Managing Certificates in your Nexus Dashboard, Release 4.2.1

Table of Contents

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.2.1	Certificate signing request (CSR) certificates	Beginning with Nexus Dashboard 4.2.1, you can create Certificate Signing Request (CSR) for a **System** or **Fabric** certificate role. For more information, see Certificate signing request (CSR).

Understanding certificate management

Nexus Dashboard provides a mechanism to manage X.509 certificates required by various TLS servers and clients on the system. For example, the web server on NX-OS requires an X.509 certificate for its TLS server functionality. Features such as remote authentication, peer controller connections, and several others run a TLS client, which also needs a X.509 certificate.

By default, all TLS servers start with self-signed certificates that you can replace with Certificate Authority (CA)-signed certificates. Self-signed certificates cannot be trusted because peers cannot verify these certificates, hence, you need to install CA signed certificates to establish trust.

Similarly, TLS clients must verify peer certificates presented by TLS servers, which requires access to the signer's certificate, commonly referred to as a CA certificate. Nexus Dashboard provides utility to manage both server and client certificates, as well as CA certificates.

Nexus Dashboard supports the following types of certificates:

CA certificates

These are certificates of the signers for the System and Fabric certificates, regardless of whether a certificate is used by a server or a client. The CA certificate bundle is common to the entire system and available to every functionality which needs to verify a certificate, including NX-API server certificates offered by switches.

System certificates

These are certificates used by Nexus Dashboard features which are either running a TLS server or a TLS client, such as the Webserver, Bootstrap server, CyberArk, and MessageBus. Depending upon requirements of the features, one or more certificates may be required.

Fabric Certificates

These are certificates installed on managed devices, such as NX-OS switches, which run a TLS server meant for NX-API functionality.

Certificate management differs based on your Nexus Dashboard deployment type and user role.

- Only ASCII encoded (PEM) format is supported, binary encoded certificates are not supported.
- Key and certificate files must have the same filename, for example, a certificate and its key pair must be named 'mycert.pem' and 'mycert.key'.
- Only X.509 certificates are supported.
- Nexus Dashboard accepts an identity (ID) certificate (server or client) after verifying the signature, which means CA certificate is required before a server or client certificate can be accepted.
- You can bring your own generated and signed certificate/key pair or use Nexus Dashboard CSR mechanism to generate a CSR, have it signed by your CA, and then upload it back to the system

LAN deployments

- For users with the super admin role, all certificate management options are enabled.
- For users with the fabric admin role and "All" security domain, all of tasks are enabled except

System Certificates. For system certificates, the list API is allowed.

- For any remaining user roles, only the certificates list is available.

SAN deployments

- For users with the super admin role, **CA Certificates** and **System Certificates** options are available with the following criteria:
  - In the **CA Certificate** page, **Install** on a device is disabled.
  - In the **System Certificate** page, **Manage feature attachments**, "aiComputeVisibility", “bootStrapServer”, “messageBus” and “cyberArk” is disabled.
  - The **Fabric Certificates** page is not available.
- For users with the fabric admin role and “All” security domain, the behavior is the same as that for users with the super admin role.
- For any remaining user roles, only the certificates list is available.

Handling passphrases

At certain points in the certificate management process, such as when you are generating a key, the process prompts you to provide a mandatory PEM passphrase.

When you enter a passphrase as part of the certificate management process, do not lose the passphrase information. If you lose the passphrase, you will not be able to upload the certificates later in the process. Cisco is not able to aid you if you lose the passphrase related to the certificate management process.

CA certificates

CA certificates

To install server or client certificates on Nexus Dashboard, you must provide the CA certificates of the issuers of those certificates. This is important because peer trust depends on verifying the certificates presented by a server or client. Therefore, only certificates with a corresponding CA certificate present on the system will be accepted.

Certificate validation

Nexus Dashboard release 4.1.1 introduced enhanced certificate validation that includes strict X.509 checks, aligning with industry-standard cryptographic practices. This enhanced validation enforces all X.509 options and extensions (including extended key usage (EKU)) according to CA rules, ensuring robust security.

While Nexus Dashboard does not specifically mandate a particular EKU, it rigorously enforces any EKU values present in a certificate. If a certificate contains supported X.509 extensions or options with non-compliant values, Nexus Dashboard may reject it. This means certificates that functioned in earlier Nexus Dashboard versions (3.2.x and earlier versions) may now be deemed invalid if they do not meet these stricter criteria.

For example, if a certificate is intended for a web server, the X509v3 EKU field must include *TLS Web Server Authentication* or be entirely absent. If the certificate does not meet these conditions, Nexus Dashboard marks it as invalid.

Troubleshoot certificate validation failures

If certificate validation fails, Nexus Dashboard displays a generic error message, such as cannot find matching CA, and it may not always specify the exact issue. This message often indicates that the certificate does not comply with the strict X.509 checks introduced in Nexus Dashboard release 4.1.1.

To inspect the details of your certificate, including its X509v3 extensions, use the following command:

```
openssl x509 -noout -text -in <certfile>
```

Review the output, particularly the X509v3 extensions section. For example, look for X509v3 EKU field. If this field is present, ensure it contains appropriate values like *TLS Web Server Authentication* for server certificates, or ensure it is absent if the certificate does not require a specific EKU for its purpose.

Example output (illustrating *TLS Web Server Authentication* present)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
```

```
            xxxxxxxxxxxxxxxxxxxxxxx
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, O=Example Corp, CN=Example Root CA
        Validity
            Not Before: Sep 26 21:48:09 2025 GMT
            Not After : Dec 30 21:48:09 2027 GMT
        Subject: C=US, ST=California, L=San Jose, O=Example Corp, CN=Example Root CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    xxxxxxxxxxxxxxxx
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication  <-- This line is
critical
            X509v3 Subject Key Identifier:
                xxxxxxxxxxxxx
            X509v3 Authority Key Identifier:
                xxxxxxxxxxxxx
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        Xxxxxxxxxxxxxxxxxxx
```

Example output (illustrating absence of X509v3 EKU extension)

This certificate is also valid for server authentication because the X509v3 EKU extension is not present, meaning there are no explicit restrictions on its extended use.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            xxxxxxxxxxxxx
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, O=Example Corp, CN=Example Root CA
        Validity
            Not Before: Sep 28 17:21:03 2025 GMT
            Not After : Jan  1 17:21:03 2028 GMT
        Subject: C=US, ST=California, L=San Jose, O=Example Corp, CN=Example Root CA
```

```
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                xxxxxxxxxxxxx              Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            xxxxxxxxxxxxx          X
        509v3 Authority Key Identifier:
            xxxxxxxxxxxxx
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
    xxxxxxxxxxxxx
```

Power-on Auto Provisioning (POAP) and CA certificates

The bootstrap server on Nexus Dashboard offers its certificate to POAP clients (i.e., switches), and these switches require the corresponding CA certificate to verify the server's certificate. In POAP terminology, there is a designated switch, referred to as the "Bench Router", that is programmed with CA certificates. Nexus Dashboard certificate management provides a utility to program one or more CA certificates on a given Bench Router, which is an NX-OS device.

Upload CA certificates

To upload the CA certificates onto Nexus Dashboard, perform the following steps:

1. Navigate to the **Certificate Management** window:

   Admin > Certificate Management

2. Click the **CA Certificates** tab, then click **Add CA certificate** to upload the appropriate license file.

   For Secure POAP enabled switches, you must upload Root CA Certificate files. You can upload multiple files at a single instance.

3. Browse your local directory and choose the certificate to upload.

   You can upload certificates with the .pem/.cer/.crt/ file extensions.

   

   Root CA certificates are public certificates and do not contain keys. Switches require these Root CA bundles to verify Nexus Dashboard POAP/PnP server certificate which is signed by one of the Root CA in the bundle.

4. Click **Save** to upload the selected files to Nexus Dashboard.

A successful upload message appears. The uploaded certificates are listed in the table.

Install certificate bundles on a bootstrap bench router

Nexus Dashboard does not assign the Root CA certificate bundle to the Bench Routers. Hence, after installing new certificates, ensure that you install the new certificates on the Bench Router (BR).

Follow these steps to install certificate bundles on a bootstrap bench router (BR):

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **CA Certificates** tab.
3. Choose the appropriate certificate, then click **Actions > Install Certificate Bundle to POAP Bench Router (BR)**.

   The **Install Certificate Bundle to Bootstrap Bench Router (BR)** page appears.

4. Click **Assign**, and choose the relevant switches.

Delete CA certificates

You can delete CA certificates after uploading new certificates.

1. Unassign the bench router to delete the certificate.
2. Choose one or more certificates to delete, then click **Actions > Delete**.

System certificates

Upload system certificates

Follow these steps to upload system certificates.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **System Certificates** tab, then click **Add system certificate** to upload the appropriate license file.
3. Browse your local directory and choose the certificate-key pair to upload.

   You can upload certificates with the .pem/.cer/.key/.crt/ file extensions.

4. Click **Save** to upload the chosen files to Nexus Dashboard.

   A successful upload message appears. The uploaded certificates are listed in the table.

You must reload the browser URL once the new certificate is uploaded for webServer and Saved. It is possible that for a few seconds the Nexus Dashboard URL might show as disconnected.

Map a feature to a system certificate

After you have uploaded system certifications using the procedures provided in Upload system certificates, you can map a feature to a system certificate in the **System Certificates** page.

Follow these steps to map a feature to a system certificate.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **System Certificates** tab.
3. Attach and install the certificate.

   - In the row **Manage Feature Attachments**, click the ellipse (...) and choose the feature to attach and install the certificate,

     or

   - Choose the certificate to see the **Manage Feature Attachments** button, then click to choose the feature to attach and install the certificate, then click **Save**.

   You can choose from these feature attachments:

   - aiComputeVisibility
   - bootStrap
   - messageBus

- cyberArk
- webServer

All feature attachments are visible for LAN profile. For SAN profile, only the webServer feature attachment is visible.

Delete system certificates

You can delete system certificates after uploading new certificates.

Follow these steps to delete system certificate.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **System Certificates** tab and choose the certificates you want to delete.
3. Click **Actions > Delete** to delete the certificate from Cisco Nexus Dashboard.

Enable NX-API certificate verification

The NX-API certificate verification is enabled using the toggle button on the **Fabric Certificates** page. However, this must be done only after all the switches managed by Cisco Nexus Dashboard are installed with CA-signed certificates and the corresponding CA Root certificates (one or more) are uploaded to Cisco Nexus Dashboard. When this is enabled, the Cisco Nexus Dashboard SSL client starts verifying the certificates that are offered by the switches. If the verification fails, the NX-API calls fail.

- Verification of the NX-API certificates cannot be enforced per switch; it is for either all or none. Hence, it is important that the verification is enabled only when all the switches have their corresponding CA-signed certificates installed.
- It is also required that all the CA certificates are installed on the Cisco Nexus Dashboard.
- When an NX-API call fails for a given switch because of verification issues, you can use the toggle button to disable enforcement, and all goes back to the previous state without any consequences.
- Because of the above mentioned points, you must enable the enforcement during a maintenance window.

To enable NX-API certificate verification:

1. Navigate to the **Certificate Management** window:

   Admin > Certificate Management

2. Click the **Fabric Certificates** tab, then click the toggle switch next to the **Enable NX-API certificate verification** field.

   A Warning popup appears, asking for verification that you want to perform this action.

3. Confirm that you have met all the guidelines described earlier in this section, then click **Enable** to enable NX-API certificate verification.

Fabric certificates

Upload fabric certificates

To upload fabric certificates onto Nexus Dashboard, perform the following steps:

1. Navigate to the **Certificate Management** window:

   Admin > Certificate Management

2. Click the **Fabric Certificates** tab, then click **Add fabric certificate** to upload the appropriate license file.
3. Browse your local directory and choose the certificate-key pair to upload.

   You can upload certificates with the .pem/.cer/.key/.crt/ file extensions.

4. Click **Save** to upload the selected files to Nexus Dashboard.

   A successful upload message appears. The uploaded certificates are listed in the table.

Delete fabric certificates

You can delete fabric certificates after uploading new certificates.

1. Navigate to the **Certificate Management** window:

   Admin > Certificate Management

2. Click the **Fabric Certificates** tab.
3. Click **Actions > Delete** to delete the certificate from Cisco Nexus Dashboard.

Assign switches and install certificates

1. Navigate to **Admin > Certificate Management > Fabric Certificates**.
2. Locate the row with the uploaded Fabric certificate and click **Install** on a device, or click the ellipses (...) to launch **Install** on a device.

   > NOTE: You can install unencrypted, encrypted keys, and a certificate in a single bulk install. However, you must provide the key password used for encrypted keys.

3. For each certificate, click on the **Assign** arrow and choose the switch to associate with the certificate.
4. Click **Install Certificates** to install all the certificates on their respective switches.

Guidelines and limitations: Fabric certificates

- When assigning fabric certificates to switches using one-to-one mapping, it may take a few minutes for the assignment task to complete.

Unlink certificates

After the certificates are installed on the switch, Nexus Dashboard cannot uninstall the certificate from Nexus Dashboard. However, you can always install a new certificate on the switch. The certificates that are not installed on the switches can be deleted. To delete the certificate installed on the switch, you must unlink the certificate from the switch, and then delete it from Nexus Dashboard.

Unlinking the certificate from the switch does not delete the certificate on the switch. The certificate still exists on the switch. Nexus Dashboard cannot delete the certificate on the Switch.

Follow these steps to delete certificates from Nexus Dashboard repository.

1. Choose the certificate(s) that you need to delete.
2. From the **Actions** drop-down list, choose **Unlink**.
3. Click **OK** to unlink the certificates from the switches. The switch name is removed from the **Attached To** column.
4. Choose the certificate that is now unlinked from the switch.

Certificate signing request (CSR)

CSR help you establish secure communication using SSL/TLS certificates. You use CSR to request digital certificates from a Certificate Authority (CA), which encrypt traffic to and from Nexus Dashboard and protect data integrity and confidentiality.

Nexus Dashboard provides comprehensive certificate management. You can install a certificate and key pair on Nexus Dashboard and assign it to a specific feature. For example, Nexus Dashboard's web server starts with a self-signed certificate, which browsers do not trust. You can install a CA-signed certificate and key pair on the web server. If browsers recognize the CA, they can verify the server's identity.

Nexus Dashboard supports only encrypted private keys to help protect user security. Password-based mechanisms can introduce risks, and uploading private keys usually offers less security.

Generate CSR

Follow these steps to generate CSR.

Make sure to upload the signing CA certificate (root CA) first. For more information on uploading certificates, see Upload CA certificates.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **Certificate signing request (CSR)** tab, then click **Generate CSR** to generate a CSR.
3. On the **Generate Certificate Signing Request (CSR)** page, enter the following:
   - **Certificate name** : Enter a name for the CSR
   - **Certificate role** : Select if you want to generate a **Fabric** or **System** certificate
   - **Common name (CN)** : Enter a common name
   - (Optional) **Country name (c)** : Enter the country name
   - (Optional) **State or province name** : Enter the state or province name
   - (Optional) **Locality name (L)** : Enter the locality name
   - (Optional) **Organization name (O)** : Enter the organization name
   - (Optional) **Organizational unit name (OU)** : Enter the organizational unit name
   - **Email address** : Enter an email address
   - **Subject Alternative Name (SAN) IP address** : Enter the SAN IP address
   - **DNS** : Enter the DNS name
   - **Extensions** : Enter the extensions that refers to basicConstraints(CA) and extended key usage. For example, " CA: false, ExtendedKeyUsage: [serverAuth, clientAuth]"
   - **Key Type** : Choose the key type between **ECDSA** or **RSA**
4. Click **Save**.

The generated certificate is listed under the **Certificate signing request (CSR)** tab.

The generated CSR will only include the public key. The private key is not displayed for security reasons.

Download the CSR

After you have generated the CSR using the procedures provided in Generate CSR, you must download the CSR in the **Certificate signing request (CSR)** page.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **Certificate signing request (CSR)** tab.
3. Under **CSR name**, choose one or more CSRs to download. The CSRs are downloaded as a zip archive.
4. Click **Actions > Download CSR** to download the CSR.

Bind the CSR

After you have downloaded the CSR using the procedures provided in Download the CSR, you must take the CSR to a CA for it to be signed. Signed CSR creates a signed certificate, and this must be uploaded to ND using CSR bind mechanism on the **Certificate signing request (CSR)** page.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **Certificate signing request (CSR)** tab.
3. On the **Bind Certificate** page, under **CA signed certificate**, browse your local directory and upload the the CA signed certificate obtained using the CSR.
4. Click **Bind Certificate**.

   After bind is successful, CSR disappears from the **Certificate signing request (CSR)** tab and a signed certificates is available on the **System certificates** or **Fabric certificates** tab depending on which feature was chosen during CSR generation.

Delete CSR

You can delete CSR after uploading new certificates.

1. Navigate to the **Certificate Management** page:

   Admin > Certificate Management

2. Click the **Certificate signing request (CSR)** tab.
3. Click **Actions > Delete** to delete the certificate from Cisco Nexus Dashboard.

Viewing certificate expiry date anomalies

The **CA certificates** page displays the **Expires on** date for certificates. For certificates that are due to expire in 90 days or lesser, the system generates an alarm notification or anomaly every 24 hours. The system will not change the anomaly if one already exists for certificate expiry.

Certificate expiry does not automatically disable any system features. Each feature is responsible for handling its own behavior in response to an expired certificate. For example, the Nexus Dashboard web server will continue to operate even if its certificate has expired. While a web client may display an error due to the expired certificate, the server itself remains functional.

Follow these steps to view certificate expiry date anomalies.

1. Navigate to **Analyze** > **Anomalies**.

The system includes certificate expiry as one of its anomalies. To view the certificates that are expiring soon, click the **Include system anomalies** toggle button and check under **Anomaly type**.

2. Choose the certificate to update.
3. On the **Certificates Expired** page, upload the latest certificate.

The certificate expiry anomaly is not automatically cleared after you update the certificate. Choose **Actions** > **Clear anomaly** to clear the anomaly.

Copyright

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883