Cisco Secure Network Analytics

SSL/TLS Certificates for Managed Appliances 7.4.2

Table of Contents

Introduction

Use this guide to change SSL/TLS certificate-related configurations on your Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.2 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).

Planning Time

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

Best Practices

- **Review Procedures:** Before you get started, review the procedures to make sure you understand the requirements and instructions. Also, make sure you follow the instructions in order.

- **Rebooting:** Do not force the appliance to reboot while it is restarting or making configuration changes.

- **One at a Time:** Configure one appliance at a time. Make sure the Appliance Status is shown as **Connected** before you start the next appliance configuration.

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

- **Removing/Adding Appliances:** Many procedures in this guide include removing your appliances from Central Management temporarily. Make sure you follow the order and instructions for removing appliances from Central Management and adding them back to Central Management (using the Appliance Setup Tool).

- **Managers:** 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.

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: • A unique Subject Name (date, identifier, string, etc.) or • A unique Authority Key Identifier and a Subject Key Identifier. If you use these key identifiers, confirm the certificate you are replacing	Confirm the self-signed appliance identity certificate uses: • A unique Subject Name (date, identifier, string, etc.) or • 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
	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.

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>
```

Appliance Setup Tool

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

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

Manager Failover

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

Client Identity Certificates

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

Certificate Requirements

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, we recommend uploading the CA certificate chain file as part of the instructions. Your chain file includes the root and intermediate certificates.

Make sure your chain file meets the following requirements:

- **Contents:** Make sure the chain file includes all signing certificates and the Certificate Authority certificate. Do not include the identity certificate in the chain file upload.

- **Order:** If you build the certificate chain manually, build the certificates in descending order, so the last intermediate certificate is first in the file, followed by the remaining intermediate certificates in descending order. Your root certificate is last in the file order.

  For example:

  — BEGIN CERTIFICATE —

  Intermediate Certificate #3

  — END CERTIFICATE —

  — BEGIN CERTIFICATE —

  Intermediate Certificate #2

  — END CERTIFICATE —

  — BEGIN CERTIFICATE —

  Intermediate Certificate #1

  — END CERTIFICATE —

  — BEGIN CERTIFICATE —

  Root CA Certificate

  — END CERTIFICATE —

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

Trust Store Requirements

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

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

- identity
- chain (root and intermediate certificates)

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

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

Wild Card Certificates (Client Identity Only)

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

Additional Certificate Configurations

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

- **Audit Log Destination:** Follow the instructions in the Help. 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."

> ℹ️ 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.
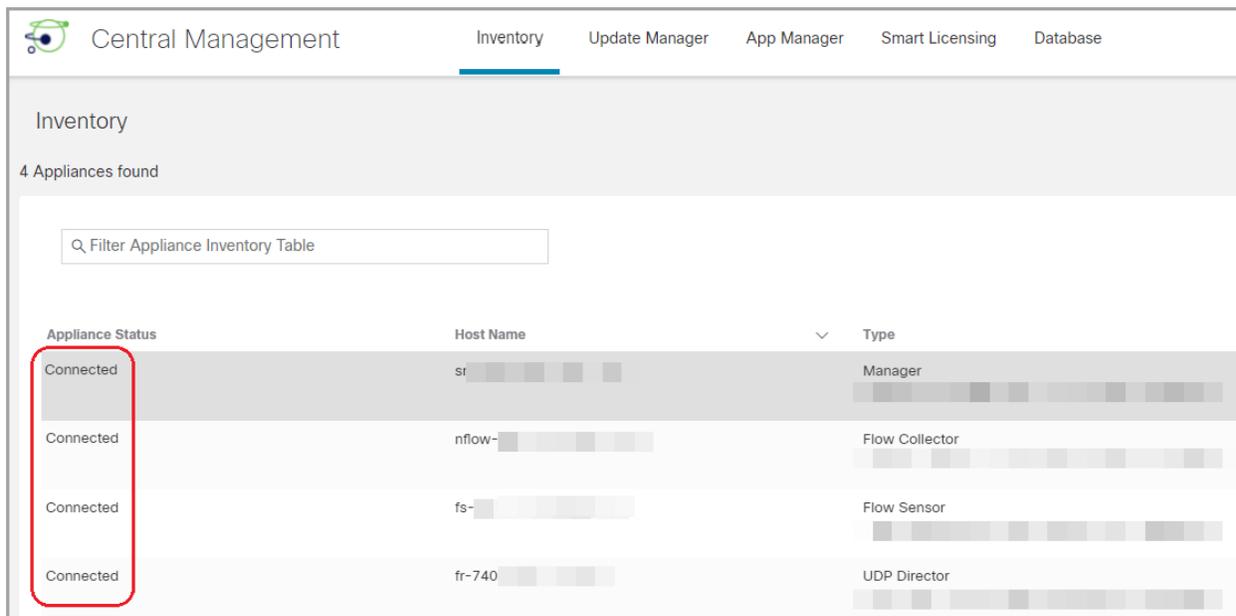
Overview

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.
Changing the Certificate Validity Period	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)**. To review additional options for replacing your unexpired or expired certificates, review **Changing the Certificate Validity Period (Overview)**.
Replacing the Appliance Identity Certificate	Each Secure Network Analytics appliance is installed with a unique, self-signed appliance identity certificate. Follow the instructions to replace the

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

Reviewing Certificates

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

1. [Open Central Management](#).

2. Click the ••• (**Ellipsis**) icon for the appliance.

3. Choose **Edit Appliance Configuration**.

4. Choose the **Appliance** tab.

5. **To review the appliance identity certificate,** go to the SSL/TLS Appliance Identity section.

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

Saving Certificates

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

> ℹ️ 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.

Certificate Check in Updates

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

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

Receiving Notifications for Expiring Certificates

With the v7.4.2 release of Secure Network Analytics, you'll see **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.

> ℹ️ 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.
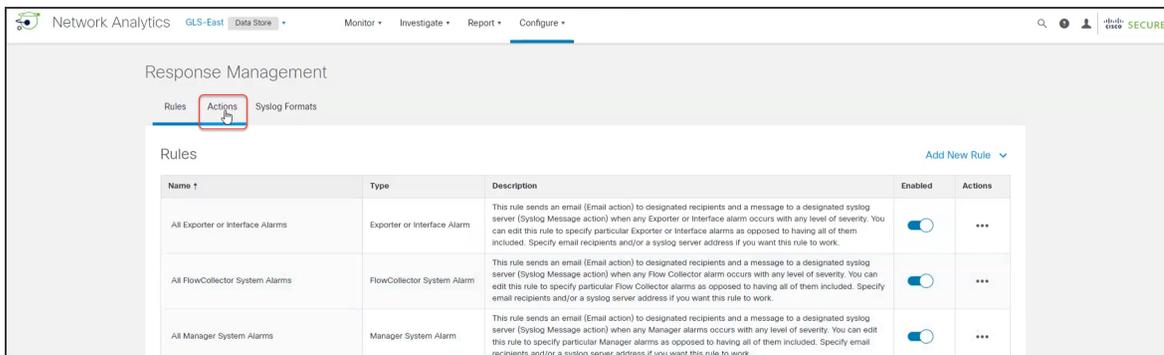
3. In the Actions area, select **Email** from the **Add New Actions** menu.
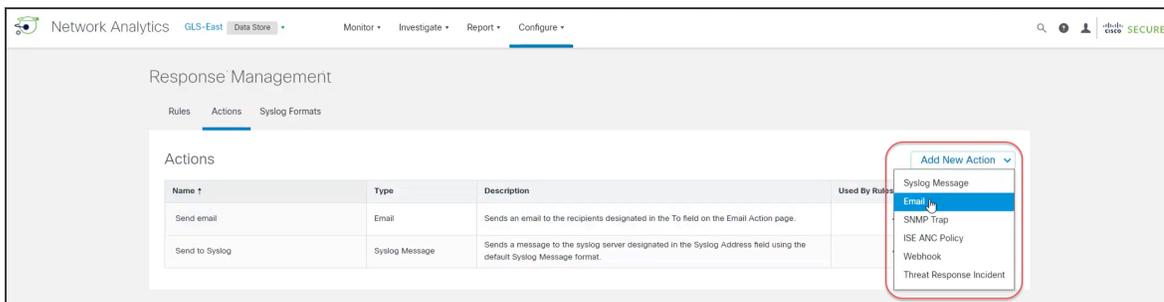
4. In the **Name** field, type a name; "Send Cert Expiration Email" for example. You may also want to add a description in the **Description** field.

> ℹ️ Make sure the **Enabled** button is toggled on.

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

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

- It displays highlighted in green after it is added.

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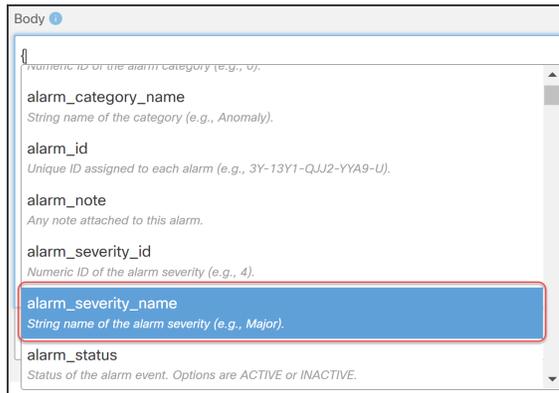
7. Copy your selections, then paste them in the **Subject** field.

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	🔵
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	⚪
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	⚪

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

Name ↑	Type	Description	Used By Rules	Assigned
Send Cert Expiration Email	Email		0	🔵
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	⚪
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	⚪

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.

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

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

Rule is triggered if:

ANY ▼ of the following is true:

Type ▼ is Appliance Certificate Expiration less than 90 days ▼
Processing Time
Severity
Type ✓
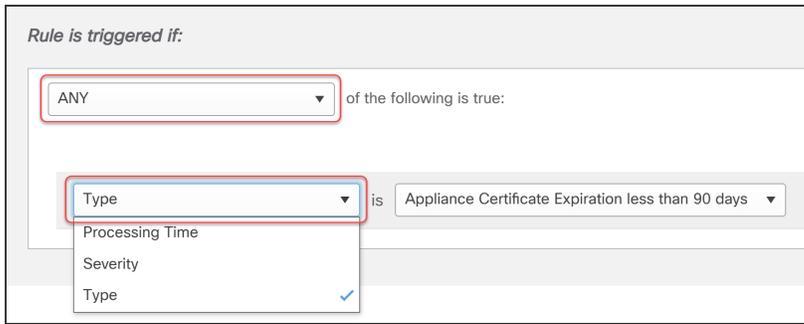
8. Select **Type**, then scroll through the list to select each email notifications you'd like to receive.

9. Click the **+** (Plus) icon to add a type; click the **–** (Minus) icon to remove a type.

10. Click **Save**.

Disabling an Email Notification

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

1. From the main menu, select **Configure > DETECTION Response Management**.

2. Locate the **All Manager System Alarms** row of the Rules table, then click the (**Ellipsis**) icon in the Actions column.

3. Select **Edit**.
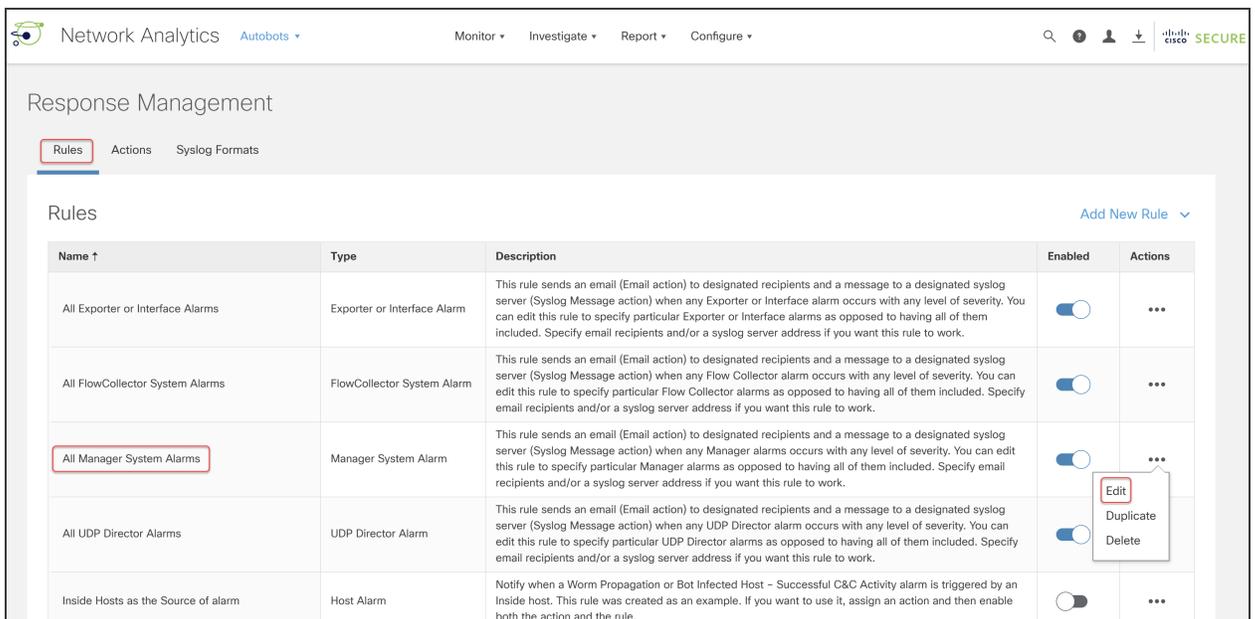
The page displays as follows.

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**.

Changing the Certificate Validity Period (Overview)

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

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

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

Replacing Unexpired Cisco Default Certificates (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.

> ℹ️ 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:

- **Patch:** You need to install a patch on all appliances as part of this procedure.

- **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.

> ⚠️ 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. **Install the Required Patch**

2. **Review the Appliance Status**

3. **Generate Certificates**

4. **Review Central Management**

5. **Review the Trust Stores**

1. Install the Required Patch

You need to install patch ROLLUP20231122-v2-01.swu (or the latest, most recent patch) on all appliances to access the Certificate Refresh menu.

Review Patch Installation: To check your list of installed patches before you start, log in to your primary Manager. Select **Configure > GLOBAL Central Management**. On the **Update Manager** tab, click **Actions > View Update Log** for each appliance. If you've already installed the patch, go to **2. Review the Appliance Status**.

1. Follow the patch readme instructions to install patch ROLLUP20231122-v2-01.swu (or the latest, most recent patch) on all appliances. There is a separate patch readme for each appliance posted to Patch Readmes 7.4.2.

2. Wait approximately 10 minutes while your appliances restart.

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

2. 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.

3. 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.

```
                            Recovery
Select a menu:

   RemoveAppliance      Remove appliance from Central Management
   Factory Defaults     Restore the appliance to its factory defaults.
   Refresh Image        Refresh the appliance image.
   Certificate Refresh  Generate new appliance identity certificates.




                 <Select>            < Exit >
```
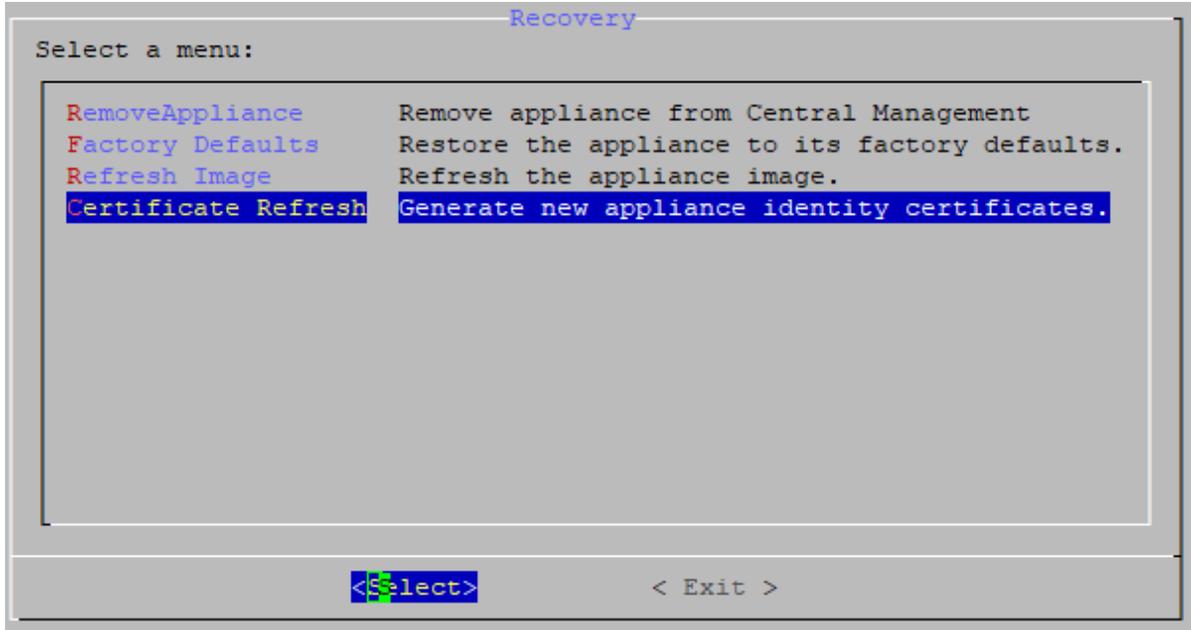
5. Enter a validity period between 1 and 5 years. Click **OK**.

```
Enter a certificate validity period between 1 and 5 years.

 5



              <  OK  >              <Cancel>
```
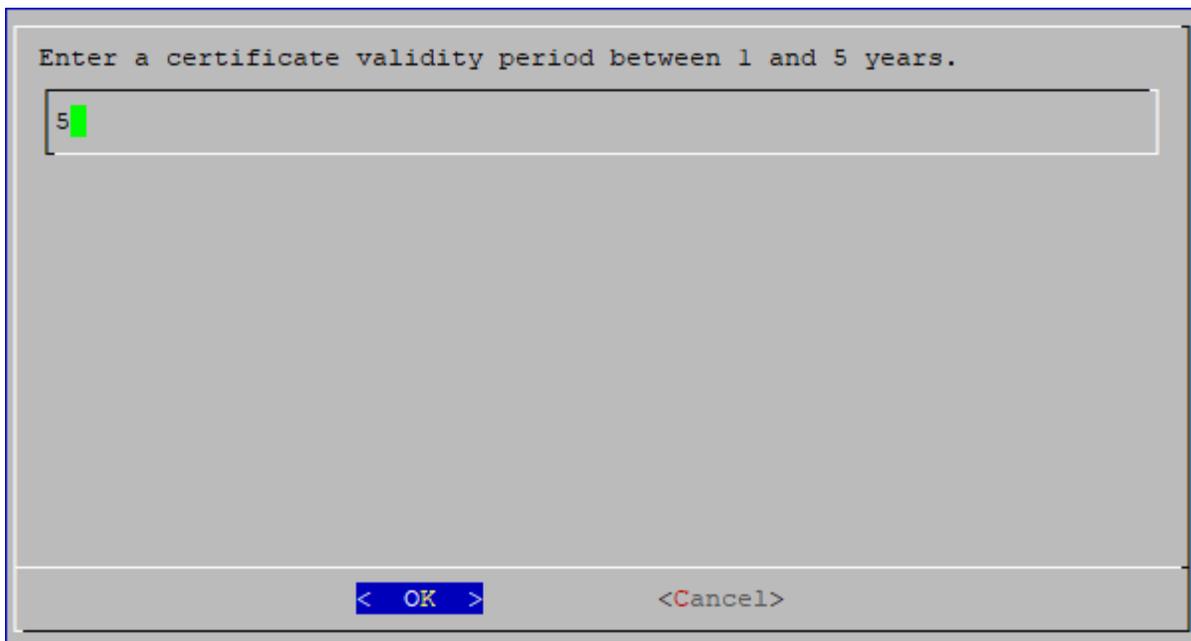
6. Review the appliance list and certificate expiration dates. You can generate certificates for all appliances in the list or for selected, individual appliances.

    -   [*] 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.

```
You can generate new identity certificates for all appliances or
individual appliances. 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 confirm.

    [*] sdbn-74                                        2028-09-17
    [*] nflow-7                                        2028-09-17
    [*] smc-                                           2028-09-17




                    <  OK  >              <Cancel>
```
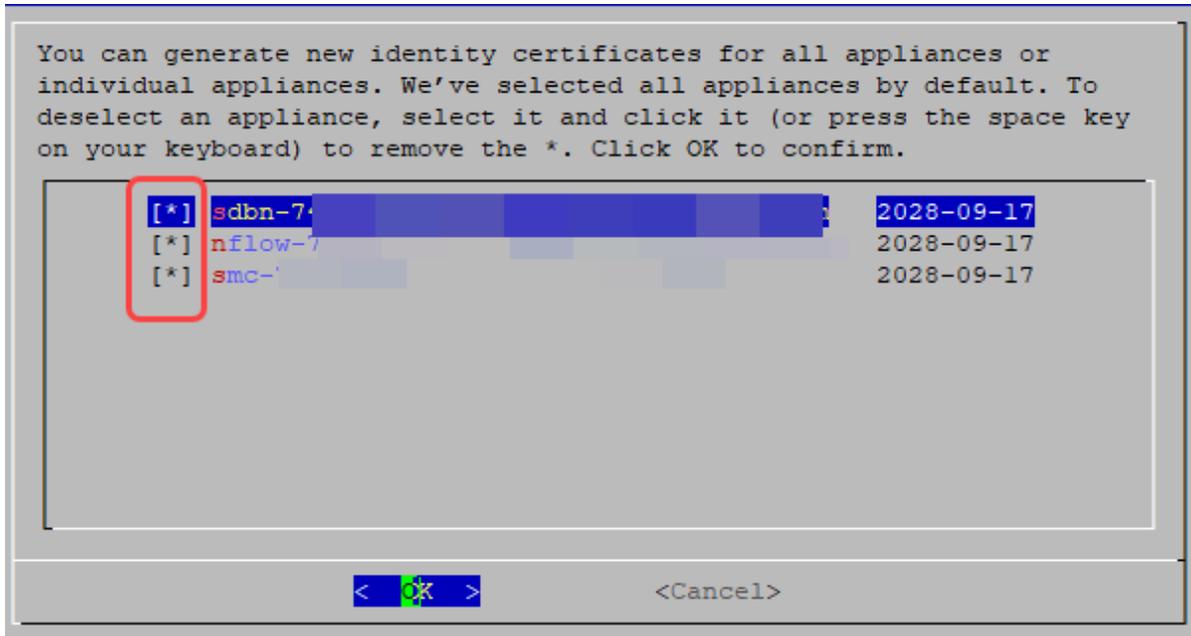
7. Follow the on-screen prompts.

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                                    : COMPLETED
 nflow                         _           : RUNNING
 smc-                                      : 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.
```

4. 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**.
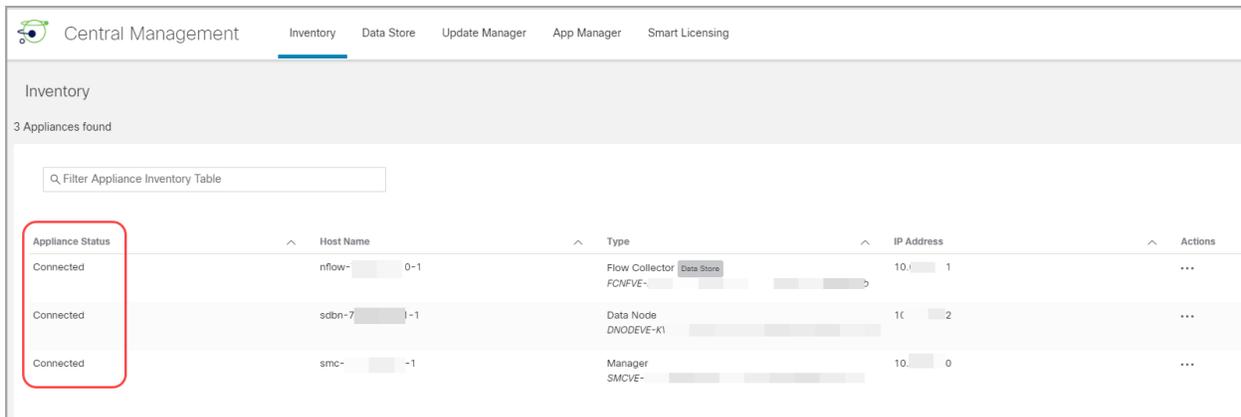
5. Review the Trust Stores

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.

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 on your **expired** appliance identity certificates.

- **Host Information:** The appliance host information (IP address, host name, domain name) is preserved. If you need to change the host information in addition to the validity period, use the instructions in **Changing Network Interfaces** or **Changing the Host Name or Network Domain Name** (instead of the instructions in this section).

- **Custom Certificates:** We do not support this procedure on appliances with custom appliance identity certificates. Refer to **Replacing the SSL/TLS Appliance Identity Certificate** for instructions.

> **i** If your certificates have not yet 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**.

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

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.

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

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

Overview

The overall steps are as follows:

1. **Stop the Data Store Database**

2. **Remove Appliances and Regenerate Certificates**

3. **Register your Manager in Central Management**

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

5. **Add Appliances to Central Management**

6. **Start the Data Store Database**

7. **Delete Expired 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.

> ℹ️ If you are not generating new certificates on your Data Nodes, go to **2. Remove Appliances and Regenerate Certificates**.

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 and Regenerate Certificates

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

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

- **First:** Complete these instructions on all Flow Collectors, Flow Sensors, UDP Directors, and Data Nodes.

- **Last:** Complete these instructions on the Manager last.

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

> ⚠️ Remove the Manager from Central Management last.

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

   - **First:** Remove your Flow Collectors, Flow Sensors, UDP Directors, and Data Nodes first.

   - **Last:** Remove your primary Manager after you have completed steps 1 through 9 on all other appliances.

2. Log in to the appliance console as sysadmin.

   - **First:** Log in to your Flow Collectors, Flow Sensors, UDP Directors, and Data Nodes first.

   - **Last:** Log in to your primary Manager after you have completed steps 1 though 9 on all other appliances.

3. Type **SystemConfig**. Press Enter.

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

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x  We couldn't load all System Configuration menus. Please contact Cisco    x
x              Support at                                                   x
x  https://www.cisco.com/c/en/us/support/index.html.                       x
x                                                                          x
x   DataStore: HTTPSConnectionPool(host='          ', port=443): Max       x
x  retries exceeded with url:                                              x
x  /token/v2/service-authenticate/systemconfig_datastore_plugin (Caused by x
x  SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED]   x
x  certificate verify failed: certificate has expired (_ssl.c:1056)')))     x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                              < OK >                                       x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

4. From the main menu, select **Recovery**.

5. Select **RemoveAppliance**.

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

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

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

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

- **Exit:** Click **OK** and close the console.

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

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x You've successfully replaced the appliance identity certificate.  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
x                                                                  x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                           <  OK  >                               x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

9. Repeat steps 1 through 8 on each appliance.

3. Register your Manager in Central Management

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

Manager Failover: If you have two Managers, you only need to complete this procedure on the primary Manager. You will register the secondary Manager in **5. Add Appliances to Central Management**.

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

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

- This installs Central Management on the Manager.
- The Manager IP address is detected automatically and cannot be changed.

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

Inventory

1 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	⌃	HOST NAME	⌃	TYPE	⌃	IP ADDRESS	⌃	ACTIONS
Connected				Manager				⊙
				/E-KVM-(				

4. Delete Expired Certificates from the Manager Trust Store

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

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

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

5. Add Appliances to Central Management

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

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

- **Order:** Follow the [appliance configuration order](#).
- **Access:** You need admin privileges to access Central Management.

Appliance Configuration Order

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

	Appliance	Details
1.	UDP Directors (also known as FlowReplicators)	
2.	Flow Collector 5000 Series Database	Make sure the Flow Collector 5000 series database is shown as **Connected** before you start the engine configuration.
3.	Flow Collector 5000 Series Engine	Make sure the Flow Collector 5000 series database is shown as **Connected** before you start the engine configuration.
4.	All Other Flow Collectors (NetFlow and sFlow)	
5.	Flow Sensors	Make sure your Flow Collector is shown as **Connected** before you start the Flow Sensor configuration.
6.	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**.

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

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

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

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

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

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

    All Other Appliances: Skip to step 4.

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

    Use the following criteria:

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

User	Default Password
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).

5. Add the appliance to Central Management as follows:

- **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **8. Configure the Manager Failover Pair**.

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

> ℹ️ The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, you will select a Flow Collector as part of the setup.

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

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

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

6. Start the Data Store Database

> ℹ️ If you don't have Data Nodes in your deployment, go to **7. 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**.

7. Delete Expired Certificates from the Trust Stores

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

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

1. Click the ••• (**Ellipsis**) icon for the appliance.

2. Choose **Edit Appliance Configuration**.

3. Choose the **General** tab.

4. Review the **Trust Store** list. Locate all expired certificates (identity, root, and intermediate certificates) from the appliance, Manager, and other appliances.

5. Click **Delete** to delete each old certificate.

6. Click **Apply Settings**. Follow the on-screen prompts.

7. On the Central Management Inventory 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.

8. Configure the Manager Failover Pair

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

Individual, Non-Manager Appliances

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 in a later procedure.

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

Overview

The overall steps are as follows:

1. **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**

> ℹ️ 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.

> ℹ️ If you are not generating new certificates on your Data Nodes, go to **2. Remove the Appliance and Regenerate Certificates**.

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 and Regenerate Certificates

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

2. Log in to the appliance console as sysadmin.

3. Type **SystemConfig**. Press Enter.

4. From the main menu, select **Recovery**.

5. Select **RemoveAppliance**.

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

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqRecoveryqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Select a menu:                                                          x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x RemoveAppliance    Remove appliance from Central Management       x x
x x Factory Defaults   Restore the appliance to its factory defaults.   x x
x x Refresh Image      Refresh the appliance image.                  x x
x x                                                                  x x
x x                                                                  x x
x x                                                                  x x
x x                                                                  x x
x x                                                                  x x
x x                                                                  x x
x x                                                                  x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                  <Select>              < Exit >                          x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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

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

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

- **Exit:** Click **OK** and close the console.

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

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x You've successfully replaced the appliance identity certificate.    x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
x                                                                     x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                        <   OK   >                                   x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

9. Repeat steps 1 through 8 on each appliance.

3. Delete Expired Certificates from the Manager Trust Store

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

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

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

4. Add the Appliance to Central Management

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

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

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

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

2. Click **Next** and scroll to the **Central Management** tab.

3. Add the appliance to Central Management as follows:

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

> ℹ️ The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, you will select a Flow Collector as part of the setup.

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

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

5. Start the Data Store Database

> ℹ 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 Certificates 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**.

> ℹ️ 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 Certificates to the Trust Stores

Before you update the appliance identity, add your certificates to the required trust stores.

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

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

Make sure you upload the following certificates:

- identity
- chain (root and intermediate certificates)

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

1. [Open Central Management](#).

2. On the Inventory tab, click the ••• (**Ellipsis**) icon for the appliance.

   Order: Select your appliances in the following order:

   - Flow Collectors
   - Flow Sensors
   - UDP Directors
   - Data Nodes
   - Managers

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

3. Choose **Edit Appliance Configuration**.

4. On the **General** tab, locate the Trust Store section.

5. Click **Add New**.

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

7. Click **Choose File**. Select the new certificate.

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

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

- Make sure you add the appliance identity certificate and certificate chain (if applicable) to the appliance trust store (its own trust store) and the trust stores shown in the **Trust Store Requirements** table.

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

Trust Store Requirements

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

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

Appliance Identity Certificates	Details	Add to Trust Stores
Manager/ Central Manager	Add the Manager certificates to the Manager trust store and the trust store of every appliance in Central Management.	- Primary Manager - 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 you are replacing the secondary Manager identity certificate, add the new secondary Manager certificates to the secondary Manager trust store, the primary Manager trust store,	- Flow Collectors - Flow Collector Databases (5000 series only) - Flow Sensors - UDP Directors - Data Nodes

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

		• Primary Manager
UDP Director in High Availability Pair	• Add the secondary UDP Director certificates to the primary UDP Director trust store. • Add the primary UDP Director certificates to the secondary UDP Director trust store.	• Secondary UDP Director (High Availability only) • Primary UDP Director (High Availability only) • Secondary Manager (Failover only) • Primary Manager
Data Node	Add the Data Node certificates to the Data Node trust store and to the Manager trust store.	• Primary Manager • Data Nodes • 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.

> **i** If you are not generating new certificates on your Data Nodes, 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 your appliances will be experiencing relatively low volumes of traffic.

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. Return to the **Appliance** tab > **SSL/TLS Appliance Identity**.

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

5. Click **Choose File**. Select the new certificate.

   Also, complete these steps for your certificate file format:

   - **PKCS#12:** In the Bundle Password field, enter the password required to decrypt the file. The password is not stored.

   - **PEM:** In the Certificate Chain File field, upload the certificate chain file separately (click Choose File). Make sure the chain file is in the correct order and meets the requirements. Refer to **PEM Chain File Requirements** in the Introduction for details.

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

6. Click **Replace Identity**.

7. Click **Apply Settings**.

8. Follow the on-screen prompts. The appliance reboots automatically.

9. Review the inventory in **Central Management**. 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

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 Certificates 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 Certificates to the Trust Stores

Before you update the appliance identity, add the certificates to the required trust stores.

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

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

Make sure you upload the following certificates:

- identity
- chain (root and intermediate certificates)

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

1. Open Central Management.

2. On the Inventory tab, click the ⋯ (**Ellipsis**) icon for the appliance.

   Order: Select your appliances in the following order:
   - Flow Collectors
   - Flow Sensors
   - UDP Directors
   - Data Nodes
   - Managers

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

3. Choose **Edit Appliance Configuration**.

4. On the **General** tab, locate the Trust Store section.

5. Click **Add New**.

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

7. Click **Choose File**. Select the new certificate.

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

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

   - Make sure you add the appliance identity certificate and certificate chain (if applicable) to the appliance trust store (its own trust store) and the trust stores shown in the **Trust Store Requirements** table.

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

Trust Store Requirements

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

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

Appliance Identity Certificates	Details	Add to Trust Stores
Manager Central Manager	Add the Manager certificates to the Manager trust store and the trust store of every appliance in Central Management.	• Primary Manager • 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 you are replacing the secondary Manager identity certificate, add the new secondary Manager certificates to the secondary Manager trust store, the primary Manager trust store, and the trust store of every appliance in Central Management. If you have not yet	• 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	Add the Flow Collector certificates to the Flow Collector trust store and the Manager trust store. **5000 Series Only:** • Add the Flow Collector engine certificates to the Flow Collector database trust store. • Add the Flow Collector database certificates to the Flow Collector engine trust store.	• Flow Collector • Flow Collector Databases (5000 series only) • Secondary Manager (Failover only) • Primary Manager
Flow Sensor	Add the Flow Sensor certificates to the Flow Sensor trust store and the Manager trust store.	• Flow Sensor • Secondary Manager (Failover only) • Primary Manager
UDP Director	Add the UDP Director certificates to the UDP Director trust store and the Manager trust store.	• UDP Director • Secondary Manager (Failover only) • Primary Manager
UDP Director in High Availability Pair	• Add the secondary UDP Director	• Secondary UDP Director (High Availability only)

	certificates to the primary UDP Director trust store. • Add the primary UDP Director certificates to the secondary UDP Director trust store.	• Primary UDP Director (High Availability only) • Secondary Manager (Failover only) • Primary Manager
Data Node	Add the Data Node certificates to the Data Node trust store and to the Manager trust store.	• Primary Manager • Data Nodes • 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 are not generating new certificates on your Data Nodes, 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 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

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.

Deleting Certificates from the Trust Stores

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

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

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

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

Trust Store							Add New
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
mmxm nzq1o rmi0yz wnmzd	fs-7 1.la m	fs-7 1.la m	2020-11-20 17:51:53	2025-11-20 17:51:53	3	8192 bits	Delete
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 appliance identity certificates (identity and chain) are saved. If the chain file was uploaded to the trust stores, the root and intermediate certificate files are listed individually.

Appliance Identity Certificates	Trust Stores
Manager Central Manager	• Primary Manager • Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes • Secondary Manager (Failover only)
Secondary Manager (Failover Only)	• Flow Collectors • Flow Collector Databases (5000 series only) • Flow Sensors • UDP Directors • Data Nodes

	• Secondary Manager (Failover only) • Primary Manager **Manager Failover:** If you delete an Manager failover relationship, delete the secondary Manager certificates from the trust stores of all appliances. Refer to the [Failover Configuration Guide](#) for details and instructions.
Flow Collector	• Flow Collector • Secondary Manager (Failover only) • Primary Manager **5000 Series Only:** • 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	• Flow Sensor • Secondary Manager (Failover only) • Primary Manager
UDP Director	• UDP Director • Secondary Manager (Failover only) • Primary Manager
UDP Director in High Availability Pair	• Secondary UDP Director (High Availability only) • Primary UDP Director (High Availability only) • Secondary Manager (Failover only)

	• Primary Manager
Data Node	• Primary Manager • 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 the Appliance Setup Tool. The Host Naming section of Central Management shows this information as read-only.

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

Reviewing the Current Configuration

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

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

Changing the Host Name or Network Domain Name

Use the following instructions to change the appliance host name or network domain name. As part of this procedure, you will remove the appliance from Central Management temporarily, and the appliance identity certificate is replaced automatically.

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

Requirements

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

- A unique host name 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.

- **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.

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

Overview

The overall steps are as follows:

1. Stop the Data Store Database

2. Remove Appliances from Central Management

3. Change the Manager Host Name or Network Domain Name

4. Add Appliances to Central Management

5. Start the Data Store Database

6. Delete Outdated Manager Certificates from the Trust Stores

7. 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.

> ℹ If your system does not include Data Nodes, 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**.

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 (and register the appliance in Central Management) using the Appliance Setup Tool.

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

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

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

2. Click **Continue/Next** and scroll to the **Host Name and Domains** tab.

3. Enter the new host name or network domain name in the fields.

> ⚠️ 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.

4. Click **Next** until the **Review and Restart** dialog opens.

5. Confirm your new configuration is correct. Click **Restart and Proceed**. Follow the on-screen prompts to restart the Manager.

6. Log in to the Manager again.

7. On the **Register Your Appliance** tab, review the IP address and click **Save**.
   - This installs Central Management on the Manager.
   - The Manager IP address is detected automatically and cannot be changed.

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

Inventory
1 Appliances found

| 🔍 Filter Appliance Inventory Table | | | | |

APPLIANCE STATUS ⌃	HOST NAME ⌃	TYPE ⌃	IP ADDRESS ⌃	ACTIONS ⌃
Connected		Manager /E-KVM-⊙		⊙

4. Add Appliances to Central Management

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

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Connected** before you start configuring the next appliance in your cluster.
- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.
- **Order:** Follow the <u>appliance configuration order</u>.
- **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 **7. Configure the Manager Failover Pair**.

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

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

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

   All Other Appliances: Skip to step 4.

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

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

User	Default Password
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).

5. Add the appliance to Central Management as follows:
   - **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **7. Configure the Manager Failover Pair**.

- **All Other Appliances:** Enter the IP address of your primary Manager. Click **Save**. Follow the on-screen prompts to trust the primary Manager appliance identity certificate and enter the Manageradmin user name and password. Select the Secure Network Analytics domain and complete any other required info.

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

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

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

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

5. Start the Data Store Database

> ℹ️ If you don't have Data Nodes in your deployment, go to **6. 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**.

6. 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.

7. 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).

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

Overview

The overall steps are as follows:

1. Stop the Data Store Database

2. Remove the Appliance from Central Management

3. Change the Appliance Host Name or Network Domain Name

4. Start the Data Store Database

> ℹ️ 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.

> ℹ️ If you are not generating new certificates on your Data Nodes, go to **Changing the Host Name or Network Domain Name**.

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

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

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

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

2. Click **Continue/Next** and scroll to the **Host Name and Domains** tab.

3. Enter the new host name or network domain name in the fields.

> ⚠️ 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.

4. Click **Next** until the **Review and Restart** dialog opens.

5. Review your settings. Click **Restart and Proceed**.

6. The appliance restarts.

7. Log in to the appliance.

8. Click **Continue/Next** to scroll to the **Central Management** tab in the Appliance Setup Tool.

- Enter the IP address of your primary Manager/Central Manager. Click **Save**.

- Follow the on-screen prompts to finish the changes in the Central Management tab.

9. Log in to the primary Manager.

- Confirm the appliance is shown in the Central Management inventory.

- Confirm the Appliance Status is shown as **Connected**.

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

4. Start the Data Store Database

> ℹ️ 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 the Appliance Setup Tool. You can change selected network interfaces in Central Management, or you can change the IP address (eth0 network interface) using the Appliance Setup Tool.

- **IP Address:** To change the appliance IP address, refer to **Changing the Appliance IP Address**.

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

> ⚠️ **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, and the appliance identity certificate is replaced automatically.

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

Requirements

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

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

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

Select the Procedure for your Appliance

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

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

Manager

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

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

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

Overview

The overall steps are as follows:

1. **Remove Appliances from Central Management**
2. **Change the Manager IP Address**
3. **Add Appliances to Central Management**
4. **Delete Outdated Manager Certificates from the Trust Stores**
5. **Configure the Manager Failover Pair**

> ⚠️ **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**.

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 and register it in Central Management using the Appliance Setup Tool.

Manager Failover: If you have two Managers, you only need to complete this procedure on the primary Manager. You will register the secondary Manager in **3. Add Appliances to Central Management**.
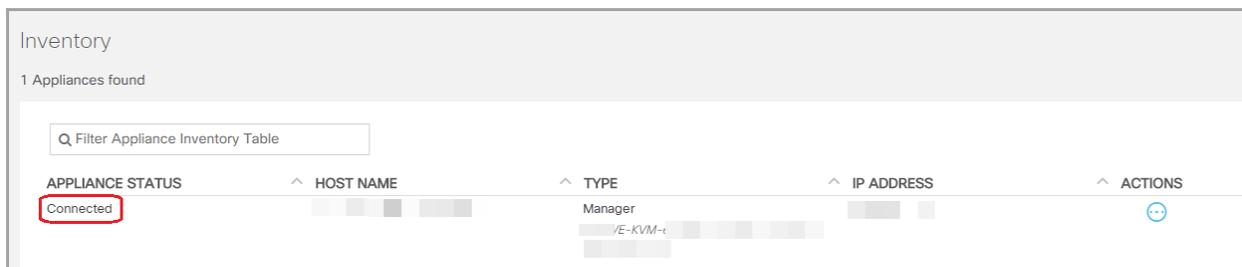
1. Log in to the Manager as admin: https://<IP address>

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

2. Click **Continue/Next** and scroll to the **Management Network Interface** tab.

3. Enter the new IP address in the field.

   When you change the IP address or Subnet Mask, the **Gateway and Broadcast Address** revert to their default settings. Make sure these fields are correct for your network before you proceed to the next step.

4. Click **Next** until the **Review and Restart** dialog opens.

5. Confirm your new configuration is correct. Click **Restart and Proceed**. Follow the on-screen prompts to restart the Manager.

6. Log in to the Manager (using the new IP address).

7. On the **Register Your Appliance** tab, review the IP address and click **Save**.

   - This installs Central Management on the Manager.
   - The Manager IP address is detected automatically and cannot be changed.

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

3. Add Appliances to Central Management

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

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

- **Central Management:** You need the Manager IP address, Manager password, and the Secure Network Analytics domain.

- **Order:** Follow the appliance configuration order.

- **Access:** You need admin privileges to access Central Management.

Appliance Configuration Order

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

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

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

   - **Connected:** Confirm each appliance is **Connected** before you add the next appliance to Central Management.

- **Order:** Make sure you [configure your appliances in order](#) so they communicate correctly.

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

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

   All Other Appliances: Skip to [step 4](#).

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

   Use the following criteria:

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

User	Default Password
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

4. Click **Next** and scroll to the **Central Management** tab or the **Register Your Appliance** tab (secondary Manager only).

5. Add the appliance to Central Management as follows:

   - **Secondary Manager:** If you have a secondary Manager, it selects itself as Central Manager. Choose the Secure Network Analytics domain and complete any other required info. Configure Failover after all appliances are configured in the Appliance Setup Tool. Refer to **5. Configure the Manager Failover Pair**.

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

> **ⓘ** The menus may vary, depending on the appliance. For example, if you are configuring a Flow Sensor, you will select a Flow Collector as part of the setup.

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

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

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

4. Delete Outdated Manager Certificates from the Trust Stores

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

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

1. Click the ••• (**Ellipsis**) icon for the appliance.

2. Choose **Edit Appliance Configuration**.

3. Choose the **General** tab.

4. Review the **Trust Store** list. Locate all outdated Manager certificates (identity, intermediates, and root).

5. Click **Delete** to delete each outdated certificate.

6. Click **Apply Settings**. Follow the on-screen prompts.

7. On the Central Management Inventory 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.

5. Configure the Manager Failover Pair

To reconfigure your Managers as a failover pair, follow the instructions in the [Failover Configuration Guide](#).

Non-Manager Appliances

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

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

Overview

The overall steps are as follows:

1. Remove the Appliance from Central Management

2. Change the Appliance IP Address

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

1. Remove the Appliance from Central Management

1. Open Central Management.

2. Review the Appliance Status column. Confirm all appliances are shown as **Connected**.

3. Locate the appliance you are going to change. Click the ⋯ (**Ellipsis**) icon.

4. Choose **Remove This Appliance**.

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

2. Change the Appliance IP Address

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

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

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

2. Click **Continue/Next** and scroll to the **Management Network Interface** tab.

3. Enter the new IP address in the field.

   When you change the IP address or Subnet Mask, the **Gateway and Broadcast Address** revert to their default settings. Make sure these fields are correct for your network before you proceed to the next step.

4. Click **Next** until the **Review and Restart** dialog opens.

5. Review your settings. Click **Restart and Proceed**.

   The appliance restarts.

6. Log in to the appliance (using the new IP address).

7. Click **Continue/Next** to scroll to the **Central Management** tab in the Appliance Setup Tool.

   - Enter the IP address of your primary Manager/Central Manager. Click **Save**.
   - Follow the on-screen prompts to finish the changes in the Central Management tab.

8. Log in to the primary Manager.

   - Confirm the appliance is shown in the Central Management inventory.
   - Confirm the Appliance Status is shown as **Connected**.

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

Adding SSL/TLS Client Identities

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

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

Additional Certificate Configurations

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

- **Audit Log Destination:** Follow the instructions in the Help. 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."

ℹ️ 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**.

> ℹ️ 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.

> ℹ️ 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**.

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**.

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**.

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

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

8. Click **Choose File**. Select the new certificate.

   - **Format:** PKCS#12. For details, refer to **Certificate Requirements**.
   - **Password:** In the Bundle Password field, enter the password required to decrypt the file. The password is not stored.

9. Click **Add Client Identity**.

10. Click **Apply Settings**.

11. Review the Additional SSL/TLS Client Identities list. Confirm the new certificate is shown.

Deleting a Client Identity Certificate

1. [Open Central Management](#).

2. Click the ••• (**Ellipsis**) icon for the appliance.

3. Choose **Edit Appliance Configuration**.

4. Choose the **Appliance** tab.

5. On the **Additional SSL/TLS Client Identities** list, locate the certificate you want to delete.

6. Click **Delete**.

Troubleshooting

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

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

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

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

> ⚠️ Check your company policy before you proceed.

Why is my appliance identity certificate invalid?

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

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

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

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

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

1. Log in to the appliance console as sysadmin.

   - **First:** If you are removing more than one appliance, log in to your Flow Collectors, Flow Sensors, 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 though 5 on all other appliances as needed).

> ⚠️ Remove the Manager from Central Management last.

2. Type **SystemConfig**. Press Enter.

3. From the main menu, select **Recovery**.

4. Select **RemoveAppliance**.

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

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqRecoveryqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Select a menu:                                                     x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x RemoveAppliance    Remove appliance from Central Management    x x
x x Factory Defaults   Restore the appliance to its factory defaults. x x
x x Refresh Image      Refresh the appliance image.                x x
x x                                                                x x
x x                                                                x x
x x                                                                x x
x x                                                                x x
x x                                                                x x
x x                                                                x x
x x                                                                x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                    x
x                                                                    x
x                                                                    x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x            <Select>              < Exit >                           x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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

The Appliance Status shows Initializing instead of Connected

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

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

Contacting Support

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

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

Change History

Document Version	Published Date	Description
1_0	March 2, 2023	Initial Version.
2_0	October 12, 2023	Updated the *Replacing Unexpired Cisco Default Certificates (Certificate Refresh)* section.
3_0	January 23, 2024	Added Data Store to applicable procedures. Updated patch installation instructions in the *Replacing Unexpired Cisco Default Certificates (Certificate Refresh)* section.

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)