



Set Up Cisco DNA Center to Use Assurance

Before you begin using the Assurance application, you must configure Assurance. This chapter provides the basic tasks you must do to set up Assurance. Use this chapter in conjunction with the [Cisco Digital Network Architecture Center User Guide](#).

- [Limitations and Restrictions, on page 1](#)
- [Basic Setup Workflow, on page 1](#)
- [Discover Devices, on page 4](#)
- [Design Network Hierarchy, on page 23](#)
- [Manage Inventory, on page 43](#)
- [Add a Device to a Site, on page 51](#)
- [About Cisco ISE Configuration for Cisco DNA Center, on page 51](#)
- [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 55](#)
- [Configure Cisco AI Network Analytics Data Collection, on page 56](#)
- [Update the Machine Reasoning Knowledge Base, on page 58](#)
- [Enable Localization, on page 59](#)
- [Role-Based Access Control Support for Assurance, on page 61](#)

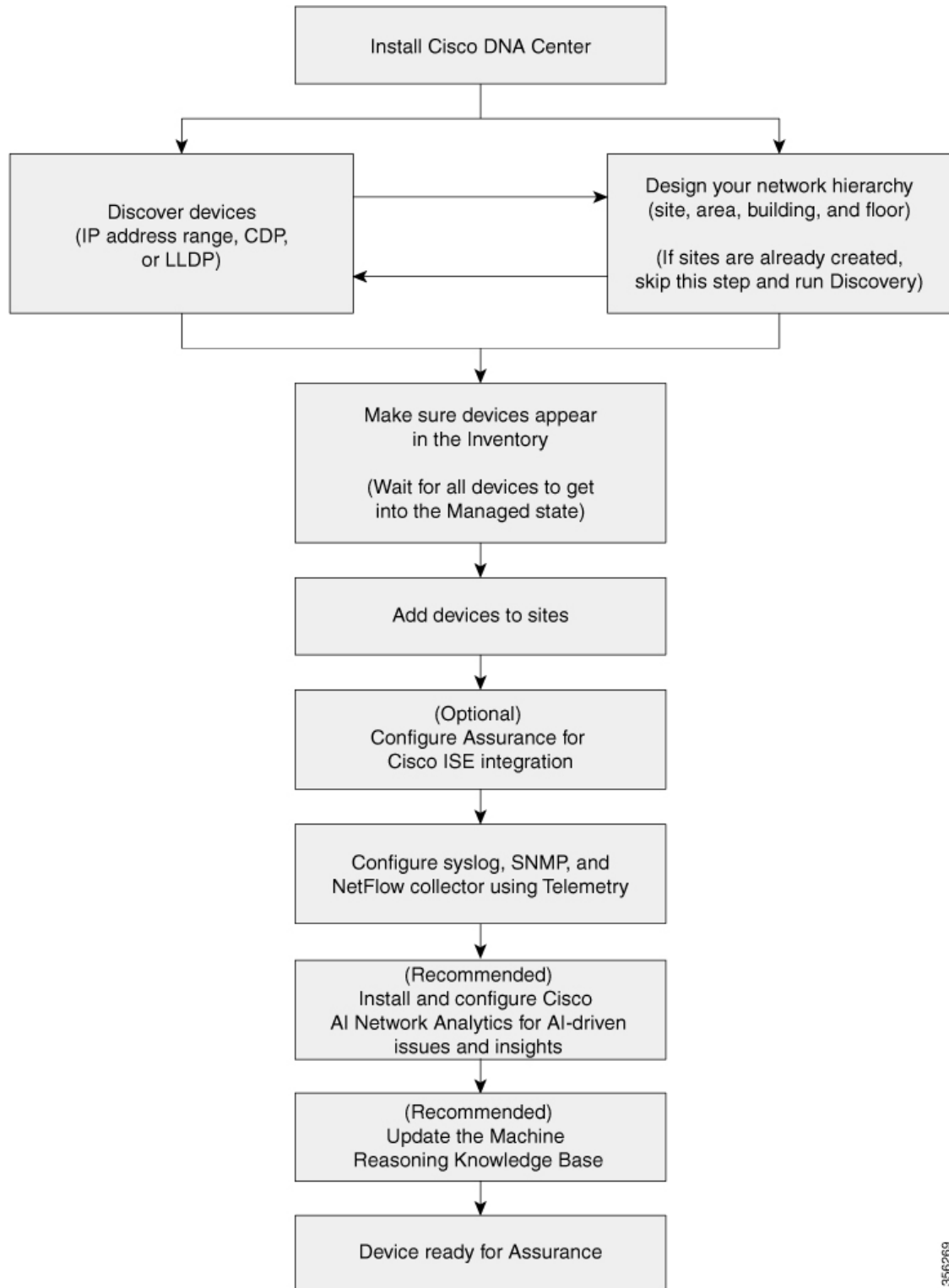
Limitations and Restrictions

Assurance is not supported over NATed connections to managed devices.

Basic Setup Workflow

Before you begin using the Assurance application, you must set up Cisco DNA Center to use Assurance. 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](#), 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 11, [Discover Your Network Using CDP](#), on page 6, or [Discover Your Network Using LLDP](#), on page 16.
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.
 - Design your network hierarchy. Configure the location of the device, such as area, site, building, and floor.
See [Create a Site in a Network Hierarchy](#), on page 24, [Add a Building](#), on page 25, and [Add a Floor to a Building](#), on page 26.
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 44.
Note 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 51.
- Step 5** If you are adding APs, we recommend that you assign and position them on a floor map.
See [Add, Position, and Delete APs](#), on page 31.
- Step 6** If your network uses Cisco Identity Services Engine 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 51.
- 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 55.
- 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 Data Collection](#), on page 56.
- 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 58.

Step 10 Start using the Assurance application.

Discover Devices

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

About Discovery

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

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

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's loopback address.



Note For Cisco SD-Access Fabric and Cisco DNA Assurance, we recommend that you specify the device's 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 like Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory 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 [Supported Devices List](#).
- 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 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). This is 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 pages will not display any data.

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 11](#) and [Discover Your Network Using LLDP, on page 16](#).




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**. 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:

- a) For **Discovery Type**, click **CDP**.
- b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
- c) (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 configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created or configure your own Discovery credentials. If you configure your own credentials, you can save them only for the current job by clicking **Save** or you can save them for the current and future jobs by checking the **Save as global settings** check box and then clicking **Save**.

- a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
- b) To add additional credentials, click **Add Credentials**.
- c) To configure CLI credentials, configure the following fields:

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>

Field	Description
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>

d) Click **SNMP v2c** and configure the following fields:

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>

e) (Optional) Click **SNMP v3** and configure the following fields:

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.
Mode	<p>Security level that an SNMP message requires. Choose one of the following modes:</p> <ul style="list-style-type: none"> • noAuthNoPriv: Does not provide authentication or encryption. • AuthNoPriv: Provides authentication, but does not provide encryption. • AuthPriv: Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.
Auth Password	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>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	Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: CBC mode AES for encryption. • None: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. <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.

- f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 4: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

- g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 5: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .
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 from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 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 from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 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>

- h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

- Note** To discover Cisco Catalyst 9800 Series Wireless Controller devices, you must enable NETCONF and set the port to one of the following:
- 830 (the default port number)
 - Any other port that is available on the device
 - A custom port that Cisco DNA Center configures (if Device Controllability is enabled)

NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices. NETCONF will be disabled if you choose **Telnet** in the **Advanced** area.

- Step 6** 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 green 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 7** Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** to cancel the scheduled discovery job before it starts.

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 6](#) and [Discover Your Network Using LLDP, on page 16](#).

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 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.
- 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 configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created or configure your own Discovery credentials. If you configure your own credentials, you can save them for only the current job by clicking **Save**, or you can save them for the current and future jobs by checking the **Save as global settings** check box and then clicking **Save**.

- a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
- b) To add additional credentials, click **Add Credentials**.
- c) To configure CLI credentials, configure the following fields:

Table 6: 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>

- d) Click **SNMP v2c** and configure the following fields:

Table 7: 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>

- e) (Optional) Click **SNMP v3** and configure the following fields:

Table 8: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv: Does not provide authentication or encryption. • AuthNoPriv: Provides authentication, but does not provide encryption. • AuthPriv: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.

Field	Description
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 AuthPriv as the authentication mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> AES128: CBC mode AES for encryption. None: No privacy.
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. 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.

- f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 9: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

- g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 10: 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 from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 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 from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 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>

- h) (Optional) If you have network devices with NETCONF enabled, click **NETCONF** and enter a port number in the **Port** field.

Note To discover Cisco Catalyst 9800 Series Wireless Controller devices, you must enable NETCONF and set the port to one of the following:

- 830 (the default port number)
- Any other port that is available on the device
- A custom port that Cisco DNA Center configures (if Device Controllability is enabled)

NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices. NETCONF will be disabled if you choose **Telnet** in the **Advanced** area.

Step 6 (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 green 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 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** if you want to cancel the scheduled discovery job before it starts.

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 6](#) and [Discover Your Network Using an IP Address Range, on page 11](#).




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 and configure the following fields:

- a) For **Discovery Type**, click **LLDP**.
- b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
- c) (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 **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.

- f) 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 configure the credentials that you want to use for the Discovery job.

Choose any of the global credentials that have already been created, or configure your own Discovery credentials. If you configure the credentials, you can choose to save them for future jobs by checking the **Save as global settings** check box.

- a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.
- b) To add additional credentials, click **Add Credentials**.
- c) For CLI credentials, configure the following fields:

Table 11: 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>

- d) Click **SNMP v2c** and configure the following fields:

Table 12: 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>

- e) (Optional) Click **SNMP v3** and configure the following fields:

Table 13: 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	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv: Does not provide authentication or encryption. • AuthNoPriv: Provides authentication, but does not provide encryption. • AuthPriv: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5: Authentication based on HMAC-MD5.
Auth Password	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>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	Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: CBC mode AES for encryption. • None: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. <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.

f) (Optional) Click **SNMP PROPERTIES** and configure the following fields:

Table 14: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout	Number of seconds between retries.

g) (Optional) Click **HTTP(S)** and configure the following fields:

Table 15: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .
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 from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 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>

Field	Description
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 from 7 to 128 characters, including at least one:</p> <ul style="list-style-type: none"> • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 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>

Step 6 (Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

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

Step 7 Click **Discover** and select whether to run the discovery now or schedule the discovery for a later time.

- To run the discovery now, click the **Now** radio button and click **Start**.
- To schedule the discovery for a later time, click the **Later** radio button, define the date and time, and click **Start**.

Click the notifications icon to view the scheduled discovery tasks. Click **Edit** to edit the discovery task before the discovery starts. Click **Cancel** if you want to cancel the scheduled discovery job before it starts.

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

Stop and Start a Discovery Job

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

The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

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

- a) From the **Discoveries** pane, select the corresponding job.
- b) Click **Stop**.

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

- a) From the **Discoveries** pane, select the corresponding job.
- b) Click **Re-discover** to restart the selected job.

Clone a Discovery Job

You can clone a Discovery job and retain all of 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**.

The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job.

Step 4 Click **Copy & Edit**.

Cisco DNA Center creates a copy of the Discovery job, named Copy of *Discovery_Job*.

Step 5 (Optional) Change the name of the Discovery job.

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**.

The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job that you want to delete.

Step 4 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**. The **Discovery** window appears with dashlets.
- Step 2** Click **View All Discoveries**.
- Step 3** From the **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 when 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. Your network hierarchy can contain sites, which contains buildings and areas.

Design a New Network Infrastructure

The **Design** area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the **Design** workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the **Discovery** feature. For more information, see [About Discovery, on page 4](#).

You can perform these tasks in the **Design** area:

-
- Step 1** Create your network hierarchy.
- Step 2** Define global network settings.

Step 3 Define network profiles.

About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. Your network hierarchy can contain sites, which in turn contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later. By default, there is one site called **Global**.

The network hierarchy has a predetermined hierarchy:

- **Areas** or **Sites** do not have a physical address, such as the United States. You can think of areas as the largest element. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea called California, and the subarea California can contain a subarea called San Jose.
- **Buildings** have a physical address and contain floors and floor plans. When you create a building, you must specify a physical address and latitude and longitude coordinates. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.
- **Floors** are within buildings and consist of cubicles, walled offices, wiring closets, and so on. You can add floors only to buildings.

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

The following is a list of tasks that you can perform:

- Create a new network hierarchy. For more information, see [Create a Site in a Network Hierarchy, on page 24](#).
- Upload an existing network hierarchy from Cisco Prime Infrastructure. For more information, see [Upload an Existing Site Hierarchy, on page 27](#).

Guidelines for Image Files to Use in Maps

- Use a graphical application that can save the map image files to any of these formats: .jpg, .gif, .png, .pdf, .dxf, and .dwg.
- Ensure that the dimension of an image is larger than the combined dimension of all the buildings and outside areas that you plan to add to the campus map.
- Map image files can be of any size. Cisco DNA Center imports the original image to its database at a full definition, but during display, it automatically resizes them to fit the workspace.
- Obtain the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.

Create a Site in a Network Hierarchy

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**.

Result: A world map appears in the right pane.

Step 2 From the map toolbar, click + **Add Site** and choose **Add Area**.

Note You can also hover your cursor over the ellipsis ... next to the parent site in the left pane, and then choose **Add Area**.

Step 3 Enter the site name in the **Area Name** field.

Note The **Area Name** field has the following restrictions:

- The area name cannot exceed 40 characters.
- Special characters & > < ? ' " / [] aren't allowed.

Step 4 From the **Parent** drop-down list, choose a parent node.

Note By default, **Global** is the parent node.

Step 5 Click **Add**.

Result: The site is created under the parent node in the left pane.

Add a Building

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

Step 2 In the **Network Hierarchy** window, click +**Add Site > Add Building**.

Note Alternatively, you can hover your cursor over the ellipsis ... next to the parent site in the left pane, and choose **Add Building**.

Step 3 Add the building details in the **Add Building** pop-up:

a) In the **Building Name** field, enter a name for the building.

Note The **Building Name** field has the following restrictions:

- The building name cannot exceed 40 characters.
- Special characters & > < ? ' " / [] aren't allowed.

b) From the **Parent** drop-down list, choose a parent node.

Note By default, **Global** is the parent node.

c) In the **Address** field, enter an address.


Note Alternatively, you can click on the map to input the address. Adding an address causes the **Longitude** and **Latitude** coordinates fields to be automatically populated. You can manually change the longitude and latitude coordinates to change the address.


Step 4 Click **Add**.

Result: The building is created and appears under the parent site in the left pane.

Add a Floor to a Building

After you add a building, you will need to create floors for it.

Step 1 Click the **Menu** icon  and choose **Design > Network Hierarchy**.

Step 2 In the left pane, hover your cursor over the ellipsis  next to the building of the floor and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Note The **Floor Name** field has the following restrictions:

- The floor name cannot exceed 40 characters.
- Special characters & > < ? ' " / [] aren't allowed.

Step 4 For the **Type (RF Model)** drop-down list, choose the RF model to apply for the floor.

Note The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 5 In the **Floor Image** area, drag and drop the floor plan file to upload the floor plan.

Note Cisco DNA Center supports the file types DXF, DWG, JPG, GIF, PNG, and PDF for floor plans.

Figure 2: Example of a Floor Plan



Note After you import a floor plan, make sure that you enable the overlay visibility (From the floor, click **View Options** and enable the overlay toggles in **Overlay Objects**). By default, overlays are not displayed after you import a map.

Step 6 If you upload a CAD file (DXF or DWG file type), use the **Floormap** pop-up to choose the CAD layers that you want to appear as floor elements in the map:

- For the **2D** column, check the check boxes of the CAD layer that you want to appear in the 2D view.
- For the **3D Wall/Shelving Type** column, use the drop-down list for a CAD layer to specify the type for the wall or shelving.

Note For a layer to appear in the 3D view, it is required to have a **3D Wall/Shelving Type** value. The wall/shelving type affects attenuation and how the heatmap is calculated.

- Click **Use Selected Layers**.

Step 7 Enter the floor map dimensions in the **Width**, **Length**, and **Height** fields.

Step 8 Click **Add**.

Manage Network Hierarchy

Upload an Existing Site Hierarchy

You can upload a CSV file or a map archive file that contains an existing network hierarchy. For example, you can upload a CSV file with location information that you exported from Cisco Prime Infrastructure. For information about exporting maps from Cisco Prime Infrastructure, see [Export Maps Archive](#), on page 28.



Note Before importing a map archive file into Cisco DNA Center, make sure that the devices such as Cisco Wireless Controllers and the associated APs are discovered and listed on the Cisco DNA Center inventory page.

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

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

Step 3 Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import**.

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

Step 4 To import the Cisco Prime Infrastructure maps tar.gz archive file, choose **Import > Map Import**.

Step 5 Drag and drop the map archive file into the boxed area in the **Import Site Hierarchy Archive** dialog box.

Step 6 Click **Save** to upload the file.

Result: The **Import Preview** window appears, which shows the imported file.

Export Maps Archive

You can export maps archive files from Cisco Prime Infrastructure and import them into Cisco DNA Center.

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

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

Step 3 On the **Select Sites** window, configure the following. You can either select map information or calibration information to be included in the maps archive.

- **Map Information:** Click the **On or Off** button to include map information in the archive.
- **Calibration Information:** To export calibration information, click the **On or Off** button. Click the **Calibration Information for selected maps** or the **All Calibration Information** radio button. If you select **Calibration Information for selected maps**, the calibration information for the selected site maps is exported. If you select **All Calibration Information**, the calibration information for the selected map, along with additional calibration information that is available in the system, is also exported.
- In the **Sites** left pane, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the **Select All** check box to export all the maps.

Step 4 Click **Generate Map Archive**. A message `Exporting data is in progress` is displayed.

Result: A tar file is created and is saved to your local machine.

Step 5 Click **Done**.

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

To search the tree hierarchy, in the **Find Hierarchy** search field in the left pane and enter either the partial or full name of the site, building, or floor name that you are searching.

Result: The tree hierarchy is filtered based on the text you enter in the search field.

Edit a Site

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
 - Step 2** In the left pane, hover your cursor over the ellipsis ... next to the site and choose **Edit Area**.
 - Step 3** In the **Edit Area** pop-up, make the necessary edits.
 - Step 4** Click **Update** to save your changes.
-

Delete a Site

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
 - Step 2** In the left pane, hover your cursor over the ellipsis ... next to the site and choose **Delete Area**.
 - Step 3** In the dialog box, click **OK** to confirm the deletion.
-

Edit a Building

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
 - Step 2** In the left pane, hover your cursor over the ellipsis ... next to the building and choose **Edit Building**.
 - Step 3** In the **Edit Building** pop-up, make the necessary edits.
 - Step 4** Click **Update** to save your changes.
-



Delete a Building

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
 - Step 2** In the left pane, hover your cursor over the ellipsis ... next to the building and choose **Delete Building**.
 - Step 3** In the dialog box, click **OK** to confirm the deletion.
-

Note Deleting a building deletes all its container maps. APs from the deleted maps are moved to Unassigned state.





Edit a Floor

After you add a floor, you can edit the floor map so that it contains obstacles, areas, and APs on the floor.

- Step 1** Click the **Menu** icon  and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, hover your cursor over the ellipsis  next to the floor and choose **Edit Floor**.
- Step 3** In the **Edit Floor** pop-up, make the necessary changes.
- Step 4** Click **Update** to save the changes.

Monitor a Floor Map in 2D

The floor view navigation pane provides access to multiple map functions like:

- Use the **Find** feature located at the top-right corner of the floor map window to find specific floor elements such as APs, sensors, clients, and so on. The elements that match the search criteria are displayed on the floor map along with a table in the right pane. When you hover your mouse over the table, it points to the search element on the floor map with a connecting line.
- Click the  icon at the top-right corner of the floor map window to:
 - Export a floor plan as a PDF.
 - Measure the distance on the floor map.
 - Set the scale to modify the floor dimensions.
- Click the  icon at the bottom-right of the floor map window to zoom in on a location. The zooming levels depend upon the resolution of an image. A high-resolution image might provide more zoom levels. Each zoom level comprises of a different style map shown at different scales, each one showing the corresponding details. Some maps are of the same style, but at a smaller or larger scale.
- Click the  icon to see a map with fewer details.
- Click the  icon to view the map icon legend.

Edit Floor Map Elements and Overlays

While viewing a floor map, click **Add/Edit** from the map toolbar to enter edit mode. While in edit mode, you can do the following:

Add, position, and delete the following devices:

- Access Points
- Sensors

Add, edit, and delete the following overlay objects:

- Coverage Areas
- Location Regions
- Walls
- Shelvings
- Markers
- GPS Markers

Guidelines for Placing Access Points

Follow these guidelines while placing APs on the floor map:

- Place APs along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. APs placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Therefore, location is difficult to determine. Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.
- For optimal heatmap visibility on floor maps, configure the AP height to approximately 10 feet (3 meters) or lower.

Add, Position, and Delete APs

Cisco DNA Center computes heatmaps for the entire map that show the relative intensity of the Radio Frequency (RF) signals in the coverage area. For 2D wireless maps, the heatmap is only an approximation of the actual RF signal intensity because it does not consider the RF signal reflection and other effects impacting the signal.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover APs using the Discovery feature. See [About Discovery](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
 - Step 2** In the left pane, click the building floor.
 - Step 3** From the map toolbar, click **Add/Edit**.
 - Step 4** Ensure the **APs** toggle is enabled from the map toolbar.
 - Step 5** From the map left pane, click **Add APs**.

Step 6 From the **Add APs** slide-in pane, check the check boxes of the access points to select the APs in bulk, and click **Add Selected**. Alternatively click **Add** next to an access point.

Note You can search for access points using the search option available. Use the **Filter** field to search for access points using the AP name, MAC address, model, or Cisco Wireless Controller. The search is case-insensitive. The search result appear in a table. Click **Add** to add one or more of these APs to the floor area.

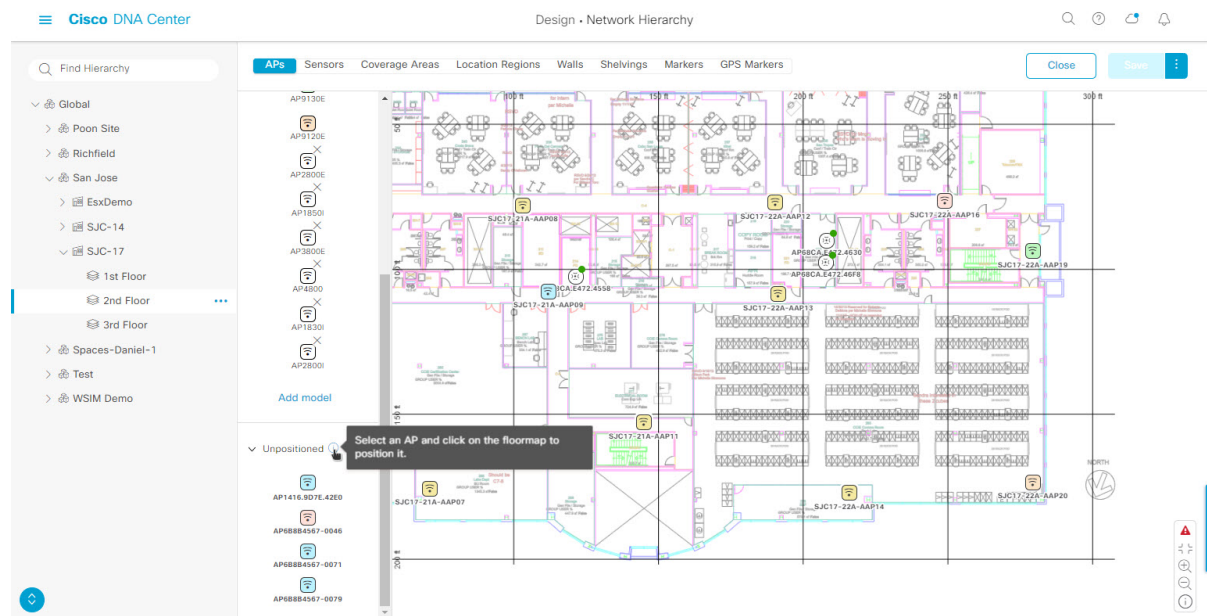
Result: Newly added APs appear in the **Unpositioned** category from the map left pane in edit mode.

Step 7 Close the **Add APs** window after assigning APs to the floor area.

Step 8 From the map toolbar, click **Add/Edit**.

Step 9 From the map left pane, click an AP from the **Unpositioned** category to position the AP.

Figure 3: Unpositioned APs



Step 10 To position the AP, do one of the following:

- Click on the location of the floor map to position the AP.
- From the **Edit AP** slide-in pane, enter the x and y coordinates in the corresponding fields.
- You can draw three points on the floor map and position the AP by using the selected points. To do this:
 - a. From the **Edit AP** slide-in pane, click **Position by 3 points**.
 - b. To define the points, click anywhere on the floor map to start drawing the first point. Click again to finish drawing a point. A dialog box appears to set the distance to first point. Enter the distance, in meters, and click **Set Distance**.
 - c. Define the second and third points similarly, and click **Save**.
- You can define two walls on the floor map and position APs between the defined walls. This helps you to know the position of APs between the two walls. This helps you to understand the AP position between the walls.
 - a. From the **Edit AP** slide-in pane, click **Position by 2 walls**.

- b. To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing a line. A dialog box appears to set the distance to the first wall. Enter the distance in meters and click **Set Distance**.
- c. Define the second wall similarly and click **Save**.

Result: The AP is placed automatically based on the defined distance between the walls.

Step 11 Use the **Edit AP** slide-in pane to configure details of the AP such as:

- **AP Name:** Shows the AP name.
- **MAC Address:** Displays the MAC address.
- **AP Model:** Indicates the AP model of the selected access point.
- **x:** Indicates the x-axis coordinate of the AP. You can manually enter the value.
- **y:** Indicates the y-axis coordinate of the AP. You can manually enter the value.
- **AP Height:** Indicates the height of the access point. You can manually enter the value.
- **Antenna:** Antenna type for this access point.

Note For external APs, you must select an antenna, or the AP will not be present in the map.

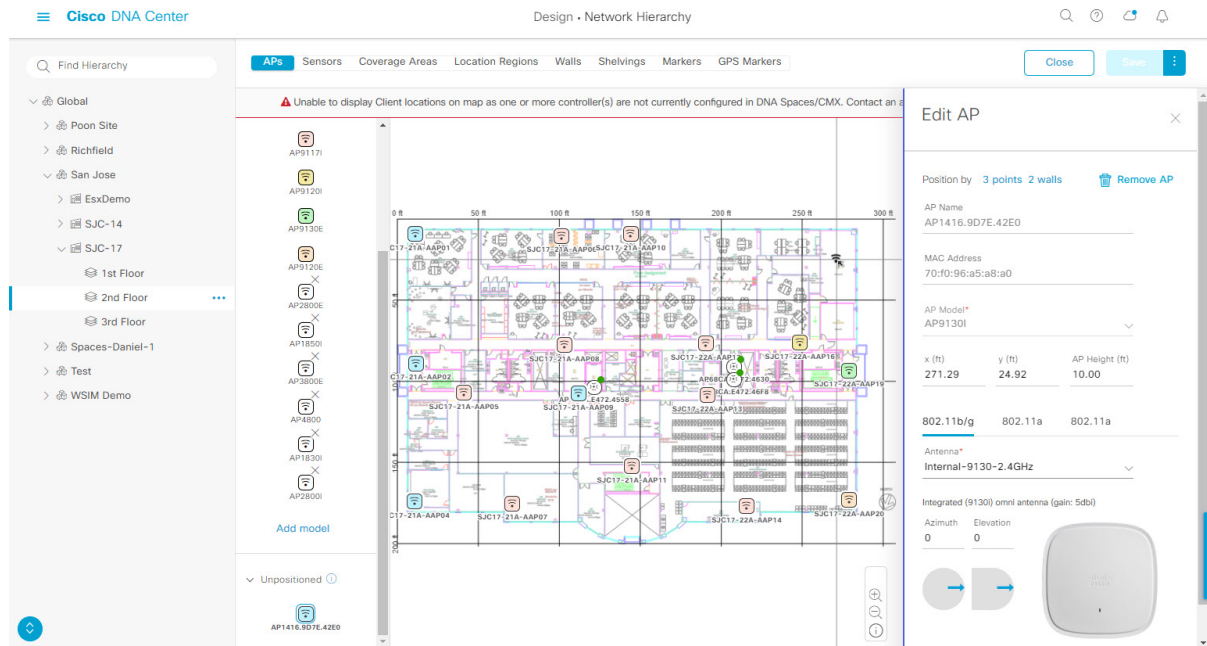
- **Azimuth:** The azimuth is the angle of the antenna measured relative to the x axis. The azimuth range is 0 to 360. In Cisco DNA Center, north is 0 or 360 degrees; east is 90 degrees.

You can manually enter the value or use the blue arrow under the field to change the value.

Note This option does not appear for omnidirectional antennas because their pattern is nondirectional in azimuth.

- **Elevation:** Displays the elevation in degrees. You can manually enter the value or use the blue arrow under the field to change the value.

Figure 4: Edit AP Slide-In Pane



Step 12 After you have completed placing and configuring access points, click **Save** from the map toolbar.

Note If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, you can view the location of clients on the heatmap. See [Create Cisco CMX Settings](#).

Result: The heatmap is generated based on the new position of the AP.

Step 13 To delete APs from the floor map, click **Remove APs** from the map left pane while in edit mode.

Step 14 From the **Delete APs** slide-in pane, check the check boxes next to the access points that you want to delete, and click **Delete Selected**.

- To delete all the access points, click **Select All** and then **Delete Selected**.
- To delete an access point from the floor, click the **Delete** icon.
- Use **Quick Filter** and search using the AP name, MAC address, model, or controller. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete the APs from the floor area.

Quick View of APs

Hover your cursor over the AP icon on the floor map to view AP details, Rx neighbor information, client information, and Device 360 information.

- Click **Info** to view the following AP details:
 - **Associated:** Indicates whether an AP is associated or not.
 - **Name:** AP name.
 - **MAC Address:** MAC address of the AP.

- **Model:** AP model number.
 - **Admin/Mode:** Administration status of the AP mode.
 - **Type:** Radio type.
 - **OP/Admin:** Operational status and AP mode.
 - **Channel:** Channel number of the AP.
 - **Antenna:** Antenna name.
 - **Azimuth:** Direction of the antenna.
- Click the **Rx Neighbors** radio button to view the immediate Rx neighbors for the selected AP on the map with a connecting line. The floor map also shows whether the AP is associated or not along with the AP name.
 - Click **Device 360** to get a 360° view of a specific network element (router, switch, AP, or Cisco wireless controller). See the *Monitor and Troubleshoot the Health of a Device* topic in the [Cisco DNA Assurance User Guide](#).



Note For Device 360 to open, you must have the Assurance application installed.

Add, Position, and Delete Sensors



Note 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. See the *Provision the Wireless Cisco Aironet 1800s Active Sensor* topic in the [Cisco DNA Assurance User Guide](#).

A *sensor device* is a dedicated AP 1800s sensor. The Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After it obtains the Assurance server reachability details, it directly communicates with the Assurance server.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, click the building floor.
- Step 3** From the map toolbar, click **Add/Edit**.
- Step 4** From the map toolbar, click the **Sensors** toggle.
- Step 5** From the **Add Sensors** slide-in pane, check the check boxes of the sensors that you want to add. Alternatively, click **Add** next to the sensor row to add sensors.
- Note** You can search for specific sensors using the search option. Use the **Filter** field and search using the name, MAC address, or model of a sensor. The search is case-insensitive. The search results are displayed in the table. Click **Add** to add one or more these sensors to the floor area.
- Result:** Newly added sensors appear in the **Unpositioned** category from the map left pane in edit mode.
- Step 6** Close the **Add Sensors** slide-in pane after assigning sensors to the floor map.

Add Coverage Areas

- Step 7** From the map toolbar, click **Add/Edit**.
- Step 8** From the map left pane, click a sensor in the **Unpositioned** category to position the sensor.
- Step 9** Click on the location of the floor map to position the sensor.
- You can use the **x**, **y**, and **sensorHeight** fields in the **Sensor Details** slide-in pane to enter the exact x, y, and z coordinates for the sensor.
- Step 10** After you have completed placing and adjusting sensors, click **Save**.
- Step 11** To delete a sensor from the floor map, click **Remove APs** from the map left pane while in edit mode.
- Step 12** Check the check boxes of the sensors that you want to delete, and click **Delete Selected**.
- To delete all the sensors, click **Select All**, and click **Delete Selected**.
 - To delete a sensor from the floor, click the **Delete** icon next to that sensor.
 - Use **Quick Filter** and search using the name, MAC address, or model. The search is case-insensitive. The search results are displayed in a table. Click the **Delete** icon to delete one or more sensors from the floor area.

Add Coverage Areas

By default, any floor area or outside area defined as part of a building map is considered as a wireless coverage area.

If you have a building that is nonrectangular or you want to mark a nonrectangular area within a floor, you can use the map editor to draw a coverage area or a polygon-shaped area.

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, click the building floor.
- Step 3** From the map toolbar, click **Add/Edit**.
- Step 4** From the map toolbar, click the **Coverage Areas** toggle.
- Step 5** From the map left pane, click the **Coverage Area** icon.
- Step 6** In the **Coverage Area** pop-up window, enter a name for the coverage area in the field and click **Add Coverage**.
- Step 7** Use the drawing tool to create the coverage area shape:
- Click on the map to create a point and continue creating points to define the coverage area shape.
- Note** The coverage area shape must have at least 3 points.
- You can click and drag any points to redefine the coverage area shape.
 - Double-click to exit the drawing tool and finalize the coverage area shape.
- Step 8** After you can finish creating the coverage area, click **Save** from the map toolbar.
- Step 9** To edit a coverage area, do the following:
- From the map toolbar, click **Add/Edit**.
 - From the map toolbar, click the **Coverage Areas** toggle.
 - You can click and drag the points of the coverage area to redefine the shape.
 - To edit the coverage area name, right-click a coverage area and choose **Edit**.
 - After finishing making edits, click **Save** from the map toolbar.

- Step 10** To delete a coverage area, do the following:
- From the map toolbar, click **Add/Edit**.
 - From the map toolbar, click the **Coverage Areas** toggle.
 - Right-click the coverage area and choose **Delete**.
 - After finishing deleting, click **Save** from the map toolbar.
-

Create Obstacles

You can create obstacles so that they can be considered while computing Radio Frequency (RF) prediction heatmaps for access points.

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, select the floor.
- Step 3** Click **Edit**, which is located above the floor plan in the middle pane.
- Step 4** In the **Overlays** panel, next to **Obstacles**, click **Add**.
- Step 5** In the **Obstacle Creation** dialog box, choose an obstacle type from the **Obstacle Type** drop-down list. The type of obstacles that you can create are **Thick Wall**, **Light Wall**, **Heavy Door**, **Light Door**, **Cubicle**, and **Glass**. The estimated signal loss for the obstacle type you selected is automatically populated. The signal loss is used to calculate RF signal strength near these objects.
- Step 6** Click **Add Obstacle**.
- Step 7** Move the drawing tool to the area where you want to create an obstacle.
- Step 8** Click the drawing tool to start and stop a line.
- Step 9** After you have outlined the area, double-click the area to highlight it.
- Step 10** In the **Obstacle Creation** window, click **Done**.
- Step 11** Click **Save** to save the obstacle on the floor map.
- Step 12** To edit an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Edit**.
All the available obstacles are highlighted on the map.
- Step 13** Click **Save** after the changes.
- Step 14** To delete an obstacle, in the **Overlays** panel, next to **Obstacles**, click **Delete**.
All the available obstacles are highlighted on the map.
- Step 15** Hover your cursor over the obstacle and click to delete.
- Step 16** Click **Save**.
-

Location Region Creation

You can create inclusion and exclusion areas to further refine location calculations on a floor. You can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building, but include a work area, such as cubicles, labs, or manufacturing floors.

Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map

- Inclusion and exclusion areas can be any polygon-shaped area and must have at least 3 points.
- You can only define 1 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.
- You can define multiple exclusion regions on a floor area.

Define an Inclusion Region on a Floor

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, click a building floor.
- Step 3** From the map toolbar, click **Add/Edit**.
- Step 4** From the map toolbar, click the **Location Regions** toggle.
- Step 5** From the map left pane, click the **Inclusion** icon.
- Step 6** Use the drawing tool to create the inclusion area:
- Click on the map to create point and continue creating points until you have created the shape for the inclusion area.
 - To finalize the shape, click the **Inclusion** icon from the left pane to exit drawing mode. Alternatively, you can double-click on the map to finalize the shape. If you want to cancel the shape, right-click on the map.
 - To move an existing inclusion area, drag and drop the shape to the new location.
 - To remove an existing inclusion area, right-click the shape and choose **Delete**.
- Step 7** After you are finish creating inclusion areas, click **Save** from the map toolbar.
-

Define an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are defined within the borders of an inclusion area.

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, click a building floor.
- Step 3** From the map toolbar, click **Add/Edit**.
- Step 4** From the map toolbar, click the **Location Regions** toggle.
- Step 5** From the map left pane, click the **Exclusion** icon.
- Step 6** Use the drawing tool to create the exclusion area:
- Click on the map to create point and continue creating points until you have created the shape for the exclusion area.
 - To finalize the shape, click the **Exclusion** icon from the left pane to exit drawing mode. Alternatively, you can double-click on the map to finalize the shape. If you want to cancel the shape, right-click on the map.
 - To move an existing exclusion area, drag and drop the shape to the new location.

- To remove an existing exclusion area, right-click the shape and choose **Delete**.

Step 7 After you are finish creating exclusion areas, click **Save** from the map toolbar.

Edit Location Regions

Step 1 In the **Overlays** panel, next to **Location Regions**, click **Edit**.
The available location regions are highlighted on the map.

Step 2 Make the necessary changes, and click **Save**.

Delete Location Regions

Step 1 In the **Overlays** panel, next to **Location Regions**, click **Delete**.
The available location regions are highlighted on the map.

Step 2 Hover your cursor over the region that you want to delete, and click **Delete**.

Step 3 Click **Save**.

Create a Rail

You can define a rail line on a floor that represents a conveyor belt. Also, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

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

Step 2 In the left pane, select the floor.

Step 3 Click **Edit**, which is located above the floor plan in the middle pane.

Step 4 In the **Overlays** panel, next to **Rails**, click **Add**.

Step 5 Enter a snap-width (feet or meters) for the rail, and click **Add Rail**.

A drawing icon appears.

Step 6 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 7 Click the drawing icon twice when the rail line is drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

Step 8 Click **Save**.

Step 9 In the **Overlays** panel, next to **Rails**, click **Edit**.

The available rails are highlighted on the map.

Place Markers

- Step 10** Make changes, and click **Save**.
- Step 11** In the **Overlays** panel, next to **Rails**, click **Delete**.
All the available rail lines are highlighted on the map.
- Step 12** Hover your cursor over the rail line that you want to delete, and click **Delete**.
- Step 13** Click **Save**.

Place Markers

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** In the left pane, click a building floor.
- Step 3** From the map toolbar, click **Add/Edit**.
- Step 4** From the map toolbar, click the **Markers** toggle.
- Step 5** Enter the name for the marker, and then click **Add Marker**.
- Step 6** Use the drawing tool to place the marker:
- Click on the map to place the marker.
 - To move the marker,
 - To edit an existing marker, right-click the marker and choose **Edit**.
 - To remove an existing marker, right-click the marker and choose **Delete**.
- Step 7** Click **Save** from the map toolbar.

Floor View Options

Click the **View Options**, which is located above the floor plan in the middle pane. The floor map along with these panels appear in the right pane: **Access Points**, **Sensor**, **Overlay Objects**, **Map Properties**, and **Global Map Properties**.

You can modify the appearance of the floor map by selecting or unselecting various parameters. For example, if you want to view only the access point information on the floor map, check the **Access Point** check box. You can expand each panel to configure various settings available for each floor element.

View Options for Access Points

To view access points on a map, click the **On/Off** button next to **Access Points**. Expand the **Access Points** panel to configure these settings:

- **Display Label:** From the drop-down list, choose a text label that you want to view on the floor map for the AP. The available display labels are:
 - **None:** No labels are displayed for the selected access point.
 - **Name:** AP name.
 - **AP MAC Address:** AP MAC address.

- **Controller IP:** IP address of Cisco Wireless Controller to which the access point is connected.
 - **Radio MAC Address:** Radio MAC address.
 - **IP Address**
 - **Channel:** Cisco Radio channel number or **Unavailable** (if the access point is not connected).
 - **Coverage Holes:** Percentage of clients whose signal has become weaker until the client lost its connection. It shows **Unavailable** for access points that are not connected and **MonitorOnly** for access points that are in monitor-only mode.
 - **TX Power:** Current Cisco Radio transmit power level (with 1 being high) or **Unavailable** (if the access point is not connected). If you change the radio band, the information on the map changes accordingly.

The power levels differ depending on the type of access point. The Cisco Aironet 1000 Series Lightweight Access Point accepts a value between **1** and **5**; the Cisco Aironet 1230AG Series Access Point accepts a value between **1** and **7**; and the Cisco Aironet 1240AG Series Access Point and Cisco Aironet 1100 Series Access Point accept a value between **1** and **8**.
 - **Channel and Tx Power:** Channel and transmit power level (or **Unavailable** if the access point is not connected).
 - **Utilization:** Percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays **Unavailable** for disassociated access points and **MonitorOnly** for access points in monitor-only mode.
 - **Tx Utilization:** Transmitted (Tx) utilization for the specified interface.
 - **Rx Utilization:** Received (Rx) utilization for the specified interface.
 - **Ch Utilization:** Channel utilization for the specified access point.
 - **Assoc. Clients:** Total number of clients associated.
 - **Dual-Band Radios:** Identifies and marks the XOR dual-band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
 - **Health Score:** AP health score.
 - **Issue Count**
 - **Coverage Issues**
 - **AP Down Issues**
- **Heatmap Type:** Heatmap is a graphical representation of Radio Frequency (RF) wireless data where the values taken by variable are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, antenna orientation, and AP transmit power. From the **Heatmap Type** drop-down list, select the heatmap type:
- **None**
 - **AP RSSI:** Coverage heatmap, which identifies the strength of wireless signal in the specific band.
 - **RSSI Cut off (dBm):** Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.

- **Heatmap Opacity (%)**: Drag the slider between 0 to 100 to set the heatmap opacity.
- **Heatmap Color Scheme**: The color green indicates good heatmap coverage, and the color red indicates poor heatmap coverage.
- **Client Density**: Density of associated clients.
 - **Map Opacity (%)**: Drag the slider to set the map opacity.
- **IDS**: Heatmap that shows the monitor mode access point coverage provided to the wireless clients on a floor map.
- **Planned Heatmap**: A planned heatmap is a hypothetical heatmap that shows the possible coverage of planned access points on a floor map.
- **Coverage**: Heatmap that excludes monitor-mode access points. (Available only if monitor-mode access points are on the floor plan.)

The AP details are reflected on the map immediately. Hover your cursor over the AP icon on the map to view AP details, RX neighbors details, client details, and switch information.

View Options for Sensors

Click the **Sensors** button to view sensors on the map. Expand the **Sensors** panel to configure these settings:

- **Display Label**: From the drop-down list, choose a text label that you want to view on the floor map for the selected access point. The available display labels are:
 - **None**
 - **Name**: Sensor name.
 - **Sensor MAC Address**: Sensor MAC address.

View Options for Overlay Objects

Expand the **Overlay Objects** panel to configure these settings. Use the **On/Off** buttons to view these overlay objects on the map.

- **Coverage Areas**
- **Location Regions**
- **Obstacles**
- **Rails**
- **Markers**

Configure Map Properties

Expand the **Map Properties** panel to configure:

- **Auto Refresh**—Provides an interval drop-down list to set how often you want to refresh maps data from the database. From the **Auto Refresh** drop-down list, set the time intervals: **None**, **1 min**, **2 mins**, **5 mins**, or **15 mins**.

Configure Global Map Properties

Expand the **Global Map Properties** panel to configure:

- **Unit of Measure**—From the drop-down list, set the dimension measurements for maps to either **Feet** or **Meters**.

Filter Device Data in a Network Hierarchy Map

For 2D wireless maps, you can apply various filters to access points and sensors. Click **Data** in the map toolbar to begin. Based on the filter criteria, the search results appear in a table.

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 End-point 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 six hours. However, you can change this interval up to 24 hours, as required for your network environment. For more information, see [Update the Device Polling Interval, on page 43](#). 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** Click **Update Polling Interval**.
- Step 4** From the **Update Resync Interval** dialog box, in the **Status** field, click **Enabled** to turn on polling or click **Disabled** to turn off polling.
- Step 5** In the **Polling Time** field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24 hours).
- Note** 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** 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 show 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.

By default, 25 entries are shown in the **Inventory** table. Click **Show More** to view more entries. You can view up to 200 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 number of entries persists 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 16: Inventory

Column	Description
Device Name	

Column	Description
	<p>Name of the device.</p> <p>Click the device name to view the following device details:</p> <p>Details: Displays details such as the device name, reachability status, manageability status, IP address, device model, role, uptime, site, and so on.</p> <ul style="list-style-type: none"> • View Assurance 360: Displays the Assurance 360 window. For 360 to open, you must have installed the Assurance application. • Interfaces <ul style="list-style-type: none"> • Ethernet Ports (For all devices): Displays the operational status and administrative status of the Ethernet ports. <p>For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series Switches and Aggregation Services Routers (ASR) 1000 Series Routers, the ports view displays the details of line cards and supervisor cards if they are available.</p> <p>The line card includes the details of the platform, address, serial number, role, and stack member number. The supervisor card includes the details of the part number, serial number, switch number, and slot number.</p> <p>The Ports table displays the operational status, admin status, type, MAC address, PoE status, speed, MTU, and Description. The table also displays the ID of the following types of VLANs:</p> <ul style="list-style-type: none"> • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN <p>For Cisco Catalyst 2000, 3000, and 9000 Series Switches, either click a port in the ports view or click the port name in the Ports table to view the maximum allocated power and power drawn details of the port.</p> • Color Code drop-down list catalogs the following views: <ul style="list-style-type: none"> • Status: Displays the default view of Ethernet ports. • VLANs: Displays the VLAN assigned to a particular port. VLANs view allows you to select a maximum of 5 VLANs and lists only VLANs that are associated with the port. <p>VLANs view displays the Selected, Not Configured, Default, and VLAN color code of the VLAN port mapping.</p> • Port Channels: Displays the top 5 port channels configured on the device. <p>Port channels view displays the Selected and the Port-channel color code of configured port channels on the device.</p> • Port Actions: <ul style="list-style-type: none"> • Clear Mac Address: You can clear the MAC address of a port. Click a port in the ports view. Then, from the Port Actions drop-down list, choose Clear Mac Address.

Column	Description
	<ul style="list-style-type: none"> • Port Shut: You can shut down a port. Click a port in the ports view. Then, from the Port Actions drop-down list, choose Port Shut. Click Okay in the warning message. The admin status of the port goes to Down. To make the admin status of the port Up, from the Port Actions drop-down list, choose Port No Shut. Click Okay in the warning message. <p>Error-disabled ports are shown in yellow. Click an error-disabled port in ports view to view the error reason. To activate an error-disabled port, clear the MAC address and shut down the port.</p> <ul style="list-style-type: none"> • Port Description: Click the Edit icon next to PORT DESCRIPTION, enter a description, click Save, and then click Okay to add a description to the port. Click the Delete icon to delete the description. • Update VLAN: Click the edit icon next to VLAN, choose a VLAN from the Edit VLAN drop-down list, and then click Save to update the VLAN. You cannot update VLAN for the ports that have two VLANs preconfigured. <ul style="list-style-type: none"> • The device software type must be IOS/IOS-XE to update the VLAN, add a port description, clear the MAC address, and shut down the port. • For Wireless Controller (WLC) devices, VLAN update, clear MAC address, and port shut are not supported. • VLAN update, clear MAC address, and port shut are supported only on access ports. • Port shutdown disrupts traffic on the port. • VLANs (Only for switches and hubs): The VLAN table displays the operational status, admin status, VLAN type, and IP address. The table also displays the ID of the following types of VLANs: <ul style="list-style-type: none"> • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN <p>You can click the Search or Filter option to view the details of the desired VLAN.</p> • Virtual Ports (Only for wireless devices, controllers, and routers): The Ports table displays the operational status, admin status, type, MAC address, PoE status, speed, and MTU. You can click the Search or Filter option to view the details of the desired ports. • Hardware and Software: Displays the hardware and software details of the device. • Configuration: Displays detailed configuration information, similar to what is displayed in the output of the show running-config command. <p>This feature is not supported for access points (APs) and wireless controllers. Therefore, configuration data is not returned for these device types.</p>

Column	Description
	<ul style="list-style-type: none"> • Power: Displays details about the power budgeted for, power consumed by, and power remaining for the device. The Power Supplies table shows the operational status, serial number, and vendor equipment type details. • Fans: Displays the operational status, serial number, and vendor equipment type of fans. • SFP Modules: Displays the details of the platform, serial number, manufacturer, and ports to which Small Form-Factor Pluggable (SFP) modules are connected. You can click the Search or Filter option to view the details of the desired ports. • User Defined Fields: Displays the user-defined fields associated with the device. • Config Drift: Displays the configuration changes and allows you to pick any two versions of the same device and compare their running configuration data. Note Running configuration data is not supported for devices such as wireless or legacy controllers. • Wireless Info: Displays the primary and secondary managed locations. • Mobility: Displays the mobility group name, RF group name, virtual IP, and mobility MAC address. <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 as follows:</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. • Unsupported: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You may try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, we do not expect you to 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 will 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.
Manageability	<p>Shows the device status as follows:</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 due to 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 that the device has been up and running.
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. The following device roles are available:</p> <ul style="list-style-type: none"> • Unknown • Access • Core • Distribution • Border Router

Column	Description
Site	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 About Network Hierarchy, on page 24 .
Last Updated	Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.
Device Family	Group of related devices, such as routers, switches, hubs, or wireless controllers.
Device Series	Series number of the device; for example, Cisco Catalyst 4500 Series Switches.
Resync Interval	The polling interval for the device. This interval can be set globally in Settings or for a specific device in Inventory. For more information, see the Cisco DNA Center Administrator Guide .
Last Sync Status	Status of the last Discovery scan for the device: <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 due to 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 noted. • In Progress: Inventory collection is occurring.


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 configure global telemetry settings.

Step 1 In the Cisco DNA Center GUI, 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**. The **Assign Device to Site** slide-in pane appears.

Step 4 In the **Assign Device to Site** slide-in pane, click the link next to the  icon for the device. The **Choose a floor** slide-in pane appears.

Step 5 In the **Choose a floor** slide-in pane, select the floor to assign to the device.

Step 6 Click **Save**.

Step 7 (Optional) If you selected multiple devices to add to the same location, you can check the **Apply to All** check box for the first device to assign its location to the rest of the devices.

Step 8 Click **Assign**.

Step 9 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 [Cisco DNA Center Supported Devices](#). 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 pxGrid connection.

If you want to use the Cisco DNA Center system certificate as the pxGrid client certificate (sent to 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 will fail).
- 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 as follows:

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, the syslog server, the NetFlow Collector, or the wired client.

Before you begin

Create a site and assign a device to the site. See [Create a Site in a Network Hierarchy, on page 24](#).

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

Step 2 Expand the **SNMP Traps** area if it is not visible and do one of the following:

- a) Check the **Cisco DNA Center as SNMP trap server** check box.
- b) 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 Expand the **Syslogs** area if it is not visible and do one of the following:

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

Step 4 Expand the **NetFlow** area if it is not visible and do one of the following:

- a) Check the **Use Cisco DNA Center as NetFlow collector server** check box.

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.

- b) Check the **Add an external NetFlow collector server** check box and enter the IP address and port number of the NetFlow Collector server.

The selected server is the destination server for NetFlow export from the network devices. If the NetFlow Collector is not selected, the application telemetry enablement will not work.

Step 5 Expand the **Wired Client Data Collection** area and check the **Monitor wired clients** check box.

This selection turns on IP Device Tracking (IPDT) on the access devices of the site.

By default, IPDT is disabled for the site.

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

Step 6 Expand the **Wireless Controller, Access Point and Wireless Clients Health** area and check the **Enable Wireless Telemetry** check box.

When selected, you can monitor the health of your network's wireless controller, access points, and wireless clients.

Step 7 Click **Save**.

Configure Cisco AI Network Analytics Data Collection

Use this procedure to enable Cisco AI Network Analytics to export network event data from wireless controllers as well as the site hierarchy to the Cisco DNA Center.

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 you have downloaded and installed the **AI Network Analytics** application. 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:

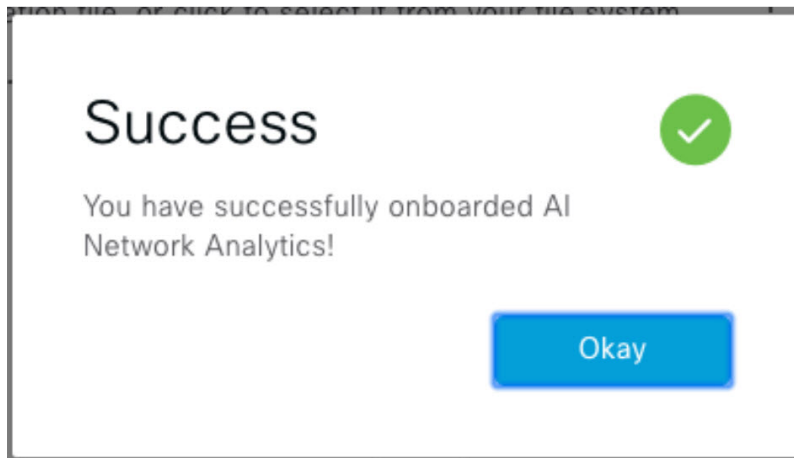
a. Click **Recover from a config file**.

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)**.

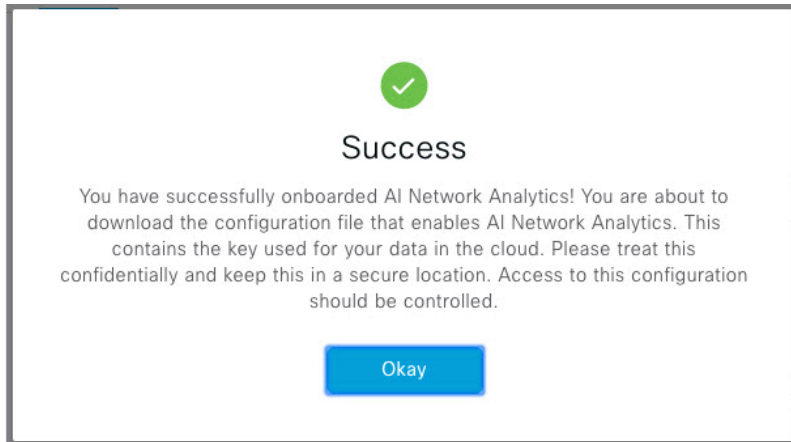
The system starts testing cloud connectivity as indicated by the **Testing cloud connectivity...** tab. After cloud connectivity testing completes, the **Testing cloud connectivity...** tab changes to **Cloud connection verified**.

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 **Cloud Connection** area displays .
- Step 5** (Recommended) In the **AI Network Analytics** window, click **Download Configuration** file.

Disable Cisco AI Network Analytics Data Collection

To disable Cisco AI Network Analytics data collection, you must turn off (disable) the connection to the Cisco AI Network Analytics cloud service. This will disable all of the Cisco AI Network Analytics-related features, such as AI-Driven Issues, Network Heatmap, Site Comparison, and Peer Comparison.

- 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.
- Step 3** In the **Cloud Connection** area, click the button to off, such that appears.
- 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.

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.



Enable Localization

You can view the Cisco DNA Center GUI screens 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. Scroll down and click **Advanced**.
 - c. From the **Languages > Language** drop-down list, choose **Add languages**.
The **Add languages** pop-up window appears.
 - d. 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 **Options**.
 - b. From the **Language and Appearance > Language** area, choose **Search for more languages**.
The **Firefox Language Settings** pop-up window appears.
 - 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 screens are shown in the selected language.

Figure 5: Example Localized Login Screen




Cisco DNA Center
 ネットワークの設計、自動化、保証

ユーザ名*

パスワード*

ログイン

Role-Based Access Control Support for Assurance

Assurance supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict users access to certain Assurance features.

For more information, see the "Manage Users" chapter in the [Cisco DNA Center Administrator Guide](#).


Use this procedure to define a custom role and then assign a user to that role.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1

Define a custom role.

- a) Click the menu icon () and choose **System > Users and Roles > Role Based Access Control**.
- b) Click + **Create New Role**.

The **Create a Role** window appears. After you create the new role, you are asked to assign users to the new role.

- c) Click **Let's Do it**.

If you want to skip this screen in the future, check the **Don't show this to me again** check box.

The **Create a New Role** window appears.

- d) Enter a name for the role and then click **Next**.
The **Define the Access** window appears with a list of options.
- e) Click > next to **Assurance** to expand it.

The following options appear, which allow you to set **Deny**, **Read** (the default), or **Write** permissions for the new role.

- **Monitor and Troubleshooting**: Allows you to monitor your network using the following dashboards: Health, Issues, and Sensors. It also allows you to analyze trends and gain insights, and troubleshoot using the 360° views and issue details.

If you set the permission level to **Deny**, the user to whom you assign this role cannot view any of the Assurance features.

- **Monitoring Settings**: Allows you to manage data retention and health settings.

You must have System permissions to manage data retention settings.

- **Troubleshooting Tools**: Allows you to create and schedule sensor tests and manage Intelligent Capture settings.

- f) Click **Next**.

The **Summary** window appears.

- g) Review the summary. If the information is correct, click **Create Role**. Otherwise, click **Edit** and make the appropriate changes.
The **Done, Role-Name** window appears.

Step 2

To assign a user to the custom role you just created, click **Add Users**.

The **User Management > Internal Users** window appears, which allows you to assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:
 - a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

The **Update Internal User** slide-in pane appears.
 - b. From the **Role List** drop-down list, choose the custom role, and then click **Save**.
- To assign the custom role to a new user, do the following:
 - a. Click + **Add**.

The **Create Internal User** slide-in pane appears.
 - b. Enter the first name, last name, and username in the fields provided.
 - c. From the **Role List** drop-down list, choose the custom role to assign to the new user.
 - d. Enter the password and then confirm it.
 - e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was making changes to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.
