...	8192 bits	Delete
sdbn-7...	sdbn-74...	sdbn-74...	2023-09-15 16:10:56	2028-09-15 16:10:56	...	8192 bits	Delete

6 Certificates

5. Click **Apply Settings**.
6. Return to your Central Management inventory.
7. Click the **⋮ (Ellipsis)** icon for the next appliance in your list. Repeat steps 2 through 5 to review the trust store on each appliance in your Central Management inventory.

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 and generate new Cisco self-signed appliance identity certificates when your existing certificates are **expired**.

- **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. If you follow this procedure, your custom certificates will be replaced with Cisco self-signed appliance identity certificates. To use custom appliance identity certificates, refer to [Replacing the SSL/TLS Appliance Identity Certificate](#) for instructions.



If your certificates have not expired, refer to [Replacing Unexpired Cisco Default Certificates \(Certificate Refresh\)](#). 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. From the main menu, select **Configure > GLOBAL Central Management**.

- Review the Appliance Status column. If the appliance status is shown as **Config Channel Down**, your certificates have expired.

Inventory

2 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Channel Down	nflow-	Flow Collector FCNFVE-KVM-1	1.1.1.5	
Config Channel Down		Manager MVE-KVM	1.1.1.4	

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, UDP Directors, or Data Nodes). 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.

Default Validity Period: The regenerated certificate defaults to 5 years. However, you can change this period as part of the procedure.

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. If you follow this procedure, your custom certificates will be replaced with a Cisco self-signed appliance identity certificates. To use custom appliance identity certificates, refer to [Replacing the SSL/TLS Appliance Identity Certificate](#) for instructions.

Overview

The overall steps are as follows:

1. [Stop the Data Store Database](#)
2. [Remove Appliances from Central Management](#)
3. [Regenerate the Appliance Identity Certificate](#)
4. [Register your Manager in Central Management](#)
5. [Delete Expired Certificates from the Manager Trust Store](#)
6. [Add Appliances to Central Management](#)
7. [Start the Data Store Database](#)
8. [Delete Expired Certificates from the Trust Stores](#)
9. [Configure the Manager Failover Pair](#)

1. Stop the Data Store Database

If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.



If you don't have Data Nodes in your deployment, go to **2. Remove Appliances from Central Management**.

1. Go to **Central Management > Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Up**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Stop**.
5. Confirm the Database Status is shown as **Down**.

2. Remove Appliances from Central Management

i If you only need to change the Manager certificate, 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. [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 Inventory tab, 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**.

The screenshot shows the 'Inventory' section of the management interface. It displays a table with one appliance. The 'APPLIANCE STATUS' column for this appliance is highlighted with a red box and contains the text 'Connected'. The table has columns for APPLIANCE STATUS, HOST NAME, TYPE, IP ADDRESS, and ACTIONS. The 'TYPE' column shows 'Manager' and the 'ACTIONS' column has an ellipsis icon.

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		⋮

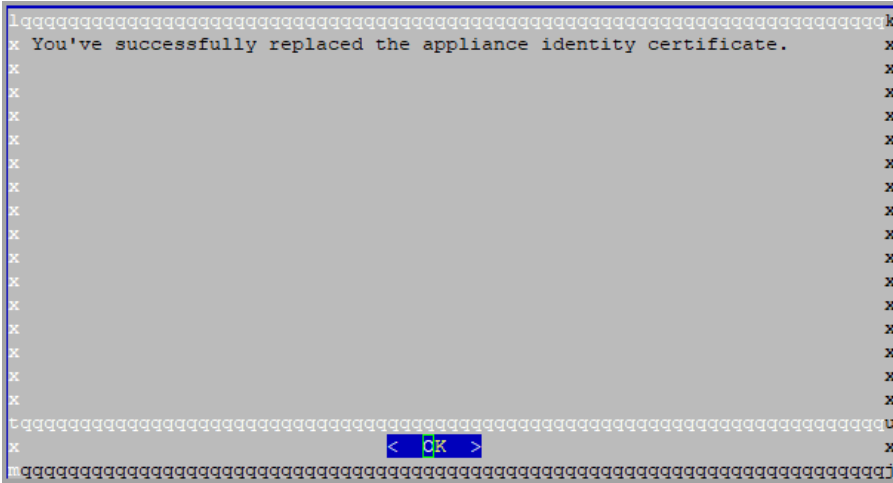
⚠ Remove the Manager from Central Management last.

4. Remove the primary Manager from Central Management.
 - On the Inventory tab, 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**.

3. Regenerate the Appliance Identity Certificate

Use the following instructions to regenerate the appliance identity certificate on the Manager and other appliances.

- **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.




7. Repeat steps 1 through 6 on each appliance.

4. Register your Manager in Central Management

Use the following instructions to register your Manager using the appliance console (SystemConfig). 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 appliance console as sysadmin.
2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the Manager IP address, user name, and password.
5. 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

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		

5. 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. In the Central Management inventory, 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 page, confirm the Manager appliance status returns to **Connected**.

6. Add Appliances to Central Management

Use the appliance console (SystemConfig) 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.	Data Nodes	
7.	Secondary Manager (if used)	Make sure the primary Manager is shown as Connected before you start the secondary Manager configuration. The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to 9. Configure the Manager Failover Pair .

Use the following instructions to configure each appliance using the appliance console (SystemConfig). Note that your appliance configuration for the 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. Log in to the appliance console as sysadmin.

Secondary Manager Only: If you have a secondary Manager, log in as sysadmin. Follow the prompts for First Time Setup (refer to the [System Configuration Guide](#) for instructions). The Manager selects itself as Central Manager. You will configure Failover after all appliances are connected to Central Management.

User	Default Password
sysadmin	lan1cope
admin	lan411cope

2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the IP address and admin password for the Manager. Click OK.
5. 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](#).

Central Management

Inventory Update Manager App Manager Smart Licensing Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

6. Repeat steps 1 through 5 to add each appliance to Central Management.

7. Start the Data Store Database



If you don't have Data Nodes in your deployment, go to **8. Delete Expired Certificates from the Trust Stores**.

1. From Central Management, select **Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Down**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Start**.
5. Confirm the Database Status is shown as **Up**.

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

9. 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, UDP Directors, or Data Nodes). 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 as part of the 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. If you follow this procedure, your custom certificates will be replaced with a Cisco self-signed appliance identity certificate. To use custom appliance identity certificates, refer to [Replacing the SSL/TLS Appliance Identity Certificate](#) for instructions.

Overview

The overall steps are as follows:

1. [Stop the Data Store Database](#)
2. [Remove the Appliance and Regenerate Certificates](#)
3. [Delete Expired Certificates from the Manager Trust Store](#)
4. [Add the Appliance to Central Management](#)
5. [Start the Data Store Database](#)



If you need to change the Manager certificate validity period, refer to [Manager and Managed Appliances](#).

1. Stop the Data Store Database

If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.



If you don't have Data Nodes in your deployment, go to [2. Remove the Appliance and Regenerate Certificates](#).

4. Add the Appliance to Central Management

When you add your appliance to Central Management, the 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. Log in to the appliance console as sysadmin.
 2. Select **Recovery**.
 3. Select **Add Appliance**.
 4. Enter the IP address and admin password for the Manager. Click OK.
 5. When the appliance setup is completed, review the inventory in Central Management. Confirm the appliance status is shown as **Connected**.

The screenshot shows the Central Management web interface. The 'Inventory' tab is selected, displaying '4 Appliances found'. A search filter is present. Below is a table with columns for Appliance Status, Host Name, and Type. A red box highlights the 'Connected' status for all four appliances.

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

5. Start the Data Store Database



If you don't have Data Nodes in your deployment, you can skip this section.

1. From Central Management, select **Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Down**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Start**.
5. Confirm the Database Status is shown as **Up**.

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 appliance identity certificate with a custom appliance identity certificate using the following procedures.



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

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.

- 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 current appliance identity certificate with a new appliance identity certificate.

Overview

The overall steps are as follows:

1. [Generate a Certificate Signing Request](#)
2. [Add the Root CA Certificate to the Trust Stores](#)
3. [Stop the Data Store Database](#)
4. [Replace the Appliance Identity Certificate](#)
5. [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 Inventory 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**.

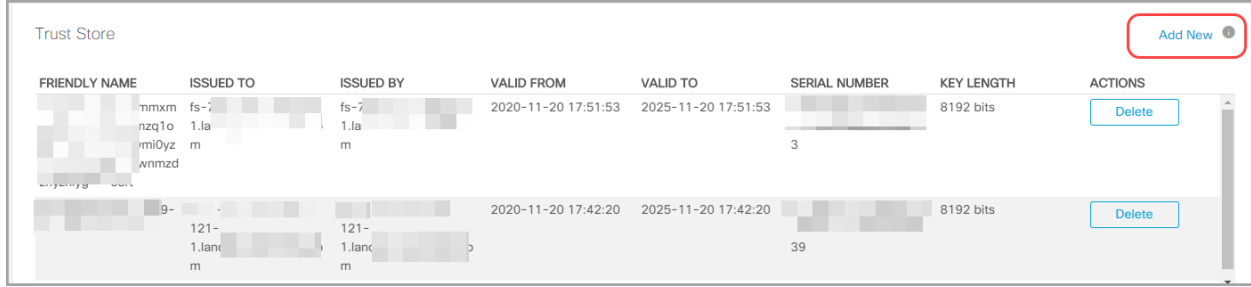


If you do not need to generate a CSR, go to [Skipping the CSR in Central Management](#).


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 identity 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 the Root CA Certificate to the Trust Stores

1. [Open Central Management](#).
2. On the Inventory tab, click the **⋮ (Ellipsis)** icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. On the **General** tab, locate the Trust Store section.
5. Click **Add New**.



6. In the **Friendly Name** field, enter a unique name for the root certificate.

 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.

7. Click **Choose File**. Select the new root certificate.
8. Click **Add Certificate**. Confirm the new certificate is shown in the Trust Store list.
9. Repeat steps 1 through 8 on each appliance trust store.

Trust Store Requirements

Use this table to add the root CA certificate to the appliance trust stores.

Appliance Identity Certificates	Details	Trust Stores
Manager/ Central Manager	Add the Manager root certificate to the Manager trust store and the trust store of every appliance in Central Management.	<ul style="list-style-type: none"> • Primary Manager • Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only)
Secondary Manager (Failover Only)	If your Managers are configured for failover, and	<ul style="list-style-type: none"> • Flow Collectors • Flow Collector

	<p>you are replacing the secondary Manager identity certificate, add the new secondary Manager root certificate to the secondary Manager trust store, the primary Manager trust store, and the trust store of every appliance in Central Management.</p> <p>If you have not yet configured the failover pair, finish replacing the appliance identity, and then configure failover using the Failover Configuration Guide.</p>	<p>Databases (5000 series only)</p> <ul style="list-style-type: none"> • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only) • Primary Manager
Flow Collector	<p>Add the Flow Collector root certificate to the Flow Collector trust store and the Manager trust store.</p> <p>5000 Series Only:</p> <ul style="list-style-type: none"> • Add the Flow Collector engine root certificate to the Flow Collector database trust store. • Add the Flow Collector database root certificate to the Flow Collector engine trust store. 	<ul style="list-style-type: none"> • Flow Collector • Flow Collector Databases (5000 series only) • Secondary Manager (Failover only) • Primary Manager
Flow Sensor	<p>Add the Flow Sensor root certificate to the Flow</p>	<ul style="list-style-type: none"> • Flow Sensor • Secondary Manager

	Sensor trust store and the Manager trust store.	(Failover only) <ul style="list-style-type: none"> • Primary Manager
UDP Director	Add the UDP Director root certificate to the UDP Director trust store and the Manager trust store.	<ul style="list-style-type: none"> • UDP Director • Secondary Manager (Failover only) • Primary Manager
UDP Director in High Availability Pair	<ul style="list-style-type: none"> • Add the secondary UDP Director root certificate to the primary UDP Director trust store. • Add the primary UDP Director root certificate to the secondary UDP Director trust store. 	<ul style="list-style-type: none"> • Secondary UDP Director (High Availability only) • Primary UDP Director (High Availability only) • Secondary Manager (Failover only) • Primary Manager
Data Node	Add the Data Node root certificate to the Data Node trust store and to the Manager trust store.	<ul style="list-style-type: none"> • Primary Manager • Data Node • Secondary Manager (Failover only)

3. Stop the Data Store Database

If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.



If you don't have Data Nodes in your deployment, go to **4. Replace the Appliance Identity Certificate**.

1. Go to **Central Management > Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Up**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Stop**.
5. Confirm the Database Status is shown as **Down**.

4. Replace the Appliance Identity Certificate

Preparation: Each appliance reboots automatically as part of this process, so plan to replace certificates at a time when you can manage a reboot of your appliances.

1. [Open Central Management](#).
2. On the Inventory page, click the **⋮ (Ellipsis)** icon for the appliance.
Multiple Appliances: Start with the Flow Collector, Flow Sensor, UDP Director, or Data Node.
3. Choose 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 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 (leaf) 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**. 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.

5. Trust the Certificate in the Desktop Client

If you use the Desktop Client, complete these steps. The Desktop Client is only available in deployments without a Data Store.

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 that meet the **Appliance Identity Certificates** requirements, use the following instructions to replace the current appliance identity certificate with a new appliance identity certificate.

Overview

The overall steps are as follows:

1. **Add the Required Certificate to the Trust Stores**
2. **Stop the Data Store Database**
3. **Replace the Appliance Identity Certificate**
4. **Trust the Certificate in the Desktop Client**

1. Add the Required Certificate to the Trust Stores

Before you start, review the required certificate information in **Trust Store Requirements**.

1. [Open Central Management](#).
2. On the Inventory tab, click the **⋯ (Ellipsis)** icon for the appliance.
3. Choose **Edit Appliance Configuration**.
4. On the **General** tab, locate the Trust Store section.
5. Click **Add New**.

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
mmxm	fs-7	fs-7	2020-11-20 17:51:53	2025-11-20 17:51:53	3	8192 bits	Delete
9-	121-	121-	2020-11-20 17:42:20	2025-11-20 17:42:20	39	8192 bits	Delete

6. In the **Friendly Name** field, enter a unique name for the certificate.



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.

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

9. Repeat steps 1 through 9 on each appliance trust store.

Trust Store Requirements

Use this table to add the required certificates to the appliance trust stores. The required certificates are determined by the following:

- **Self-Signed:** If you have self-signed certificates, add them to the trust stores.
- **Chain/Root:** If you have chain certificates, you only need to add the root certificate to the trust stores.

Appliance Identity Certificates	Details	Trust Stores
<p>Manager/ Central Manager</p>	<p>Add the required certificate to the Manager trust store and the trust store of every appliance in Central Management.</p>	<ul style="list-style-type: none"> • Primary Manager • Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only)
<p>Secondary Manager (Failover Only)</p>	<p>If your Managers are configured for failover, and you are replacing the secondary Manager identity certificate, add the required certificate to the secondary Manager trust store, the primary Manager trust store, and the trust store of every appliance in Central Management.</p> <p>If you have not yet</p>	<ul style="list-style-type: none"> • Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only) • Primary Manager

	configured the failover pair, finish replacing the appliance identity, and then configure failover using the Failover Configuration Guide .	
Flow Collector	<p>Add the required certificate to the Flow Collector trust store and the Manager trust store.</p> <p>5000 Series Only:</p> <ul style="list-style-type: none"> • Add the required engine certificate to the Flow Collector database trust store. • Add the required database certificate to the Flow Collector engine trust store. 	<ul style="list-style-type: none"> • Flow Collector • Flow Collector Databases (5000 series only) • Secondary Manager (Failover only) • Primary Manager
Flow Sensor	Add the required certificate to the Flow Sensor trust store and the Manager trust store.	<ul style="list-style-type: none"> • Flow Sensor • Secondary Manager (Failover only) • Primary Manager
UDP Director	Add the required certificate to the UDP Director trust store and the Manager trust store.	<ul style="list-style-type: none"> • UDP Director • Secondary Manager (Failover only) • Primary Manager
UDP Director in High Availability Pair	Add the required certificates to the primary UDP Director trust store, the secondary UDP Director trust store, and to the	<ul style="list-style-type: none"> • Secondary UDP Director (High Availability only) • Primary UDP Director

	Manager trust stores.	(High Availability only) <ul style="list-style-type: none"> • Secondary Manager (Failover only) • Primary Manager
Data Node	Add the required certificate to the Data Node trust store and to the Manager trust store.	<ul style="list-style-type: none"> • Primary Manager • Data Node • Secondary Manager (Failover only)

2. Stop the Data Store Database

If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.



If you don't have Data Nodes in your deployment, go to **3. Replace the Appliance Identity Certificate.**

1. Go to **Central Management > Data Store > Database Control.**
2. Review the **Database Status** column and confirm the database is shown as **Up.**
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Stop.**
5. Confirm the Database Status is shown as **Down.**

3. 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 Inventory tab, click the **⋮ (Ellipsis)** icon for the appliance.

Multiple Appliances: Start with the Flow Collector, Flow Sensor, UDP Director, or Data Node. 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.

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 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 (leaf) in the chain file.


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**. 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.

4. Trust the Certificate in the Desktop Client

If you use the Desktop Client, complete these steps. The Desktop Client is only available in deployments without a Data Store.

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.

The screenshot shows the 'Trust Store' configuration page in the Cisco Central Management console. The 'Inventory' tab is selected, and the 'General' sub-tab is active. A table lists certificates with columns for Friendly Name, Issued To, Issued By, Valid From, Valid To, Serial Number, Key Length, and Actions. Three certificates are visible, each with a 'Delete' button. The 'Trust Store' label is highlighted with a red box.

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	721477	7c5c 8192 bits	Delete
[Redacted]	[Redacted]	[Redacted]	2021-07-22 11:30:06	2026-07-23 11:30:06	d9e533	180c 8192 bits	Delete
[Redacted]	[Redacted]	[Redacted]	2019-12-19 15:48:06	2024-12-19 15:48:06	c0a64c	ee69 8192 bits	Delete

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 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.

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
[blurred]	mmxm fs-7 nzzq1o 1.la mi0yz m wnmzd	fs-7 1.la m	2020-11-20 17:51:53	2025-11-20 17:51:53	[blurred]	8192 bits	Delete
[blurred]	9- 121- 1.lanc m	121- 1.lanc m	2020-11-20 17:42:20	2025-11-20 17:42:20	39	8192 bits	Delete

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

Trust Store Location

Refer to the Trust Stores column to confirm where certificates are saved.

Appliance Identity Certificates	Trust Stores
<p>Manager Central Manager</p>	<ul style="list-style-type: none"> • Primary Manager • Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only)
<p>Secondary Manager (Failover Only)</p>	<ul style="list-style-type: none"> • Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only) • Primary Manager

	<p>Manager Failover:</p> <p>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.</p>
Flow Collector	<ul style="list-style-type: none"> • Flow Collector • Secondary Manager (Failover only) • Primary Manager <p>5000 Series Only:</p> <ul style="list-style-type: none"> • The Flow Collector engine certificates are saved to the Flow Collector database trust store. • The Flow Collector database certificates are saved to the Flow Collector engine trust store.
Flow Sensor	<ul style="list-style-type: none"> • Flow Sensor • Secondary Manager (Failover only) • Primary Manager
UDP Director	<ul style="list-style-type: none"> • UDP Director • Secondary Manager (Failover only) • Primary Manager
UDP Director in High Availability Pair	<ul style="list-style-type: none"> • Secondary UDP Director (High Availability only) • Primary UDP Director (High Availability only) • Secondary Manager (Failover only) • Primary Manager
Data Node	<ul style="list-style-type: none"> • Primary Manager

	<ul style="list-style-type: none">• Data Node• Secondary Manager (Failover only)
--	---

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 First Time Setup. The Host Naming section of Central Management shows this information as read-only.

- To change the appliance IP address, refer to [Changing Network Interfaces](#).
- **If you are using custom certificates**, save your certificates before you change your network settings (host name, network domain name, or eth0 IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

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.

Also, make sure you follow the on-screen prompts and review if regenerating the certificate is required or if you can choose to preserve it.



If you are using custom certificates, save your certificates before you change your network settings (host name, network domain name, or IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

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** is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.
- **Flow Collector 5000 Series Database:** If you have more than one database and engine pair, name each database and engine pair so you can identify them in Central Management (for example: database1 and engine1, database2 and engine2).
- **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, UDP Director, or Data Nodes:** **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 Manager host 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](#).

 **If you are using custom certificates**, save your certificates before you change your network settings (host name, network domain name, or eth0 IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

Overview

The overall steps are as follows:

1. [Stop the Data Store Database](#)
2. [Remove Appliances from Central Management](#)
3. [Change the Manager Host Name or Network Domain Name](#)
4. [Register the Manager in Central Management](#)
5. [Add Appliances to Central Management](#)
6. [Start the Data Store Database](#)
7. [Delete Outdated Manager Certificates from the Trust Stores](#)
8. [Configure the Manager Failover Pair](#)

1. Stop the Data Store Database

If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.

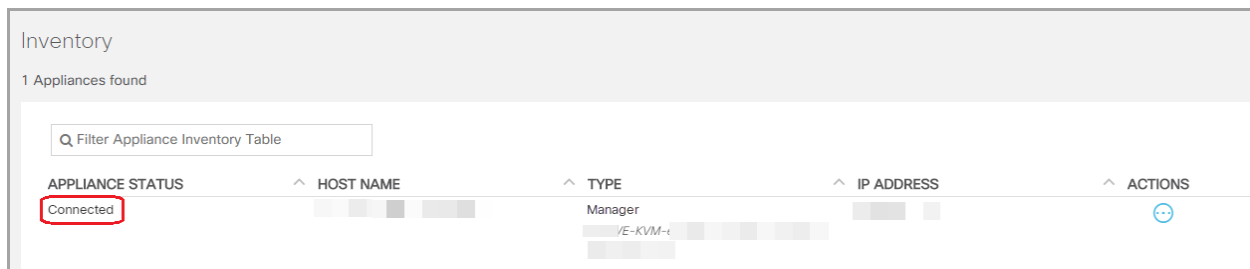


If you don't have Data Nodes in your deployment, go to [2. Remove Appliances from Central Management](#).

1. Go to **Central Management > Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Up**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Stop**.
5. Confirm the Database Status is shown as **Down**.

2. 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 Inventory tab, 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**.



The screenshot shows the 'Inventory' page with the heading '1 Appliances found'. Below the heading is a search bar labeled 'Filter Appliance Inventory Table'. A table with the following columns is displayed: APPLIANCE STATUS, HOST NAME, TYPE, IP ADDRESS, and ACTIONS. The 'APPLIANCE STATUS' column contains the value 'Connected', which is highlighted with a red box. The 'TYPE' column contains the value 'Manager'. The 'ACTIONS' column contains an ellipsis icon (⋮).

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		⋮

5. Remove the primary Manager from Central Management.
 - On the Inventory tab, 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**.

3. Change the Manager Host Name or Network Domain Name

Use the following instructions to change the Manager host name or network domain name.

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 **5. Add Appliances to Central Management**.

1. Log in to the Manager appliance console (SystemConfig) as sysadmin.
2. Select **Network**.
3. Select **Management**.
4. Select a network IP mode for the appliance or leave it unchanged.
5. Select the **Host Name** field or **Domain** field. Enter the new information.



A unique host name is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.

6. Follow the on-screen prompts to confirm your changes.

4. Register the Manager in Central Management

1. Log in to the Manager appliance console as sysadmin.
2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the Manager IP address, user name, and password.
5. 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				
Q Filter Appliance Inventory Table				
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		

5. Add Appliances to Central Management

Use each appliance console (SystemConfig) to add your other appliances to Central Management.

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

in your cluster.

- **Central Management:** You need the Manager IP address, Manager admin 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.	Data Nodes	
7.	Secondary Manager (if used)	Make sure the primary Manager is shown as Connected before you start the secondary Manager configuration. The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to 8. Configure the Manager Failover Pair .

1. Log in to the appliance console as sysadmin.

Secondary Manager Only: If you have a secondary Manager, log in as sysadmin. Follow the prompts for First Time Setup (refer to the [System Configuration Guide](#) for instructions). The Manager selects itself as Central Manager. You will configure Failover after all appliances are connected to Central Management.

User	Default Password
sysadmin	lan1cope
admin	lan411cope

2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the IP address and admin password for the Manager. Click OK.
5. 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](#).

Central Management

Inventory Update Manager App Manager Smart Licensing Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

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

6. Start the Data Store Database



If you don't have Data Nodes in your deployment, go to [7. Delete Outdated Manager Certificates from the Trust Stores](#).

1. From Central Management, select **Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Down**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Start**.
5. Confirm the Database Status is shown as **Up**.

7. 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, UDP Director, and Data Node.

8. 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, UDP Director, or Data Nodes).

 **If you are using custom certificates**, save your certificates before you change your network settings (host name, network domain name, or eth0 IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

Overview

The overall steps are as follows:

1. [Stop the Data Store Database](#)
2. [Remove the Appliance from Central Management](#)
3. [Change the Appliance Host Name or Network Domain Name](#)
4. [Add the Appliance to Central Management](#)
5. [Start the Data Store Database](#)

 To change the Manager host name or network domain name, use the [Manager](#) instructions.

1. Stop the Data Store Database

If you don't want to stop the database, and you have 3 or more Data Nodes, please contact [Cisco Support](#) for assistance.

 If you don't have Data Nodes in your deployment, go to [2. Remove the Appliance from Central Management](#).

1. Go to **Central Management > Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Up**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Stop**.
5. Confirm the Database Status is shown as **Down**.

2. 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**.

3. Change the Appliance Host Name or Network Domain Name

1. Log in to the appliance console (SystemConfig) as sysadmin.
2. Select **Network**.
3. Select **Management**.
4. Select a network IP mode for the appliance or leave it unchanged.
5. Select the **Host Name** field or **Domain** field. Enter the new information.



A unique host name is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.

6. Follow the on-screen prompts to confirm your changes.

4. Add the Appliance to Central Management

1. Log in to the appliance console as sysadmin.

Secondary Manager Only: If you have a secondary Manager, log in as sysadmin. Follow the prompts for First Time Setup (refer to the [System Configuration Guide](#) for instructions). The Manager selects itself as Central Manager. You will configure Failover after all appliances are connected to Central Management.

User	Default Password
sysadmin	lan1cope

admin	lan411cope
-------	------------

2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the IP address and admin password for the Manager. Click OK.
5. 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.

5. Start the Data Store Database



If you don't have Data Nodes in your deployment, you can skip this section.

1. From Central Management, select **Data Store > Database Control**.
2. Review the **Database Status** column and confirm the database is shown as **Down**.
3. Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
4. Select **Start**.
5. Confirm the Database Status is shown as **Up**.

Changing Network Interfaces

The appliance network interfaces are configured as part of the installation process using First Time Setup. You can change [selected network interfaces in Central Management](#), or you can change the IP address (eth0 network interface) using the appliance console (SystemConfig).

- **IP Address:** To change the appliance IP address, refer to [Changing the Appliance IP Address](#). To change the eth0 IP address on any Data Nodes, contact [Cisco Support](#) for assistance.
- **Host Name or Domain Name:** To change the appliance host name or domain name, refer to [Changing the Host Name or Network Domain Name](#).
- **If you are using custom certificates,** save your certificates before you change your network settings (host name, network domain name, or eth0 IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).



Do not change the eth0 network interface on Data Nodes using this procedure. To change the eth0 IP address on any Data Nodes, contact [Cisco Support](#) for professional assistance.

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
 - Data Node 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.

Also, make sure you follow the on-screen prompts and review if regenerating the certificate is required or if you can choose to preserve it.



If you are using custom certificates, save your certificates before you change your network settings (host name, network domain name, or IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

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.

- **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](#).



If you are using custom certificates, save your certificates before you change your network settings (host name, network domain name, or eth0 IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

Overview

The overall steps are as follows:

1. [Remove Appliances from Central Management](#)
2. [Change the Manager IP Address](#)
3. [Register the Manager in Central Management](#)
4. [Add Appliances to Central Management](#)
5. [Delete Outdated Manager Certificates from the Trust Stores](#)
6. [Configure the Manager Failover Pair](#)

Do not change the eth0 network interface on Data Nodes using this procedure. To change the eth0 IP address on any Data Nodes, contact [Cisco Support](#) for professional assistance.

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 Inventory tab, 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**.

The screenshot shows the 'Inventory' page with the heading '1 Appliances found'. Below the heading is a search bar labeled 'Filter Appliance Inventory Table'. A table with the following columns is displayed: APPLIANCE STATUS, HOST NAME, TYPE, IP ADDRESS, and ACTIONS. The 'APPLIANCE STATUS' column contains the word 'Connected', which is highlighted with a red box. The 'TYPE' column shows 'Manager' and 'VE-KVM-I'. The 'ACTIONS' column contains an ellipsis icon.

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager VE-KVM-I		⋮

5. Remove the primary Manager from Central Management.
 - On the Inventory tab, 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 (eth0).

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](#).

1. Log in to the Manager appliance console (SystemConfig) as sysadmin.
2. Select **Network**.
3. Select **Management**.
4. Select a network IP mode for the appliance or leave it unchanged.
5. Select the **IP Address** field. Enter the new information.
6. Follow the on-screen prompts to confirm your changes.

3. Register the Manager in Central Management

1. Log in to the Manager appliance console as sysadmin.
2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the Manager IP address, user name, and password.
5. When the appliance setup is completed, review the inventory in Central Management. Confirm the Manager appliance status is shown as **Connected**.

The screenshot shows the 'Inventory' page in Central Management. It displays a table with one appliance found. The 'APPLIANCE STATUS' column for this appliance is highlighted with a red box and contains the text 'Connected'. The table has columns for APPLIANCE STATUS, HOST NAME, TYPE, IP ADDRESS, and ACTIONS.

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		

4. Add Appliances to Central Management

Use the appliance console (SystemConfig) 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. The secondary Manager selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to 6. Configure the Manager Failover Pair .

1. Log in to the appliance console as sysadmin.

Secondary Manager Only: If you have a secondary Manager, log in as sysadmin. Follow the prompts for First Time Setup (refer to the [System Configuration Guide](#) for instructions). The Manager selects itself as Central Manager. You will configure Failover after all appliances are connected to Central Management.

User	Default Password
sysadmin	lan1cope

admin

lan411cope

2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the IP address and admin password for the Manager. Click OK.
5. 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](#).

The screenshot shows the 'Central Management' interface with the 'Inventory' tab selected. It displays '4 Appliances found' and a search filter. Below is a table with the following data:

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

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

5. 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 page, 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](#).

Non-Manager Appliances

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


Also, make sure you follow the on-screen prompts and review if regenerating the certificate is required or if you can choose to preserve it.

 **If you are using custom certificates**, save your certificates before you change your network settings (host name, network domain name, or IP address) in case you accidentally overwrite them. To replace Cisco self-signed appliance identity certificates with custom certificates, follow the instructions in [Replacing the SSL/TLS Appliance Identity Certificate](#).

Overview

The overall steps are as follows:

1. **Remove the Appliance from Central Management**
2. **Change the Appliance IP Address**
3. **Add the Appliance to Central Management**

 **Do not change the eth0 network interface on Data Nodes using this procedure.** To change the eth0 IP address on any Data Nodes, contact [Cisco Support](#) for professional assistance.

 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

1. Log in to the appliance console (SystemConfig) as sysadmin.
2. Select **Network**.
3. Select **Management**.
4. Select a network IP mode for the appliance or leave it unchanged.
5. Select the **IP Address** field. Enter the new information.
6. Follow the on-screen prompts to confirm your changes.

3. Add the Appliance to Central Management

1. Log in to the appliance console as sysadmin.

Secondary Manager Only: If you have a secondary Manager, log in as sysadmin. Follow the prompts for First Time Setup (refer to the [System Configuration Guide](#) for instructions). The Manager selects itself as Central Manager. You will configure Failover after all appliances are connected to Central Management.

User	Default Password
sysadmin	lan1cope
admin	lan411cope

2. Select **Recovery**.
3. Select **Add Appliance**.
4. Enter the IP address and admin password for the Manager. Click OK.
5. 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.

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. Click the (**Help**) icon. Choose **Help**. 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. Click the (**Help**) icon. Choose **Help**. Search "LDAP."
- **Packet Analyzer:** Follow the instructions in the Help. Click the (**Help**) icon. Choose **Help**. Search "Packet Analyzer."
- **SAML SSO:** Follow the instructions in the [System Configuration Guide](#).
- **SMTP Configuration for Response Management:** Follow the instructions in the Help. Click the (**Help**) icon. Choose **Help**. Search "SMTP Configuration."



For additional configuration guides, refer to [Configuration Guides](#).

Certificate Requirements

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 Inventory tab, 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**.



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 client identity 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 Inventory tab, 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**.

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

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 Inventory tab, 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 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 that meet the **Client Identity Certificates** requirements, use the following 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 Inventory tab, 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								Add New
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS	
mmxm	fs-7	fs-7	2020-11-20 17:51:53	2025-11-20 17:51:53		8192 bits	Delete	
nzq1o	1.la	1.la						
mi0yz	m	m			3			
wnmzd								
enymyg								
	9-		2020-11-20 17:42:20	2025-11-20 17:42:20		8192 bits	Delete	
	121-	121-						
	1.lanc	1.lanc			39			
	m	m						

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 Inventory tab, 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**.



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.
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 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.
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, UDP Directors, and Data Nodes first.
 - **Last:** If you are removing more than one appliance, log in to the Manager last (after you have completed steps 1 through 5 on all other appliances as needed).

Contacting Support

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

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

Change History

Document Version	Published Date	Description
1_0	December 13, 2023	Initial Version.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

