CONTENTS

Preface  vii
  Audience  vii
  Related Documentation  vii

CHAPTER 1  Get Started with Cisco DNA Center  1
  About Cisco DNA Center  1
  Log In  1
  Default Home Page  2
  Use Search  4
  Start Using DNA Center  5

CHAPTER 2  Configure System Settings  7
  About System Settings  7
  System 360  7
  About DNA Center and Cisco ISE Integration  8
  Configure Authentication and Policy Servers  8
    Configure Access to an AAA Server  8
    Configure Access to a Cisco ISE Server  10
  Device Controllability  11
    Configure Device Controllability  12
  Configure an IP Address Manager  12
  Configure Debugging Logs  13
  Configure the Network Resync Interval  14
  View Audit Logs  15
  Configure Security for Cisco DNA Center  16
    Enable TLS and RC4-SHA  17
Configure Proxy Certificate 18
Certificate and Private Key Support 19
  Configure Certificate 20
Certificate Management 22
  Configure Device Certificate Lifetime 22
  Change the Role of the PKI Certificate from Root to Subordinate 23
  Provision a Rollover SubCA Certificate 25
  Configure Trustpool 27
Configure SFTP Server 28
Configure SNMP Properties 28
About Telemetry Collection 29
  Configuring Telemetry Collection 29

CHAPTER 3 Manage Applications 31
  Application Management 31
  Installing Applications 32
  Updating Applications 33
  Uninstalling Applications 34

CHAPTER 4 Manage Users 37
  About User Profiles 37
  About User Roles 37
  Create Local Users 38
  Edit Local Users 38
  Delete Local Users 39
  Change Your Own User Password 39
  Reset Forgotten Password 40
  Display Role-Based Access Control Statistics 40
  Configure External Authentication 41
  Display External Users 42

CHAPTER 5 Manage Licenses 43
  About Smart License Management 43
  Set Up License Manager 43
Visualize License Usage and Expiration 44
See License Details 45
Change License Level 46
Export License Information 47

CHAPTER 6
Back Up and Restore 49
About Backup and Restore 49
Backup Server Requirements 50
Back Up DNA Center 51
Restore DNA Center 53
Schedule a Backup 54
Preface

Audience

This publication is intended for experienced system administrators who will configure and maintain the Cisco Digital Network Architecture Center (DNA Center), primarily through the use of the system settings functionality. This guide is part of a documentation set that is designed to help you install, troubleshoot, and upgrade your DNA Center. For a complete list of the DNA Center documentation set, see Related Documentation, on page vii.

Related Documentation

The following publications are available for the DNA Center.

<table>
<thead>
<tr>
<th>For this type of information...</th>
<th>See this document...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release information, including new features, system requirements, and open and resolved caveats.</td>
<td>Cisco Digital Network Architecture Center Release Notes</td>
</tr>
<tr>
<td>Installation and configuration of DNA Center, including post-installation tasks.</td>
<td>Cisco Digital Network Architecture Center Appliance Installation Guide</td>
</tr>
<tr>
<td>Introduction to the DNA Center GUI and its applications.</td>
<td>Cisco Digital Network Architecture Center User Guide</td>
</tr>
<tr>
<td>Configuration of user accounts, RBAC scope, security certificates, authentication and password policies, and global discovery settings. Monitoring and managing DNA Center services. Backup and restore.</td>
<td>Cisco Digital Network Architecture Center Administrator Guide</td>
</tr>
<tr>
<td>Supported devices, such as routers, switches, wireless access points, NFVIS platforms, and software releases.</td>
<td>Supported Devices Used in Cisco Digital Network Architecture Center</td>
</tr>
<tr>
<td>Licenses and notices for open source software used in DNA Center Assurance</td>
<td>Open Source Used In Cisco DNA Center Assurance, Release 1.1.x</td>
</tr>
</tbody>
</table>
Get Started with Cisco DNA Center

About Cisco DNA Center
Cisco Digital Network Architecture (DNA) offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The graphical user interface provides end-to-end visibility and uses network insights to optimize network performance and deliver the best user and application experience. DNA Center allows you to:

- Move faster—Provision thousands of devices across your enterprise network. Act fast with centralized management, and automate device deployment.
- Lower costs—Reduce errors with automation. Policy-driven deployment and onboarding deliver better uptime and improved security.
- Reduce risk—Predict problems early. Use actionable insights for optimal performance of your network, devices, and applications.

Log In
Access DNA Center by entering its network IP address in your browser. This IP address connects to the external network and was configured during the DNA Center installation. For more information, see the Cisco DNA Center Appliance Installation Guide.

The following are the supported browsers and versions for the DNA Center GUI:

- Google Chrome, version 62.0 or later
- Mozilla Firefox, version 54.0 or later
You need to continuously use DNA Center to remain logged in. If you allow too much time of inactivity to elapse, DNA Center automatically logs you out of your session.

**Procedure**

**Step 1** Enter the following address in your web browser address field, where *server-ip* is the IP address (or the hostname) of the server on which you installed DNA Center:

https://server-ip

For example, https://192.0.2.1

Depending on your network configuration, the first time your browser connects to the DNA Center web server, you might need to update your client browser to trust the server's security certificate, which ensures the security of the connection between your client and the DNA Center server.

**Step 2** Enter the username and password that was configured during the installation.

**Step 3** To log out, click the gear icon in the top-right corner and click **Sign Out**.

**Default Home Page**

After you log in to DNA Center, you are taken to the DNA Center home page, which is divided into two main areas—**Applications** and **Tools**:

**Applications** include:

- **Design**—Create the structure and framework of your network including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.

- **Policy**—Create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.

- **Provision**—Prepare and configure devices, including adding devices to sites, assigning devices to the DNA Center inventory, deploying the required settings and policies, creating fabric domains, and adding devices to the fabric.

- **Assurance**—Gather actionable insights into network-, client-, and application-related issues using both system-guided as well as self-guided troubleshooting. Review in-depth health scores for the network and its devices, clients, applications, and services. Analyze detailed application experiences, and oversee policy compliance.

**Tools**—Use the tools to help you configure and manage the network.
Click any of the icons in the two main areas to launch the corresponding application or tool.

In addition to the application and tool icons, you can click any of the icons at the top right corner of the home page to perform important common tasks:

- ✕ (search) icon—Lets you search for devices, users, hosts, and other items, anywhere they are stored in the DNA Center database. For tips on using Search, see Use Search, on page 4.

- ✗ (apps) icon—Lets you return to the home page from any other page in DNA Center (clicking on the "Cisco DNA Center" logo in the upper left corner of the home page does the same thing).

- ☑️ (settings) icon—Lets you see audit logs, configure system settings, see the DNA Center version you are using, and log out.

- 📲 (notifications) icon—Lets you see recently scheduled tasks and other notifications.

If you do not know where to start, see Start Using DNA Center, on page 5 for information.
Use Search

Use DNA Center’s global Search to search for things like:

- **Devices**: Search for them by name, IP address, serial number, software version, platform, product family, or MAC address/
- **Hosts**: Search for them by name, IP address, or MAC address.
- **Users**: Search for them by name.
- **IP Pools**: Search for them by name or IP address.
- Other items, as new versions of DNA Center are released.

To start a global Search, click the icon in the upper-right corner of any DNA Center page.

*Figure 2: Search Icon (at the top right of every page)*

DNA Center displays a global search prompt field, where you can begin entering information for the item you are looking for. As you begin entering your search information, DNA Center attempts to autocomplete your entry. It suggests a list of possible search targets matching your input, as shown in the figure below.

*Figure 3: Suggest Search Targets*

You can click on any of the suggested targets to see summary information for that item. The summary will include links to additional details appropriate for that item. For example, clicking on the 360 View and Topology links in the device detail window shown in the following figure will take you to the pages showing extensive device details and where the device fits in your network topology.
When you are finished, click \( \times \) to close the search window.

**Start Using DNA Center**

To start using DNA Center, you must first configure the DNA Center settings so that the server can communicate outside the network.

After you configure the DNA Center settings, your current environment determines how you start using DNA Center:

- **Existing infrastructure**—If you have an existing infrastructure, start by running a Discovery. After running Discovery, all your devices are displayed on the Inventory window. For information about running a Discovery, see the Cisco Digital Network Architecture Center User Guide.

- **New or nonexisting infrastructure**—If you have no existing infrastructure and are starting from scratch, you will need to create a network hierarchy. For information about creating a network hierarchy, see the Cisco Digital Network Architecture Center User Guide.
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.

  **Note**

  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 .

**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 10

**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.
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 12](#).

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 11.

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>From the DNA Center Home page, click the gear icon (⚙️) and choose &gt; System Settings &gt; Settings &gt; Device Controllability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Enable Device Control.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click the gear icon (⚙️) and select System Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the Settings tab, and then click IP Address Manager.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the IP Address Manager section, enter the required information in the following fields:</td>
</tr>
<tr>
<td>Server Name</td>
<td>Name of server.</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Server URL</td>
<td>IP address of server.</td>
</tr>
<tr>
<td>Username</td>
<td>Required username for server access.</td>
</tr>
<tr>
<td>Password</td>
<td>Required password for server access.</td>
</tr>
<tr>
<td>Provider</td>
<td>Select a provider from the drop-down menu.</td>
</tr>
</tbody>
</table>

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.

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.
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**

---

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

**Step 2**
Click the **Settings** tab, then click **Network Resync Interval**.

**Step 3**
In the **Polling Interval** field, enter a new time value (in minutes).

**Step 4**
Click **Yes** for **Override for all devices** to override the existing configured polling interval for all devices.

**Step 5**
Click **Save** to apply and save your new settings.

---

**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**

---

**Step 1**
Click 📚, then select **Audit Logs**.

The **Audit Logs** window appears. In the **Audit Logs** 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.

The following information is displayed for each policy in the window:

- **Description**—Application or policy audit log description
- **Site**—Name of the site for the specific audit log
• **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 17.

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 18.

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 19.

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 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**

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

**Step 2**
Click the Settings tab, and then click Proxy Certificate.

**Step 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.

**Step 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.

**Step 5**
Click Save.

**Step 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.

**Important**

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.

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](Image)

  **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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Click ☰, then select <strong>System Settings</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the <strong>Settings</strong> tab, then click <strong>PKI Certificate Management</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>CA Management</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Review the existing root or subordinate CA certificate configuration information from the GUI.</td>
</tr>
</tbody>
</table>

<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>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>In the <strong>CA Management</strong> tab, for <strong>Change to Sub CA mode</strong> click <strong>Yes</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>In the <strong>CA Management</strong> tab, click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Review the <strong>Root CA to Sub CA</strong> warnings that appears:</td>
</tr>
<tr>
<td><strong>•</strong></td>
<td>Changing from root CA to subordinate CA is a process that cannot be reversed.</td>
</tr>
<tr>
<td><strong>•</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>•</strong></td>
<td>Network devices must come online only after this subordinate CA configuration process is finished.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>OK</strong> to proceed.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Drag and drop your root CA certificate into the <strong>Import External Root CA Certificate</strong> field and click <strong>Upload</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>•</strong></td>
<td>The root CA certificate will then be uploaded into the DNA Center and used to generate a Certificate Signing Request (CSR).</td>
</tr>
<tr>
<td><strong>•</strong></td>
<td>When the upload process is finished a <strong>Certificate Uploaded Successfully</strong> message appears.</td>
</tr>
</tbody>
</table>
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><strong>External Root CA Certificate</strong></td>
<td>Displays Root CA certificate.</td>
</tr>
<tr>
<td><strong>Sub CA Certificate Lifetime</strong></td>
<td>Displays the lifetime value of the subordinate CA certificate in days.</td>
</tr>
<tr>
<td><strong>Current CA Mode</strong></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 23.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click ⚙, then select System Settings.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Settings tab, then click PKI Certificate Management.</td>
</tr>
<tr>
<td>3</td>
<td>Click the CA Management tab.</td>
</tr>
<tr>
<td>4</td>
<td>Review the CA certificate configuration information from the GUI.</td>
</tr>
</tbody>
</table>

<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>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Click Renew.</td>
</tr>
<tr>
<td></td>
<td>The DNA Center will then use the existing subordinate CA to generate and display the rollover subordinate CA Certificate Signing Request (CSR).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>View the generated CSR in the GUI and perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Click the Download link to download a local copy of the CSR file.</td>
</tr>
<tr>
<td></td>
<td>You can then attach this CSR file to an email to send to your root CA.</td>
</tr>
<tr>
<td></td>
<td>• Click the Copy to the Clipboard link to copy the CSR file's content.</td>
</tr>
<tr>
<td></td>
<td>You can then paste this CSR content to an email or attachment to an email and send to your root CA.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Send the CSR file to your root CA.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>After receiving the rollover subordinate CA file from your root CA, return to the PKI Certificate Management window.</td>
</tr>
</tbody>
</table>
**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/](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 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</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>SFTP</strong>.</td>
</tr>
</tbody>
</table>
| 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>Retries</td>
<td>Number of attempts to connect to the device. Valid values are from 0-4. The default is 3.</td>
</tr>
<tr>
<td>Timeout (in Seconds)</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.
CHAPTER 3

Manage Applications

- Application Management, on page 31
- Installing Applications, on page 32
- Updating Applications, on page 33
- Uninstalling Applications, on page 34

Application Management

DNA Center treats many of its functions as individual applications, packaged separately from the DNA Center's core infrastructure. This allows you to install and run just the applications you want, and uninstall those you are not using, depending on your preferences.

The number and type of application packages you see displayed on the App Management tab will vary, depending on the release version of DNA Center you have deployed at the moment, and your DNA Center licensing level (for example, DNA Essentials or DNA Advantage). All application packages available to you will be displayed, whether they are currently installed or not.

Some applications are so basic, they are required on nearly every DNA Center deployment. To get a pop-up description of any package and whether it is required or not, hover your mouse cursor over that package's name in the App Management listing.

To ensure you have the latest information on available packages, click the Refresh button.

Each DNA Center application package consists of service bundles, meta data files, and scripts.

For this specific release, application packages are provided as part of the installed ISO image only.

Important

All application management procedures should be performed using the DNA Center GUI. Although you are able to perform many of these same procedures using the CLI (after logging into the shell), this is not recommended. In particular, if you use the CLI to deploy or upgrade packages, you must ensure that no deploy or upgrade command is issued unless the results of the "maglev package status" command show all packages as either NOT_DEPLOYED, DEPLOYED or DEPLOYMENT_ERROR. Any other state indicates activity in progress, and parallel deployments or upgrades are not supported.
Installing Applications

DNA Center treats individual applications as separate from the core infrastructure. Specifically, individual applications can be installed to run on the DNA Center.

You can perform the application management procedures from the App Management tab in the DNA Center GUI.

Note
Application installation may take time to install and deploy. Therefore, install an application during a maintenance period for your network.

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 App Management tab.
Step 3  Review the App Management window that now appears.

The App Management window consists of the following side tabs:

• Packages & Updates—Packages currently installed and updates available for installation from the Cisco cloud.

• System Updates—Updates that have been downloaded from the Cisco cloud.

Important  The download option will not display if DNA Center does not have internet access or access via a proxy server. For DNA Center application upgrades, DNA Center must be able to reach the Cisco update server either directly or indirectly via a proxy server.

Step 4  In the Packages & Updates side tab, review the listed applications, status (running or disabled), and versions.

The following application information is available.

<table>
<thead>
<tr>
<th>Package</th>
<th>Name of the package.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status of package:</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Not Deployed</td>
</tr>
<tr>
<td>Installed Version</td>
<td>Software version of the package currently installed.</td>
</tr>
<tr>
<td>Downloaded Version</td>
<td>Software version downloaded from the Cisco cloud and available for installation.</td>
</tr>
</tbody>
</table>
### Updating Applications

DNA Center treats individual applications as separate from the core infrastructure. Specifically, individual applications can be installed and subsequently updated to run on the DNA Center.

You can perform the application management procedures from the App Management tab in the DNA Center 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 App Management tab.

**Step 3**

Review the App Management window that now appears.

The App Management window consists of the following side tabs:

- **Packages & Updates**—Packages currently installed and updates available for installation from the Cisco cloud.
- **System Updates**—Updates that have been downloaded from the Cisco cloud.

**Step 4**

Click the Packages & Updates side tab.

Review the listed packages and their status.

**Step 5**

Review the Available Update column for any currently available package updates.

**Step 6**

Click the Refresh icon.
After clicking this icon, the window is refreshed so that you can check again for any updates.

**Step 7**  
Review the list of packages in the **Packages & Updates** side tab again and make a determination as to which packages to update.

**Step 8**  
If an update appears in the **Available Update** column, click the **Download** link to download it to the DNA Center.

**Step 9**  
Click the **System Updates** side tab.

**Step 10**  
Locate the update in the **System Updates** side tab.

**Step 11**  
Click the **Deploy** link in the **Action** column to update the specific package.

**Step 12**  
Ensure that the application has been updated, by reviewing the **Status** and **Current Version** columns. The current version should be updated and the status should change to **Running** with a check mark icon.

---

**Uninstalling Applications**

DNA Center treats individual applications as separate from the core infrastructure. Specifically, individual applications can be installed and uninstalled on the DNA Center.

You can perform the application management procedures from the **App Management** tab in the DNA Center 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 **App Management** tab.

**Step 3**  
Review the **App Management** window that now appears.

The **App Management** window consists of the following side tabs:

- **Packages & Updates**—Packages currently installed and updates available for installation from the Cisco cloud.

- **System Updates**—Updates that have been downloaded from the Cisco cloud.

**Step 4**  
In the **Packages** side tab, review the listed applications, status (running or disabled), and versions.

The following application information is available:

<table>
<thead>
<tr>
<th>Package</th>
<th>Name of the package.</th>
</tr>
</thead>
</table>
### Uninstalling Applications

<table>
<thead>
<tr>
<th>Status</th>
<th>Status of package:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Not Deployed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Installed Version</th>
<th>Software version of the package currently installed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloaded Version</td>
<td>Software version downloaded from the Cisco cloud and available for installation.</td>
</tr>
<tr>
<td>Available Update</td>
<td>Software version available for download from the Cisco cloud.</td>
</tr>
</tbody>
</table>

**Note**  
Place your cursor next to an application for additional application information to display.

**Step 5**  
To uninstall a package to the DNA Center, locate the package to be uninstalled and click the **Uninstall** link.  
**Important**  
After clicking **Uninstall**, a message may appear providing additional information about the package, as well as requirements as to other package dependencies. Review and follow the information in these messages, including any required package uninstall order.

**Step 6**  
Ensure that the application has been uninstalled, by reviewing the **Packages** window for the status change.  
The status should change to **Not Deployed** with an exclamation point icon.
Manage Users

- About User Profiles, on page 37
- About User Roles, on page 37
- Create Local Users, on page 38
- Edit Local Users, on page 38
- Delete Local Users, on page 39
- Change Your Own User Password, on page 39
- Reset Forgotten Password, on page 40
- Display Role-Based Access Control Statistics, on page 40
- Configure External Authentication, on page 41
- Display External Users, on page 42

About User Profiles

A user profile defines a user's login, password, and role (permissions).

You can configure both internal and external user profiles for any user. Internal user profiles reside in DNA Center and external user profiles reside on an external AAA server.

One default user profile with SUPER-ADMIN-ROLE permissions is created when you install DNA Center.

About User Roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- **Administrator (SUPER-ADMIN-ROLE)**—Users with this role have full access to all of the DNA Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.

  Although administrators cannot directly change another user's password in the user interface, they can delete and recreate a user with new password.

  **Note** For security reasons, passwords are not displayed to any user, not even those with administrator privileges.
• **Network Administrator (NETWORK-ADMIN-ROLE)**—Users with this role have full access to all of the network-related DNA Center functions. They do not have access to system-related functions, such as App Management, Users (except for changing their own passwords), and Backup and Restore.

• **Observer (OBSERVER-ROLE)**—Users with this role have view only access to all of the DNA Center functions.

---

**Note**

A fourth default role, called TELEMETRY-ADMIN-ROLE, also exists, but this role is not accessible from the user interface and is only used for system-level functions within DNA Center.

---

### Create Local Users

You can create a user and assign it one of the following user roles: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE, or OBSERVER-ROLE. For more information, see About User Roles, on page 37.

#### 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

1. From the DNA Center home page, click ☰ > System Settings > Users > User Management.
2. Click ✉️ Add.
3. Enter a username for the new user.
4. From the Role drop-down list, choose one of the following roles: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE, or OBSERVER-ROLE.
   
   **Note** Although the TELEMETRY-ADMIN-ROLE appears as an option, it is not available for use, so you cannot choose this role.

5. Enter a password and confirm it.
6. Click Save.

---

### Edit Local Users

Only an administrator with SUPER-ADMIN-ROLE permissions may edit users. The only attribute that can be changed is the user role. The username or password cannot be changed.
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 🕒 > System Settings > Users > User Management.
Step 2  Click the radio button next to the user that you want to modify.
Step 3  Click Edit.
Step 4  From the Role drop-down list, choose a new role: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE, or OBSERVER-ROLE.
Step 5  Click Save.

Delete Local Users

Only an administrator with SUPER-ADMIN-ROLE permissions may delete a user.

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 🕒 > System Settings > Users > User Management.
Step 2  Select the radio button next to the user that you want to delete.
Step 3  Click Delete.
Step 4  Click OK.

Change Your Own User Password

Only you can change the password that you enter to log in to DNA Center. Even a user with administrator privileges cannot change another user's password. If an administrator needs to change another user's password, they need to delete and readd the user with a new password.

Procedure

Step 1  From the DNA Center home page, click 🕒 > System Settings > Users.
Step 2  Click Change Password.
Reset Forgotten Password

If you have forgotten your password, you can reset your password through CLI. Follow the below steps to reset your password:

**Procedure**

**Step 1** Check if the user is created in the system using the below command:

```
magctl user display <username>
```

This command will return the tenant-name which can be used to reset the password. The sample output will be:

```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```

**Step 2** Enter the tenant-name in the below command to reset the password.

```
magctl user password update <username> <tenant-name>
```

You will be prompted to enter a new password.

**Step 3** Enter a new password.

You will be prompted to re-enter the new password to confirm.

**Step 4** Enter the new password. The password is reset and you can login to DNA Center using the new password.

What to do next

Display Role-Based Access Control Statistics

You can display statistics that show how many users of each user role exist. You can also drill down to view a list of users who have the selected role.

**Procedure**

**Step 1** From the DNA Center home page, click 🌐 > System Settings > Users > Role Based Access Control.

**Step 2** Click See details to display a list of users with the selected role.
Configure External Authentication

If you are using an external server for authentication and authorization of external users, you need to enable external authentication in 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.
- You must configure at least one authentication server.

Procedure

Step 1 From the DNA Center home page, click  > System Settings > Users > External Authentication.

Step 2 To enable external authentication on DNA Center, select the Enable External User checkbox.

Step 3 (Optional) Configure the AAA attribute.

For most cases, the default AAA attribute setting is sufficient, as long as you have set the DNA Center user profile on the AAA server with cisco-av-pair as the AAA attribute. You only need to change the default setting in DNA Center if you have a different value set in the DNA Center user profile on the AAA server.

a) In the AAA Attribute field, leave the default value of Cisco-AVPair or enter the new AAA attribute value.

b) Click Update.

Step 4 (Optional) Configure the AAA server(s). You need to configure these settings only if the order (primary/secondary) or the AAA servers that you configured in System Settings > Settings > Authentication and Policy Servers need to be different.

a) From the Primary AAA Server IP Address drop-down field, choose an IP address of one of the preconfigured AAA servers.

b) From the Secondary AAA Server IP Address drop-down field, choose an IP address of one of the preconfigured AAA servers.

c) Click View Advanced Settings and update the settings, if necessary.

- 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 Cisco ISE before abandoning the attempt to connect. The default number of attempts is 1.

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

---

**Display External Users**

You can view a list of external users, including their user names and roles.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the DNA Center home page, click 🌐 &gt; <strong>System Settings</strong> &gt; <strong>Users</strong> &gt; <strong>External Authentication</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Scroll to the bottom of the screen. The <strong>External Users</strong> area lists the external users.</td>
</tr>
</tbody>
</table>
Manage Licenses

This chapter contains the following topics:

• About Smart License Management, on page 43
• Set Up License Manager, on page 43
• Visualize License Usage and Expiration, on page 44
• See License Details, on page 45
• Change License Level, on page 46
• Export License Information, on page 47

About Smart License Management

Cisco DNA Center supports Cisco Smart Accounts, an online Cisco service that provides simplified, flexible, automated software- and device-license purchasing, deployment, and management across your organization.

If you already have a Cisco Smart Account, you can use DNA Center to:

• Track your license consumption and expiration.
• Apply and activate new licenses, without intervention.
• Promote each device's license level from Essentials to Advantage (or vice versa) and reboot the device with the newly changed level of feature licensing.
• Identify and re-apply unused licenses.
• Retire unused licenses.

You can accomplish this automatically, without leaving DNA Center.

For more on the service itself, see Cisco Smart Accounts on Cisco.com. For more on setting up your Cisco Smart Account for use with DNA Center, see Set Up License Manager, on page 43.

Set Up License Manager

You must set up access to your Cisco Smart Account before you can use the DNA Center License Manager tools.
Before you begin

You will need to:

- Make sure you have SUPER-ADMIN-ROLE permissions and the appropriate RBAC scope to perform this procedure. For information about the user permissions required to perform tasks using the DNA Center, see the chapter, Managing Users and Roles, in this guide.

- Collect the Cisco user ID and password for your Smart Account.

- If you have one or more Smart Accounts: Select the smart Account that you want to use with DNA Center, and collect that account's user ID and password.

Procedure

**Step 1** Log on using a DNA Center system administrator username and password.

**Step 2** Click \> System Settings > Settings > Cisco Credentials.

**Step 3** Under Cisco.com Credentials, enter the username and password for your Smart Account.

**Step 4** To access your Smart Account using a virtual or subordinate Smart Account name and password, under Link Your Smart Account, choose:

- Use Cisco.com user ID if your cisco.com and Smart Account credentials are the same.

- Use different credentials if your cisco.com and Smart Account credentials are different, and then enter your Smart Account credentials.

**Step 5** Click View all virtual accounts to view all virtual Smart License Accounts.

**Step 6** When you are finished, click Apply.

Visualize License Usage and Expiration

DNA Center can display graphical representations of your purchased DNA licenses, how many of them are in use (that is, assigned to devices), and their duration.

Procedure

**Step 1** Select Tools > Licenses

**Step 2** Select the type of device category whose license usage you want to see: Switches, Routers, or Access Points.

The License Usage graphs at the top of the page display the aggregate number of purchased DNA licenses and the number of those licenses currently in use for the device category you selected. The graphs also indicate the proportion of Essentials versus Advantage licenses within each total.

Under the graphs, the License Usage table gives subtotals for used and unused licenses, listed alphabetically by product family name.

**Step 3** To see detailed comparisons for a particular product family, click on the name of the product family given in the Model column in the table.
DNA Center displays a window giving details for the product family you selected. When you are finished, click **View All** to close the detail window.

**Step 4**
To see a graphical representation of license duration, scroll down to the **License Timeline** section of the page. The timeline graph for each product family is a visual representation of when the DNA licenses in the configured Smart Account will expire for that product family.

---

## See License Details

There are many ways to find and view license details in DNA Center. For example, you can click on the license usage and term graphs displayed in the **Switches**, **Routers**, and **Access Points** tabs in the License Manager window. Each of these will display popups with aggregated facts about licenses for each of these product families.

The simplest method for getting the most comprehensive license details for a single device is to use the License Manager's **All Licenses** table, as explained in the following steps.

### Procedure

**Step 1**
Select **Tools > Licenses > All Licenses**

The License Manager window displays a table listing all of your discovered devices and their licenses. Information in the table includes only basic device and license information, such as device type, license expiration dates, and so on.

**Step 2**
Scroll through the table to find the device whose license details you want to see. If you are having trouble finding the device you want, you can:

- **Filter**: Click ⚫ and then enter your filter criteria in the appropriate field (for example: enter all or part of the device name in the **Device Name** field). You may enter filter criteria in multiple fields. When you click **Apply**, the table displays only the rows displaying information that matches your filter criteria.

- **Find**: Click in the **Find** field and enter the text you want to find in any of the table columns. When you press **Enter**, the table scrolls to the first row with text matching your entry in the **Find** field.

- **Customize**: Click ⚫ and select the columns you want displayed in the table. For example: Deselect **Device Model** or select **Days to Expiry**. When you click **Apply**, the table displays only the columns you selected.

**Step 3**
When you have found the device you want, click the **Device Name** link in the row for that device.

DNA Center displays a popup **License Details** window giving complete license details for the device you selected. Links in the window also allow you to **See More** license details, **View Device Config**, **View Device 360**, and see other **Actions** that can be performed on the device or its licenses.

When you are finished, click ⏹️ to close the **License Details** window.
Change License Level

You can upgrade or downgrade the feature level of your device licenses. You can do this with both your legacy Network (non-subscription) and DNA (subscription) licenses. In both cases, your feature level choices are either the basic Essentials level or the comprehensive Advantage level.

Whenever you change your license level, DNA Center will automatically purchase, download and apply your licenses behind the scenes, using your Smart Account. As applying the changed licenses includes a device reboot, License Manager will prompt you to confirm that you want to make the change.

Scheduling for license-level changes is planned for a later release.

Procedure

Step 1  Select Tools > Licenses > All Licenses

The License Manager window displays a table listing all of your discovered devices and their licenses.

Step 2  Scroll through the table to find the devices whose license level you want to change. If you are having trouble finding the device you want, or want to select multiple devices, follow the tips in the related topic, See License Details, on page 45, to change the table to display just the devices you want.

Step 3  When you have found the devices you want, click the checkbox next to each device's **Device Name** link. Then:

• If the license is a legacy Network license, click **Change Network License**.

• If the license is a subscription DNA license, click **Change DNA License**.

Step 4  With your devices selected, click **Change Network License** or **Change DNA License**. DNA Center displays a Change License Level window appropriate for the license type you want to change.

Step 5  Click the license level you want for these devices: **Essentials** or **Advantage**.

Step 6  Click Next to continue. DNA Center asks if you are sure you want to make the change, and if so, whether you want the change to be applied right away or at a later time.

To continue:

• If you are not ready to make the change: Click **Back** to change your License Level selection, or click ✗ to close the window and cancel the change.

• If you are ready to make the change immediately: Click **Run Now** then click **Confirm**. Note that devices using this license will reboot as soon as the change is applied.

• If you are want the change to be applied later: Click **Schedule Later** and specify the date and time when you want the change to be applied. Optionally, you can give the change a task name, or specify a different time zone for the schedule. Then click **Confirm**.
Export License Information

You can quickly export license information from DNA Center to backup PDF or Microsoft Excel files. These license backup files are intended to assist your organization’s accounting and reporting needs.

Procedure

Step 1  Select Tools > Licenses
Step 2  Select All Licenses. DNA Center displays a list of all your currently assigned licenses.
Step 3  Click Export. DNA Center displays the Export Licenses window.
Step 4  Select the destination file format.
Step 5  (Optional) Click on the checkboxes next to each type of license information you want to exclude or include in the export. Click the checkbox at the bottom if you want to save your choices as the default for later exports.
Step 6  When you are finished, click Export and specify the location and file name for the exported license file. Then click OK to complete the export.
Chapter 6

Back Up and Restore

- About Backup and Restore, on page 49
- Backup Server Requirements, on page 50
- Back Up DNA Center, on page 51
- Restore DNA Center, on page 53
- Schedule a Backup, on page 54

About Backup and Restore

The backup and restore procedures for DNA Center can be used for the following purposes:

- To create backup files for disaster recovery for the appliance
- To create backup files to restore to a different appliance (if required for your network configuration)

Backup

When you perform a backup, DNA Center creates a copy of the following files and exports the files to a specific location on a remote server:

- DNA Center databases
- DNA Center credentials
- DNA Center file system and files

Important

The backup files should not be modified by the user.

The backup files are created and posted to a remote server. You are able to restore the backup files from the remote server using DNA Center. For information about the remote server requirements, see Backup Server Requirements, on page 50.

Note

DNA Center does not support using FTP (port 21) when performing a backup. Use SSH (port 22)/Rsync when backing up the DNA Center.
Only a single backup can be performed at a time. Performing multiple backups at once are not permitted. Additionally, only a full backup is supported. Other types of backups (for example, incremental backups) are not supported.

While a backup is being performed, you will be unable to delete any files that have been uploaded to the file service and any changes that you make to files might not be captured by the backup process.

When performing a backup, we recommend the following:

- Perform a backup everyday to maintain a current version of your database and files.
- Perform a backup after making any changes to your configuration. For example, when changing or creating a new policy on a device.
- Only perform a backup during a low impact or maintenance time period.

**Note**

You are able to schedule or automate a backup for a specific date and time using the DNA Center's GUI. For information about this procedure, see Schedule a Backup, on page 54.

**Restore**

When you restore the backup files, DNA Center removes and replaces the existing database and files with the backup files. You restore the backup files from the remote server. When a restore is being performed, DNA Center is unavailable.

You cannot take a backup from one version of DNA Center and restore it to another version of DNA Center. You can only restore a backup to an appliance that is running the same DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current applications and versions on DNA Center, click ☰, then System Settings, then App Management.

You can restore a backup to a DNA Center system with a different IP address. This could happen if for any reason the IP address is changed on DNA Center and you need to backup from an older system.

**Backup Server Requirements**

The following are the requirements for the backup server:

- Running Red Hat Enterprise Linux 6 or greater, or any of its derivatives such as CentOS, Ubuntu 16.04 or greater and its derivatives (Mint), or any other modern Linux operating system.
- Linux rsync utility must be installed.
- The destination folder for the backup should be owned by the backup user or the backup user should have read-write permissions for the user's group. For example, assuming the backup user is 'backup' and user's group is 'staff', then the following sample outputs show the required permissions for the backup directory:

```
$ ls -l /srv/
drwxr-xr-x  4 backup root  4096 Apr 10 15:57 dnac
```
• Example 2: 'backup' user's group has required permissions:

```bash
$ ls -l /srv/
drwxrwxr-x. 7 root staff 4096 Jul 24 2017 dnac
```

• Ensure that the SFTP sub-system is enabled. The following line needs to be uncommented and present in the SSHD configuration:

```bash
Subsystem sftp /usr/libexec/openssh/sftp-server
```

The file where you need to uncomment the above line is generally located in: `/etc/ssh/sshd_config`

---

## Back Up DNA Center

You can back up and restore the DNA Center database and files. When you perform a backup, DNA Center copies and exports the database and files to a location on a remote server that you configure. When you restore the backup files, DNA Center removes and replaces the existing database and files with the backup files. For more information, see About Backup and Restore, on page 49.

**Note**

Data is backed up using SSH/Rsync. DNA Center does not support using FTP (port 21) when performing a backup.

### 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 then choose System Settings > Backup & Restore.

The Backup & Restore window appears consisting of three tabs: Backups, Schedule, and Activity. The first time you access this window, the Set up backup server field also appears.

#### Step 2

Click Configure in this field.

The Remote Backup Server side panel appears.

#### Step 3

Configure the remote backup server for the DNA Center backups.

Enter configuration values for the remote backup server.

<table>
<thead>
<tr>
<th>SSH IP Address</th>
<th>IP address of the remote server that you can SSH into.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Port</td>
<td>Port address of the remote server that you can SSH into.</td>
</tr>
</tbody>
</table>
Step 4 Click **Apply** to save the **Remote Backup Server** configuration.

Note Other options are **Cancel** to cancel this configuration or **Remove** to remove an earlier remote backup server configuration.

Step 5 Click **Create New Backup**.

To view the backup's progress, click the **Activity** tab and review the **Status** column.

During the backup process, DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the backup process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. DNA Center displays an error message stating the cause of the backup failure. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.

Step 6 (Optional) Verify the final backup status in the **Backup & Restore** window (**Backups** tab).

The following information is displayed:

- **Date**—Local date and time of the backup or restore.
- **Backup Name**—Name of the file that was backed up or restored.
- **File Size**—Size of the file that was backed up or restored.
- **Status**—Success or failure status of the operation.
  
  Note Place your cursor over the failure status to display additional details about the failure.

- **Operation**—Type of operation, either backup or restore.
  
  - **Action**—Possible actions to take with the backup files. For example, restore the DNA Center with the backup files or proceed to delete the backup files.
Step 7  (Optional) To download a .CSV file of what is displayed in this window for your records, click Export.

What to do next
When necessary and at the appropriate time, you can restore the backup file to DNA Center by clicking the Restore link in the Backups tab for the backup. You can also schedule a future backup using the configuration options displayed in the Schedule tab. For information about this procedure, see Schedule a Backup, on page 54.

Restore DNA Center
You can restore DNA Center database from the backup files on the remote server that you configured. When you restore from the backup files located on the remote server, DNA Center removes and replaces the existing database and files. For more information, see About Backup and Restore, on page 49.

Caution
The DNA Center restore process only restores the database and files. The restore process does not restore your network state and any changes made since the last back up, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates and trustpool bundles.

Note
You cannot do a backup from one version of DNA Center and restore to another version of DNA Center. You can only restore a backup to an appliance that is running the same DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current apps and versions, click ⊕, then System Settings, then App Management.

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 then choose System Settings > Backup & Restore.

The Backup & Restore window displays the following three tabs: Backups, Schedule, and Activity. The default tab that displays is Backups.

If you have already successfully created a backup on a remote server, then it will display in the Backups tab.

Step 2  In the Backup Name column, locate the backup that you wish to restore.

Step 3  In the Actions column, select Restore.
The DNA Center restore process restores the database and files. The restore process does not restore your network state and any changes made since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates and trustpool bundles.

During a restore, the backup files remove and replace the current database.

**Step 4**
To view the progress of the restore process, click the **Activity** tab.

If you stop the backup, then an **ABORTED** message is displayed in the **Status** column of the **Activity** tab. If the backup fails, then a **FAILURE** message is displayed in the **Status** column of the **Activity** tab. By clicking on the icon next to the **FAILURE** message, information about where in the backup process the failure occurred is displayed. Review the information under **Error Type**. You can use this information to troubleshoot a backup failure.

**Step 5**
Click the **Backups** tab to view the results for a successful restore process.

---

**Schedule a Backup**

You can schedule a backup of the DNA Center database and files at a future date and time. You schedule this backup using the DNA Center 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**
From the DNA Center home page, click the gear icon (⚙️) and then choose **System Settings > Backup & Restore**.

The **Backup & Restore** window displays the following three tabs: **Backups**, **Schedule**, and **Activity**. The default tab that displays is **Backups**.

**Step 2**
Click the **Schedule** tab header.

The **Schedule** window appears.

**Step 3**
Click + **Add** at the upper right of the **Schedule** tab.

The **Create Backup** side panel appears.

**Step 4**
Enter a name for the backup file.

**Step 5**
Click the **Schedule Later** option.

**Step 6**
Enter the date for the scheduled backup or use the month icon to select a date.

**Step 7**
Enter a time for the scheduled backup including an AM or PM value.

**Step 8**
Click the **Schedule** button.

**Step 9**
Click the close icon at the upper right of the side panel to close the panel.
After scheduling a future backup, the following information is displayed:

- **Date**—Date of scheduled backup
- **Backup Name**—Name of the backup
- **Status**—Whether backup is scheduled or not
- **Operation**—Backup operation
- **Scheduled Run**—Date and time of scheduled backup
- **Action**—Option to delete scheduled backup

**Note**  
With the current release, you can only configure one scheduled backup at a time. Not more than one scheduled backup is permitted.

---

**What to do next**

When necessary and at the appropriate time, you can restore the backup files to DNA Center.
Schedule a Backup