



Set Up Cisco DNA Center to Use Assurance

- [Limitations and Restrictions of Assurance, on page 1](#)
- [Basic Setup Workflow, on page 1](#)
- [Discover Devices, on page 4](#)
- [Design Network Hierarchy, on page 18](#)
- [Manage Inventory, on page 37](#)
- [Add a Device to a Site, on page 43](#)
- [About Cisco ISE Configuration for Cisco DNA Center, on page 44](#)
- [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 48](#)
- [Configure Cisco AI Network Analytics, on page 49](#)
- [Update the Machine Reasoning Knowledge Base, on page 52](#)
- [Enable Localization, on page 53](#)

Limitations and Restrictions of Assurance

Assurance does not support devices that are connected through Network Address Translation (NAT).

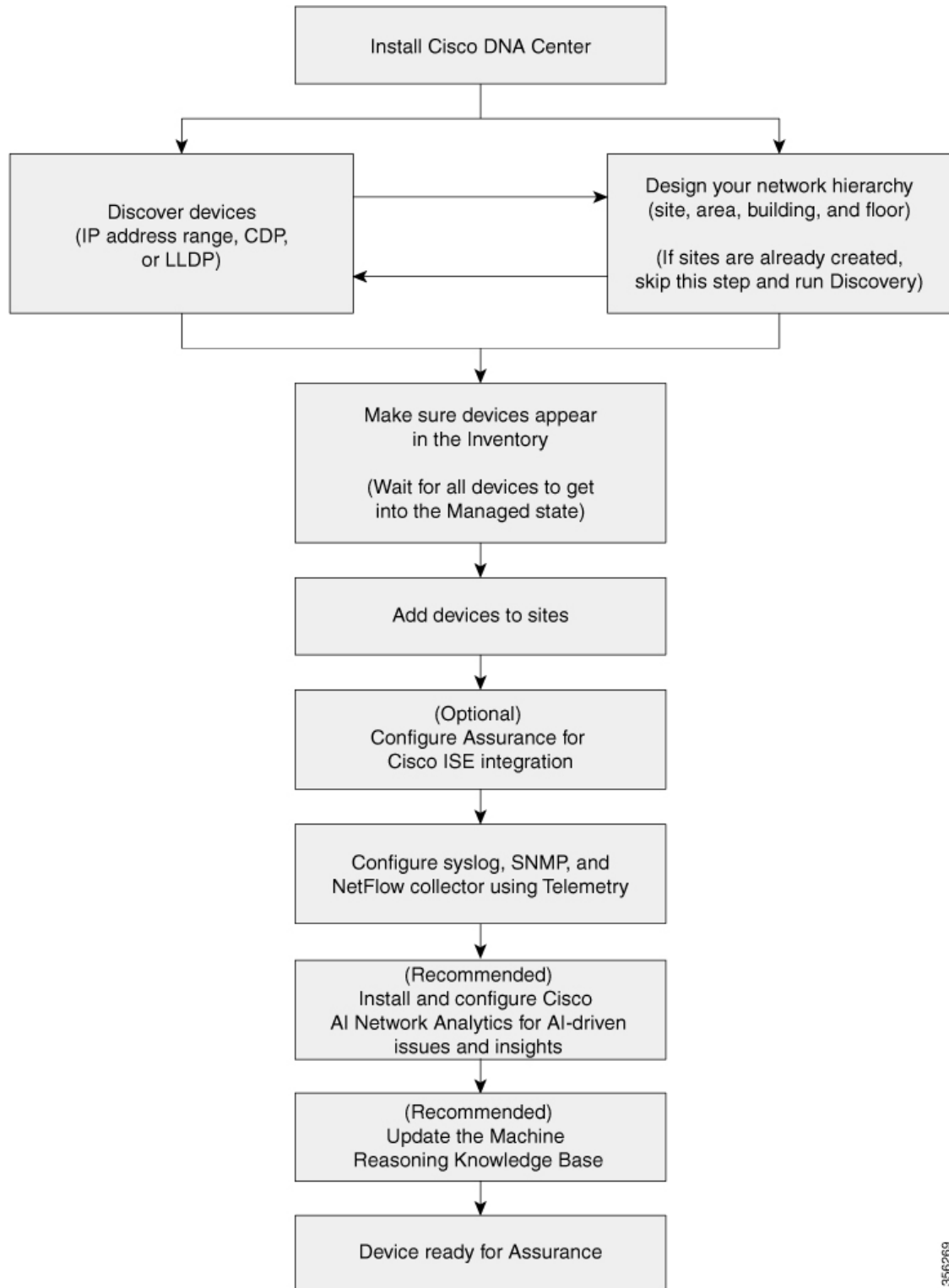
Basic Setup Workflow

Before you begin using the Assurance application, you must set up Cisco DNA Center to use Assurance.

This chapter provides the basic tasks you must do to set up Assurance. Use this chapter in conjunction with the [Cisco DNA Center User Guide](#).

See the following illustration and the procedure that follows to understand the basic workflow.

Figure 1: Basic Workflow for Setting Up Cisco DNA Center to Use Assurance



356269

Before you begin

See [Limitations and Restrictions of Assurance](#), on page 1.

- Step 1** Install Cisco DNA Center.
See the [Cisco DNA Center Installation Guide](#).
- Step 2** Do the following in any order:
- Discover devices (routers, switches, wireless controllers, and access points).
See [Discover Your Network Using an IP Address Range](#), on page 13, [Discover Your Network Using CDP](#), on page 11 and [Discover Your Network Using LLDP](#), on page 14.
Note Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.
 - Design a new network hierarchy or use an existing one.
See [Create a New Network Hierarchy](#), on page 18 or [Use an Existing Cisco Network Hierarchy](#), on page 21.
Note If sites are already created, you can skip this step and run Discovery.
- Step 3** Make sure that the devices appear in the device Inventory.
See [Display Information About Your Inventory](#), on page 38.
Note Before you add devices to sites, you must wait for all the devices to get into a Managed state.
- Step 4** Add devices to sites.
See [Add a Device to a Site](#), on page 43.
- Step 5** If you have APs, we recommend that you add them to a floor map.
- Step 6** If your network uses Cisco Identity Services Engine (ISE) for user authentication, you can configure Assurance for Cisco ISE integration. This enables you to see more information about wired clients, such as the username and operating system, in Assurance.
See [About Cisco ISE Configuration for Cisco DNA Center](#), on page 44.
- Step 7** Configure the syslog, SNMP traps, and NetFlow Collector servers using Telemetry.
See [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry](#), on page 48.
- Step 8** (Recommended) To view AI-driven issues and gain network insights, configure Cisco AI Network Analytics data collection.
See [Configure Cisco AI Network Analytics](#), on page 49.
- Step 9** (Recommended) To have access to the latest Machine Reasoning workflows, update the Machine Reasoning Knowledge Base.
See [Update the Machine Reasoning Knowledge Base](#), on page 52.

Step 10 Start using the Assurance application.

Discover Devices

Use the Cisco DNA Center Discovery feature to scan the devices in your network.

Discovery Overview

The Discovery feature scans the devices in your network and sends the list of discovered devices to inventory.

The Discovery feature also works with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the devices.

There are three ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.

When configuring the Discovery criteria, remember that there are settings that you can use to help reduce the amount of time it takes to discover your network:

- **CDP Level** and **LLDP Level**: If you use CDP or LLDP as the Discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. So, if fewer devices have to be discovered, you can set the level to a lower value.
- **Subnet Filters**: If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.
- **Preferred Management IP**: Whether you use CDP, LLDP, or an IP address range, you can specify whether you want Cisco DNA Center to add any of the device's IP addresses or only the device loopback address.



Note For Cisco SD-Access Fabric and Cisco DNA Assurance, we recommend that you specify the device loopback address.

Regardless of the method you use, you must be able to reach the device from Cisco DNA Center and configure specific credentials and protocols in Cisco DNA Center to discover your devices. These credentials can be configured and saved in the **Design > Network Settings > Device Credentials** window or on a per-job basis in the **Discovery** window.



Note If a device uses a first hop resolution protocol, such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory along with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that Cisco DNA Center retrieves for analysis.

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the [Cisco DNA Center Compatibility Matrix](#).
- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure that at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential.
- Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following criteria is met:
 - The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).
 - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see [Discovery Configuration Guidelines and Limitations, on page 6](#).

Preferred Management IP Address

When Cisco DNA Center discovers a device, it uses one of the device's IP addresses as the preferred management IP address. The IP address can be that of a built-in management interface of the device, another physical interface, or a logical interface such as Loopback0. You can configure Cisco DNA Center to use the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

When you choose **Use Loopback IP** as the preferred management IP address, Cisco DNA Center determines the preferred management IP address as follows:

- If the device has one loopback interface, Cisco DNA Center uses that loopback interface IP address.
- If the device has multiple loopback interfaces, Cisco DNA Center uses the loopback interface with the highest IP address.
- If there are no loopback interfaces, Cisco DNA Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.)
- If there are no Ethernet interfaces, Cisco DNA Center uses the serial interface with the highest IP address.

After a device is discovered, you can update the management IP address from the **Inventory** window.

Discovery Configuration Guidelines and Limitations

The following are the guidelines and limitations for Cisco DNA Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:

- Configure the CLI username and password with privileged EXEC mode (level 15). These credentials are the same CLI username and password that you configure in Cisco DNA Center for the Discovery function. Cisco DNA Center requires the highest access level to the device.
- Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
- Do not change the default login method for a device's console port and the VTY lines. If a device is already configured with a AAA (TACACS) login, make sure that the CLI credential defined in the Cisco DNA Center is the same as the TACACS credential defined in the TACACS server.
- Cisco wireless controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.

Discovery Credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, HTTP(S), and NETCONF configuration values for the devices that you want to discover. You must specify the credentials based on the types of devices you are trying to discover:

- Network devices: CLI and SNMP credentials.



Note For NETCONF-enabled devices such as embedded wireless controllers, you must specify SSH credentials with admin privilege and select the NETCONF port.

- Compute devices (NFVIS): CLI, SNMP, and HTTP(S) credentials.

Because the various devices in a network can have different sets of credentials, you can configure multiple sets of credentials in Cisco DNA Center. The discovery process iterates through all sets of credentials that are configured for the Discovery job until it finds a set that works for the device.

If you use the same credential values for the majority of devices in your network, you can configure and save them to reuse in multiple Discovery jobs. To discover devices with unique credentials, you can add job-specific Discovery credentials when you run Discovery jobs. You can configure up to 10 global credentials for each credential type and define any five of them. If you need to define a job-specific credential, you can define five global credentials and one job-specific credential for each credential type.

To define credentials for a Discovery, click the menu icon (≡) and choose **Tools > Discovery > Add Discovery**. To continue, use the following procedures and discovery credential information:

- [Discover Your Network Using CDP, on page 11](#)
- [Discover Your Network Using an IP Address Range, on page 13](#)
- [Discover Your Network Using LLDP, on page 14](#)

Table 1: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	<p>Password that is used to log in to the CLI of the devices in your network.</p> <p>For security reasons, re-enter the password as confirmation.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, re-enter the enable password.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Table 2: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Table 3: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.

Field	Description
Mode	<p>Security level that an SNMP message requires. Choose one of the following modes:</p> <ul style="list-style-type: none"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	<p>Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode.) Choose one of the following authentication types:</p> <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.
Auth. Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Discovery and Inventory features support only CISCOAES192 and CISCOAES256 privacy types. • Cisco DNA Assurance does not support any of these privacy types.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 4: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

Table 5: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .

Field	Description
Read	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

Table 6: NETCONF Setting

Field	Description
Port	<p>Port on the device. You can use one of the following ports:</p> <ul style="list-style-type: none"> • Port 830 (default). • Any other port that is available on the device. • A custom port that Cisco DNA Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the Cisco DNA Center Administrator Guide.)

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see [Discover Your Network Using an IP Address Range, on page 13](#) and [Discover Your Network Using LLDP, on page 14](#).




Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in [Discovery Prerequisites, on page 5](#).
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 Click the menu icon (☰) and choose **Tools > Discovery**.

Step 2 In the **Discovery** window, click  **Add Discovery**.
The window appears.

Step 3 In the **New Discovery** window, enter a name in the **Discovery Name** field.

Step 4 Expand the **IP Address/Range** area if it is not already visible, and configure the following fields:

- For **Discovery Type**, click **CDP**.
- In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
- (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$), where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.

d) Click .

Repeat Step c and Step d to exclude multiple subnets from the Discovery job.

e) (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, CDP level 3 means that CDP will scan up to three hops from the seed device.

f) For **Preferred Management IP**, choose one of the following options:

- **None:** Allows the device to use any of its IP addresses.
- **Use Loopback IP:** Specify the device's loopback interface IP address.

Note If you choose **Use Loopback IP** and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 5](#).

Note To use the loopback interface IP address as the preferred management IP address, make sure that the CDP neighbor's IP address is reachable from Cisco DNA Center.

Step 5 Expand the **Credentials** area and choose any of the global credentials that have already been created or configure your own.

If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.

Step 6 To configure your own credentials, click **Add Credentials**.

You must configure CLI and SNMP v2c credentials. All other credentials are optional. For field information, see [Discovery Credentials, on page 6](#).

To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 7 To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the names of the protocols that you want to use. A check mark indicates that the protocol is selected.

Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 8 Click **Start**.

- Note**
- You can configure up to five devices to be scheduled with recurrence.
 - The recurring discovery discovers only new devices. If a device is already present in Cisco DNA Center, it is not updated as part of discovery.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other Discovery methods, see [Discover Your Network Using CDP, on page 11](#) and [Discover Your Network Using LLDP, on page 14](#).

Before you begin


Your devices must have the required device configurations, as described in [Discovery Prerequisites, on page 5](#).

Step 1 Click the menu icon (☰) and choose **Tools > Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click  **Add Discovery**.
The **New Discovery** window appears.

Step 3 In the **Discovery Name** field, enter a name.

Step 4 Expand the **IP Address/Ranges** area, if it is not already visible, and configure the following fields:

- a) For **Discovery Type**, click **IP Address/Range**.
- b) In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Cisco DNA Center to scan, and click .

You can enter a single IP address range or multiple IP addresses for the discovery scan.

Note Cisco Wireless Controllers must be discovered using the Management IP address instead of the Service Port IP address. If not, the related wireless controller 360 and AP 360 pages will not display any data.

- c) (Optional) Repeat Step b to enter additional IP address ranges.
- d) (Optional) In the **Subnet Filter** field, enter an IP address/range or subnet to exclude from the Discovery scan. You can enter addresses either as an individual IP address ($x.x.x.x$) or as a classless interdomain routing (CIDR) address ($x.x.x.x/y$), where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.
- e) For **Preferred Management IP Address**, choose one of the following options:
 - **None**: Allows the device to use any of its IP addresses.
 - **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose **Use Loopback IP** and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 5](#).

Step 5 Expand the **Credentials** area and choose any of the global credentials that have already been created or configure your own.

If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.

Step 6 To configure your own credentials, click **Add Credentials**.

You must configure CLI and SNMP v2c credentials. All other credentials are optional. For field information, see [Discovery Credentials, on page 6](#).

To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 7 (Optional) To configure the protocols that are to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the protocols that you want to use. A check mark indicates that the protocol is selected.

Valid protocols are **SSH** (default) and **Telnet**.

b) Drag and drop the protocols in the order that you want them to be used.

Step 8 Click **Start**.

- Note**
- You can configure up to five devices to be scheduled with recurrence.
 - The recurring discovery discovers only new devices. If a device is already present in Cisco DNA Center, it is not updated as part of discovery.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Discover Your Network Using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see [Discover Your Network Using CDP, on page 11](#) and [Discover Your Network Using an IP Address Range, on page 13](#).





- Note**
- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
 - CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in [Discovery Prerequisites, on page 5](#).

- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

-
- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**. The **Discovery** window appears with dashlets.
- Step 2** Click  **Add Discovery**. The **New Discovery** window appears.
- Step 3** In the **Discovery Name** field, enter a name.
- Step 4** Expand the **IP Address/Range** area if it is not already visible, and configure the following fields:
- For **Discovery Type**, click **LLDP**.
 - In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
 - (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.
You can enter addresses either as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$), where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.
 - Click .
Repeat Step c and Step d to exclude multiple subnets from the Discovery job.
 - (Optional) In the **LLDP Level** field, enter the number of hops from the seed device that you want to scan.
Valid values are from 1 to 16. The default value is 16. For example, LLDP level 3 means that LLDP will scan up to three hops from the seed device.
 - For **Preferred Management IP**, choose one of the following options:
 - **None**: Allows the device use any of its IP addresses.
 - **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose this option and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 5](#).

Note To use the loopback interface IP address as the preferred management IP address, make sure that the LLDP neighbor's IP address is reachable from Cisco DNA Center.
- Step 5** Expand the **Credentials** area and choose any of the global credentials that have already been created or configure your own.
If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.
- Step 6** To configure your own credentials, click **Add Credentials**.
You must configure CLI and SNMP v2c credentials. All other credentials are optional. For field information, see [Discovery Credentials, on page 6](#).
To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 7 (Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

- a) Click the names of the protocols that you want to use. A check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.
- b) Drag and drop the protocols in the order that you want them to be used.

Step 8 Click **Start**.

- Note**
- You can configure up to five devices to be scheduled with recurrence.
 - The recurring discovery discovers only new devices. If a device is already present in Cisco DNA Center, it is not updated as part of discovery.

The **Discoveries** window displays the results of your scan.

The **Discovery Details** pane shows the status (active or inactive) and the Discovery configuration. The **Discovery Devices** pane displays the host names, IP addresses, and status of the discovered devices.

Manage Discovery Jobs

The following sections provide information about how to manage the Discovery jobs.

Stop and Start a Discovery Job

Step 1 Click the menu icon (☰) and choose **Tools > Discovery**.

Step 2 In the **Discovery** window, click **View All Discoveries**.

Step 3 To stop an active Discovery job, perform these steps:

- a) In the left pane, click a Discovery job.
- b) In the bottom pane, click **Stop**.

Step 4 To restart an inactive Discovery job, perform these steps:

- a) In the left pane, click a Discovery job.
- b) In the bottom pane, click **Re-discover**.

Clone a Discovery Job

You can clone a Discovery job and retain all the information defined for that job.

Before you begin

You should have run at least one Discovery job.

Step 1 Click the menu icon (☰) and choose **Tools > Discovery**.

Step 2 In the **Discovery** window, click **View All Discoveries**.

- Step 3** In the left pane, click a Discovery job.
- Step 4** In the bottom pane, click **Copy & Edit**.
Cisco DNA Center creates a copy of the Discovery job, named Clone of *Discovery_Job*.
- Step 5** (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.
- Step 6** Define or update the parameters for the new Discovery job.
-

Delete a Discovery Job

You can delete a Discovery job whether it is active or inactive.

- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** In the **Discovery** window, click **View All Discoveries**.
- Step 3** In the left pane, click the Discovery job that you want to delete.
- Step 4** In the bottom pane, click **Delete**.
- Step 5** Click **OK** to confirm.
-

View Discovery Job Information

You can view information about a Discovery job, such as the settings and credentials that were used. You also can view the historical information about each Discovery job that was run, including information about the specific devices that were discovered or that failed to be discovered.

Before you begin

Run at least one Discovery job.

- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** In the **Discovery** window, click **All discoveries page from previous release**.
- Step 3** In the left **Discoveries** pane, select the Discovery job. Alternatively, use the **Search** function to find a Discovery job by device IP address or name.
- Step 4** Click the down arrow next to one of the following areas for more information:
- **Discovery Details:** Displays the parameters that were used to run the Discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.
 - **Credentials:** Provides the names of the credentials that were used.
 - **History:** Lists each Discovery job that was run, including the time the job started, and whether any devices were discovered.

To successfully discover embedded wireless controllers, the NETCONF port must be configured. If the NETCONF port is not configured, wireless data is not collected.

Use the **Filter** function to display devices by any combination of IP addresses or ICMP, CLI, HTTPS, or NETCONF values.

Design Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. The hierarchical organization enables you to easily apply design settings or configurations to a specific hierarchical element. For example, you can apply design settings to an entire area or to only a floor.

You can name hierarchical elements to help you identify where to apply design settings later.

The hierarchical elements that you can create have rules that dictate under which elements they can reside and which elements can reside under them.

- **Global:** Default element under which all other hierarchical elements reside. are the only elements that can reside directly under **Global**.
- **Areas and Sites:** Areas and sites reside under **Global** or under other areas or sites. They do not have a physical address. As the largest element, they identify a geographic region. They provide a way to group areas and sites.
- **Buildings:** Buildings reside under areas or sites. When you create a building, you need to specify a physical address or latitude and longitude coordinates. Buildings can't contain areas. However, they can contain floors.
- **Floors:** Floors reside under buildings. You can add floors to buildings with or without maps that contain various building components, like walls and windows. If you decide to use floor maps, you can manually create them or import them from files, such as DXF, DWG, JPG, GIF, PNG, or PDF file types. Then you can position your wireless devices on the floor maps to visualize your wireless network coverage.

You can change the site hierarchy for unprovisioned devices while preserving AP locations on floor maps. Note, however, that you can't move an existing floor to a different building.

To get started, build your network hierarchy using one of the following methods:

- Create a new network hierarchy. For more information, see [Create a New Network Hierarchy, on page 18](#).
- Import an existing network hierarchy from Cisco Prime Infrastructure or Ekahau Pro. For more information, see the [Cisco DNA Center User Guide. Use an Existing Cisco Network Hierarchy, on page 21](#) or [Use an Existing Ekahau Network Hierarchy, on page 25](#).

Create a New Network Hierarchy

Create a new network hierarchy by creating new sites (or areas), building, and floors.

Create, Edit and Delete a Site

Cisco DNA Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the

same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

A world map appears in the right pane.

Step 2 From this window, you can add, edit, and delete sites. See the following table for details.

Action	Steps
Add a site.	<p>a. From the map toolbar, click + Add Site > Add Area.</p> <p>Alternatively, you can hover your cursor over the ellipsis ... next to the parent site in the left pane, and choose Add Area.</p> <p>b. In the Area Name field, enter the site name.</p> <p>The Area Name field has the following restrictions:</p> <ul style="list-style-type: none"> • The area name cannot exceed 40 characters. • Special characters & > < ? ' " / [] aren't allowed. <p>c. From the Parent drop-down list, choose a parent node. Global is the default parent node.</p> <p>d. Click Add.</p>
Edit a site.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the site and choose Edit Area.</p> <p>b. In the Edit Area dialog box, make the necessary edits.</p> <p>c. Click Update.</p>
Delete a site.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the site and choose Delete Area.</p> <p>b. Click OK.</p>

Add, Edit, and Delete a Building

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a building. See the following table for details.


Action	Steps
Add a building.	<p>a. In the Network Hierarchy window, click +Add Site > Add Building.</p> <p>Alternatively, you can hover your cursor over the ellipsis ... next to the parent site in the left pane, and choose Add Building.</p> <p>b. In the Add Building dialog box, add the building details.</p> <p>The Building Name field has the following restrictions:</p> <ul style="list-style-type: none"> • The building name cannot exceed 40 characters. • Special characters & < ? ' " / [] aren't allowed. <p>You can enter the address in the field or click the map. Adding an address causes the Longitude and Latitude coordinate fields to be automatically populated. These coordinates correspond to the northwest corner of the building and are used by location services, such as Cisco DNA Spaces or Cisco Connected Mobile Experiences (CMX), if they are integrated with Cisco DNA Center.</p> <p>c. Click Add.</p>
Edit a building.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the site and choose Edit Building.</p> <p>b. In the Edit Building dialog box, make the necessary edits.</p> <p>c. Click Update.</p>
Delete a building.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the building and choose Delete Building.</p> <p>b. Click OK.</p>

Add, Edit, and Delete a Floor

After you add a building, you can add floors to it. You can add a basic floor that doesn't have a floor map and add the floor map later, or you can add a floor and include a floor map at the same time.

To add a basic floor to a building, use this procedure.

To add a floor and a floor map at the same time, see the [Cisco DNA Center User Guide](#).

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a floor. See the following table for details.

Action	Steps
Add a basic floor.	<ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the desired building and choose Add Floor. b. In the Floor Name field, enter a name for the floor. The Floor Name field has the following restrictions: <ul style="list-style-type: none"> • The floor name cannot exceed 40 characters. • Special characters & > < ? ' " / [] aren't allowed. c. If you have wireless devices, for the Type (RF Model) drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated when computing 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. d. Configure the Floor Number, Floor Type and Floor Thickness fields. The floor type and thickness are used when calculating a heatmap for wireless devices. e. Skip uploading a floor map image in Floor Image area. f. Configure map dimensions in the Width, Length, and Height fields. g. Click Add.
Edit a floor.	<ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the floor and choose Edit Floor. b. In the Edit Floor dialog box, make the necessary changes. c. Click Update to save the changes.
Delete a floor.	<ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the floor and choose Delete Floor. b. Click Ok.

Use an Existing Cisco Network Hierarchy

If you have an existing network hierarchy in Cisco Prime Infrastructure, you can export it and then import it into Cisco DNA Center, saving time and effort spent in creating a new network hierarchy.

The following information is available for you to re-create your network hierarchy:

- **Site Hierarchy:** Your existing site hierarchy is downloaded in a CSV file format. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

- **Map Archive:** Map information is downloaded as a map archive in a TAR file format. The map archive file contains data such as the date and time, number of floors, and APs. Depending on what you choose to download, the map archive can also include map information, such as floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps. You can also choose to download calibration information, such as the RF attenuation model that has been applied to each floor.

You can choose to base the map archive on the global hierarchy or the hierarchy of a single site, building, or floor, as follows:

- **Site:** The chosen site and all of its subsites, buildings, and floors are exported.
- **Building:** The chosen building and all of its floors are exported.
- **Floor:** The chosen floor is exported.



Note Cisco DNA Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Cisco DNA Center image. By default, FIPS mode is disabled.

FIPS mode has the following impact on the export and import of map archives.

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.
- Both encrypted and unencrypted map archives can be imported.

For details, see the [Cisco DNA Center User Guide](#).

Export Your Site Hierarchy from Cisco Prime Infrastructure

You can export your site hierarchy from Cisco Prime Infrastructure in a CSV file format. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

Before you begin

Site hierarchy export is supported in Cisco Prime Infrastructure, Release 3.2 and later.

-
- Step 1** In Cisco Prime Infrastructure, choose **Inventory > Group Management > Network Device Groups**.
 - Step 2** In the **Device Groups** window, click **Export Groups**.
 - Step 3** In the **Export Groups** dialog box, click the **APIC-EM** radio button.
 - Step 4** To download the CSV file, click **OK**.

The CSV file is downloaded.

Export Your Map Archive from Cisco Prime Infrastructure

You can export map archive files from Cisco Prime Infrastructure and import them into Cisco DNA Center. Map archives contain map information, such as floor dimensions, and calibration information, such as the Radio Frequency (RF) attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

Step 1 From the Cisco Prime Infrastructure GUI, choose **Maps > Wireless Maps > Site Maps (New)**.

Step 2 From the **Export** drop-down list, choose **Map Archive**.

The **Export Map Archive** window opens, and the **Select Sites** window opens by default.

Step 3 Check the check box adjacent to a specific site, campus, building, or floor that you want to export. Alternatively, check the **Select All** check box to export all the maps.

Step 4 Select at least one of the following options:

- **Map Information:** Click the **On** button to export floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps.
- **Calibration Information:** Click the **On** button to export the RF attenuation model that has been applied to each floor. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must re-enter the calibration details manually.

If you choose to include calibration information, you also need to specify whether to include information for the selected maps or all the information, as follows:

- **Calibration Information for selected maps:** Calibration information for the selected site maps is exported.
- **All Calibration Information:** Calibration information for the selected map and any additional calibration information that is available in the system is exported.

Step 5 Click **Generate Map Archive**.

The following message shows the progress of the operation:

```
Exporting data is in progress
```

A TAR file is created and is saved to your local machine.

Step 6 Click **Done**.

Import Your Site Hierarchy to Cisco DNA Center

You can import a site hierarchy that you exported from Cisco Prime Infrastructure as a CSV file. For information about exporting the site hierarchy, see the [Cisco DNA Center User Guide](#).

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your Cisco DNA Center inventory. If not, discover them using the **Discovery** feature.

- Add and position APs on a floor map.
- If you manually created sites in Cisco DNA Center that are present in Cisco Prime Infrastructure, you must remove them from Cisco DNA Center before you can import them.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the map tool bar, click **Import** and choose **Import Sites**.

Step 3 In the dialog box, click one of the following radio buttons:

- **Merge with Existing Sites:** The downloaded site information is combined with the existing site information.
- **Overwrite Existing Sites:** If the same site already exists in Cisco DNA Center, the existing site information is overwritten with the downloaded site information.

Step 4 In the dialog box, drag and drop your CSV file into the download area. Alternatively, you can click **Choose a file** and navigate to where your CSV file is located, then click **Upload**.

Note If you do not have a CSV file, click **Download Template** to download a CSV file that you can edit and upload.

Import Your Map Archive to Cisco DNA Center

You can import a map archive TAR file into Cisco DNA Center. For example, you can upload the TAR file that you exported from Cisco Prime Infrastructure.



Note Cisco DNA Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Cisco DNA Center image. By default, FIPS mode is disabled.

For information about exporting site hierarchy, see [Export Your Map Archive from Cisco Prime Infrastructure, on page 23](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the map toolbar, click **Import** and choose **Import Maps**.

Step 3 In the **Import Maps** dialog box, drag and drop the map archive file.

Step 4 Click **Import**.

The map archive file is imported.

Use an Existing Ekahau Network Hierarchy

The Ekahau Pro tool allows you to create a complete network plan for your enterprise, including floor layout, AP locations, and obstacles. After creating the floor layout, you can export the simulated network plan as an Ekahau project file. You can also export the real-world site survey data into a format that Cisco DNA Center can use.

Export an Ekahau Project from Cisco DNA Center

You can export your network hierarchy from Ekahau Pro and import it into Cisco DNA Center for further planning.

Before you begin

Cisco DNA Center supports Ekahau Pro tool version 10.2.

-
- Step 1** In the Ekahau Pro tool, plan the floor layout:
- Create buildings and floors.
It is not mandatory to create buildings in the Ekahau Pro tool.
 - Import the floor plan.
 - Add the planned APs or hypothetical APs.
 - Add building coordinates.
 - Define the site name.
The AP name that you provide here will be used to update the AP name on the Cisco Wireless Controller during the wireless controller configuration.
 - Add obstacles.
 - Export the project.
- Step 2** Deploy the planned APs at locations designed on the floor layout.
- The physical AP is mounted at the designed location that is specified on the floor layout. The MAC address of the planned AP is updated with the MAC address of the physical AP.
 - The physical AP is connected to the VLAN of the intended wireless controller.
- Step 3** In Cisco DNA Center, configure the Cisco Wireless Controller .
- a. Discover the Cisco Wireless Controller and APs in your network by running the **Discovery** job, so that the discovered wireless controllers and APs are listed on the **Inventory** window.
 - b. Update the AP name on the wireless controller with the AP name given in the Ekahau Pro project during the floor planning.
- Step 4** Import the Ekahau project into Cisco DNA Center.

Step 5 Map the planned APs to real APs in Cisco DNA Center.

Import an Ekahau Project to Cisco DNA Center

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 Design your network hierarchy by adding sites, buildings, and floors.

Note For more information, see [Create, Edit and Delete a Site, on page 18](#), [Add, Edit, and Delete a Building, on page 19](#), and [Add, Edit, and Delete a Floor, on page 20](#).

While adding floors, make sure that you create floors with the same name given in the Ekahau project.

Step 3 In the left pane, hover your cursor over the ellipsis **...** icon next to the site where you want to import the Ekahau project and choose **Import Ekahau Project**.

The **Import Ekahau Project** dialog box appears.

Step 4 Drag and drop the ESX file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the ESX file.

Note To import buildings, they need to contain coordinates inside the Ekahau Project. You can add coordinates in Ekahau Pro. After successfully importing an Ekahau Project, each planned AP is mapped to an existing real AP in the inventory using the AP name. The planned AP is displayed with an icon **P** on the floor map. For example, if the name of the planned AP is SJC01-02-AP-B-1, the import process searches for the real AP with the same name.

Step 5 If an AP is not found in the inventory and remains unmapped, the planned AP is retained on the floor.

To see the reason for the mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.

The following attempts are made to map the planned APs to real APs:

- If the newly discovered APs match the planned AP, the planned AP is replaced with the discovered real AP.
- If a planned AP remains unmapped, you can manually replace the planned AP with the real AP, providing reasons for the failure.

Step 6 To manually assign the planned AP to a real AP, hover your cursor over the planned AP icon on the floor map, and click **Assign > Assign**.

The **Assign Planned APs** panel appears.

Step 7 In the **Assign Planned APs** panel, map the planned AP to a real AP by AP name, AP type, or All APs.

Step 8 Click the radio button next to the AP Name, and click **Assign** to manually assign the planned AP.

Step 9 Click **Save**.

Import an Ekahau Site Survey to Cisco DNA Center

You can upload an Ekahau site survey to create the buildings and floors in your network hierarchy. The site survey includes information about wireless devices, including the site, building, and floor to which it is assigned and its position on the floor map. However, it doesn't include the AP antenna information. So, you need to upload this information separately using a CSV file.

Cisco DNA Center includes a CSV template file that you can download and edit to define the required AP antenna information.

Figure 2: The CSV template file contains the following fields and defaults:

	A	B	C	D	E	F	G	H	I	J
1	model	antennaName0	antennaAzimuth0	antennaElevation0	antennaName1	antennaAzimuth1	antennaElevation1	antennaName2	antennaAzimuth2	antennaElevation2
2	AP2700I	Internal-2700-5GHz	90d	0d	Internal-2700-2.4GHz	90d	0d			
3	AP1850I	Internal-1850-5GHz	90d	0d	Internal-1850-2.4GHz	90d	0d			
4	AP3800E	AIR-ANT2524DB-R-5GHz	179.9543762d	0d	AIR-ANT2524DB-R-2.4GHz	179.9543762d	0d			
5										

If an AP isn't in the Cisco DNA Center device inventory, it's imported as a planned AP. However, you can use a naming convention so that when you add an AP to the device inventory, Cisco DNA Center can automatically convert it to an actual AP.

The naming convention is AP, followed by the last four digits of the AP's MAC address, for example, AP-c4:e0. Using this information, Cisco DNA Center attempts to match the provided digits with the last four digits of an AP's Ethernet MAC or radio MAC address. If this information isn't available or a match is unsuccessful, Cisco DNA Center attempts to match AP names.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 Click **Add Site > Add Area**.

Alternatively, you can hover your cursor over the ellipsis ... next to the parent site or **Global** in the left pane, and choose **Add Area**. For more information, see [Create, Edit and Delete a Site, on page 18](#).

Step 3 In the left pane, hover your cursor over the ellipsis ... icon next to the site you just created and choose **Import Ekahau Survey**.

Step 4 In the **Import Ekahau Survey** dialog box, drag and drop the Ekahau Survey file into the **Ekahau Survey** boxed area, or click the **Choose a file** link and browse to the ESX file.

Step 5 Drag and drop the CSV file into the **AP Mapping CSV** boxed area, or click the **Choose a file** link and browse to the CSV file.

Note If you do not have a CSV file, click **Download AP Mapping Template** to download a CSV file that you can edit and upload.

Step 6 Click **Import**.

After the files are successfully downloaded, a success message is displayed.

Step 7 Click **View Hierarchy** and navigate to the floors to verify that the devices have been imported and positioned properly. Hover the cursor over a device to view its details.

Configure 2D Floor Map Devices and Overlay Objects

In 2D maps, you can configure devices and overlay objects on your floor maps. The Cisco DNA Assurance User Guide provides basic guidance on working with 2D maps. In addition to 2D maps, Cisco DNA Center supports 3D maps with more capabilities. For a full description of both 2D and 3D map features, see the [Cisco DNA Center User Guide](#).

Devices

- **APs:** An access point (AP) serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In 2D maps, an AP represents an actual, installed device. For a list of APs that Cisco DNA Center supports, see the [Cisco DNA Center Compatibility Matrix](#).
- **Planned APs:** Planned APs are representations of APs that have not been installed yet. By placing planned APs on a map, you can envision your wireless network RF coverage and make changes before you actually install the APs.
- **Sensors:** A sensor is a dedicated Cisco Aironet 1800S Active Sensor that gets bootstrapped using Cisco PnP. After it obtains the Assurance server reachability details, it communicates directly with the Assurance server. For more details, including information about sensor tests, see the [Manage Sensors and Sensor-Driven Tests](#).

Overlay Objects

- **Coverage Areas:** By default, any area defined as part of a floor map is considered as a wireless coverage area. However, if you have a building that is nonrectangular or you want to mark a nonrectangular or polygon-shaped area on a floor, you can use the **Coverage Areas** drawing tool to create a coverage area.
- **Openings:** An opening, also called an atrium, is an open-air or skylight-covered area within a building. An opening can extend through multiple floors and can affect wireless signal coverage areas.
- **Location Regions:** Location regions define areas that are included in or excluded from the computation of heatmaps. Inclusion areas are included in the calculations, and exclusion areas are not included. For example, you might want to exclude areas such as openings, atriums, or stairwells within a building, but include a work area, such as cubicles, labs, or manufacturing floors.
- **Walls:** Walls are exterior or interior vertical structures in a building and can be made of different materials and thicknesses. As such, they affect how heatmaps are calculated.
- **Shelving Units:** Shelving units are obstacles that affects signal attenuation. An example of a location with shelving units would be a high-ceiling warehouse.
- **Markers:** A marker identifies a location on a map. When you create a marker, you can name it and position it to help you identify it later.
- **GPS Markers:** When integrated with Cisco DNA Center, location services, such as Cisco DNA Spaces or Cisco Connected Mobile Experiences (CMX), use GPS markers to calculate the approximate geographical location of clients.
- **Align Points:** Align points are markers that are used to position multiple floors that have different physical shapes. In 3D maps, floors are aligned at the top-left corner of the map (point 0,0). If you manage each floor independently, the misalignment is not a problem. However, to use some of the features of 3D maps, the floors need to be aligned as they are in reality. To compensate this misalignment, you can

insert one or more align points on two or more floors, so that the floors align properly one on top of the other in a 3D map.

Add, Position, Edit, and Remove APs

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left hierarchy tree, choose a floor.
- Step 3** From the map toolbar, click **2D > Add/Edit > APs**.
- Step 4** From this window, you can add, position, edit, and remove APs. See the following table for details.

Action	Steps
Add APs.	<ol style="list-style-type: none"> a. In the map left pane, click Add APs. b. Click Add next to the AP that you want to add, or to add multiple APs, check the check boxes next to APs you want to add and click Add Selected. Newly added APs appear in the Unpositioned category in the map left pane. c. From the Unpositioned category in the map left pane, click an AP. d. Click the location on the map where you want to position the AP.
Add planned APs.	<ol style="list-style-type: none"> a. From the map left pane, in the AP Models area, click the AP model of the planned AP that you want to add. If the AP model isn't listed, click Add Model and choose the AP model to add to the list. b. Click the location on the map where you want to place the planned AP. c. From the Edit Planned AP slide-in pane, click the gear icon and add a unique name pattern. d. Define the antenna type and the azimuth and elevation, if necessary. e. To continue to add planned APs with the same properties, click locations on the map. f. To stop adding planned APs, click Esc or right-click the floor map.

Action	Steps
Edit an AP.	<p>a. In the map, right click the AP and choose Edit.</p> <p>b. Change any of the editable AP settings. Note the information about the following fields:</p> <ul style="list-style-type: none"> • Antenna: For external APs, you must select an antenna, or the AP will not be present in the map. • Azimuth: The azimuth is the angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is 0 to 360. In Cisco DNA Center, pointing right is 0 or 360 degrees; pointing down is 90 degrees. You can manually enter the value or use the blue arrow under the field to change the value. For omnidirectional antennas, the azimuth is not relevant if the elevation is 0. • Elevation: You can manually enter the elevation in degrees or use the blue arrow under the field to change the value. For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values means pointing down. <p>c. Click Update.</p>
Remove an AP.	<p>a. Click the AP, or to select multiple APs, click the first AP and while pressing the Shift key, click the rest of the APs.</p> <p>b. In the Edit pane, click Remove Selected.</p> <p>c. From the map toolbar, click Save.</p>

Add, Position, and Remove Sensors

Before you begin

Make sure you have the Cisco AP 1800S sensor in your inventory. The Cisco Aironet 1800s Active Sensor must be provisioned using Plug and Play for it to show up in the Inventory.

- Step 1** Click the menu icon (☰) and choose .
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** From the map toolbar, click **2D > Add/Edit > Sensors**.
- Step 4** From this window, you can add, position, edit, and remove sensors. See the following table for details.

Action	Steps
Add sensors.	<p>a. From the Add Sensors slide-in pane, click Add next to the sensor that you want to add, or to add multiple sensors, check the check boxes next to sensors you want to add and click Add Selected.</p> <p>Newly added sensors appear in the Unpositioned category in the map left pane.</p> <p>b. From the Unpositioned category in the map left pane, click a sensor.</p> <p>c. Click the location on the map where you want to position the sensor.</p> <p>d. Click Save.</p>
Remove sensors.	<p>a. Click the sensor, or to select multiple sensors, click the first sensor and while pressing the Shift key, click the rest of the sensors.</p> <p>b. In the Edit pane, click Remove.</p> <p>c. From the map toolbar, click Save.</p>

Add, Edit, and Remove Coverage Areas

This procedure shows you how to mark a nonrectangular or polygon-shaped area as a coverage area on a floor map.

For more information about coverage areas, see [Configure 2D Floor Map Devices and Overlay Objects](#), on page 28.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > Coverage Areas**.

Step 4 To add a coverage area, do the following:

- a) In the **Coverage Area** dialog box, enter a name for the coverage area in the field.
- b) Click **Add Coverage**.
- c) Click on the map to create a point and initiate the drawing tool.
- d) Continue creating points to define the coverage area shape.

Note The coverage area shape must have at least three points. Click and drag a point to redefine the coverage area shape.

- e) Double-click to exit the drawing tool and finalize the coverage area shape.

Step 5 To edit a coverage area, do the following:

- a) In the map toolbar, click **Add/Edit > Coverage Areas**.
- b) To redefine the shape of a coverage area, click and drag a point.
- c) To edit a coverage area name, right-click the coverage area and choose **Edit**.

Step 6 To delete a coverage area, do the following:


- a) In the map toolbar, click **Add/Edit** > **Coverage Areas**.
- b) Right-click the coverage area and choose **Remove**.

Step 7 In the map toolbar, click **Save**.

Add, Edit, Copy, and Remove Openings

Creating an opening is similar to creating an open space or atrium on a floor. On multifloor buildings, typically the opening extends vertically through multiple floors. This procedure shows you how to add, edit, and remove openings on a floor map. It also shows you how to copy openings to other floors.

For more information about openings, see [Configure 2D Floor Map Devices and Overlay Objects, on page 28](#).

Step 1 Click the menu icon () and choose **Design** > **Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D** > **Add/Edit** > **Overlays** > **Openings**.

Step 4 To add an opening, do the following:

- a) From the left pane of the map, click **Opening**.
- b) Click on the map to create a point and initiate the drawing tool.
- c) Continue creating points to define the opening shape.

Note The opening shape must have at least three points. Click and drag a point to redefine the opening shape.

d) Double-click to exit the drawing tool and finalize the shape.

Step 5 To edit an opening, do the following:

- a) In the map toolbar, click **Add/Edit** > **Openings**.
- b) To redefine the shape of an opening, click and drag a point.
- c) To move an opening, click inside the shaded area. Then, drag and drop the opening where you want to place it.

Step 6 To copy an opening from one floor to another, do the following:

- a) In the map toolbar, click **Add/Edit** > **Openings**.
- b) Right-click the opening and choose **Copy to other floors**.
- c) In the dialog box, check the check boxes next to the relevant floors.
- d) Click **Copy**.
- e) Click **Close**.

Step 7 To remove an opening, do the following:

- a) In the map toolbar, click **Add/Edit** > **Openings**.
- b) Right-click the opening and choose **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, Edit, and Remove Location Regions

Location regions are areas on the map that are either included in or excluded from the heatmap calculation. The following topics show you how to add, edit, and remove location regions.

Add, Edit, and Remove an Inclusion Region

This procedure shows you how to add, edit, and remove an inclusion region. Use the following guidelines to define an inclusion region on a floor map:

- Inclusion regions can be any polygon-shaped area and must have at least three points.
- You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

For more information about inclusion regions, see [Configure 2D Floor Map Devices and Overlay Objects, on page 28](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Location Regions**.
- Step 4** In the left pane of the map, click the **Inclusion** icon.
- Step 5** To create an inclusion region, use the drawing tool:
- a) Click the map to create a point where you want the inclusion region to begin.
 - b) Move the cursor to the next point and click again.
 - c) Continue creating points to define the inclusion region shape.
 - d) To finalize the shape, double-click the map.
- Alternatively, from the left pane of the map, click the **Inclusion** icon.
- e) To exit the drawing tool, double-click the map again.
- Step 6** To edit the location of an inclusion region, drag and drop the shape to the new location.
- Step 7** To remove an inclusion region, right-click the shape and choose **Remove**.
- Step 8** In the map toolbar, click **Save**.
-

Add, Edit, and Remove an Exclusion Region

This procedure shows you how to add, edit, and remove an exclusion region. Use the following guidelines to define exclusion regions on a floor map:

- Exclusion regions can be any polygon-shaped area and must have at least three points.
- Exclusion regions are defined within the borders of an inclusion region.
- You can define multiple exclusion regions on a floor map.

For more information about exclusion regions, see [Configure 2D Floor Map Devices and Overlay Objects, on page 28](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Location Regions**.

- Step 4** From the left pane of the map, click the **Exclusion** icon.
- Step 5** To create an exclusion region, use the drawing tool:
- Click the map to create a point where you want the exclusion region to begin.
 - Move the cursor to the next point and click again.
 - Continue creating points to define the exclusion region shape.
 - To finalize the shape, double-click the map.
- Alternatively, from the map left pane, click the **Exclusion** icon.
- To exit the drawing tool, double-click the map again.
- Step 6** To edit the location of an exclusion region, drag and drop the shape to the new location.
- Step 7** To remove an exclusion region, right-click the shape and choose **Remove**.
- Step 8** In the map toolbar, click **Save**.
-

Add, Edit, and Remove Walls

This procedure shows you how to add, edit, move, and remove walls on a floor map.

For more information about walls, see [Configure 2D Floor Map Devices and Overlay Objects, on page 28](#).

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Walls**.
- Step 4** To add walls, do the following:
- In the left pane of the map, click a wall type from the **Others** or **On this floor** category.
- Note** If a wall type isn't listed, click **Add Wall Type** to create a custom wall type.
- Click the map to create a point where you want the wall to begin.
 - Move the cursor to the next point, where you want to end the wall or where you want to create a corner and click again.
 - Continue creating points to define the wall shape.
 - To end a wall, double-click the map.
- Alternatively, from the left pane, click the wall type.
- To exit the drawing tool, double-click the map again.
- Step 5** To change a wall type, and depending on the wall type also configure its parameters, do the following:
- Click the wall that you want to change.
- The **Wall Type** dialog box opens.
- From the **Wall Type** drop-down list, choose the type of wall.
 - Configure any other parameters that are appropriate for the new wall type.
 - Click **Update**.
- Step 6** To move a wall, do the following:
- Hover your cursor over the wall that you want to move.

The wall turns black, which means it's selected.

- b) Click the wall and drag and drop it to the new location.

Step 7 To remove a wall, right-click the wall and choose **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, Copy, Edit, and Remove Shelving Units

This procedure shows you how to add, copy, edit, and remove shelving units on a floor map.

For information about shelving units, see [Configure 2D Floor Map Devices and Overlay Objects](#), on page 28.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > Shelving Units**.

Step 4 To add shelving units, do the following:

- a) In the left pane of the map, click the shelving type you want to add.
- b) In the shelving dialog box, configure the name, dimensions, orientation, and whether the unit is double-sided, or leave the default values. Orientation means the angle of the shelving unit. A shelving unit with an orientation of 0 means that the shelving unit is vertical and parallel to the y-axis.

If a shelving type is not in the list, click **Add Shelving Type** to create a shelving type.

- c) Click **Add Shelving**.

The shelving unit is displayed on the map.

- d) Drag and drop the shelving unit to its location on the map.

Step 5 To create a copy or an array of a shelving unit, do one of the following:

- To create a copy, right-click the shelving unit and choose **Clone**.
- To create an array, right-click the shelving unit and choose **Array**. Then specify the number of units and the distance between them.

Step 6 To edit the name, dimensions, orientation, and whether it is two-sided, right-click the shelving unit and choose **Edit**.

Step 7 To remove a shelving unit, right-click the shelving unit and choose **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, Edit, and Remove Markers

The following procedure shows you how to add, edit, and remove markers.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.


- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Markers**.
- Step 4** In the left pane of the map, click the **Markers** icon.
- Step 5** In the **Place Markers** dialog box, enter the name for the marker, and click **Add Marker**.
- Step 6** To place the marker, click the map where you want to place the marker.
- Step 7** To move a marker, hover your cursor over the marker until it turns blue. Then drag and drop it in the new location.
- Step 8** To edit a marker, right-click the marker and choose **Edit**.
- Step 9** To remove a marker, right-click the marker and choose **Remove**.
- Step 10** In the map toolbar, click **Save**.

Add, Edit, and Remove GPS Markers

This procedure shows you how to add, edit, and remove GPS markers. For more information about GPS markers, see [Configure 2D Floor Map Devices and Overlay Objects, on page 28](#).



Note The GPS marker is an attribute of the building. You can apply it to all the floors of the building.

- Step 1** Click the menu icon () and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > GPS Markers**.
- Step 4** To add a GPS marker, do the following:
 - a) In the left pane of the map, click the **GPS Markers** icon.
 - b) On the map, click the location where you want to place the GPS marker.

GPS markers must be positioned inside the outer-perimeter walls, typically at the building corners.
 - c) In the **Place Markers** dialog box, enter the name, latitude, longitude, and the x and y coordinates in the appropriate fields.

The latitude and longitude coordinates of the GPS marker located in the northwest corner of a floor must match the building coordinates.
 - d) Click **Add GPS Marker**.
- Step 5** To edit a GPS marker, right-click the GPS marker and choose **Edit**.
- Step 6** To remove a GPS marker, right-click the GPS marker and choose **Remove**.
- Step 7** In the map toolbar, click **Save**.

Add, Edit, and Remove Align Points

This procedure shows you how to add, edit, and remove align points. For more information about align points, see [Configure 2D Floor Map Devices and Overlay Objects, on page 28](#).

- Step 1** Click the menu icon () and choose **Design > Network Hierarchy**.

- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Align Points**.
- Step 4** To add an alignment point, do the following:
- In the left pane of the map, click the **Align Points** icon.
 - On the map, click the location where you want to place the alignment point.
- Step 5** To edit the name of an alignment point, do the following:
- Right-click the alignment point and choose **Edit**.
 - Change the name and click **Edit Marker**.
- Step 6** To change the location of an alignment point, do the following:
- Right-click the alignment point and choose **Edit**.
 - Click **Edit Marker**.
 - Drag and drop the alignment point to the new location.
- Step 7** To remove an alignment point, right-click the alignment point and choose **Remove**.
- Step 8** In the map toolbar, click **Save**.
-

Manage Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

About Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

The Inventory feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device.

Inventory uses the following protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
- LLDP Media Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see [Discovery Prerequisites, on page 5](#).

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see [Update the Device Polling Interval, on page 38](#). Also, a configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes.


Update the Device Polling Interval

You can update the polling interval at the global level for all devices by choosing **System > 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

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

Step 1 Click the menu icon () and choose **Provision > Network Devices > Inventory**.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory > Edit Device**.

Step 4 In the **Edit Device** slide-in pane, click **Resync Interval**.

Step 5 Select the resync type.


- Note**
- To set the resync type as global, go to **System > Settings**.
 - The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Cisco DNA Center continues to use the device-specific polling time.

Step 6 In the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles.

Step 7 Click **Update**.

Display Information About Your Inventory

The **Inventory** table displays information for each discovered device. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

To choose which columns to display or to hide in the table, click . Note that the column selection does not persist across sessions.

When you select devices and choose a different view from the **Focus** drop-down list, your selection persists in each new view.

If you choose the **Default** view from the **Focus** drop-down list, the **Inventory** table displays only the **Device Name**, **IP Address**, **Device Family**, and **MAC Address** of the listed devices.

By default, 25 entries are shown in the **Inventory** table. Click **Show More** to view more entries. You can view up to 500 entries in the **Inventory** table.

If there are more than 25 entries in the **Inventory** table and you choose a different view from the **Focus** drop-down list, the same number of entries is displayed in each new view.

Before you begin

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

Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.


The **Inventory** window displays the device information gathered during the discovery process. The following table describes the information that is available.

Table 7: Inventory

Column	Description
Device Name	<p>Name of the device.</p> <p>Click the device name for more information about that device.</p> <p>Note A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.</p>
IP Address	IP address of the device.
Support Type	<p>Shows the device support level:</p> <ul style="list-style-type: none"> • Supported: The device pack is tested for all applications on Cisco DNA Center. You can open a service request if any of the Cisco DNA Center functionalities for these devices do not work. • Limited: The device pack for legacy devices is tested only for the following features on Cisco DNA Center. <ul style="list-style-type: none"> • Discovery • Topology • Device Reachability • Config Change Audit • Inventory • Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.) • Template Provisioning (Applicable only for switches.) <p>For more information, see the Cisco DNA Center Compatibility Matrix.</p> • Unsupported: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You can try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, you cannot raise a service request or a bug if Cisco DNA Center features do not work as expected. • Third Party: Device pack is built by customers or business partners and goes through the certification process. Third-party devices support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC provides an initial level of support for these devices. However, if there is a problem with the device pack, you need to contact the business partner.

Column	Description
Reachability	<p>The following is a list of the various statuses:</p> <ul style="list-style-type: none"> • Reachable: The device is reachable by Cisco DNA Center using SNMP, HTTP(S), and NETCONF polling. • Ping Reachable: The device is reachable by Cisco DNA Center using ICMP polling and not reachable using SNMP, HTTP(S), and NETCONF polling. • Unreachable: The device is not reachable using SNMP, HTTP(S), NETCONF, or ICMP polling.
EoX Status	<p>Shows the EoX scan status:</p> <ul style="list-style-type: none"> • Success: The device is scanned for EoX alerts successfully. • Not Scanned: The device is not scanned for EoX alerts. • Scan Failed: Cisco DNA Center is not able to scan the device for EoX alerts. • Scanning: Cisco DNA Center is scanning the device for EoX alerts. <p>Hover your cursor over the i icon next to EoX Status, and click Click here to accept to initiate an EoX scan.</p> <p>For the devices that are scanned successfully, the EoX Status column shows the number of alerts, if any.</p> <p>Click the number of alerts to view the alerts in detail.</p> <p>In the slide-in pane, click the Hardware, Software, and Module tabs to view the hardware, software, and module EoX alerts.</p>
Manageability	<p>Shows the device status:</p> <ul style="list-style-type: none"> • Managed with green tick icon: Device is reachable and is fully managed. • Managed with orange error icon: Device is managed with some error, such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. You can hover the cursor over the error message to view more details about the error and the impacted applications. • Unmanaged: Device cannot be reached and no inventory information was collected because of device connectivity issues.
MAC Address	MAC address of the device.
Image Version	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Uptime	Period of time for which the device has been up and running.

Column	Description
Device Role	<p>Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center is unable to determine a device role, it sets the device role to Unknown.</p> <p>Note If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.</p> <p>If required, you can use the drop-down list in this column to change the assigned device role.</p>
Site	<p>The site to which the device is assigned. Click Assign if the device is not assigned to any site. Click Choose a Site, select a site from the hierarchy, and click Save. For more information, see Design Network Hierarchy, on page 18.</p>
Last Updated	<p>Most recent date and time on which Cisco DNA Center scanned the device and updated the database with new information about the device.</p>
Device Family	<p>Group of related devices, such as routers, switches, hubs, or wireless controllers.</p>
Device Series	<p>Series number of the device, such as Cisco Catalyst 4500 Series Switches.</p>
Resync Interval	<p>The polling interval for the device. Set the resync interval from the Inventory window by choosing Actions > Edit Device > Resync Interval. To set the resync type as Global, from the main menu, choose System > Settings. For more information, see the Cisco DNA Center Administrator Guide.</p>
Last Sync Status	<p>Status of the last Discovery scan for the device:</p> <ul style="list-style-type: none"> • Managed: Device is in a fully managed state. • Partial Collection Failure: Device is in a partial collected state and not all the inventory information has been collected. Hover the cursor over the Information (i) icon to display additional information about the failure. • Unreachable: Device cannot be reached, and no inventory information was collected because of device connectivity issues. This condition occurs when periodic collection takes place. • Wrong Credentials: If device credentials are changed after adding the device to the inventory, this condition is displayed. • In Progress: Inventory collection is occurring.

Column	Description
Provisioning Status	<p>Shows the status of the last provisioning operation attempted on a device. Click See Details to view the status of past provisioning operations.</p> <ul style="list-style-type: none"> • Success: The latest operation on the device was successful. • Success with a warning icon: The latest operation on the device was successful, but there are failures from past provisioning operations that may need user attention. • Failed: The latest operation on the device has failed. • Failed with a warning icon: The latest operation on the device has failed and there are failures from past provisioning operations that may need user attention. • Configuring: The device is currently being configured. • Pending: The system is trying to determine if the device will be impacted by an ongoing provisioning operation. • Not Provisioned: The device has never been provisioned. • Out of Sync: The network settings or network profiles for a device have been modified after the last provisioning operation.
Credential Status	<p>Shows the device credential status:</p> <ul style="list-style-type: none"> • Not Applied: The device credential is not applied on the device. • Success: The device credential is applied on the device successfully. • Failed: The device credential failed on the device. <p>Click See Details to view the details about the credentials.</p> <p>The Credential Status slide-in pane shows the Type, Name/Description, Status, and Details of the credential.</p> <p>For a device whose status is Failed, hover the cursor over the ellipsis icon () in the Actions column and choose Retry or Clear.</p> <ul style="list-style-type: none"> • Retry: Applies the credential on the device. • Clear: Clears the device credential.
AP Ethernet Mac Address	Displays details about the AP Ethernet MAC address.
AP CDP Neighbors	Displays details about the switch and port connected to an AP in the inventory listing window. This window displays information about AP CDP neighbors even if the connected access switch is managed by Cisco DNA Center.

Delete a Network Device

You can delete devices from the Cisco DNA Center database, as long as they have not already been added to a site.

When you remove a wireless sensor from the inventory, the sensor is reset to the factory defaults so that when it rejoins, it gets the current configuration.


Before you begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** Check the check box next to the device or devices that you want to delete.
- Note** You can select multiple devices by checking additional check boxes, or you can select all the devices by checking the check box at the top of the list.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Delete Device**.
- Step 4** In the **Warning** window, check the **Config Clean-Up** check box to remove the network settings and telemetry configuration from the selected device.
- Step 5** Confirm the action by clicking **OK**.
-

Add a Device to a Site

Adding devices to a site configures Cisco DNA Center as the syslog and SNMP trap server, which enables Syslog Level 2 and configures global telemetry settings.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**. The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** Check the check box for the devices that you want to assign to a site.
- Step 3** From the **Actions** menu, choose **Provision > Assign Device to Site**.
- Step 4** In the **Assign Device to Site** slide-in pane, click the link next to the  icon for the device.
- Step 5** In the **Choose a floor** slide-in pane, select the floor to assign to the device and click **Save**.
- Step 6** (Optional) If you select multiple devices to add to the same location, check the **Apply to All** check box for the first device to assign its location to the rest of the devices and click **Next**.
- Step 7** Check **Application and Endpoint Visibility is enabled on all applicable devices. Check this to skip enabling it on all devices** check box.
- Note** **Application and Endpoint Visibility** enablement is skipped by default for the devices that does not support Controller-Based Application Recognition (CBAR) enablement or undeployed Application Visibility Service (AVS).

- Step 8** Review summary settings and click **Next**.
- Step 9** In the **Task Name** name field, enter a task name of your choice.
- Step 10** Choose whether you want to assign the device to a site **Now** or schedule it for later.
- Step 11** Click **Assign**.
- Step 12** To preview the CLI configuration, click the **Generate Configuration Preview** radio button and do the following:
- a. In the **Task Name** name field, enter a task name of your choice and click **Preview**.
Later, you can use the created configuration preview to deploy to the selected devices.
 - b. In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (≡) and choose **Activities > Work Items**.
 - c. In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
 - d. View the CLI configuration details and click **Deploy**.
 - e. To immediately deploy the device, click the **Now** radio button, and click **Apply**.
 - f. To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
 - g. In the confirmation window, click **Yes**.

Note The CLI task is marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.
- Step 13** When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.
From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled Device Controllability.

About Cisco ISE Configuration for Cisco DNA Center

If your network uses Cisco ISE for user authentication, you can configure Cisco DNA Center for Cisco ISE integration. This enables you to see more information about wired clients, such as the username and operating system.

Cisco ISE configuration is centralized within NCP (Network Control Platform), which enables you to configure Cisco ISE at one GUI location. The workflow for configuring Cisco ISE is as follows:

1. Click the menu icon (≡) and choose **System > Settings > External Services > Authentication and Policy Servers**, and enter the Cisco ISE server details.
2. After the Cisco ISE server is successfully added, NCP establishes a connection with NDP (Network Data Platform) and sends the details of the pxGrid nodes, keystore, and truststore files.
3. NDP uses the configuration received from NCP to establish a pxGrid session.
4. NCP automatically detects pxGrid node failovers, persona moves, and communicates it to NDP.

5. If there are ISE deployment changes, NDP starts a new pxGrid session with a new pxGrid ACTIVE node.

Configure Authentication and Policy Servers

Cisco DNA Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

Before you begin

- If you are using Cisco ISE to perform both policy and AAA functions, make sure that Cisco DNA Center and Cisco ISE are integrated.
- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
 - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.
 - Define an attribute name for Cisco DNA Center on the AAA server.
 - For a Cisco DNA Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.
- Before you configure Cisco ISE, confirm that:
 - You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the [Cisco DNA Center Compatibility Matrix](#). For information on installing Cisco ISE, see the [Cisco Identity Services Engine Install and Upgrade guides](#).
 - If you have a standalone ISE deployment, you must integrate Cisco DNA Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.



Note Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

- If you have a distributed Cisco ISE deployment:
 - You must integrate Cisco DNA Center with the primary policy administration node (PAN), and enable ERS on the PAN.



Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.


- You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.

- The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and PACs must also be defined in **Work Centers > Trustsec > Trustsec Servers > Trustsec AAA Servers**. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).
- You must enable communication between Cisco DNA Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Cisco DNA Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the Subject Alternative Name (SAN).
- The Cisco DNA Center system certificate must list both the Cisco DNA Center appliance IP address and FQDN in the SAN field.



Note For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue does not occur in Cisco ISE 3.0 and later. For more information, see the [Cisco ISE Release Notes](#).

Step 1 Click the menu icon () and choose **System > Settings > External Services > Authentication and Policy Servers**.

Step 2 From the **Add** drop-down list, choose **AAA** or **ISE**.

Step 3 To configure the primary AAA server, enter the following information:

- **Server IP Address:** IP address of the AAA server.
- **Shared Secret:** Key for device authentications. The shared secret can contain up to 100 characters.

Step 4 To configure a Cisco ISE server, enter the following details:

- **Server IP Address:** IP address of the ISE server.
- **Shared Secret:** Key for device authentications.
- **Username:** Username that is used to log in to the Cisco ISE CLI.

Note This user must be a Super Admin.

- **Password:** Password for the Cisco ISE CLI username.
- **FQDN:** Fully qualified domain name (FQDN) of the Cisco ISE server.

- Note**
- We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration > Deployment > Deployment Nodes > List**) and paste it directly into this field.
 - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

The FQDN consists of two parts, a hostname and the domain name, in the following format:

hostname.domainname.com

For example, the FQDN for a Cisco ISE server can be ise.cisco.com.

- **Virtual IP Address(es)**: Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

Step 5 Click **Advanced Settings** and configure the settings:

- **Connect to pxGrid**: Check this check box to enable a pxGrid connection.

If you want to use the Cisco DNA Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Cisco DNA Center system as a pxGrid client), check the **Use Cisco DNA Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same CA. If this option is disabled, Cisco DNA Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

When you enable this option, ensure that:

- The Cisco DNA Center certificate is generated by the same Certificate Authority (CA) as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
 - The Certificate Extended Key Use (EKU) field includes "Client Authentication."
- **Protocol**: **TACACS** and **RADIUS** (the default). You can select both protocols.
- Attention** If you do not enable TACAS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design > Network Settings > Network** when configuring a AAA server for network device authentication.
- **Authentication Port**: Port used to relay authentication messages to the AAA server. The default UDP port is 1812.
 - **Accounting Port**: Port used to relay important events to the AAA server. The default UDP port is 1813.
 - **Port**: The default TACACS port is 49.
 - **Retries**: Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
 - **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Note After the required information is provided, Cisco ISE is integrated with Cisco DNA Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window:

Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"
- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"
- **System 360** window: "Primary Available" and "pxGrid Available"

If the status of the configured Cisco ISE server is shown as "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.

Step 6 Click **Add**.

Step 7 To add a secondary server, repeat the preceding steps.

Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry

With Cisco DNA Center, you can configure global network settings when devices are assigned to a specific site. Telemetry polls network devices and collects telemetry data according to the settings in the SNMP server, syslog server, NetFlow Collector, or wired client.

Before you begin

Create a site and assign a device to the site. See [Create, Edit and Delete a Site, on page 18](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Telemetry**.

Step 2 In the **SNMP Traps** area, do one of the following:

- Check the **Use Cisco DNA Center as SNMP trap server** check box.
- Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server. The selected server collects SNMP traps and messages from the network devices.

Step 3 In the **Syslogs** area, do one of the following:

- Check the **Use Cisco DNA Center as syslog server** check box.
- Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

Step 4 In the **NetFlow** area, do one of the following:

- Click the **Use Cisco DNA Center as NetFlow collector server** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.

- Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.

Note Cisco DNA Center must be configured as a destination in Cisco Telemetry Broker to receive NetFlow records. If Cisco DNA Center is not configured as a destination, the Application Experience does not work.

Step 5 In the **Wired Endpoint Data Collection** area, click the **Enable Cisco DNA Center Wired Endpoint Data Collection At This Site** radio button to turn on IP Device Tracking (IPDT) on the access devices of the site.

If you don't want to enable IPDT for the site, click the **Disable** radio button (the default).

Note You must enable IPDT to preview the CLI configuration. When provisioning a device, you can preview the CLI configuration before deploying it on the device.

Step 6 In the **Wireless Controller, Access Point and Wireless Clients Health** area, check the **Enable Wireless Telemetry** check box to monitor the health of the wireless controllers, APs, and wireless clients in your network.

Step 7 Click **Save**.

Configure Cisco AI Network Analytics

Use this procedure to enable the Cisco AI Analytics features to exports network event data from network devices as well as inventory, site hierarchy, and topology data to the Cisco AI Cloud.

Before you begin

- Make sure that you have the Cisco DNA Advantage software license for Cisco DNA Center. The **AI Network Analytics** application is part of the Cisco DNA Advantage software license.
- Make sure that the latest version of the AI Network Analytics application is installed. See the "Download and Install Packages and Updates" topic in the [Cisco Digital Network Architecture Center Administrator Guide](#).
- Make sure that your network or HTTP proxy is configured to allow outbound HTTPS (TCP 443) access to the following cloud hosts:
 - **api.use1.prd.kairos.ciscolabs.com** (US East Region)
 - **api.euc1.prd.kairos.ciscolabs.com** (EU Central Region)

Step 1 Click the menu icon (☰) and choose **System > Settings**.

Step 2 Scroll down to **External Services** and choose **Cisco AI Analytics**.
The **AI Network Analytics** window appears.

AI Network Analytics

Using AI and Machine Learning, AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

[Configure](#)

[Recover from a config file](#) ⓘ

Step 3

Do one of the following:

- If you have an earlier version of Cisco AI Network Analytics installed in your appliance, do the following:

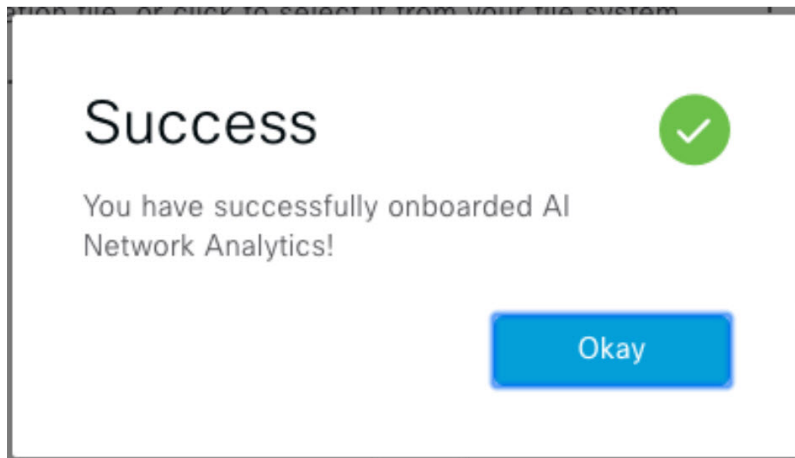
- a. Click **Recover from a config file**.

The Restore AI Network Analytics window appears.

- b. Drag-and-drop the configuration files in the area provided or choose the files from your file system.

- c. Click **Restore**.

Cisco AI Network Analytics might take a few minutes to restore, and then the **Success** dialog box appears.



- If this is the first time you are configuring Cisco AI Network Analytics, do the following:

- a. Click **Configure**.

- b. In the **Where should we securely store your data?** area, choose the location to store your data. Options are: **Europe (Germany)** or **US East (North Virginia)**.

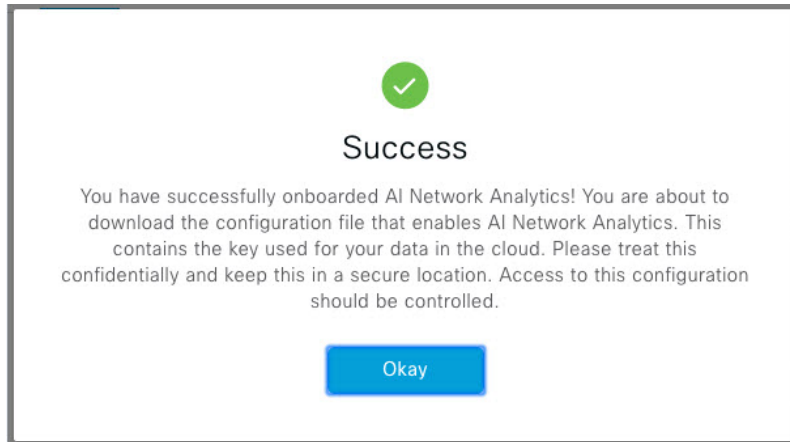
The system starts testing cloud connectivity as indicated by the **Testing cloud connectivity...** tab. After cloud connectivity testing completes, the **Testing cloud connectivity...** tab changes to **Cloud connection verified**.

- c. Click **Next**.

The terms and conditions window appears.

- d. Click the **Accept Cisco Universal Cloud Agreement** check box to agree to the terms and conditions, and then click **Enable**.

Cisco AI Network Analytics might take a few minutes to enable, and then the **Success** dialog box appears.



- Step 4** In the **Success** dialog box, click **Okay**.
The **AI Network Analytics** window appears, and the **Enable AI Network Analytics** toggle button displays .
- Step 5** (Recommended) In the **AI Network Analytics** window, click **Download Configuration** file.

Disable Cisco AI Network Analytics

To disable Cisco AI Network Analytics data collection, you must disable the AI Network Analytics feature, as follows:

- Step 1** Click the menu icon (☰) and choose **System > Settings**.
- Step 2** Scroll down to **External Services** and choose **Cisco AI Analytics**.
For each feature, a check mark () indicates that the feature is enabled. If the check box is unchecked (), the feature is disabled.
- Step 3** In the **AI Network Analytics** area, click the **Enable AI Network Analytics** toggle button so that it is unchecked ().
- Step 4** Click **Update**.
- Step 5** To delete your network data from the Cisco AI Network Analytics cloud, contact the Cisco Technical Response Center (TAC) and open a support request.
- Step 6** (Optional) If you have misplaced your previous configuration, click **Download configuration file**.

Update the Machine Reasoning Knowledge Base

Machine Reasoning knowledge packs are step-by-step workflows that are used by the Machine Reasoning Engine (MRE) to identify security issues and improve automated root cause analysis. These knowledge packs are continuously updated as more information is received. The Machine Reasoning Knowledge Base is a repository of these knowledge packs (workflows). To have access to the latest knowledge packs, you can either configure Cisco DNA Center to automatically update the Machine Reasoning Knowledge Base on a daily basis, or you can perform a manual update.

Step 1 Click the menu icon (☰) and choose **System > Settings**.

Step 2 Scroll down to **External Services** and choose **Machine Reasoning Knowledge Base**. The **Machine Reasoning Knowledge Base** window shows the following information:

- **INSTALLED:** Shows the installed version and installation date of the Machine Reasoning Knowledge Base package.

When there is a new update to the Machine Reasoning Knowledge Base, the **AVAILABLE UPDATE** area appears in the **Machine Reasoning Knowledge Base** window, which provides the **Version** and **Details** about the update.

- **AUTO UPDATE:** Automatically updates the Machine Reasoning Knowledge Base in Cisco DNA Center on a daily basis.
- **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY:** Integrates Cisco DNA Center with CX Cloud that allows you to perform an automated config. This integration provides enhanced vulnerability detection on devices directly from security advisories tool on Cisco DNA Center.

Step 3 (Recommended) Check the **AUTO UPDATE** check box to automatically update the Machine Reasoning Knowledge Base.

The **Next Attempt** area shows the date and time of the next update.

You can perform an automatic update only if Cisco DNA Center is successfully connected to the Machine Reasoning Engine in the cloud.

Step 4 To manually update the Machine Reasoning Knowledge Base in Cisco DNA Center, do one of the following:

- Under **AVAILABLE UPDATES**, click **Update**. A **Success** pop-up window appears with the status of the update.
- Manually download the Machine Reason Knowledge Base to your local machine and import it to Cisco DNA Center. Do the following:
 - a. Click **Download**.
The **Opening mre_workflow_signed** dialog box appears.
 - b. Open or save the downloaded file to the desired location in your local machine, and then click **OK**.
 - c. Click **Import** to import the downloaded Machine Reasoning Knowledge Base from your local machine to Cisco DNA Center.

Step 5 Check the **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY** check box to enable Cisco CX Cloud connection with network bug identifier and security advisory.



Step 6 In the **Security Advisories Settings** area click the **RECURRING SCAN** toggle button to enable or disable the weekly recurring scan.

Step 7 Click the **CISCO CX CLOUD** toggle button to enable or disable the Cisco CX cloud.

Enable Localization

You can view the Cisco DNA Center GUI windows in English (the default), Chinese, Japanese, or Korean. To change the default language, perform the following task:

Step 1 In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

- From Google Chrome, do the following:
 - a. Click the  icon in the top-right corner, and then choose **Settings**.
 - b. Click **Languages**.
 - c. Click **Add languages**.
 - d. In the **Add languages** dialog box, choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
- From Mozilla Firefox, do the following:
 - a. Click the  icon in the top-right corner, and then choose **Settings**.
 - b. From the **Language and Appearance > Language** area, click **Choose**.
 - c. From the **Select a language to add** drop-down list, choose **Chinese**, **Japanese**, or **Korean**.
 - d. Click **OK**.

Step 2 Log in to Cisco DNA Center.
The GUI is shown in the selected language.
