Configure System Settings

• About System Settings, on page 1
• System 360, on page 1
• About DNA Center and Cisco ISE Integration, on page 2
• Configure Authentication and Policy Servers, on page 2
• Device Controllability, on page 5
• Configure an IP Address Manager, on page 6
• Configure Debugging Logs, on page 7
• Configure the Network Resync Interval, on page 8
• View Audit Logs, on page 9
• Configure Security for Cisco DNA Center, on page 10
• Configure SFTP Server, on page 22
• Configure SNMP Properties, on page 22
• About Telemetry Collection, on page 23

About System Settings

To start using DNA Center, you must first configure the system settings so that the server can communicate outside the network, ensure secure communications, authenticate users, and perform other key tasks. Use the procedures described in this chapter to properly configure the system settings.

System 360

The System 360 view provides at-a-glance information about DNA Center. Data is accessible under the following categories:

• **Hosts**—Displays information about the DNA Center host or hosts. Information displayed includes the IP address or addresses of the hosts, as well as detailed data about services running on the hosts (name, status, version, modification date and time, and logs).

---

**Important** Three hosts are required for high availability for DNA Center.
• IP Address Manager—Displays IP address manager configuration data. Click the Configure settings link to configure the IP address manager.

• Cisco ISE—Displays Cisco ISE configuration data. Click the Configure settings link to configure DNA Center for integration with Cisco ISE.

About DNA Center and Cisco ISE Integration

Cisco ISE has two different use cases in DNA Center. Cisco ISE can be used as a AAA server for user, device, and client authentication or it can be used with an access control policy to enforce access control. If you are not using access control policies or if you are not using Cisco ISE as a AAA server for device authentication, you do not need to install and configure Cisco ISE.

For more information about using Cisco ISE for device authentication, see the Cisco Digital Network Architecture Center User Guide.

Before you can create and use access control policies, you need to configure DNA Center and Cisco ISE to integrate with one another. The process involves installing and configuring Cisco ISE with specific services and configuring Cisco ISE settings in DNA Center. For more information about installing and configuring Cisco ISE with DNA Center, see the Cisco DNA Center Appliance Installation Guide.

After Cisco ISE has successfully registered and its trust established with DNA Center, DNA Center shares information with Cisco ISE. DNA Center device inventory is propagated to Cisco ISE, and whenever you update device credentials in DNA Center, DNA Center updates Cisco ISE with the changes. Similarly, if you change the Radius shared secret for Cisco ISE, Cisco ISE updates DNA Center with the changes. However, Cisco ISE does not share existing device information with DNA Center. The only way for DNA Center to know about the devices in Cisco ISE is if the devices have the same name in DNA Center; DNA Center and Cisco ISE uniquely identify devices for this integration through the device's hostname variable.

DNA Center integrates with the primary Administration ISE node. When you access Cisco ISE from DNA Center, you connect with this node.

DNA Center polls Cisco ISE every 15 minutes. If the ISE server is down, the System 360 page (System Settings > System 360) shows the Cisco ISE server as red, which means the Cisco ISE server is unreachable.

When the Cisco ISE server is unreachable, DNA Center increases polling to 15 seconds, then doubles the polling time to 30 seconds, 1 minute, 2 minutes, 4 minutes, and so on, until it reaches the maximum polling time of 15 minutes. DNA Center continues to poll every 15 minutes for 3 days. If DNA Center has not regained connectivity, it stops polling, and updates the Cisco ISE server status to Untrusted. If this happens, you will need to reestablish trust between DNA Center and the Cisco ISE server.

Configure Authentication and Policy Servers

Configure Access to an AAA Server

You can configure access to a primary and a secondary authentication, authorization, and accounting (AAA) server.
Before you begin

You must be a super administrator or network administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

You must have the AAA server already preconfigured, set up, and running. You must also configure the AAA server to interact with the DNA Center. When configuring the AAA server to interact with the DNA Center, perform the following additional steps:

- Register the DNA Center with the AAA server.

  This could also involve configuring a shared-secret on both the AAA server and the DNA Center.

- Configure an attribute name with a value on the AAA server

- For a DNA Center multi-host configuration, configure all individual host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server.

Procedure

Step 1 From the DNA Center Home page, click the gear icon (⚙️) and choose > System Settings > Settings > Authentication and Policy Servers.

Step 2 Click add.

Step 3 Configure the primary AAA server by providing the following information:

  - **Server IP Address**—IP address of the AAA server.
  
  - **Shared Secret**—Key for device authentications. The shared secret can be up to 128 characters in length.
  
  - **Cisco ISE server**—Toggle that configures either an AAA server or a Cisco ISE server. Leave the toggle set as is. Do not choose Cisco ISE as configuring Cisco ISE is covered in a different procedure. To configure a Cisco ISE server, see Configure Access to a Cisco ISE Server, on page 4

Step 4 Click View Advanced Settings and configure the settings:

  - **Protocol**—TACACS or RADIUS
  
  - **Authentication Port**—Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
  
  - **Accounting Port**—Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.
  
  - **Retries**—Number of times that DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 1.
  
  - **Timeout**—The length of time that device waits for the AAA server to respond before abandoning the attempt to connect.

Step 5 Click Add.
Step 6: To add a secondary AAA server, click + AAA Server and repeat Step 3 through Step 5.

---

Configure Access to a Cisco ISE Server

To use access control policies, you need to configure access to a Cisco ISE server.

Before you begin

You must be a super administrator or network administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

You must have the Cisco ISE server already preconfigured, set up, and running. You must also configure the Cisco ISE server to interact with the DNA Center. When configuring the Cisco ISE server to interact with the DNA Center, refer to your Cisco ISE documentation and procedures. Ensure that you have configured the appropriate Cisco ISE software version, prior to beginning this procedure.

Procedure

Step 1: From the DNA Center home page, click the gear icon (⚙️) and choose > System Settings > Settings > Authentication and Policy Servers.

Step 2: Click + AAA Server.

Step 3: Configure the Cisco ISE settings by providing the following information:

- **IP Address**—IP address of the Cisco ISE server.
- **Shared Secret**—Key for device authentications. The shared secret can be up to 128 characters in length.
- **Cisco ISE**—Setting that indicates whether the server is a Cisco ISE server. Click the Cisco ISE setting to enable Cisco ISE.
- **Username**—Name that is used to log in to Cisco ISE.
- **Password**—Password that is used to log in to Cisco ISE.
- **FQDN**—Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts: the hostname and the domain name in the following format: hostname.domainname.com.
  
  For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
- **Subscriber Name**—A unique text string, for example dnac, that is used during DNA Center to Cisco ISE integration to setup a new pxGrid client in Cisco ISE.
- **SSH Key**—Diffie-Hellman-Group14-SHA1 SSH key used to connect and authenticate with Cisco ISE.

Step 4: Click View Advanced Settings and configure these settings:

- **Protocol**—TACACS or RADIUS
- **Authentication Port**—Port used to relay authentication messages to the AAA server. The default is UDP port 1812.
- **Accounting Port**—Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. The default UDP port is 1813.

- **Retries**—Number of times the device attempts to connect with Cisco ISE before abandoning the attempt to connect.

- **Timeout**—The length of time that DNA Center waits for Cisco ISE to respond before abandoning the attempt to connect.

**Step 5**
Click Add.

---

**What to do next**
Click the **System 360** tab and check to ensure that your Cisco ISE configuration was successful.

---

**Device Controllability**

When Device Controllability is enabled and under certain circumstances, DNA Center configures devices with the network settings for the site to which the device belongs.

When device controllability is disabled, DNA Center does not configure any settings on the devices.

**Note**
Device controllability is enabled by default. If you do not want device controllability enabled, you have to manually disable it. For more information, see Configure Device Controllability, on page 6.

Device controllability configures SNMP (SNMPv2c and SNMPv3) credentials and Syslog on devices under the following circumstances:

- **Device in Global Site**—When you successfully add, import, or discover a device, DNA Center places the device in the **Managed** state and assigns it to the Global site by default. Even if you have defined Syslog and SNMP server settings for the Global site, DNA Center does not change the Syslog and SNMP server settings on the device.

- **Device Moved to Site**—If you move the device from the Global site to a new site, for example Site A, that has Syslog and SNMP server settings configured, DNA Center changes the Syslog and SNMP server settings on the device to the settings configured for Site A.

- **Device Removed from Site**—If you remove a device from a site, for example Site A, DNA Center does not remove the Syslog and SNMP server settings from the device.

- **Device Moved from Site to Site**—If you move a device, for example from Site A to Site B, DNA Center replaces the Syslog and SNMP server settings on the device with the settings assigned to Site B.

After discovering devices and when device controllability is enabled, DNA Center configures the following features and protocols on the devices:

- **SNMP Trap server**—If you have Device Controllability enabled, DNA Center configures these SNMP traps for you. Otherwise, you need to enable SNMP traps and configure DNA Center's server IP address as the SNMP server. For information, see SNMP Trap Configuration.
• IP Device Tracking—DNA Center automatically enables IP device tracking (IPDT) or Switch Integrated Security Features (SISF) on any network device where IPDT is supported and not enabled. DNA Center configures IPDT or SISF IPDT on the device based on the device type and image version that is running.

• NetFlow controller

Configure Device Controllability

Device controllability automatically configures discovered devices with SNMP credentials, SNMP Trap servers, IP Device Tracking, NetFlow, Syslog, and NETCONF. Device controllability is enabled by default. If you want, you can disable device controllability and reenable it at any time. For more information, see Device Controllability, on page 5.

Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

Procedure

Step 1
From the DNA Center Home page, click the gear icon (⚙️) and choose > System Settings > Settings > Device Controllability.

Step 2
Click Enable Device Control.

Configure an IP Address Manager

You can configure DNA Center to communicate with an External IP Address Manager.

Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

You should have an external IP Address Manager already set up and functional.

Note

Although both BlueCat and Infoblox can be configured to work with the DNA Center IP address manager, the BlueCat integration is currently a beta feature for this release.

Procedure

Step 1
Click the gear icon (⚙️) and select System Settings.

Step 2
Click the Settings tab, and then click IP Address Manager.

Step 3
In the IP Address Manager section, enter the required information in the following fields:
### Configure System Settings

#### Configure Debugging Logs

To assist in troubleshooting service issues, you can change the logging level for the DNA Center services by using the **Debugging Logs** window in the GUI.

A logging level determines the amount of data that is captured in the log files. Each logging level is cumulative, that is, each level contains all the data generated by the specified level and any higher levels. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs. You may want to adjust the logging level to assist in troubleshooting any issues by capturing more data. For example, by adjusting the logging level you can capture more data to review in a root cause analysis or RCA support file.

The default logging level for services is informational (**Info**). You can change the logging level from informational (**Info**) to a different logging level (**Debug** or **Trace**) to capture more information.

**Caution**

Due to the type of information that may be disclosed, logs collected at the **Debug** level or higher should have restricted access.

**Note**

The log files are created and stored in a centralized location on your DNA Center. From this location, the DNA Center can query and display them in the GUI. The total compressed size of the log files is 2 GB. If log files created are in excess of 2 GB, then the pre-existing log files are overwritten with the newer log files.

---

<table>
<thead>
<tr>
<th><strong>Server Name</strong></th>
<th>Name of server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server URL</strong></td>
<td>IP address of server.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Required username for server access.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Required password for server access.</td>
</tr>
</tbody>
</table>

**Provider**

Select a provider from the drop-down menu.

**Note**

When selecting BlueCat as your provider, ensure that your user has been granted API access in the BlueCat Address Manager. Refer to your BlueCat documentation for information about configuring API access for your user or users.

---

**Step 4**

Click **Apply** to apply and save your settings.

---

**What to do next**

Click the **System 360** tab and check to ensure that your External IP Address Manager configuration was successful.
Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

Procedure

**Step 1**
Click the gear icon (⚙️), and select System Settings.

**Step 2**
Click the Settings tab, and then click Debugging Logs.

The Debugging Logs window containing the following fields appear:

- Services
- Logging Level
- Timeout

**Step 3**
In the Debugging Logs window, choose a service from the Services field to adjust its logging level.

*Note* The Services field displays the services that are currently configured and running on the DNA Center.

**Step 4**
In the Debugging Logs window, choose the new logging level for the service from the Logging Level field.

The following logging levels are supported on the DNA Center:

- Trace—Trace messages
- Debug—Debugging messages
- Info—Normal, but significant condition messages
- Warn—Warning condition messages
- Error—Error condition messages

**Step 5**
In the Debugging Logs window, choose the time period for the logging level from the Timeout field for the logging level adjustment.

You configure logging level time periods in increments of 15 minutes up to an unlimited time period.

**Step 6**
Review your selection and click Apply.

To cancel your selection, click Cancel.

The logging level for the specified service is set.

---

**Configure the Network Resync Interval**

You can update the polling interval at the global level for all devices by choosing Settings > Network Resync Interval or at the device level for a specific device by choosing Device Inventory. When you set the polling
interval using the **Network Resync Interval**, that value takes precedence over the **Device Inventory** polling interval value.

If you do not want a device to be polled, you can disable polling.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

Make sure that you have devices in your inventory. If not, discover devices using the Discovery function.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click ☰, then select <strong>System Settings</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>Settings</strong> tab, then click <strong>Network Resync Interval</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Polling Interval</strong> field, enter a new time value (in minutes).</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Yes</strong> for <strong>Override for all devices</strong> to override the existing configured polling interval for all devices.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong> to apply and save your new settings.</td>
</tr>
</tbody>
</table>

**View Audit Logs**

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

You can view audit logs using the **Audit Logs** window in the GUI. The DNA Center also supports the ability to download the audit logs to a local system.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click ☰, then select <strong>Audit Logs</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Audit Logs</strong> window appears. In the <strong>Audit Logs</strong> window, you can view logs about the current policies in your network. These policies were applied to network devices by the applications installed on the DNA Center.</td>
</tr>
<tr>
<td></td>
<td>The following information is displayed for each policy in the window:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong>—Application or policy audit log description</td>
</tr>
<tr>
<td></td>
<td>• <strong>Site</strong>—Name of the site for the specific audit log</td>
</tr>
</tbody>
</table>
• **Device**—Device or devices for the audit log
• **Requestor**—User requesting the audit log
• **Source**—Source of the audit log
• **Created On**—Date application or policy audit log was created.

**Step 2**  Click the addition icon (+) next to an audit log to view the children audit logs in the Audit Logs window.

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

**Note**  An audit log captures data about a task performed by the DNA Center. Children audit logs are sub-tasks to that one task performed by the DNA Center.

**Step 3**  Filter the audit logs by clicking the Filter icon in the Audit Logs window, entering a specific parameter, and then clicking the Apply button.

You can filter for a specific audit log by the following parameters:
• **Description**
• **Site**
• **Device**
• **Requestor**
• **Source**
• **Start Date**
• **End Date**

**Step 4**  Click the dual arrow icon to refresh the data displayed in the window.

The data displayed in the window is refreshed with the latest audit log data.

**Step 5**  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 the DNA Center.

---

**What to do next**

Proceed to review any additional log files using the DNA Center's GUI, or download individual audit logs as .csv files for further review or archiving purposes.

---

**Configure Security for Cisco DNA Center**

The DNA Center provides many security features for itself, as well as the hosts and network devices that it monitors and manages. We strongly suggest that the following security recommendations be followed:
Deploy DNA Center behind a firewall that does not expose the management ports to an untrusted network, such as the Internet.

Enable TLS and RC4-SHA for the DNA Center HTTPS servers. Both TLS and RC4-SHA are disabled by default. You enable these security features using the CLI. For additional information about this procedure, see Enable TLS and RC4-SHA, on page 11.

Configure a proxy gateway between DNA Center and the network devices it monitors and manages. For additional information about this procedure, see Configure Proxy Certificate, on page 12.

Replace the self-signed server certificate from DNA Center with one signed by a well-known Certificate Authority. For additional information about this procedure, see Certificate and Private Key Support, on page 13.

When using the DNA Center discovery functionality, use SNMPv3 with authentication and privacy enabled for the network devices. For additional information about this procedure, refer to the SNMP configuration procedures in the Cisco Digital Network Architecture Center User Guide.

Enable TLS and RC4-SHA

Northbound REST API requests from the external network to the DNA Center (from northbound REST API based apps, browsers, and network devices connecting to the DNA Center using HTTPS) are made secure using the Transport Layer Security protocol (TLS). RH4-SHA is a stream cipher that is also used to secure the DNA Center.

You enable TLS and RC4-SHA for the DNA Center by logging into the appliance and using the CLI.

Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

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

Important

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

Procedure

Step 1

Using a Secure Shell (SSH) client, log into the DNA Center appliance with the IP address that you specified using the configuration wizard.

Note: 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 enable TLS on the cluster.
$ magctl service tls_version --tls-v1=enable kong

Enabling TLSv1 is recommended only for legacy devices
Do you want to continue? [y/N]: y
deployment “kong” patched

**Step 4**
Enter the following command to enable RC4 on the cluster.

$ magctl service ciphers --ciphers-rc4=enable kong

Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
deployment “kong” patched

**Step 5**
Enter the following command at the prompt to confirm that TLS and RC4-SHA are configured.

$ magctl service display kong

containers:
  - env:
    - name: TLS_V1
      value: enabled
    - name: RC4_CIPHERS
      value: enable

If RC4 and TLS_V1 are set respectively, then they will appear listed in the env: of the magctl service display kong command. If these values are not set, then they will not appear in the env.

**Step 6**
Log out of the DNA Center appliance.

---

**Configure Proxy Certificate**

In some network configurations, proxy gateways may exist between DNA Center and the remote network it manages (containing various network devices). Common ports, such as 80 and 443, pass through the gateway proxy in the DMZ, and for this reason SSL sessions from the network devices meant for the DNA Center terminate at the proxy gateway. Therefore, the network devices located within these remote networks can only communicate with the DNA Center via the proxy gateway. In order for the network devices to establish secure and trusted connections with the DNA Center, or if present, a proxy gateway, then the network devices should have their PKI trust stores appropriately provisioned with the relevant CA root certificates or the server’s own certificate under certain circumstances.

In network topologies where there is a proxy gateway present between DNA Center and the remote network it manages, perform the procedure described below to import a proxy gateway certificate into DNA Center.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

Additionally, in your network, an HTTP proxy gateway exists between DNA Center and the remote network it manages (containing various network devices). These network devices use the proxy gateway's IP address to reach DNA Center and its services.
You have the certificate file currently being used by the proxy gateway. The certificate file contents can consist any of the following:

- The proxy gateway’s certificate in PEM or DER format, with the certificate being self-signed.
- The proxy gateway’s certificate in PEM or DER format, with the certificate being issued by a valid, well-known CA.
- The proxy gateway's certificate and its chain in PEM or DER format.

The certificate used by the devices and proxy gateway must be imported into the DNA Center by following this procedure.

**Procedure**

1. Click the gear icon (⚙️) and select **System Settings**.
2. Click the **Settings** tab, and then click **Proxy Certificate**.
3. In the **Proxy Certificate** window, view the current proxy gateway certificate data (if it exists).
   - **Note**: The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the DNA Center's GUI 2 months before the expiration date and time of the certificate.
4. To add a proxy gateway certificate, drag and drop the self-signed or CA certificate into the **Drag n' Drop a File Here** field.
   - **Note**: Only PEM or DER files (public-key cryptography standard file formats) can be imported into the DNA Center using this field. Additionally, private keys are neither required nor uploaded into the DNA Center for this procedure.
5. Click **Save**.
6. Refresh the **Proxy Certificate** window to view the updated proxy gateway certificate data. The information displayed in the **Proxy Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

**Certificate and Private Key Support**

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

The DNA Center can import the following files (in either PEM or PKCS file format) using the DNA Center's GUI:

- X.509 certificate
- Private key
For the private key, DNA Center supports the import of RSA keys. You should not import DSA, DH, ECDH, and ECDSA key types; since they are not supported. You should also keep the private key secure in your own key management system.

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

We recommend against using and importing a self-signed certificate into the DNA Center. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended. Additionally, you must replace the self-signed certificate (installed in the DNA Center by default) with a certificate that is signed by a well-known certificate authority for the Network PnP functionality to work properly.

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

If the external IP address changes for your DNA Center for any reason, then you need to re-import a new certificate with the changed or new IP address.

**Configure Certificate**

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

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

The DNA Center itself does NOT interact with any external CA directly; therefore, it does not check any Certificate Revocation Lists and it has no way to learn of revocation of its server certificate by an external CA. Note, also, that the DNA Center does not automatically update its server certificate. Replacement of an expired or revoked server certificate requires explicit action on the part of a SUPER-ADMIN-ROLE user. Although the DNA Center has no direct means of discovering the revocation of its server certificate by an external CA, it does notify the admin of expiration of its server certificate as well as self-signed key being operational.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

You must have acquired an X.509 certificate and private key from a well-known certificate authority (CA) for the import.
Procedure

Step 1  Click ☐, then select System Settings.

Step 2  Click the Settings tab, then click Certificate.

Step 3  In the Certificate window, view the current certificate data.

When first viewing this window, the current certificate data that is displayed is the DNA Center's self-signed certificate. The self-signed certificate's expiration 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 will appear in the DNA Center's GUI 2 months before the expiration date and time of the certificate.

Additional displayed fields in the Certificate window include:

- Current Certificate Name—The name of the current certificate.
- Issuer—The issuer name identifies the entity that has signed and issued the certificate.
- Certificate Authority—Either self-signed or name of the CA.
- Expires On—Expiration date of the certificate.

Step 4  To replace the current certificate, click the Replace Certificate button.

The following new fields appear:

- Certificate—Fields to enter certificate data
- Private Key—Fields to enter private key data

Step 5  In the Certificate fields, choose the file format type of the certificate:

- PEM—Privacy enhanced mail file format
- PKCS—Public-key cryptography standard file format

Choose one of the above file types for the certificate that you are importing into the DNA Center.

Step 6  If you choose PEM, then perform the following tasks:

- For the Certificate field, import the PEM file by dragging and dropping this file into the Drag n' Drop a File Here field.
  
  Note  For a PEM file, it must have a valid PEM format extension (.pem, .cert, .crt). The maximum file size for the certificate is 10KB

- For the Private Key field, import the private key by dragging and dropping this file into the Drag n' Drop a File Here field.
  
  - Choose the encryption option from the Encrypted drop-down menu for the private key.
  - If encryption is chosen, enter the passphrase for the private key in the Passphrase field.
    
    Note  For the private keys, they must have a valid private key format extension (.pem or .key).
Step 7  If you choose PKCS, then perform the following tasks:

- For the Certificate field, import the PKCS file by dragging and dropping this file into the Drag n' Drop a File Here field.
  
  Note  For a PKCS file, it must have a valid PKCS format extension (.pfx, .p12). The maximum file size for the certificate is 10KB

- For the Certificate field, enter the passphrase for the certificate using 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 using the drop-down menu.
- For the Private Key field, if encryption is chosen, enter the passphrase for the private key in the Passphrase field.

Step 8  Click the Upload/Activate button.

Step 9  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 certificate authority.

---

Certificate Management

Configure Device Certificate Lifetime

The DNA Center enables the user to change the certificate lifetime of network devices managed and monitored by the private (internal) DNA Center's CA. The DNA Center's default value for the certificate lifetime is 365 days. After the certificate lifetime value is changed using the DNA Center's GUI, then any network devices subsequently requesting a certificate from the DNA Center are assigned this lifetime value.

Note  The device certificate lifetime value cannot exceed the CA certificate lifetime value. Additionally, if the remaining time of CA certificate lifetime is less than configured device's certificate lifetime, then the device will get a certificate lifetime value equal to the remaining CA certificate lifetime.

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

Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

Procedure

Step 1  Click ☀, then select System Settings.

Step 2  Click the Settings tab, then click PKI Certificate Management.
Step 3  Click the **Device Certificate** tab.
Step 4  Review the device certificate and current device certificate lifetime.
Step 5  In the **Device Certificate Lifetime** field, enter a new value in days.
Step 6  Click the **Apply** button.

**What to do next**

Refresh the **PKI Certificate Management** window to confirm the new device certificate lifetime value.

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

DNA Center permits the user to change the role of the Device PKI CA from a root CA to a subordinate CA. When changing the private DNA Center’s CA from a root CA to a subordinate CA note the following:

- If you intend to have the DNA Center act as a subordinate CA, then it is assumed that you already have a root CA (for example, Microsoft CA) and you are willing to accept the DNA Center as a subordinate CA.

- As long as the subordinate CA is not fully configured, then the DNA Center will continue to operate as an internal root CA.

- You will need to generate a Certificate Signing Request (CSR) file for the DNA Center (as described in this procedure) and manually have it signed by your external root CA.

![Note]

The DNA Center will continue to run as an internal root CA during this time.

- Once the CSR is signed by the external root CA, then this signed file must be imported back into the DNA Center using the GUI (as described below in this procedure).

After the import, the DNA Center will initialize itself as the subordinate CA and provide all the existing functionality of a subordinate CA.

- The switch over from internal root CA to subordinate CA is not automatically supported; therefore, it is assumed that no devices have yet been configured with the internal root CA. In case any devices are configured, then 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 itself; it is not computed against the system time. So if you install a certificate with a lifespan of one year today and then look at it in the GUI next July, then the GUI will still show that the certificate has a one year lifetime.

- The subordinate CA certificate must be in PEM or DER format only.

- The subordinate CA does not interact with the higher CAs, so it will not be aware of any revocation of the certificates at a higher level. Due to this fact, any information about certificate revocation will also not be communicated from the subordinate CA to the network devices. Since the subordinate CA does not have this information, all the network devices will only use the subordinate CA as the CDP source.
You change the role of the private (internal) DNA Center's CA from a root CA to a subordinate CA using the PKI Certificate Management window in the GUI.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

You must have a copy of the root CA certificate to which you will subordinate the private (internal) DNA Center's PKI certificate.

**Procedure**

**Step 1** Click ☀️, then select System Settings.

**Step 2** Click the Settings tab, then click PKI Certificate Management.

**Step 3** Click the CA Management tab.

**Step 4** Review the existing root or subordinate CA certificate configuration information from the GUI.

<table>
<thead>
<tr>
<th><strong>Root CA Certificate</strong></th>
<th>Displays current root CA certificate (either external or internal root CA certificate).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Root CA Certificate Lifetime</strong></td>
<td>Displays the current lifetime value of the current root CA certificate in days.</td>
</tr>
<tr>
<td><strong>Current CA Mode</strong></td>
<td>Displays the current CA mode: root CA or subordinate CA.</td>
</tr>
<tr>
<td><strong>Change to Sub CA mode</strong></td>
<td>Button used to change from a root CA to subordinate CA.</td>
</tr>
</tbody>
</table>

**Step 5** In the CA Management tab, for Change to Sub CA mode click Yes.

**Step 6** In the CA Management tab, click Next.

**Step 7** Review the Root CA to Sub CA warnings that appears:

- Changing from root CA to subordinate CA is a process that cannot be reversed.
- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Any network devices accidentally enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after this subordinate CA configuration process is finished.

**Step 8** Click OK to proceed.

The PKI Certificate Management window changes and displays an Import External Root CA Certificate field.

**Step 9** Drag and drop your root CA certificate into the Import External Root CA Certificate field and click Upload. The root CA certificate will then be uploaded into the DNA Center and used to generate a Certificate Signing Request (CSR).

When the upload process is finished a Certificate Uploaded Successfully message appears.
Step 10  After the upload process is finished and the success message appears, click Next to proceed.
The DNA Center will then generate and display the CSR.

Step 11  View the DNA Center generated Certificate Signing Request (CSR) in the GUI and perform one of the following actions:
  • Click the Download link to download a local copy of the CSR file.
    You can then attach this CSR file to an email to send to your root CA.
  • Click the Copy to the Clipboard link to copy the CSR file's content.
    You can then paste this CSR content to an email or attachment to an email and send to your root CA.

Step 12  Send the CSR file to your root CA.
         You must send the CSR file to your root CA. Your root CA will then return to you a subordinate CA file that you must import back into the DNA Center.

Step 13  After receiving the subordinate CA file from your root CA, access the DNA Center's GUI again and return to the PKI Certificate Management window.

Step 14  Click the CA Management tab.

Step 15  Click Yes for the Change CA mode button in the CA Management tab.
         After clicking Yes, the GUI view with the CSR is displayed.

Step 16  Click Next in the GUI view with the CSR being displayed.
         The PKI Certificate Management window changes and displays an Import Sub CA Certificate field.

Step 17  Drag and drop your subordinate CA certificate into the Import Sub CA Certificate field and click Apply.
         The subordinate CA certificate will then be uploaded into the DNA Center.
         After the upload finishes, the GUI window changes to display the subordinate CA mode in the CA Management tab.

Step 18  Review the fields in the CA Management tab.

<table>
<thead>
<tr>
<th>Sub CA Certificate</th>
<th>Displays current subordinate CA certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Root CA Certificate</td>
<td>Displays Root CA certificate.</td>
</tr>
<tr>
<td>Sub CA Certificate Lifetime</td>
<td>Displays the lifetime value of the subordinate CA certificate in days.</td>
</tr>
<tr>
<td>Current CA Mode</td>
<td>Displays SubCA mode.</td>
</tr>
</tbody>
</table>

**Provision a Rollover SubCA Certificate**

DNA Center permits the user to apply a subordinate certificate as a rollover sub CA when 70 percent of the existing subordinate CA's lifetime has elapsed.
Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

To initiate subordinate CA rollover provisioning, you must have already changed the PKI certificate role to subordinate CA mode. For details on how to change to subordinate CA mode, see Change the Role of the PKI Certificate from Root to Subordinate, on page 17.

Seventy percent or more of the lifetime of the current subordinate CA certificate must have expired. DNA Center indicates when this has happened by displaying a Renew button on the CA Management tab.

You must have a signed copy of the rollover subordinate CA PKI certificate.

Procedure

Step 1
Click ⚙, then select System Settings.

Step 2
Click the Settings tab, then click PKI Certificate Management.

Step 3
Click the CA Management tab.

Step 4
Review the CA certificate configuration information from the GUI.

<table>
<thead>
<tr>
<th>Sub CA Certificate</th>
<th>Displays the current subordinate CA certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Root CA Certificate</td>
<td>Displays the Root CA certificate.</td>
</tr>
<tr>
<td>Sub CA Certificate Lifetime</td>
<td>Displays the lifetime value of the current subordinate CA certificate in days.</td>
</tr>
<tr>
<td>Current CA Mode</td>
<td>Displays SubCA mode.</td>
</tr>
</tbody>
</table>

Step 5
Click Renew.

The DNA Center will then use the existing subordinate CA to generate and display the rollover subordinate CA Certificate Signing Request (CSR).

Step 6
View the generated CSR in the GUI and perform one of the following actions:

- Click the Download link to download a local copy of the CSR file.
  You can then attach this CSR file to an email to send to your root CA.

- Click the Copy to the Clipboard link to copy the CSR file's content.
  You can then paste this CSR content to an email or attachment to an email and send to your root CA.

Step 7
Send the CSR file to your root CA.

You must send the CSR file to your root CA. Your root CA will then return to you a rollover subordinate CA file that you must import back into the DNA Center.

The CSR for the SubCA rollover must be signed by the same rootCA who signed the SubCA you imported when you switched from RootCA to SubCA mode.

Step 8
After receiving the rollover subordinate CA file from your root CA, return to the PKI Certificate Management window.
Configure Trustpool

The DNA Center contains a pre-installed Cisco trustpool bundle (Cisco Trusted External Root Bundle). The DNA Center also supports the import and storage of an updated trustpool bundle from Cisco. The trustpool bundle is used by supported Cisco networking devices to establish a trust relationship with the DNA Center and its applications.

Note

The Cisco trustpool bundle is an ios.p7b file that only supported Cisco devices can unbundle and use. This ios.p7b file contains root certificates of valid certificate authorities including Cisco itself. This Cisco trustpool bundle is available on the Cisco cloud (Cisco InfoSec). The link is located at: http://www.cisco.com/security/pki/

The trustpool bundle provides you with a safe and convenient way to use the same CA to manage all your network device certificates, as well as your DNA Center certificate. The trustpool bundle is used by the DNA Center to validate its own certificate as well as a proxy gateway certificate (if any), to determine whether it is valid CA signed certificate or not. Additionally, the trustpool bundle is available to be uploaded to the Network PnP enabled devices at the beginning of their PnP workflow so that they can trust the DNA Center for subsequent HTTPS-based connections.

You import the Cisco trust bundle using the Trustpool window in the GUI.

Before you begin

You must be a super administrator to perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.

Procedure

Step 1  Click ☰, then select System Settings.
Step 2  Click the Settings tab, then click Trustpool.
Step 3  In the Trustpool window, view the Update button.

The Update button in the DNA Center's Trustpool window becomes active when an updated version of the ios.p7b file is available and Internet access is available. The Update button remains inactive if there is no Internet access or if there is no updated version of the ios.p7b file.
Step 4  Click the Update button to initiate a new download and install of the trustpool bundle.

Note After the new trustpool bundle is downloaded and installed on the DNA Center, the DNA Center then makes this trustpool bundle available to the supported Cisco devices to download.

Configure SFTP Server

You can configure the DNA Center to upload files to a remote SFTP server. You configure the DNA Center using the SFTP GUI window.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

**Procedure**

**Step 1**  Click 🌐, then select System Settings.

**Step 2**  Click the Settings tab, then click SFTP.

**Step 3**  Configure the SFTP settings as follows:

- **Host**—IP address of the SFTP server.
- **Username**—Name that is used to log into the SFTP server.
- **Password**—Password that is used to log into the SFTP server.
- **Port**—Port that is used to log into the SFTP server.
- **Root Location**—Enter the location of the SFTP root directory.

**Step 4**  Click Apply.

**Step 5**  Review the new SFTP settings in the SFTP window.

Configure SNMP Properties

You can configure retry and timeout values for SNMP.

**Before you begin**

You must be a super administrator to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*. 
Procedure

**Step 1**  
Click the gear icon (⚙) and select **System Settings**.

**Step 2**  
Click the **Settings** tab, then click **SNMP Properties**.

**Step 3**  
Configure the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retries</strong></td>
<td>Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.</td>
</tr>
<tr>
<td><strong>Timeout (in Seconds)</strong></td>
<td>Number of seconds DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 5-120 in intervals of 5 seconds. The default is 5.</td>
</tr>
</tbody>
</table>

**Step 4**  
Click **Apply**.

**Note**  
To return to the default settings, click **Revert to Defaults**.

---

**About Telemetry Collection**

DNA Center collects information about user's experience with DNA Center and securely transfers it to the Cisco Clean Access Agent (CAA) infrastructure at Cisco.

This information is collected for the following reasons:

- To proactively identify issues, if any, with DNA Center.
- To better understand the DNA Center features that are most frequently used.
- To improve and enhance the overall user experience.

Telemetry collection is enabled by default, but you can disable it if you want to opt out.

**Configuring Telemetry Collection**

**Before you begin**

You must be a telemetry administrator user permissions to perform this procedure. For more information, see the *Cisco Digital Network Architecture Center Administrator Guide*.

**Procedure**

**Step 1**  
Click ⚙, then select **System Settings**.
Step 2  Click the **Settings** tab.

Step 3  Click **Telemetry Collection**.

**Note**  Telemetry collection is enabled by default.

Step 4  (Optional) To review the agreement for telemetry collection, click **End User License Agreement**.

Step 5  (Optional) To disable telemetry collection, uncheck the **Telemetry Collection** check box and click **Update**.