



Certificates

- [Retaining the CA Signed Certificate, on page 1](#)
- [Certificates Management for SAN Windows/Linux, on page 2](#)
- [Certificate Management for SAN OVA/ISO, on page 8](#)

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

When you configure a 3-node federation setup and apply external CA certificate, do the following:

1. Stop DCNM servers in Federation.
 - For Windows – Navigate to `C:\Program Files\Cisco Systems\dcn\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
 - For Linux – Logon to `/root`. Execute `/root/Stop_DCNM_Servers` command to stop services.
2. Generate CA certificates for Primary Servers, and apply the same CA certificate in the three secondary servers.
3. Start the Primary server first, then the secondary, third server thereafter, on Federation.

Note that if you change the keystore password or alias, you need to update it in the `standalone-san.xml` document located at:

```
<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

Update the password in the `keystore` tag and alias:

```
<keystore key-password>=<<storepass-pwd>> key-alias="updated-key-alias"  
keystore-password="updated-password"  
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```



Note <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.

Procedure

- Step 1** Backup the signed certificate from the location:
- For Windows: `<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks`
 - For Linux: `<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks`
- Step 2** Upgrade to Cisco DCNM Release 11.5(1).
- Step 3** After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.
- Note** You must load the certificates to the same location as mentioned in [Step 1, on page 2](#).
- Step 4** Restart the DCNM Services.
-

Certificates Management for SAN Windows/Linux

This section describes three ways on how to configure the certificates in Cisco DCNM.

Note that if you change the keystore password or alias, you need to update it in the `standalone-san.xml` document located at:

```
<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

Update the password in the **keystore** tag and alias in the **key-alias** tag:

```
<keystore key-password>="<<storepass-pwd>> key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```



Note `<<storepass-pwd>>` is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the **dcnm.fmserver.token** value for the **storepass-pwd**.

This section contains the following topics:

Using a Self-Signed SSL Certificate

Procedure

- Step 1** Stop the DCNM services.
- Step 2** Rename the keystore located at
- ```
<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks
```
- to
- ```
<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old
```

- Step 3** From command prompt, navigate to `<DCNM install root>\dcm\java\jre1.8\bin\<DCNM install root>\dcm\java\jdk11\bin\`
- Step 4** Generate a self signed certificate using following command:
keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks -storepass <<storepass-pwd>> -validity 360 -keysize 2048
- Note** <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.
- Step 5** Start the DCNM services.

Using an SSL Certificate when certificate request is generated using Keytool on Windows

Procedure

- Step 1** Stop the DCNM services.
- Step 2** Rename the keystore located at
`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks`
to
`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old`
- Step 3** From command prompt, navigate to `<DCNM install root>\dcm\java\jre1.8\bin\<DCNM install root>\dcm\java\jdk11\bin\`
- Step 4** Generate the public-private key pair in DCNM keystore by using the following command:
keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore "<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass <<storepass-pwd>> -validity 360 -keysize 2048
- Note** <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.
- Step 5** Generate the certificate-signing request (CSR) from the public key generated in [Step 4, on page 3](#).
keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass <<storepass-pwd>>
- Note** <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.

Note The `dcnm.csr` file is created in the keytool directory, located at `/usr/local/cisco/dcm/java/jdk11/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the `.p7b` file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (`.p7b` file) or PEM (`.pem`) file. If CA provided PKCS 7 format go to [Step 7, on page 4](#) to convert it to PEM format. If CA provided PEM format, then go to [Step 8, on page 4](#).

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain using `openssl`.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of `cert-chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

keytool -importcert -trustcacerts -file cert-chain.pem -keystore "`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks`" -storepass <<storepass-pwd>> -alias sme

Note <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Create the store for each server in the Federation setup using the following command on the Primary server:

keytool -importkeystore -srckeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -srckeypass <<storepass-pwd of primary>> -srcstorepass <<storepass-pwd of primary>> -srcstoretype JKS -destkeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver2.jks -destkeypass <<storepass-pwd-of-federation-server>> -deststorepass <<storepass-pwd-of-federation-server>> -deststoretype JKS -alias sme

Note <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.

Step 10 Copy the new `fmserver2.jks` to the Federation server as `fmserver.jks` at `/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration` directory on the Federation server.

Step 11 Repeat [Step 9, on page 4](#) and [Step 10, on page 4](#) on every server in the Federation setup.

Step 12 Start the DCNM service.

Ensure that you start the primary server, second sever and the third server in the Federation setup in the sequential order.

Step 13 To enable launching of SAN Client, copy the `fmtrust.jks` on server1 located at `/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks` to both second and third servers in the Federation setup.

For further instructions, refer to [Launching SAN Client and Device Manager](#).

Using an SSL Certificate When Certificate Request Is Generated Using Keytool on Linux

Procedure

- Step 1** Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.
- Step 2** Rename the keystore that is located at:
`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks`
 To
`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old`
- Step 3** From command prompt, navigate to the appropriate folder:
`<DCNM_install_root>/dcm/java/jdk11/bin/`
- Step 4** Generate the public-private key pair in DCNM keystore by using the following command:
`./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass <<storepass-pwd>> -validity 360 -keysize 2048`
- Note** `<<storepass-pwd>>` is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.
- Step 5** Generate the certificate-signing request (CSR) from the public key that is generated in [Step 4, on page 5](#).
`./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks" -storepass <<storepass-pwd>>`
- Note** `<<storepass-pwd>>` is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.
- Note** The `dcnm.csr` file is created in the keytool directory, which is located at `/usr/local/cisco/dcm/java/jdk11/bin`.
- Step 6** Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the `.p7b` file.
 CA may provide the certificate and signing certificate as a certificate chain in PKCS 7 format (`.p7b` file) or PEM (`.pem`) file. If CA provided the certificate chain in PKCS 7 format, go to [Step 7, on page 5](#) to convert it to PEM format. If CA provided the certificate chain in PEM format, then go to [Step 8, on page 6](#).
- Step 7** Convert the PKCS 7 certificate chain to the X509 certificate chain using OpenSSL.
`openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem`

Note Ensure that the user provides either absolute or relative path to the correct location of `cert-chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

```
./keytool -importcert -trustcacerts -file cert-chain.pem -keystore
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass
<<storepass-pwd>> -alias sme
```

Note `<<storepass-pwd>>` is the password string generated while installing DCNM Server. This string is located in the `<install_dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the `dcnm.fmserver.token` value for the `storepass-pwd`.

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Create the store for each server in the Federation setup using the following command from the Primary server:

```
keytool -importkeystore -srckeystore
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -srckeypass
<<storepass-pwd of primary>> -srcstorepass <<storepass-pwd of primary>> -srcstoretype JKS
-destkeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver2.jks
-destkeypass <<storepass-pwd-of-federation-server>> -deststorepass
<<storepass-pwd-of-federation-server>> -deststoretype JKS -alias sme
```

Step 10 Copy the new `fmserver2.jks` to the Federation server as `fmserver.jks` at `/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration` directory on the Federation server.

Step 11 Repeat Step [Step 9, on page 6](#) and [Step 10, on page 6](#) on every server in the Federation setup.

Step 12 To enable launching of SAN Client, copy the `fmtrust.jks` on server1 located at `/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks` to both second and third servers in the Federation setup.

For further instructions, refer to [Launching SAN Client and Device Manager](#).

Step 13 Start the DCNM service.

Ensure that you start the primary server, second sever and the third server in the Federation setup in the sequential order.

Using a SSL Certificate when certificate request is generated using OpenSSL on Linux

To configure SSL certificates in Cisco DCNM, using certificate request generated using open SSL, perform the following steps.

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the `appmgr stop dcnm` command.

Step 2 Rename the keystore located at:

```
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks
```

to

<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old

Step 3

From command prompt, navigate to <DCNM_install_root>/dcm/java/jdk11/bin/.

Step 4

Generate the RSA private key using OpenSSL.

```
openssl genrsa -out dcnm.key 2048
```

Step 5

Generate a certificate-signing request (CSR) by using following command:

```
openssl req -new -key dcnm.key -sha256 -out dcnm.csr
```

Step 6

Submit the CSR to Certificate signing authority, and download the signed certificate chain in Base-64 format which creates the **.p7b** file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provides the PKCS 7 format, go to [Step 7, on page 7](#) to convert it to PEM format. If CA provides the PEM format, go to [Step 8, on page 7](#).

Step 7

Convert the PKCS 7 certificate chain to X509 certificate chain.

```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```

Step 8

Convert the X509 certificate chain and private key to PKCS 12 format

```
openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password pass
<<storepass-kwd>> -name sme
```

Note <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the <install_dir>/dcm/fm/conf/serverstore.properties directory. Fetch the **dcnm.fmserver.token** value for the **storepass-pwd**.

Note Ensure that the user provides either absolute path or relative path to the correct location of dcnm.key & dcnm.p12 files in the above command.

Step 9

Import the intermediate certificate, the root certificate, and the signed certificate in the same order.

```
./keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -deststoretype
JKS -alias sme -srcstorepass <<storepass-pwd>> -deststorepass <<storepass-pwd>>
```

Note <<storepass-pwd>> is the password string generated while installing DCNM Server. This string is located in the <install_dir>/dcm/fm/conf/serverstore.properties directory. Fetch the **dcnm.fmserver.token** value for the **storepass-pwd**.

Note Ensure that the user provides either absolute path or relative path to the correct location of cert-chain.pem, dcnm.key, and dcnm.p12 files in the above command.

Step 10

Create the store for each server in the Federation setup using the following command from the Primary server:

```
keytool -importkeystore -srckeystore
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -srckeypass
<<storepass-pwd of primary>> -srcstorepass <<storepass-pwd of primary>> -srcstoretype JKS
-destkeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver2.jks
-destkeypass <<storepass-pwd-of-federation-server>> -deststorepass
<<storepass-pwd-of-federation-server>> -deststoretype JKS -alias sme
```

Step 11

Copy the new fmserver2.jks to the Federation server as **fmserver.jks** at <usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration> directory on the Federation server.

Step 12 Repeat Step [Step 10, on page 7](#) and [Step 11, on page 7](#) on every server in the Federation setup.

Step 13 Start the DCNM service.

Ensure that you start the primary server, second sever and the third server in the Federation setup in the sequential order.

Step 14 To enable launching of SAN Client, copy the **fmtrust.jks** on server1 located at **/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks** to both second and third servers in the Federation setup.

For further instructions, refer to [Launching SAN Client and Device Manager](#).

Certificate Management for SAN OVA/ISO



Note This section to applicable only for DCNM OVA/ISO deployments.

From Release 11.2(1), Cisco DCNM allows new methods and new CLIs for installing, restoring after upgrade, and verifying certificates on the system.



Note From Release 11.3(1), you must use **sysadmin** role for certificate management.

Cisco DCNM stores two certificates:

- Self-signed certificate, for internal communication between the Cisco DCNM Server and various applications
- CA (Certificate Authority) Signed certificate, for communicating with the external world, such as Web UI.



Note Until you install a CA Signed certificate, Cisco DCNM retains a self-signed certificate for the communicating with the external network.

Best practices for Certificate Management

The following are the guidelines and best practices for Certificate Management in Cisco DCNM.

- Cisco DCNM provides CLI based utilities to display, install, restore, and export or import of certificates. These CLIs are available through SSH console, and only a **sysadmin** user can accomplish these tasks.
- When you install Cisco DCNM, a self-signed certificate is installed, by default. This certificate is used to communicate with the external world. After Cisco DCNM installation, you must install a CA-Signed certificate on the system.

- Generate a CSR on Cisco DCNM with a CN (common name). Provide a VIP FQDN (Virtual IP Address FQDN) as CN to install a CA Signed certificate. The FQDN is the fully qualified domain name for the management subnet VIP (VIP of eth0) interface that is used to access Cisco DCNM Web UI.
- If the CA Signed certificate was installed prior to upgrading the Cisco DCNM, then you must restore the CA Signed certificate after you upgrade the Cisco DCNM.



Note You need not take a backup of certificates when you perform inline upgrade or backup and restore.

Display Installed Certificates

You can view the details of the installed certificate by using the following command:

appmgr afw show-cert-details

In the following sample output for the **appmgr afw show-cert-details** command, **CERTIFICATE 1** represents the certificate offered to the external network and to the Web browsers. **CERTIFICATE 2** represents the internally used certificate.

```

dcnm# appmgr afw show-cert-details

****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4202 (0x106a)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=IN, ST=KA, L=BGL, O=xyz, OU=ABC, CN=<FQDN/IP>
    Validity
      Not Before: Jun  4 13:55:25 2019 GMT
      Not After : Jun  3 13:55:25 2020 GMT
    Subject: C=IN, ST=KA9, L=BGL9, O=XYZ123, OU=ABC123, CN=<FQDN/IP>
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:bb:52:1e:7f:24:d7:2e:24:62:5a:83:cc:e4:88:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till DCNM
version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation guide
to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
alias = sme, storepass = <<storepass-pwd>>
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US

```

```

Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
    MD5:  E5:F8:AD:17:4D:43:2A:C9:EE:35:5F:BE:D8:22:7D:9C
    SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
    SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
-----Certificate output is truncated to first 15 lines-----
dcnm#

```



Note <<*storepass-pwd*>> is the password string generated while installing DCNM Server. This string is located in the <install dir>/dcm/fm/conf/serverstore.properties directory. Fetch the **dcnm.fmserver.token** value for the **storepass-pwd**.

The Web UI refers to the **CERTIFICATE 1** after installation. If **CERTIFICATE 1** is not available, you must stop and restart all applications, using the following commands:



Note Ensure that you follow the same sequence of commands on the Cisco DCNM to troubleshoot this scenario.

On the Cisco DCNM Standalone appliance, run the following commands to stop and start all Cisco DCNM applications to troubleshoot **CERTIFICATE 1**:

```

dcnm# appmgr stop all /* stop all the applications running on Cisco DCNM */
dcnm# appmgr start all /* start all the applications running on Cisco DCNM */

```

Installing a CA Signed Certificate

We recommend that you install a CA Signed certificate as a standard security practice. The CA Signed certificates are recognized, and verified by the browser. You can also verify the CA Signed certificate manually.



Note The Certificate Authority can be an Enterprise Signing Authority, also.

Installing a CA Signed Certificate on Cisco DCNM Standalone Setup

To install a CA Signed certificate on the Cisco DCNM, perform the following steps.

Procedure

Step 1 Logon to the DCNM server via SSH terminal.

Step 2 Generate a CSR on the Cisco DCNM server using the **appmgr afw gen-csr** command:

Note CSR is unique to a Cisco DCNM, and only a corresponding CSR signed certificate must be installed on a given Cisco DCNM.

```

dcnm# appmgr afw gen-csr
Generating CSR...
..
...
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...

A CSR file dcnmweb.csr is created in the /var/tmp/ directory.

***** CA certificate installation not completed yet. Please do followings. *****
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.

```

Step 3 Send this CSR to your Certificate signing server.

Note The CA Signing server is local to your organization.

Step 4 Get the certificate signed by your Certificate Authority.

The Certificate Authority (CA) returns 3 certificates, namely, Primary, Intermediate (also known as Issuing/Subordinate), and Root certificates. Combine all the three certificates into one .pem file to import to DCNM.

Step 5 Copy the new CA Signed certificate to Cisco DCNM server.

Ensure that the certificate is located at /var/tmp directory on the Cisco DCNM Server.

Step 6 Install the CA Signed certificate on the Cisco DCNM by using the following commands:

Note We recommend that you run the following commands in the same sequence as shown below.

```

dcnm# appmgr stop all /* Stop all applications running on Cisco DCNM
dcnm# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway...

```

CA signed certificate CA-signed-cert.pem is installed. Please start all applications as followings:

On standalone setup execute: 'appmgr start all'

Step 7 Restart all applications with the new certificate on Cisco DCNM using the **appmgr start all** command.

```
dcnm# appmgr start all
```

Step 8 Verify the newly installed CA Signed certificate using the **appmgr afw show-cert-details** command.

The system is now armed with the CA Signed certificate, which is verified at the browser.

Note CSR is unique to a Cisco DCNM, and only a corresponding CSR signed certificate must be installed on a given Cisco DCNM.

Restoring the certificates after an upgrade

This mechanism applies to Cisco DCNM Upgrade procedure using the inline upgrade process only. This procedure is not required for the backup and restore of data on the same version of the Cisco DCNM appliance.

Note that certificate restore is a disruptive mechanism; it requires you to stop and restart applications. Restore must be performed only when the upgraded system is stable, that is, you must be able to login to Cisco DCNM Web UI. On a Cisco DCNM Native HA setup, both the Active and Standby nodes must have established peer relationship.



Note A certificate needs to be restored only in following situations:

- if a CA signed certificate was installed on the system before upgrade, and,
- if you're upgrading from a version prior to 11.2(1) to version 11.2(1) or later.

After upgrading the Cisco DCNM, you must always verify the certificate before restoring to check if **CERTIFICATE 1** is the CA signed certificate. You must restore the certificates, if otherwise.

Verify the certificates using the **appmgr afw show-cert-details** as shown in the sample output below.

```

dcnm# appmgr afw show-cert-details
****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1575924977762797464 (0x15decf6aec378798)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=CA, L=San Jose, O=Enterprise CA inc, OU=Data Center, CN=dcnm1.ca.com

    Validity
      Not Before: Dec  9 20:56:17 2019 GMT
      Not After : Dec  9 20:56:17 2024 GMT
    Subject: C=US, ST=CA, L=San Jose, O= Enterprise CA inc, OU=Data Center,
CN=dcnm1.ca.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:cf:6e:cd:c6:a9:30:08:df:92:98:38:49:9c:2a:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till DCNM
version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation guide
to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----

```

```

Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
  SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
  SHA256:
EO:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
-----Certificate output is truncated to first 15 lines-----
dcnm#

```

Restoring Certificates on Cisco DCNM Standalone setup after Upgrade

To restore the certificates after you upgrade the Cisco DCNM Standalone deployment to Release , perform the following:

Procedure

-
- Step 1** **Note** When you upgrade to Release , a backup of the CA Signed certificate is created.
- After you have successfully upgraded the Cisco DCNM Standalone appliance, logon to the DCNM server via SSH.
- Step 2** Stop all the applications using the following command:
- ```
appmgr stop all
```
- Step 3**     Restore the certificate by using the following command:
- ```
appmgr afw restore-CA-signed-cert
```
- Step 4** Enter **yes** to confirm to restore the previously installed certificate.
- Step 5** Start all the applications using the following command:
- ```
appmgr start all
```
- Step 6**     Verify the newly installed CA Signed certificate using the **appmgr afw show-cert-details** command.
- The system is now armed with the CA Signed certificate, which is verified at the browser.
- 

## Recovering and Restoring Previously Installed CA Signed Certificates

Installing, restoring, managing CA signed certificate is a time-consuming process as a third-party signing server is involved. This may also lead to omissions or mistakes which can result in installing wrong certificates. In such a scenario, we recommend that you restore the certificates that were installed prior to the latest install or upgrade.

To recover and restore the previously installed CA signed certificates, perform the following steps.

### Procedure

- Step 1** Logon to the DCNM server via SSH terminal.  
**Step 2** Navigate to the `/var/lib/dcnm/afw/apigateway/` directory.

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw----- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw----- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw----- 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt
.
..
...
```

**dcnmweb.key** and **dcnmweb.crt** are the key and certificate files that are installed on the system, currently. Similar filenames, with timestamp suffix, help you in identifying the key and certificate pairs installed prior to the recent upgrade or restore.

- Step 3** Stop all applications running on Cisco DCNM using **appmgr stop all** command.  
**Step 4** Take a backup of `dcnmweb.key` and `dcnmweb.crt` files.  
**Step 5** Identify the older key and certificate pair that you want to restore.  
**Step 6** Copy the key and certificate pair as **dcnmweb.key** and **dcnmweb.crt** (without timestamp suffix).  
**Step 7** Start all applications running on Cisco DCNM using **appmgr start all** command.  
**Step 8** Verify the details of the certificate using the **appmgr afw show-cert-details** command. CERTIFICATE 1 is the CA signed certificate.

**Note** If the CA signed certificate is not visible to Cisco DCNM Web UI, or if the DCNM Server sends any failure message, you must reboot the system.



## Verifying the installed certificate

While the installed certificate can be verified using the **appmgr afw show-cert-details** command, the web browser verifies if the certificate is effective or not. Cisco DCNM supports all standard browsers (Chrome, IE, Safari, Firefox). However, each browser display the certificate information differently.

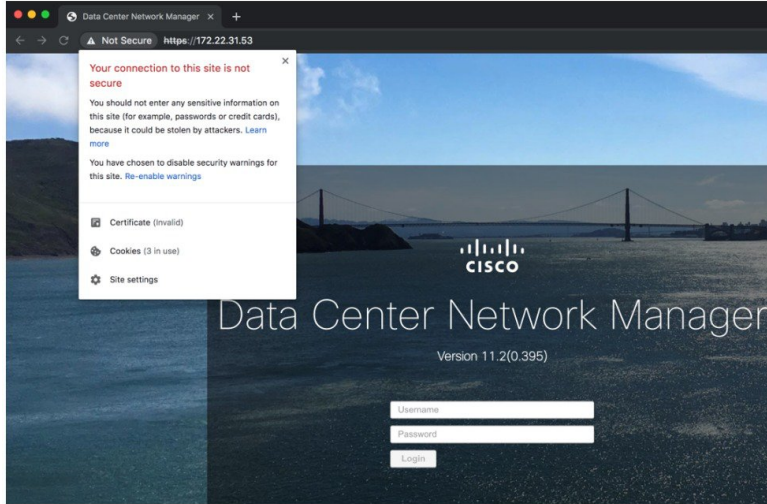
We recommend that you refer to the browser specific information on that browser provider website.

The following snippet is a sample from the Chrome Browser, Version 74.0.3729.169, to verify the certificate.

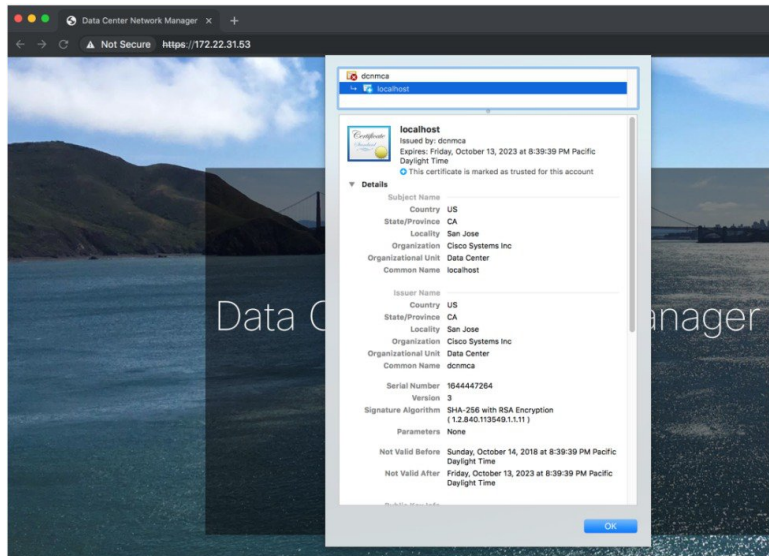
1. Enter URL **https://<dcnm-ip-address>** or **https://<FQDN>** in the address bar on the browser.  
 Press the **Return** key.

- Based on the type of certificate, the icon on the left of the URL field shows a lock icon [  ] or an alert icon [  ].

Click on the icon.



- On the card, click **Certificate** field.  
The information in the certificate is displayed.



The information that is displayed must match with the details as displayed on CERTIFICATE 1 when you view the certificate details using the `apmgr afw show-cert-details`.

