

Cisco DNA Center Security Best Practices Guide

First Published: 2018-12-19

Last Modified: 2020-01-03

Security Hardening Overview

Cisco Digital Network Architecture (Cisco DNA) Center is a highly advanced and capable enterprise controller for the Cisco network platform. As one of the most critical infrastructure components of enterprise networks, Cisco DNA Center must be deployed securely. This guide explains the best practices that must be followed to ensure a secure deployment. To mitigate possible security risks, if any, you must carefully evaluate the multilayered security considerations for Cisco DNA Center in your network infrastructure, and take the necessary actions recommended in this guide.



Note This guide is updated on a regular basis when new security features are introduced in Cisco DNA Center. We recommend that you bookmark this guide and download the latest version from [cisco.com](https://www.cisco.com).

Security for Cisco DNA Center

Cisco DNA Center provides many security features for itself, as well as for the hosts and network devices that it monitors and manages. You must clearly understand and configure the security features correctly. We strongly recommend that you follow these security recommendations:

- Deploy Cisco DNA Center behind a firewall that does not expose the management ports to an untrusted network, such as the internet.
- Replace the self-signed server certificate from Cisco DNA Center with one signed by a well-known certificate authority (CA).
- Upgrade Cisco DNA Center with critical upgrades, including security patches, as soon as possible after a patch announcement.
- Open the DNS access control list (ACL) and ports that are used by Cisco DNA Center, coupled with known IP address ranges.



Note We recommend that you configure a proxy gateway between Cisco DNA Center and the network devices it monitors and manages.

User Role Considerations

Users are assigned roles that control access to the functions that they are permitted to perform.

We strongly recommended that you restrict the number of users with the administrator role because administrators have control over the configuration of critical functions.

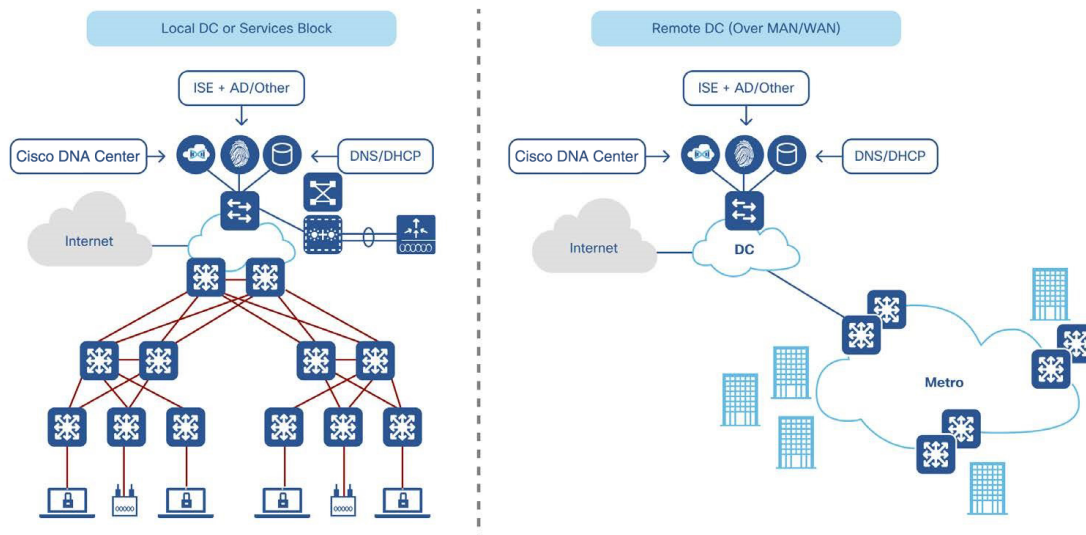
Cisco DNA Center supports the following user roles. For more information, see "About User Roles" and "Create Local Users" in the [Cisco Digital Network Architecture Center Administrator Guide](#).

- **Administrator (SUPER-ADMIN-ROLE):** Users with this role have full access to all Cisco DNA Center functions. However, they can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE. Restrict the number of users having this role.
- **Network Administrator (NETWORK-ADMIN-ROLE):** Users with this role have full access to all network-related Cisco DNA Center functions. However, they do not have access to system-related functions, such as App Management, User Management (except for changing their own passwords), and Backup and Restore.
- **Observer (OBSERVER-ROLE):** Users with this role have view-only access to Cisco DNA Center functions. They cannot access any functions that configure or control Cisco DNA Center or the devices it manages.

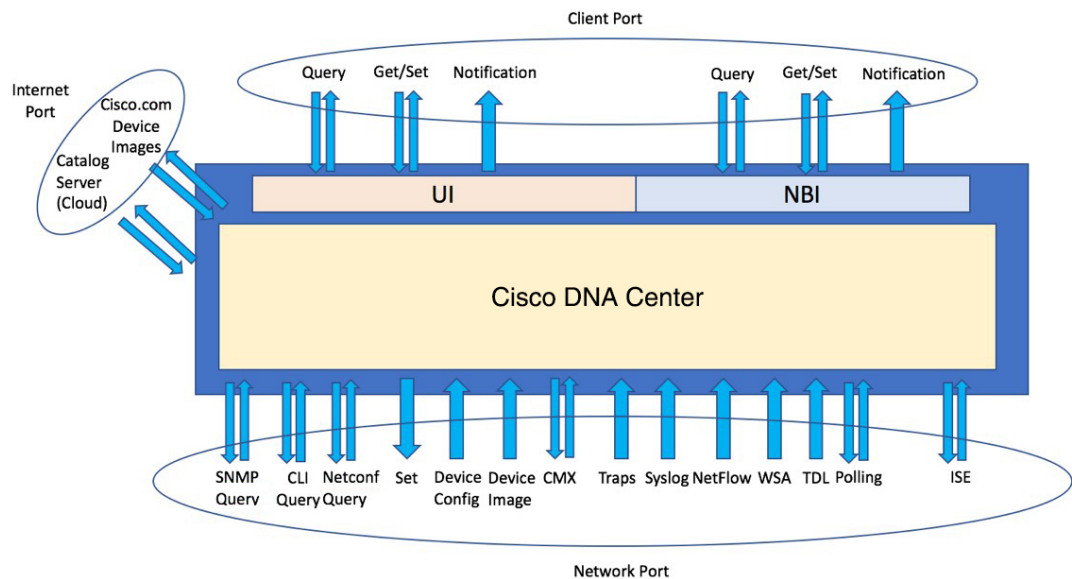
Cisco DNA Center can use Cisco Identity Services Engine (ISE) or other authentication, authorization, and accounting (AAA) servers for user authentication. For more information, see the "Configure Authentication and Policy Servers" section in the [Cisco Digital Network Architecture Center Administrator Guide](#).

Secure Your Cisco DNA Center Deployment

Cisco DNA Center provides many security features for itself, as well as for the hosts and network devices that it monitors and manages. We strongly recommend that you place Cisco DNA Center and Cisco ISE behind a firewall in either a local data center (head of campus) or remote data center as shown here.



To access Cisco DNA Center through the web GUI and to enable Cisco DNA Center to interact with network devices, specific ports must be configured on the firewall. Cisco DNA Center integrates with the cloud and is distributed across the globe for practical latency requirements.



Communication Ports

The following table lists the ports that Cisco DNA Center uses, the names of the services communicating over these ports, and the product's purpose in using them. The Recommended Action column indicates whether you can disable a port and service without affecting the functionality of Cisco DNA Center or whether you must leave the port open.



Note If you have a firewall between Cisco DNA Center and the management network, the following ports must be open in the firewall. In the following table, some destination ports in Cisco DNA Center are duplicated. The subsections call out the usage and related network service. You can limit the source IP ACL in the firewall rules or choose to not open the port if the service is not deployed in your environment.

Port(s)	Service Name	Purpose	Recommended Action
Administering/Configuring Cisco DNA Center			
TCP 443	UI, REST, HTTPS	Web UI, REST, HTTPS management port.	Port must be open.
TCP 2222	Cisco DNA Center shell	Connect to the Cisco DNA Center shell.	Port must be open. Restrict the known IP address to be the source.
TCP 9004	Web UI installation	Serves the web-UI based installation page (only needed if you choose to install Cisco DNA Center via the web-based option).	Port must be open until installation of the node is complete.
TCP 9005	Web UI installation API service	Serves the API for the web-based installation (connected by the browser client from port 9004; no external agent requires access).	Port must be open until the cluster formation is complete.

Port(s)	Service Name	Purpose	Recommended Action
Cisco DNA Center Outbound to Device/Other Systems			
TCP 22	SSH	Cisco DNA Center uses SSH to connect to devices so that it can read the device configuration for discovery, and make configuration changes.	SSH must be open between Cisco DNA Center and the managed network devices.
TCP 23	Telnet	Although Telnet is not recommended, Cisco DNA Center can use Telnet to connect to devices in order to read the device configuration for discovery, and make configuration changes.	Telnet can be used for device management, but we do not recommend it because Telnet does not offer security mechanisms like SSH.
UDP 53	DNS	Cisco DNA Center uses DNS to resolve hostnames.	Port must be open for DNS hostname resolution.
UDP 123	NTP	Cisco DNA Center uses NTP to synchronize the time from the source that you specify.	Port must be open for time synchronization.
UDP 161	SNMP	Cisco DNA Center uses SNMP to discover network devices; to read device inventory details, including device type; and for telemetry data purposes, including CPU and RAM.	Port must be open for network device management and discovery.
TCP 443	HTTPS	Used for cloud-tethered upgrades.	Port must be open for cloud tethering, telemetry, and software upgrades.
TCP 830	NETCONF	Cisco DNA Center can use NETCONF for device inventory, discovery, and configuration.	Port must be open for network device management and discovery of devices that support NETCONF.
UDP 1812 or 1645	RADIUS	Only needed if you are using external authentication with a RADIUS server.	Port must be open only if an external RADIUS server is used to authenticate user login to Cisco DNA Center.
UDP 49	TACACS	Only needed if you are using external authentication with a TACACS server.	Port must be open only if you are using external authentication with a TACACS server.
Device to Cisco DNA Center			
TCP 443, 22, 80	HTTPS, SFTP, HTTP	<p>Software image download from Cisco DNA Center through HTTPS:443, SFTP:22, HTTP:80.</p> <p>Certificate download from Cisco DNA Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry.</p> <p>Note Block port 80 if you don't use Plug and Play (PnP), Software Image Management (SWIM), Embedded Event Management (EEM), device enrollment, and Cisco 9800 Wireless Controller.</p>	<p>Ensure that firewall rules limit the source IP of hosts or network devices allowed to access Cisco DNA Center on these ports.</p> <p>Note We do not recommend the use of HTTP 80. Use HTTPS 443 wherever possible.</p>
UDP 123	NTP	Devices use NTP for time synchronization.	Port must be open to allow devices to synchronize the time.

Port(s)	Service Name	Purpose	Recommended Action
UDP 6007	NetFlow	Cisco DNA Center receives NetFlow network telemetry from devices.	Port must be open for data analytics based on NetFlow.
UDP 162	SNMP	Cisco DNA Center receives SNMP network telemetry from devices.	Port must be open for data analytics based on SNMP.
UDP 514	Syslog	Cisco DNA Center receives syslog messages from devices.	Port must be open for data analytics based on syslog.
TCP 25103	Cisco 9800 Wireless Controller	Used for Cisco 9800 Wireless Controller telemetry.	Port must be open only if a Cisco 9800 Wireless Controller is deployed with Cisco DNA Center.
TCP 32626	Intelligent Capture (gRPC) collector	Used for receiving traffic statistics and packet capture data used by the Cisco DNA Assurance Intelligent Capture (gRPC) feature.	Port must be open if you are using the Cisco DNA Assurance Intelligent Capture (gRPC) feature.
TCP 9991	Wide Area Bonjour Service	Cisco DNA Center receives multicast Domain Name System (mDNS) traffic from the Service Discovery Gateway (SDG) agents using the Bonjour Control Protocol.	Port must be open on Cisco DNA Center if the Bonjour application is installed.

Required URLs and FQDNs for Cisco DNA Center

The appliance requires secure access to the URLs and fully qualified domain names (FQDNs) listed in the following table.

Table 1: Required URLs and FQDN Access

Purpose	URL
Cisco DNA Center update package	https://*.ciscoconnectdna.com/
Smart Account and SWIM software downloads	https://apx.cisco.com https://cloudsso.cisco.com/as/token.oauth2 https://*.cisco.com/
User feedback	https://dnacenter.uservoice.com
Cisco AI Network Analytics	<ul style="list-style-type: none"> U.S. production cloud: https://api.use1.prd.kairos.ciscolabs.com European production cloud: https://api.euc1.prd.kairos.ciscolabs.com

Secure the Management Interface

If you are using Cisco Integrated Management Controller (IMC), the first security action to perform on the Cisco DNA Center appliance is to secure the out-of-band management interface (Cisco IMC) account. Change the default password of the *admin* account to a stronger value as per the password policy. See "Enable Browser Access to Cisco IMC" in the [Cisco Digital Network Architecture Center Appliance Installation Guide](#) and "Configure External Authentication" in the [Cisco Digital Network Architecture Center Administrator Guide](#).



Note You must secure the password of Maglev CLI users with super admin access. For details, see "Configure the Master Node" in the [Cisco Digital Network Architecture Center Appliance Installation Guide](#).

Rate Limit IP Traffic from a Specific Source

You can limit the incoming traffic from a specific source for various purposes, including security, monitoring, route selection, and network address translation. Cisco DNA Center allows you to throttle the ingress traffic based on IP address.

Before you begin

You must have maglev SSH access privileges to perform this procedure.

Procedure

Step 1 Using an SSH client, log in to the Cisco DNA Center appliance with the IP address that you specified using the configuration wizard.

The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your username and password for SSH access.

Step 3 Enter the following command to restrict the incoming traffic from a specific source:

```
/opt/maglev/bin/throttle_ip [options]
Options
-h show this help text
-i IP to rate limit (default: 0.0.0.0 i.e. ALL traffic)
-c Committed Information Rate in KBps (default: 100 K Bps)
-n Interface number (Mandatory parameter)
-d delete the last config and move the NIC to default configuration
-a Insert the new IP (to be throttled) in the already build filter list
-s show the current filter
```

Note If you don't enter a specific IP address, the full interface is throttled. The mandatory interface name limits the input transmission rate for all classes of traffic based on user-defined criteria.

Examples

```
#To create a new filter list
./throttle_ip -i 192.0.2.105 -n enp0s8 -c 256

#To add a new IP with different bandwidth
./throttle_ip -a 192.0.2.106 -n enp0s8 -c 512

#To delete all the IP from the List
./throttle_ip -d -n enp0s8
```

```
#To show the filters
./throttle_ip -s -n enp0s8
```

Step 4 Log out of the Cisco DNA Center appliance.

Enable TLS and RC4-SHA

Northbound REST API requests from the external network to Cisco DNA Center (from northbound REST API-based apps, browsers, and network devices connecting to Cisco DNA Center using HTTPS) are made secure using the Transport Layer Security (TLS) protocol. RC4-SHA is a stream cipher that is also used to secure Cisco DNA Center.

Enable TLS 1.0 and RC4-SHA for Cisco DNA Center by logging in to the appliance and using the CLI.



Note CLI commands can change from one release to the next. The following CLI example uses command syntax that might not apply to all Cisco DNA Center releases.

Before you begin

You must have maglev SSH access privileges to perform this procedure.



Important This security feature applies to port 443 on Cisco DNA Center. Performing this procedure may disable traffic on the port to the Cisco DNA Center infrastructure for a few seconds. For this reason, you should configure TLS infrequently and only during off-peak hours or during a maintenance period.

Procedure

Step 1 Using an SSH client, log in to the Cisco DNA Center appliance with the IP address that you specified using the configuration wizard.

The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your username and password for SSH access.

Step 3 Enter the following command to check the TLS version currently enabled on the cluster.

Example

```
Input
$ magctl service tls_version --tls-min-version show
Output
TLS minimum version is 1.1
```

Step 4 If you want to change the TLS version on the cluster, enter the following commands. For example, you might want to change the current TLS version to a lower version if your network devices under Cisco DNA Center control cannot support the existing TLS version.

Example: Change from TLS version 1.1 to 1.0

```

Input
$ magctl service tls_version --tls-min-version 1.0
Output
Enabling TLSv1.0 is recommended only for legacy devices
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.0 for api-gateway
deployment.extensions/kong patched

```

Example: Change from TLS version 1.1 to 1.2, when RC 4 is disabled

```

Input
$ magctl service tls_version --tls-min-version 1.2
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.extensions/kong patched

```

Note Setting TLS version 1.2 as the minimum version is not supported when RC4 ciphers are enabled.

Step 5 Enter the following command to enable RC4 on the cluster.

Enabling RC4 ciphers is not supported when TLS version 1.2 is the minimum version.

Example: TLS version 1.2 is not enabled

```

Input
$ magctl service ciphers --ciphers-rc4=enable kong
Output
Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
WARNING: Enabling RC4-SHA Cipher for kong
deployment.extensions/kong patched

```

Step 6 Enter the following command at the prompt to confirm that TLS and RC4-SHA are configured.

Example

```

Input
$ magctl service display kong
Output
containers:
- env:
  - name: TLS_V1
    value: "1.1"
  - name: RC4_CIPHERS
    value: "true"

```

If RC4 and TLS minimum versions are set, they are listed in the env: of the **magctl service display kong** command. If these values are not set, they do not appear in the env:.

Step 7 Log out of the Cisco DNA Center appliance.

Manage Credentials and Passwords

Cluster Password

Cisco DNA Center supports cluster formation with three nodes. For efficiency and security, we recommend the following:

- The cluster should be created with dedicated separated interfaces for connecting to the enterprise network, forming an intracluster network, and connecting to a dedicated management network.

- The intracluster network is created as an isolated Layer 2 segment and not connected or routed through any other network segments.
- You should not reuse passwords (Cisco IMC or SSH) across the Cisco DNA Center cluster members.

SSH/Maglev Password Recovery

You must secure the SSH password. Share the SSH password only with the super admin. Cisco DNA Center does not provide the functionality to recover the SSH password.

SSH Account Lockout and Recovery

After six consecutive failed login attempts over SSH, the maglev account will be temporarily locked for five minutes from the time of last failed attempt. During this lockout period, login attempts with correct password will also fail and counted as a failed login. The account will be unlocked for SSH login only after five minutes of no login activity. However, login using the Cisco IMC console will continue to work even during the lockout period. The administrator can enable SSH login during the lockout period, by executing the following command in the Linux shell:

```
sudo pam_tally2 --reset
```

Web UI Password Recovery

If a web UI user's password is lost, the password can be reset using the command-line shell, which requires SSH or console access. See "Reset a Forgotten Password" in the [Cisco Digital Network Architecture Center Administrator Guide](#).

Password Encryption

Cisco DNA Center uses SHA-512 encoding of operating system user passwords (the strongest method available for UNIX-based systems). No user-configurable action is available for Cisco DNA Center's password encryption mechanism.

Logs and Database Management

The system logs are available to the operating system administrator user with escalated privileges (sud access). The application logs are stored in Elastic search, and can be accessed through the web UI after authentication. The databases are protected by credentials, which are randomly generated during installation, and securely passed to the applications that need database access. No user-configurable action is available to change these settings.

Communication Protocol Payload Encryption

In clustered mode, Cisco DNA Center nodes communicate with each other through the intracluster network. No separate encryption is applied to the intracluster traffic. It is important to keep the intracluster network isolated.



Note

Services that exchange sensitive data among themselves use HTTPS.

Manage Certificates

Default Certificates

By default, Cisco DNA Center uses self-signed certificates. Cisco DNA Center manages the devices using the devices' self-signed certificates, unless otherwise deployed. We strongly recommend that you use a third-party, well-known CA certificate during deployment.


Note

Changing the Cisco DNA Center certificate from self-signed to third-party or from root CA to subordinate CA disrupts the network functionality. We strongly recommend that you upgrade the certificates before you begin the deployment.

Certificate and Private Key Support

Cisco DNA Center supports the PKI Certificate Management feature, which is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents called CAs. Cisco DNA Center uses the PKI Certificate Management feature to import, store, and manage X.509 certificates from well-known CAs. The imported certificate becomes an identity certificate for Cisco DNA Center, and Cisco DNA Center presents this certificate to its clients for authentication. The clients are the northbound API applications and network devices.

You can import the following files (in either PEM or PKCS file format) using the Cisco DNA Center GUI:

- X.509 certificate
- Private key


Note

For the private key, Cisco DNA Center supports the import of RSA keys. You should not import DSA, DH, ECDH, and ECDSA key types, because they are not supported. You should also keep the private key secure in your own key management system. The private key must have a minimum modulus size of 2048 bits.

Prior to import, you must obtain a valid X.509 certificate and private key from a well-known CA, or create your own self-signed certificate. After import, the security functionality based on the X.509 certificate and private key is automatically activated. Cisco DNA Center presents the certificate to any device or application that requests it. Northbound API applications and network devices can use these credentials to establish a trust relationship with Cisco DNA Center.


Note

We recommend that you do not use and import a self-signed certificate into Cisco DNA Center. We recommend that you import a valid X.509 certificate from a well-known CA. Additionally, you must replace the self-signed certificate (installed in Cisco DNA Center by default) with a certificate that is signed by a well-known CA for the PnP functionality to work correctly.

Cisco DNA Center supports only one imported X.509 certificate and private key at a time. When you import a second certificate and private key, the latter overwrites the first (existing) imported certificate and private key values.



Note If the external IP address changes for your Cisco DNA Center for any reason, reimport a new certificate with the changed or new IP address.

Certificate Chain Support

Cisco DNA Center is able to import certificates and private keys through its GUI. If subordinate certificates are involved in a certificate chain leading to the certificate that is to be imported into Cisco DNA Center (signed certificate), both the subordinate certificates as well as the root certificate of these subordinate CAs must be appended together into a single file to be imported. When appending these certificates, you must append them in the same order as the actual chain of certification.

The following certificates should be pasted together into a single PEM file. Review the certificate subject name and issuer to ensure that the correct certificates are being imported and correct order is maintained. Ensure that all of the certificates in the chain are pasted together.

- **Signed Cisco DNA Center certificate:** Its Subject field includes CN=<name or IP address of Cisco DNA Center>, and the issuer has the CN of the issuing authority.
- **Issuing (subordinate) CA certificate that issues the Cisco DNA Center certificate:** Its Subject field has CN of the (subordinate) CA that issues the Cisco DNA Center certificate, and the issuer is that of the root CA.
- **Next issuing (root/subordinate CA) certificate that issues the subordinate CA certificate:** Its Subject field is the root CA, and the issuer has the same value as the Subject field. If they are not the same, you must append the next issuer, and so on.

Generate a Certificate Request Using Open SSL

Procedure

- Step 1** Use an SSH client to log in to the Cisco DNA Center cluster and create a temporary folder under /home/magleev, for example, by entering the command **mkdir tls-cert;cd tls-cert** while in the home directory.
- Step 2** Using a text editor of your choice, create a file named `openssl.cnf` and upload it to the directory that you created in the preceding step. Use the following example as your guide, but adjust it to fit your deployment.
- The following example assumes a three-node Cisco DNA Center cluster. If you have a standalone device, use SANs for only that node and the VIP. If you cluster the device later, you might want to recreate the certificate to include the IP addresses of the new cluster members.
- Adjust **default_bits** and **default_md** if your certificate authority admin team requires 2048/sha256 instead.
 - Specify values for every field in the **req_distinguished_name** and **alt_names** sections. The only exception is the **OU** field, which is optional. Omit it if your certificate authority admin team does not require it.
 - The **emailAddress** field is optional; omit it if your certificate authority admin team does not require it.
 - Pay close attention to the **alt_names** section, which must contain all IP addresses and DNS names that are used to access Cisco DNA Center, either by a web browser or by an automated process such as PnP

or Cisco ISE. Note that you can use a wildcard when adding entries to this section. For example, **.domain.com* is a valid entry.

- If a cloud interface is not configured, omit the cloud port fields.
- In the **extendedKeyUsage** extension, the attributes `serverAuth` and `clientAuth` are mandatory. If you omit either attribute, Cisco DNA Center rejects the SSL certificate.
- Self-signed certificates must contain the X.509 Basic Constraints "CA:TRUE" extension.

Example openssl.cnf

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no
[req_distinguished_name]
C = <two-letter-country-code>
ST = <state-or-province>
L = <city>
O = <company-name>
OU = MyDivision
CN = FQDN-of-Cisco-DNA-Center-on-GUI-port
emailAddress = responsible-user@mycompany.tld

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = FQDN-of-Cisco-DNA-Center-on-GUI-port
DNS.2 = FQDN-of-Cisco-DNA-Center-on-enterprise-port
DNS.3 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
DNS.4 = *.domain.com
IP.1 = Enterprise port IP node #1
IP.2 = Enterprise port IP node #2
IP.3 = Enterprise port IP node #3
IP.4 = Enterprise port VIP
IP.5 = Cluster port IP node #1
IP.6 = Cluster port IP node #2
IP.7 = Cluster port IP node #3
IP.8 = Cluster port VIP
IP.9 = GUI port IP node #1
IP.10 = GUI port IP node #2
IP.11 = GUI port IP node #3
IP.12 = GUI port VIP
IP.13 = Cloud port IP node #1
IP.14 = Cloud port IP node #2
IP.15 = Cloud port IP node #3
IP.16 = Cloud port VIP
```

Note If you don't include the cluster IP addresses in the `openssl.cnf` file, you cannot schedule software image activation. To fix this problem, add the cluster IP addresses as SANs to the certificate.

Step 3 Enter the following command to create a public key. Adjust the key length to 2048 if required by your certificate authority admin team.

```
openssl genrsa -out csr.key 4096
```

Step 4 After populating the fields in the `openssl.cnf` file, use the public key that you created in the preceding step to generate the Certificate Signing Request.

```
openssl req -config openssl.cnf -new -key csr.key -out DNAC.csr
```

- Step 5** Verify the Certificate Signing Request content and ensure that the DNS names and IP addresses are populated correctly in the Subject Alternative Name field.

```
openssl req -text -noout -verify -in DNAC.csr
```

- Step 6** Copy the Certificate Signing Request and paste it to a CA (for example, MS CA).

Microsoft Active Directory Certificate Services -- ASSURANCE-SOL-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIFFTCCAvoCAQAwTELMAkGA1UEBhMCVVMxCzAJ
DAhTYW4gSm9zZTEWMBQGA1UECgwNQ21zY28gU31z
MRwwGgYJKoZIhvcNAQkBFg1hYmNAY21zY28uY29t
AAOCAg8AMIICGgKCAgEAvtRTBX8UGJp3jsvol1jn
GPIwNychoubCNpvRSkW/q3zRVrn6YmvZhS3qdaU9t
```

Certificate Template:


Web Server

Additional Attributes:

Attributes:

Submit >

Ensure that the certificate template you choose is configured for both client and server authentication (as illustrated in the extendedKeyUsage line in Step 2's openssl.cnf file example).

- Step 7** Download the certificate (full chain) in DER format and name it `dnac-chain.p7b`.
- Step 8** Copy the `dnac-chain.p7b` certificate that you downloaded in the preceding step to the Cisco DNA Center cluster through SSH.
- Step 9** Enter the following command:
- ```
openssl pkcs7 -in dnac-chain.p7b -inform DER -out dnac-chain.pem -print_certs
```
- Step 10** Copy the file `dnac-chain.pem` generated in the Cisco DNA Center cluster to your local system.
- Step 11** From the Cisco DNA Center home page, choose  > **System Settings** > **Settings** > **Certificates**.
- Step 12** Click **Replace Certificate**.
- Step 13** In the **Certificate** field, click the **PEM** radio button and perform the following tasks.
- For the **Certificate** field, import the `dnac-chain.pem` file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

- b) For the **Private Key** field, import the private key (csr.key) by dragging and dropping this file into the **Drag n' Drop a File Here** field.
- c) Choose **No** from the **Encrypted** drop-down list for the private key.

Use this page to view facts about or to replace the Cisco DNA Center server's currently active SSL certificate.

Certificate

Type  
☒ PEM  
☐ PKCS

dnac-chain.pem

Private Key

csr.key

Encrypted  
NO

**Step 14** Click **Upload/Activate**.

## Generate a Certificate Request Using an API

Follow this procedure to generate a Certificate Signing Request using an API or Swagger and obtain a certificate that is suitable for Cisco DNA Center from a well-known CA such as Microsoft CA:

### Procedure

**Step 1** Log in to Cisco DNA Center and enter the following URL:

`https://<cluster_IP>/dna/apitester`

**Step 2** Choose **PKI Broker > certificate management**.

- Step 3** Fill in the following optional fields. Cisco DNA Center adds all the IPs from the interfaces and the VIP to the SAN field.

GET
/certificate/csr
downloadCertCSR

### IMPLEMENTATION NOTES

This method is used to download certificate CSR

### RESPONSE CLASS

Model | Model Schema

Response Content Type: application/json

### PARAMETERS

| Parameter  | Value                       | Description | Parameter Type | Data Type |
|------------|-----------------------------|-------------|----------------|-----------|
| Country    | US                          | country     | query          | string    |
| State      | CA                          | state       | query          | string    |
| City       | SJ                          | city        | query          | string    |
| Org        | Cisco                       | org         | query          | string    |
| OrgUnit    | DNAC                        | orgUnit     | query          | string    |
| CommonName | dnac-cisco                  | commonName  | query          | string    |
| SanDNS     | www.cisco.com, www.dnac.com | sanDNS      | query          | string    |
| SanIP      | 10.28.113.79, 1.2.3.4       | sanIP       | query          | string    |
| KeyLen     | 4096                        | keyLen      | query          | string    |
| Digest     | sha512                      | digest      | query          | string    |

- Step 4** Click **Try it out!**

The window showing the Certificate Signing Request in the RESPONSE BODY section is displayed.

- Step 5** Copy the Certificate Signing Request and paste it to the CA.

**Note** Use Mozilla Firefox to view the JSON responses in the correct format.

## REQUEST URL

```
https://10.28.113.79/api/v1/certificate/csr?Country=US&State=CA&City=SJ&Org=Cisco&OrgUnit=DNAC&CommonName=DNA&Sa
```

## RESPONSE BODY

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC8DCCAdgCAQAwVDELMakGA1UEBhMCVVMxCzAJBgNVBAGMAkNBMQswCQYDVQQH
DAJTSjE0MAwGA1UECgwFQ2lzY28xDTALBgNVBAsMBER0QUMxDDAKBgNVBAMMA0R0
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANp4a+y+XDUDVoKYMIs
jhGEsQtNjSmIuYUyu1k6caTivJbPFYf27aKp04vx1usofwn/kh0Sxcm9mUbLEH7H
J8i53dXVRsCsZgCeUT1p5djYUzqoRDQjk9TptbrlUAkBWmD8HXjwxc5cktPxDa6
4t/y2SEHPEwb3HeX3cXrLxkWwIY5IEhJlschq6Y4AY46dsgAlu42hb0l2vh+6UNT
l8dJHEAQNpaSu+iM7nuAChWUJHS40H8kDBp0bWe8csof+bgUpdMrK2gnHAJD+p0x
3l6hKUpjDUekfIDW6wU2Cy0vYA5ATkv0GYCJL47atmYh3PN9752hQ14J0QPRzQdz
jakCAwEAABXMFUGCSqGSIb3DQEJJDJFIMEYwRAYDVR0RBDOw04IMd3d3LmRuYWMu
Y29tgg13d3cuY2lzY28uY29thwQKAQEBhwQBAgMEhwQKHHPPhwTAqHFPhwQFBgcI
MA0GCSqGSIb3DQEBwUAA4IBAQAUG2p7CCmhqfssHu3WBLvFRXVT77ZYBMqWP2fF
ZrwcIG/QcMPj+TV1RLbCd50PPdyoiQdP8nhxby6yKxe36G5pyLfc/vXhy9fEpbV
9yNcDIdodQTxoJ2QG7h6Shzlrp46rrwYxTYScE6/L2ziidUkBB0DvS7feKl7Nqx8
KsUJLLajYeIB9mDEBf/yCY+4Jiv9VLYmZd+3KZc8ZRLm7C0FyvRwzZh6oLLrBMY7
uHtuAxBVfZsn3ZZLFPuGtKsnjsPEkXpq0q4iU1TwIquNkHCdu7oMsQNuv5hfYSy/
rrlc/zD0CQ/x5KZ8JGY6ZGGrPN5zhb6CRDvURZ0290JjVr0f
-----END CERTIFICATE REQUEST-----
```

## RESPONSE CODE

```
200
```

**Step 6** Paste to a CA form, such as MS CA.



**Microsoft Active Directory Certificate Services -- apic-em-CA****Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded request from an external source (such as a Web server) in the Saved Request

**Saved Request:**

Base-64-encoded  
certificate request  
(CMC or  
PKCS #10 or  
PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC8DCCAdgCAQAwVDELMAkGA1UEBhMCVU
DAJTSjEOMAwGA1UECgwFQ2l2Y28xDTALBgN
QTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCC
jhGEsQtNjSmIuYUyu1k6caTlvJbPFYf27aKp04v
J8i53dXVRsCsZgCeUT1p5djYUzqoRDQjk9Tptk
4t/y2SEHPEwb3HeX3cXrLxkWWiY5IEhJlschq6
```

**Certificate Template:**

Subordinate Certification Authority 5 Year

**Additional Attributes:**

Attributes:

Submit >

**Step 7** After the CA issues the certificate, download the certificate to your PC.

**Step 8** Upload the certificate to Cisco DNA Center using the following URL:  
`https://<cluster_IP>/dna/apitester`

**Step 9** Choose **PKI Broker > certificate management**.

```
$ scp -P22 /home/maglev/tls-cert/DNAC.csr kebdwi@10.40.0.60:/Users/kebdwi/Desktop/DNAC/DNAC.csr
```

POST
/certificate/csr
importCsrCert

### IMPLEMENTATION NOTES

This method is to upload certificate generated using CSR

### RESPONSE CLASS

Model | Model Schema

```

{
 "version": "",
 "response": {
 "taskId": {},
 "url": ""
 }
}

```

Response Content Type: application/json

### PARAMETERS

| Parameter         | Value                                                                                    | Description             | Parameter Type | Data Type |
|-------------------|------------------------------------------------------------------------------------------|-------------------------|----------------|-----------|
| csrCertFileUpload | <input type="button" value="Choose File"/> <input type="text" value="certUsingCsr.p7b"/> | Upload Certificate file | form           | File      |

### REQUEST URL

```

https://10.28.113.79/api/v1/certificate/csr

```

### RESPONSE BODY

```

{"response":{"taskId":"7371df85-5df5-45e9-af1d-aa349860371b","url":"/api/v1/task/7371df85-5df5-45e9-af1d-aa349860371b"},"version":"1.0"}

```

### RESPONSE CODE

```

202

```

## Configure a Certificate

Cisco DNA Center supports the import and storage of an X.509 certificate and private key into Cisco DNA Center. After import, the certificate and private key can be used to create a secure and trusted environment between Cisco DNA Center, northbound API applications, and network devices.

You can import a certificate and a private key using the **Certificate** window in the GUI.


**Important**

Cisco DNA Center does *not* interact with any external CA directly. Therefore, it does not check any Certificate Revocation Lists and does not know if its server certificate has been revoked by an external CA. Note, also, that Cisco DNA Center does not automatically update its server certificate. Replacement of an expired or revoked server certificate requires explicit action by a SUPER-ADMIN-ROLE user. Although Cisco DNA Center has no direct means of discovering the revocation of its server certificate by an external CA, it does notify the admin about the expiry of its server certificate as well as about the self-signed key being operational.

**Before you begin**

You must have an X.509 certificate and private key from a well-known CA.

**Procedure**

**Step 1** From the Cisco DNA Center home page, choose  > **System Settings** > **Settings** > **Certificate**.

**Step 2** In the **Certificate** window, view the current certificate data.

When you first view this window, the current certificate data that is displayed is the Cisco DNA Center self-signed certificate. The self-signed certificate's expiry is set for several years in the future.

**Note** The **Expiration Date and Time** is displayed as a Greenwich mean time (GMT) value. A system notification appears in the Cisco DNA Center GUI two months before the certificate expires.

The additional fields that are displayed in the **Certificate** window include:

- **Current Certificate Name:** Name of the current certificate
- **Issuer:** Name of the entity that has signed and issued the certificate
- **Certificate Authority:** Either self-signed or the name of the CA
- **Expires On:** Expiry date of the certificate

**Step 3** To replace the current certificate, click **Replace Certificate**.

The following new fields appear:

- **Certificate:** Fields to enter certificate data
- **Private Key:** Fields to enter private key data

**Step 4** From the **Certificate** drop-down list, choose the file format type for the certificate that you are importing into Cisco DNA Center:

- **PEM:** Privacy-enhanced mail file format
- **PKCS:** Public-Key Cryptography Standard file format

**Step 5** If you choose **PEM**, perform the following tasks:

- For the **Certificate** field, import the **PEM** file by dragging and dropping the file into the **Drag n' Drop a File Here** area.

**Note** A PEM file must have a valid PEM format extension (.pem, .cert, .crt). The maximum file size for the certificate is 10 KB.

- For the **Private Key** field, import the private key by dragging and dropping the file into the **Drag n' Drop a File Here** area.
  - Choose the encryption option from the **Encrypted** drop-down list for the private key.
  - If you chose encryption, enter the passphrase for the private key in the **Passphrase** field.

**Note** Private keys must have a valid private key format extension (.pem or .key).

**Step 6** If you choose **PKCS**, perform the following tasks:

- For the **Certificate** field, import the **PKCS** file by dragging and dropping the file into the **Drag n' Drop a File Here** area.

**Note** A PKCS file must have a valid PKCS format extension (.pfx, .p12). The maximum file size for the certificate is 10 KB.

- For the **Certificate** field, enter the passphrase for the certificate in the **Passphrase** field.

**Note** For PKCS, the imported certificate also requires a passphrase.

- For the **Private Key** field, choose the encryption option for the private key.
- For the **Private Key** field, if encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

**Step 7** Click **Upload/Activate**.

**Step 8** Return to the **Certificate** window to view the updated certificate data. The information displayed in the **Certificate** window should have changed to reflect the new certificate name, issuer, and the certificate authority.

## Change the Role of the PKI Certificate from Root to Subordinate

Cisco DNA Center lets you change the role of the device PKI CA from a root CA to a subordinate CA.

When changing the private Cisco DNA Center CA from a root CA to a subordinate CA, note the following:

- If you intend to have Cisco DNA Center act as a subordinate CA, it is assumed that you already have a root CA, for example, Microsoft CA, and you are willing to accept Cisco DNA Center as a subordinate CA.
- As long as the subordinate CA is not fully configured, Cisco DNA Center continues to operate as an internal root CA.
- You must generate a Certificate Signing Request file for Cisco DNA Center (as described in the following procedure) and have it manually signed by your external root CA.



**Note** Cisco DNA Center continues to run as an internal root CA during this time period.

- After the Certificate Signing Request is signed by the external root CA, this signed file must be imported back into Cisco DNA Center using the GUI (as described in the following procedure).

After the import, Cisco DNA Center initializes itself as the subordinate CA and provides all the existing functionalities of a subordinate CA.


- The switchover from the internal root CA to the subordinate CA used by managed devices is not automatically supported. Therefore, it is assumed that no devices have been configured with the internal root CA yet. If devices are configured, it is the responsibility of the network administrator to manually revoke the existing device ID certificates before switching to the subordinate CA.
- The subordinate CA certificate lifetime, as displayed in the GUI, is just read from the certificate; it is not computed against the system time. Therefore, if you install a certificate with a lifespan of 1 year today and look at it in the GUI next July, the GUI will still show that the certificate has a 1-year lifetime.
- The subordinate CA certificate must be in PEM or DER format only.
- The subordinate CA does not interact with the higher CAs; therefore, it is not aware of revocation, if any, of the certificates at a higher level. Due to this, any information about certificate revocation is also not communicated from the subordinate CA to the network devices. Because the subordinate CA does not have this information, all the network devices use only the subordinate CA as the Cisco Discovery Protocol (CDP) source.

You can change the role of the private (internal) Cisco DNA Center CA from a root CA to a subordinate CA using the **PKI Certificate Management** window in the GUI.

### Before you begin

You must have a copy of the root CA certificate.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Cisco DNA Center home page, choose  > <b>System Settings</b> > <b>Settings</b> > <b>PKI Certificate Management</b> .                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 2</b> | Click the <b>CA Management</b> tab.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 3</b> | Review the existing root or subordinate CA certificate configuration information from the GUI: <ul style="list-style-type: none"> <li>• <b>Root CA Certificate:</b> Displays the current root CA certificate (either external or internal).</li> <li>• <b>Root CA Certificate Lifetime:</b> Displays the current lifetime value of the current root CA certificate, in days.</li> <li>• <b>Current CA Mode:</b> Displays the current CA mode (root CA or subordinate CA).</li> <li>• <b>Change to Sub CA mode:</b> Enables a change from a root CA to a subordinate CA.</li> </ul> |
| <b>Step 4</b> | In the <b>CA Management</b> tab, for <b>Change to Sub CA mode</b> , click <b>Yes</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 5</b> | Click <b>Next</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 6</b> | Review the <b>Root CA to Sub CA</b> warnings that appear: <ul style="list-style-type: none"> <li>• Changing from root CA to subordinate CA is a process that cannot be reversed.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |

- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Network devices that have been accidentally enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after the subordinate CA configuration process finishes.

**Step 7** Click **OK** to proceed.

The **PKI Certificate Management** window displays the **Import External Root CA Certificate** field.

**Step 8** Drag and drop your root CA certificate into the **Import External Root CA Certificate** field and click **Upload**. The root CA certificate is uploaded into Cisco DNA Center and used to generate a Certificate Signing Request. After the upload process finishes, a `Certificate Uploaded Successfully` message appears.

**Step 9** Click **Next**.

Cisco DNA Center generates and displays the Certificate Signing Request.

**Step 10** View the Cisco DNA Center-generated Certificate Signing Request in the GUI and perform one of the following actions:

- Click the **Download** link to download a local copy of the Certificate Signing Request file.  
You can then attach this Certificate Signing Request file to an email to send to your root CA.
- Click the **Copy to the Clipboard** link to copy the Certificate Signing Request file's content.  
You can then paste this Certificate Signing Request content to an email or include it as an attachment to an email and send it to your root CA.

**Step 11** Send the Certificate Signing Request file to your root CA.

Your root CA will then return a subordinate CA file, which you must import back into Cisco DNA Center.

**Step 12** After receiving the subordinate CA file from your root CA, access the Cisco DNA Center GUI again and return to the **PKI Certificate Management** window.

**Step 13** Click the **CA Management** tab.

**Step 14** Click **Yes** for the **Change CA mode** button.

After clicking **Yes**, the GUI view with the Certificate Signing Request is displayed.

**Step 15** Click **Next**.

The **PKI Certificate Management** window displays the **Import Sub CA Certificate** field.

**Step 16** Drag and drop your subordinate CA certificate into the **Import Sub CA Certificate** field and click **Apply**.

The subordinate CA certificate is uploaded into Cisco DNA Center.

After the upload finishes, the GUI displays the subordinate CA mode under the **CA Management** tab.

**Step 17** Review the fields under the **CA Management** tab:

- **Sub CA Certificate:** Displays the current subordinate CA certificate.
- **External Root CA Certificate:** Displays the root CA certificate.
- **Sub CA Certificate Lifetime:** Displays the lifetime value of the subordinate CA certificate, in days.

- **Current CA Mode:** Displays SubCA mode.


## Provision a Rollover Subordinate CA Certificate

Cisco DNA Center lets you apply a subordinate certificate as a rollover subordinate CA when 70 percent of the existing subordinate CA's lifetime has elapsed.

### Before you begin

- To initiate subordinate CA rollover provisioning, you must have changed the PKI certificate role to subordinate CA mode. See [Change the Role of the PKI Certificate from Root to Subordinate, on page 20](#).
- Seventy percent or more of the lifetime of the current subordinate CA certificate must have expired. When this occurs, Cisco DNA Center displays a **Renew** button under the **CA Management** tab.
- You must have a signed copy of the rollover subordinate CA PKI certificate.

### Procedure

- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Cisco DNA Center home page, choose  > <b>System Settings</b> > <b>Settings</b> > <b>PKI Certificate Management</b> .                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 2</b> | Click the <b>CA Management</b> tab.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 3</b> | Review the CA certificate configuration information: <ul style="list-style-type: none"> <li>• <b>Subordinate CA Certificate:</b> Displays the current subordinate CA certificate.</li> <li>• <b>External Root CA Certificate:</b> Displays the root CA certificate.</li> <li>• <b>Subordinate CA Certificate Lifetime:</b> Displays the lifetime value of the current subordinate CA certificate, in days.</li> <li>• <b>Current CA Mode:</b> Displays SubCA mode.</li> </ul>                                                                                                                                                     |
| <b>Step 4</b> | Click <b>Renew</b> .<br><br>Cisco DNA Center uses the existing subordinate CA to generate and display the rollover subordinate CA Certificate Signing Request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 5</b> | View the generated Certificate Signing Request in the GUI and perform one of the following actions: <ul style="list-style-type: none"> <li>• Click the <b>Download</b> link to download a local copy of the Certificate Signing Request file.<br/>You can then attach this Certificate Signing Request file to an email to send it to your root CA.</li> <li>• Click the <b>Copy to the Clipboard</b> link to copy the Certificate Signing Request file's content.<br/>You can then paste this Certificate Signing Request content to an email or include it as an attachment to an email and send it to your root CA.</li> </ul> |
| <b>Step 6</b> | Send the Certificate Signing Request file to your root CA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Your root CA will then return a rollover subordinate CA file that you must import back into Cisco DNA Center.

The Certificate Signing Request for the subordinate CA rollover must be signed by the same root CA who signed the subordinate CA you imported when you switched from RootCA mode to SubCA mode.

**Step 7** After receiving the rollover subordinate CA file from your root CA, return to the **PKI Certificate Management** window.

**Step 8** Click the **CA Management** tab.

**Step 9** Click **Next** in the GUI in which the Certificate Signing Request is displayed.

The **PKI Certificate Management** window displays the **Import Sub CA Certificate** field.

**Step 10** Drag and drop your subordinate rollover CA certificate into the **Import Sub CA Certificate** field and click **Apply**.

The rollover subordinate CA certificate is uploaded into Cisco DNA Center.

After the upload finishes, the GUI changes to disable the **Renew** button under the **CA Management** tab.

## Configure Device Certificate Lifetime


Cisco DNA Center lets you change the certificate lifetime of network devices that are managed and monitored by the private (internal) Cisco DNA Center CA. The Cisco DNA Center default value for the certificate lifetime is 365 days. After the certificate lifetime value is changed using the Cisco DNA Center GUI, network devices that subsequently request a certificate from Cisco DNA Center are assigned this lifetime value.



**Note** The device certificate lifetime value cannot exceed the CA certificate lifetime value. Additionally, if the remaining lifetime of the CA certificate is less than the configured device's certificate lifetime, the device gets a certificate lifetime value that is equal to the remaining CA certificate lifetime.

You can change the device certificate lifetime using the **PKI Certificate Management** window in the GUI.

### Procedure

**Step 1** From the Cisco DNA Center home page, choose  > **System Settings** > **Settings** > **PKI Certificate Management**.

**Step 2** Click the **Device Certificate** tab.

**Step 3** Review the device certificate and the current device certificate lifetime.

**Step 4** In the **Device Certificate Lifetime** field, enter a new value, in days.

**Step 5** Click **Apply**.

**Step 6** (Optional) Refresh the **PKI Certificate Management** window to confirm the new device certificate lifetime value.



## Cisco DNA Center Trustpool Support

Cisco DNA Center and Cisco IOS devices support a special PKI certificate store known as trustpool. The trustpool holds X.509 certificates that identify trusted CAs. Cisco DNA Center and the devices in the network use the trustpool bundle to manage trust relationships with each other and with these CAs. Cisco DNA Center manages this PKI certificate store, and an administrator (ROLE\_ADMIN) has the ability to update it through the Cisco DNA Center GUI when the certificates in the pool are due to expire, are reissued, or must be changed for other reasons.



**Note** Cisco DNA Center also uses the trustpool functionality to determine whether any certificate file that is uploaded through its GUI is a valid trustpool CA-signed certificate.

Cisco DNA Center contains a preinstalled, default Cisco-signed trustpool bundle named ios.p7b. This trustpool bundle is trusted by supported Cisco network devices natively, because it is signed with a Cisco digital signing certificate. This trustpool bundle is critical for the Cisco network devices to establish trust with services and applications that are genuine. This Cisco PKI trustpool bundle file is available at <https://www.cisco.com/security/pki/>.

To access the Cisco DNA Center PnP functionality, the supported Cisco devices that are being managed and monitored by Cisco DNA Center should import the Cisco PKI trustpool bundle file. When the supported Cisco devices boot for the first time, they contact Cisco DNA Center to import this file.

The Cisco DNA Center trustpool management feature operates in the following manner:

1. You boot the Cisco devices that support the PnP functionality within your network.  
Note that not all Cisco devices support PnP. See the [Cisco Digital Network Architecture Compatibility Matrix](#) for a list of supported Cisco devices.
2. As part of the initial PnP flow, the supported Cisco devices download a trustpool bundle directly from Cisco DNA Center using HTTP.
3. The Cisco devices are now ready to interact with Cisco DNA Center to obtain further device configuration and provisioning according to the PnP traffic flows.

Note that if an HTTP proxy gateway exists between Cisco DNA Center and these Cisco devices, you must import the proxy gateway certificate into Cisco DNA Center.



**Note** At times, you might need to update the trustpool bundle to a newer version due to some certificates in the trustpool expiring, being reissued, or for other reasons. Whenever the trustpool bundle needs to be updated, update it by using the Cisco DNA Center GUI. Cisco DNA Center can access the Cisco cloud (where the Cisco-approved trustpool bundles are located) and download the latest trustpool bundle. After download, Cisco DNA Center then overwrites the current, older trustpool bundle file. As a best practice, update the trustpool bundle before importing a new certificate from a CA.

## Check the Certificate on the PnP Server

This section explains how to check the certificate on the PnP agent of Cisco IOS and Cisco IOS XE devices during a zero-touch deployment.

The certificate provided by the PnP server must contain a valid Subject Alternative Name (SAN) field to verify the server identity.

The check is applied to the server's DNS name or the IP address that is used in the PnP profile settings:

```
pnp profile SOME_NAME
transport https ipv4 IP_ADDRESS port 443
```

```
pnp profile SOME_NAME
transport https host DNS_NAME port 443
```

The enforcement is applied by comparing the SAN field of the certificate to the value used in the PnP profile that is configured on the device.

The following table summarizes the enforcement applied:

| PnP Profile Configuration                                                                      | Certificate Enforcement                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Option-43 or Option-17 discovery of the PnP server using an explicit IPv4 or IPv6 address | The SAN field of the server certificate must contain the explicit IPv4 or IPv6 address used in Option-43 or Option-17.                                                                                                                                                                                                                                                                                         |
| DHCP Option-43 or Option-17 discovery of the PnP server using a DNS name                       | The SAN field of the server certificate must contain the specific DNS name.                                                                                                                                                                                                                                                                                                                                    |
| DNS discovery of the PnP server                                                                | The SAN field of the server certificate must contain pnpserver.<local-domain>.                                                                                                                                                                                                                                                                                                                                 |
| CCO discovery of the PnP Server                                                                | One of the following conditions applies: <ul style="list-style-type: none"> <li>• The SAN field of the server certificate must contain the explicit IP address if an IP address is used in the cloud redirection profile configuration.</li> <li>• The SAN field of the server certificate must contain the specific DNS name if a DNS name is used in the cloud redirection profile configuration.</li> </ul> |
| Day-2 (manual configuration) PnP profile creation                                              | The SAN field of the server certificate must contain either the IP address or the DNS name that is used in the PnP profile configuration.                                                                                                                                                                                                                                                                      |

We recommend that you use a discovery method based on the DNS name because the functionality is not affected by changes to the IP address.

## Procedure

- Step 1** Use the PnP server logs to diagnose the problem. Check whether the HTTPS connection is established with the device after the trustpoint is installed on the device.

The PnP server logs show that the device moves from the CERTIFICATE\_INSTALL\_REQUESTED stage to the FILESYSTEM\_INFO\_REQUESTED stage, but no further progress is made. For example:

```
2018-11-28 12:05:40,711 | INFO | qtp226594800-88458 | |
com.cisco.enc.pnp.state.ZtdState |
Device state has changed from CERTIFICATE_INSTALL_REQUESTED to FILESYSTEM_INFO_REQUESTED |
sn=SOME_SN, address=SOME_IP
```

Thereafter, PnP provisioning fails with an error that is similar to the following:

```
2018-11-28 12:25:56,289 | ERROR | eHealthCheckFirstBucket-2 | |
c.c.e.z.impl.ZtdHistoryServiceImpl |
```

Failed health check since device is stuck in non-terminal state FILESYSTEM\_INFO\_REQUESTED for more than threshold time:  
0 hours, 16 minutes, 0 seconds | sn=SOME\_SN

**Step 2** For device-side debugging, use the following recommended outputs to determine whether the issue is related to the server ID check:

```
debug crypto pki val
debug crypto pki api
debug crypto pki call
debug crypto pki tr
debug ssl openssl error
debug ssl openssl msg
debug ssl openssl state
debug ssl openssl ext

show crypto pki certificate
show running
show pnp tech
```

**Step 3** Enable debugging before you initiate a PnP discovery.

**Step 4** Check the server certificate's SAN field by entering the following command from the CLI of a Linux workstation or a Mac terminal. Be sure to replace *SERVER\_IP* with your Cisco DNA Center cluster address.

```
echo | openssl s_client -showcerts -servername SERVER_IP -connect
SERVER_IP:443 2>/dev/null | openssl x509 -inform pem -noout -text
```

**Step 5** In the output, pay close attention to the X509v3 extensions, especially the **X509v3 Subject Alternative Name**, which is the field that must be matched against the PnP server details.

The output is similar to the following:

```
[username@toolkit ~]$ echo | openssl s_client -showcerts -servername SERVER_IP -connect
SERVER_IP:443 2>/dev/null | openssl x509 -inform pem -noout -text
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 18:92:63:49:41:36:99:43:00:57:43:86:06:10:44:57:32:48:65:00
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: CN=e328c7fc-3495-4bc1-81a4-66a31d0507f6, C=US, ST=California, L=SanJose,
 OU=DNAC, O=Cisco
 Validity
 Not Before: Aug 24 05:55:29 2017 GMT
 Not After : Aug 23 05:55:29 2022 GMT
 Subject: CN=SERVER_IP, ST=California, C=US, O=Cisco, OU=DNAC
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:a2:21:ba:52:b4:9e:50:02:c0:68:2e:b3:43:0a:
 <snip>
 9e:1b:ef:19:96:f9:2b:e3:6a:58:05:b3:c5:b3:d3:
 24:ab
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 X509v3 Key Usage:
 Digital Signature, Key Encipherment
 X509v3 Extended Key Usage:
 TLS Web Server Authentication, TLS Web Client Authentication
 X509v3 Subject Alternative Name:
 IP Address:SERVER_IP
```

**Step 6**

Depending on the type of certificate you are using, do one of the following:

- If you are using a signed certificate, generate a new Certificate Signing Request that is signed by the CA, including the appropriate SAN field. See [Configure a Certificate, on page 18](#).
- If you are using a self-signed certificate, see [Generate a Certificate Request Using Open SSL, on page 11](#).

## Upgrade Legacy Devices

If you have legacy network devices, you must upgrade them to the latest device software:

- To view the software versions that Cisco SD-Access supports, see the [Cisco SD-Access Product Compatibility page](#).
- To view general device support information for Cisco DNA Center, see the [Cisco DNA Center Supported Devices spreadsheet](#).

Some devices, such as Cisco Aironet 1800 Series Access Points Version 8.5, use TLSV1, which is not secure. You must upgrade the device software version to 8.8 to upgrade the TLS version.

## Secure Network Data

Cisco DNA Center lets you use the Data Anonymization feature to hide the identity of wired and wireless end clients in the Cisco DNA Assurance dashboard. For details, see "View or Update Collector Configuration Information" in the [Cisco DNA Assurance User Guide](#).

## Syslog Management


Cisco DNA Center protects syslogs for user-sensitive data such as username, password, IP address, and so on.

## View Audit Logs

Audit logs capture information about the various applications running on Cisco DNA Center. Audit logs also capture information about device public key infrastructure (PKI) notifications. The information in these audit logs can be used to assist in troubleshooting issues, if any, involving the applications or the device PKI certificates.

### Procedure

**Step 1**

From the Cisco DNA Center home page, choose  > **Audit Logs**.

The **Audit Logs** window appears, where you can view logs about the current policies in your network. These policies are applied to network devices by the applications installed on Cisco DNA Center.

The following information is displayed for each policy:

- **Description:** Application or policy audit log description
- **Site:** Name of the site for the specific audit log

- **Device:** Devices for the audit log
- **Requestor:** User requesting an audit log
- **Source:** Source of an audit log
- **Created On:** Date on which the application or policy audit log was created

**Step 2** Click the plus icon (+) next to an audit log to view the corresponding child audit logs.

Each audit log can be a parent to several child audit logs. By clicking this plus icon, you can view a series of additional child audit logs.

**Note** An audit log captures data about a task performed by Cisco DNA Center. Child audit logs are subtasks to a task performed by Cisco DNA Center.

**Step 3** Filter the audit logs by clicking the **Filter** icon, entering a specific parameter, and then clicking **Apply**. You can filter audit logs by using the following parameters:

- **Description**
- **Site**
- **Device**
- **Requestor**
- **Source**
- **Start Date**
- **End Date**

**Step 4** (Optional) Click the dual arrow icon to refresh the data displayed.

**Step 5** (Optional) Click the download icon to download a local copy of the audit log in .csv file format.

A .csv file containing audit log data is downloaded locally to your system. You can use the .csv file for additional review of the audit log or archive it as a record of activity on Cisco DNA Center.

---

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: [www.cisco.com/go/trademarks](http://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)

© 2018–2020 Cisco Systems, Inc. All rights reserved.