



Set Up Catalyst Center to Use Assurance

- [Limitations and Restrictions of Assurance, on page 1](#)
- [Basic Setup Workflow, on page 1](#)
- [Discover Devices, on page 4](#)
- [Design Network Hierarchy, on page 19](#)
- [Manage Inventory, on page 40](#)
- [Add a Device to a Site, on page 47](#)
- [Add APs to a Map, on page 49](#)
- [Position an AP on a Map, on page 50](#)
- [About Cisco ISE Configuration for Catalyst Center, on page 54](#)
- [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 58](#)
- [Configure Cisco AI Network Analytics, on page 59](#)
- [Update the Machine Reasoning Knowledge Base, on page 61](#)
- [Enable Localization, on page 62](#)

Limitations and Restrictions of Assurance

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

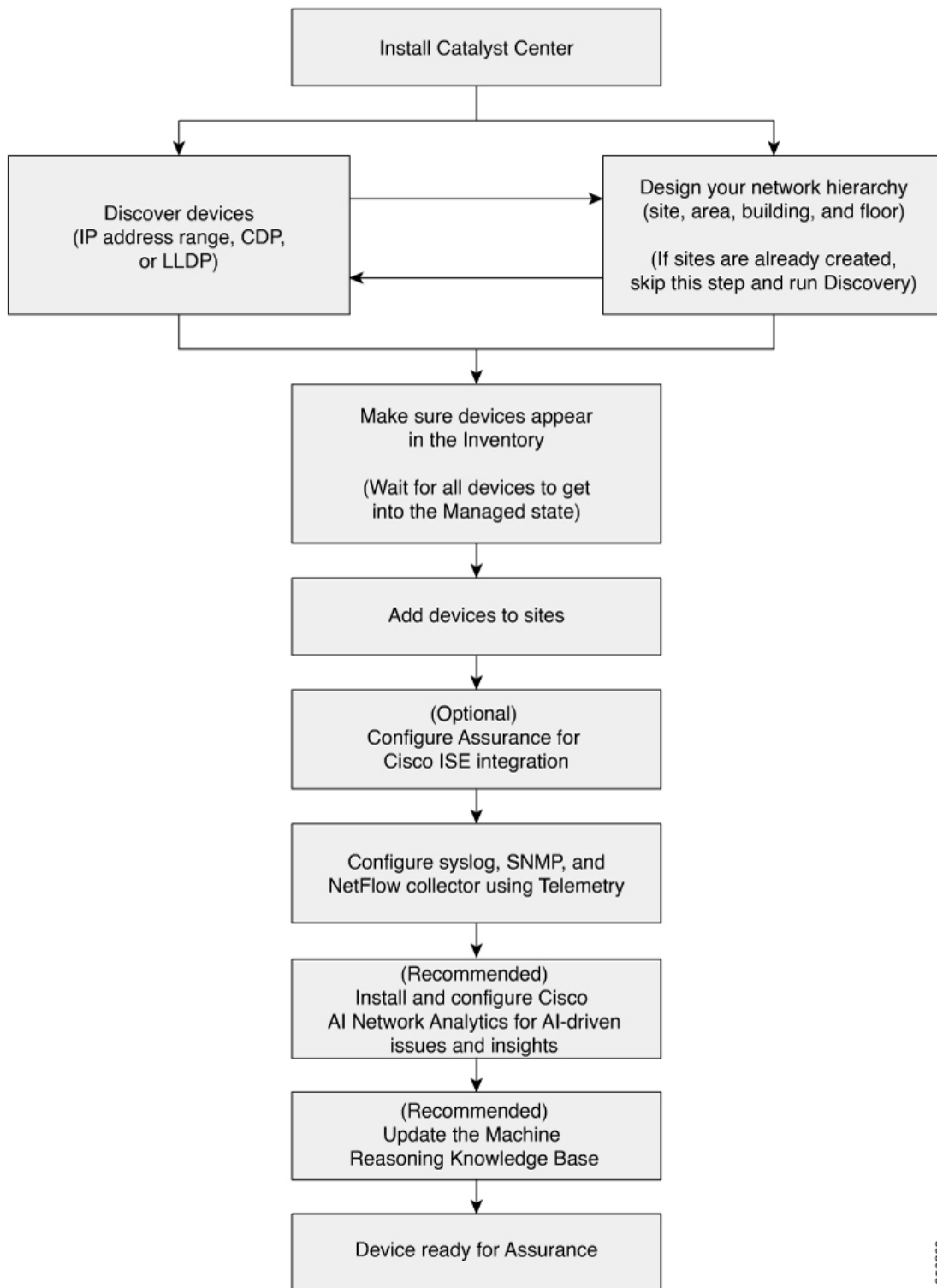
Basic Setup Workflow

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

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

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

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



356269

Before you begin

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

- Step 1** Install Catalyst Center.
See the [Cisco Catalyst 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 or CIDR, on page 13](#), [Discover Your Network Using CDP, on page 11](#) and [Discover Your Network Using LLDP, on page 15](#).
Note Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.
 - Design a new network hierarchy or use an existing one.
See [Create a New Network Hierarchy, on page 20](#) or [Use an Existing Cisco Network Hierarchy, on page 23](#).
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 41](#).
Note Before you add devices to sites, you must wait for all the devices to get into a Managed state.
- Step 4** Add devices to sites.
See [Add a Device to a Site, on page 47](#).
- Step 5** If you have APs, we recommend that you add them to a floor map.
See [Add APs to a Map, on page 49](#).
- Step 6** If your network uses Cisco Identity Services Engine (ISE) for user authentication, you can configure Assurance for Cisco ISE integration. This enables you to see more information about wired clients, such as the username and operating system, in Assurance.
See [About Cisco ISE Configuration for Catalyst Center, on page 54](#).
- 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 58](#).
- Step 8** (Recommended) To view AI-driven issues and gain network insights, configure Cisco AI Network Analytics data collection.
See [Configure Cisco AI Network Analytics, on page 59](#).
- 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 61](#).

Step 10 Start using the Assurance application.

Discover Devices

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

Discovery Overview

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

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

There are four 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.
- Use Classless Inter-Domain Routing (CIDR) 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.
- **Prefix Length**: If you use CIDR as a discovery method, you can set the prefix length value ranging from 20 to 30. The default value is 30.
- **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, CIDR, or an IP address range, you can specify whether you want Catalyst Center to add any of the device's IP addresses or only the device loopback address.



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

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



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

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Catalyst Center by viewing the [Cisco Catalyst Center Compatibility Matrix](#).
- Understand that the preferred network latency between Catalyst Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure that at least one SNMP credential is configured on your devices for use by Catalyst Center. At a minimum, this can be an SNMPv2C read credential.
- Configure SSH credentials on the devices you want Catalyst Center to discover and manage. Catalyst 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 Catalyst 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 Catalyst 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 Catalyst Center to use the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Catalyst Center.

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

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

This section describes the limitations and guidelines of device discovery.

- The following are the guidelines and limitations for Catalyst Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:
 - Configure the CLI username and password with privileged EXEC mode (level 15). These credentials are the same CLI username and password that you configure in Catalyst Center for the Discovery function. Catalyst 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 Catalyst Center is the same as the TACACS credential defined in the TACACS server.
- The following are the guidelines and limitations for Catalyst Center to discover your wireless controllers and APs:
 - Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.
 - After the wireless controllers are discovered, Catalyst Center displays the list of associated APs in the inventory. The listed APs are connected to the wireless controller during either the discovery or through inventory sync. To view any new APs that join the wireless controller after the inventory sync, you must perform a manual resync.



Note This limitation is applicable only for the devices that are not yet assigned to a site or provisioned in Catalyst Center.

- Third-party devices cannot be discovered with Catalyst Center discovery feature. You must add the third-party devices manually to your network. For more information, see "Add a Third-Party Device" in the [Cisco Catalyst Center User Guide](#).

Discovery Credentials

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

- Network devices: CLI and SNMP credentials.



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

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

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

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

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

- [Discover Your Network Using CDP, on page 11](#)
- [Discover Your Network Using an IP Address Range or CIDR, on page 13](#)
- [Discover Your Network Using LLDP, on page 15](#)

Table 1: CLI Credentials

| Field | Description |
|-------------------------|---|
| Name/Description | Name or phrase that describes the CLI credentials. If authentication fails for CLI, Catalyst Center retries the authentication process for 300 seconds (5 minutes). |
| Username | Name that is used to log in to the CLI of the devices in your network. |
| Password | Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Note Passwords are encrypted for security reasons and are not displayed in the configuration. |
| Enable Password | Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it. For security reasons, re-enter the enable password. Note Passwords are encrypted for security reasons and are not displayed in the configuration. |

Table 2: SNMPv2c Credentials

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

Table 3: SNMPv3 Credentials

| Field | Description |
|-------------------------|---|
| Name/Description | Name or description of the SNMPv3 settings that you are adding. |
| Username | Name associated with the SNMPv3 settings. |
| Mode | <p>Security level that an SNMP message requires. Choose one of the following modes:</p> <ul style="list-style-type: none"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption. |
| Auth. Type | <p>Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode.) Choose one of the following authentication types:</p> <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5. <p>Note Catalyst Center does not support device discovery if only MD5 authentication type is configured on the device for software image version 17.14.1 and later.</p> <p>If you wish to use MD5 authentication, it is recommended to configure SHA authentication as well for Catalyst Center to discover and manage devices running on software image 17.14.1 and later.</p> |

| 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 Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration. |
| Privacy Type | <p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. |
| Privacy Password | <p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Catalyst Center. • Passwords are encrypted for security reasons and are not displayed in the configuration. |

Table 4: SNMP Properties

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

Table 5: HTTP(S) Credentials

| Field | Description |
|--------------|--|
| 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 that is used to authenticate the HTTPS connection. • Password: Password that is used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?). • Port: Number of the TCP/UDP port that is used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). |
| 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 that is used to authenticate the HTTPS connection. • Password: Password that is used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?). • Port: Number of the TCP/UDP port that is used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). |

Table 6: NETCONF Setting

| Field | Description |
|-------|--|
| Port | <p>Port on the device. You can use one of the following ports:</p> <ul style="list-style-type: none"> • Port 830 (default). • Any other port that is available on the device. • A custom port that Catalyst Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the Cisco Catalyst Center Administrator Guide.) <p>If authentication fails for NETCONF, Catalyst Center retries the authentication process for 300 seconds (5 minutes).</p> <p>Discovery accepts and validates multiple credentials and only adds devices with working credentials to your inventory. So, if a NETCONF connectivity failure occurs during the discovery process, Catalyst Center adds the device without a NETCONF port. However, if you add a device (that's not NETCONF enabled) manually to your inventory with the NETCONF credential, Catalyst Center displays the error "Managed: Netconf Connection Failure" if there's no response to the RPC request on the NETCONF port. In both cases, if the device is added without the NETCONF port and if any application uses only NETCONF to collect data, Catalyst Center displays the missing NETCONF port error. If any application uses the CLI credentials when NETCONF is not configured, Catalyst Center displays the device in the managed state because the device is using the CLI credentials.</p> |

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, CIDR, 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 or CIDR, on page 13](#) and [Discover Your Network Using LLDP, on page 15](#).



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 From the top-left corner, click the menu icon and choose **Tools > Discovery**.

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

Step 3 In the **Discover Devices** window, complete the following fields:

- a) Enter a name for the discovery job.
- b) Under **Discovery Type**, choose **CDP**.
- c) In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.
- d) (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.

- e) Click .

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

- f) (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.

- g) 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, Catalyst 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 Catalyst Center.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential that Catalyst Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 6](#).

- a) In the left pane, click **CLI** to add CLI credentials.
- b) Expand **SNMP** to add SNMP credentials.
- c) Expand **Advanced Settings** and configure the following settings:
 - **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
 - **SNMP Polling Properties**: Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF and HTTP(S), if required.

Step 5 In the **Schedule Job** window, do the following:

- a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.
If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.
- b) Click the toggle button to enable or disable the **Discover new devices only** option.
- c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box is displayed with information about the settings that will be enabled on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview will not be generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, choose any one of the following options:

- **Assign to site without Configuration Preview:** Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see [Search the Network Hierarchy](#).
- **Skip site assignment for now:** Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities > Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Discover Your Network Using an IP Address Range or CIDR

You can discover devices using an IP address range, CIDR, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range, or CIDR. For more information about the other Discovery methods, see [Discover Your Network Using CDP, on page 11](#), and [Discover Your Network Using LLDP, on page 15](#).

Before you begin


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

Step 1 From the top-left corner, click the menu icon and choose **Tools > Discovery**.

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


Step 3 In the **Discover Devices** window, complete the following fields:

- a) Enter a name for the discovery job.
- b) Under **Discovery Type**, choose **IP Address/Range**, or **CIDR**.
- c) If you choose **IP Address/Range** discovery type, do the following:

1. In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Catalyst 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.

2. (Optional) Repeat previous step to enter additional IP address ranges.
- d) If you choose **CIDR** discovery type, do the following:
1. In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.
 2. 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.
 3. Click .
- (Optional) Repeat previous steps to exclude multiple subnets from the Discovery job.
4. In the **Prefix Length** field, enter the value of prefix length. The valid value ranges from 20 to 30.

- 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, Catalyst Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 5](#).

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential that Catalyst Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 6](#).

- a) In the left pane, click **CLI** to add CLI credentials.
- b) Expand **SNMP** to add SNMP credentials.
- c) Expand **Advanced Settings** and configure the following settings:
 - **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
 - **SNMP Polling Properties**: Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF and HTTP(S), if required.

Step 5 In the **Schedule Job** window, do the following:

- a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.
If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.
- b) Click the toggle button to enable or disable the **Discover new devices only** option.
- c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box is displayed with information about the settings that will be enabled on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview will not be generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, choose any one of the following options:

- **Assign to site without Configuration Preview:** Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see [Search the Network Hierarchy](#).
- **Skip site assignment for now:** Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities > Tasks** window.

What to do next

The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Discover Your Network Using LLDP

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



Note

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

Before you begin

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

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

Step 1 From the top-left corner, click the menu icon and choose **Tools > Discovery**.

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

Step 3 In the **Discover Devices** window, complete the following fields:

- Enter a name for the discovery job.
- Under **Discovery Type**, choose **LLDP**.
- In the **IP Address** field, enter a seed IP address for Catalyst Center to start the Discovery scan.
- (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

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

- Click .

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

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

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

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

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

Note If you choose this option and the device does not have a loopback interface, Catalyst 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 Catalyst Center.

Step 4 In the **Provide Credentials** window, configure the discovery credentials and other settings as required.

Enter at least one CLI credential and one SNMP credential that Catalyst Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 6](#).

- In the left pane, click **CLI** to add CLI credentials.
- Expand **SNMP** to add SNMP credentials.
- Expand **Advanced Settings** and configure the following settings:
 - **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
 - **SNMP Polling Properties**: Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Note You can configure other credentials such as, NETCONF and HTTP(S), if required.

Step 5 In the **Schedule Job** window, do the following:

- a) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.
If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.
- b) Click the toggle button to enable or disable the **Discover new devices only** option.
- c) Click the **Assign devices to an existing site** link.

The **Visibility and Control of Configurations** dialog box is displayed with information about the settings that will be enabled on the devices during site assignment. If Visibility of Configurations is enabled and a site is assigned during discovery, a configuration preview will not be generated.

During the discovery workflow, devices can be assigned to existing sites only, new site creation is not supported.

In the dialog box, choose any one of the following options:

- **Assign to site without Configuration Preview:** Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see [Search the Network Hierarchy](#).
- **Skip site assignment for now:** Use this option if you want the devices to be assigned to sites later from inventory.

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Start Discovery**.

You can view the status of the task in the **Activities > Tasks** window.

What to do next


The **Device Discovery** window displays an option to view the discovered devices based on the site assignment. Use this option to view devices assigned to a site or a network or the unassigned devices in the inventory.

Manage Discovery Jobs

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

Stop and Start a Discovery Job

Step 1 From the top-left corner, click the menu icon and choose **Tools > Discovery**.

Step 2 To stop an active Discovery job, hover your cursor over the ellipsis icon () in the **Actions** column and choose **Stop Discovery**.

Step 3 To restart an inactive Discovery job, hover your cursor over the ellipsis icon in the **Actions** column and choose **Re-discover**.

Clone a Discovery Job

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

Before you begin

Run at least one Discovery job.

-
- Step 1** From the top-left corner, click the menu icon and choose **Tools > Discovery**.
- Step 2** To copy a Discovery job, hover your cursor over the ellipsis icon (**⋮**) in the **Actions** column and choose **Copy & Edit**.
Catalyst Center creates a copy of the Discovery job, named Clone of *Discovery_Job*.
- Step 3** (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.
- Step 4** 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** From the top-left corner, click the menu icon and choose **Tools > Discovery**.
- Step 2** To delete a Discovery job, hover your cursor over the ellipsis icon (**⋮**) in the **Actions** column and choose **Delete**.
- Step 3** 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** From the top-left corner, click the menu icon and choose **Tools > Discovery**.
- Step 2** In the **Discovery** window, click **All discoveries page from previous release**.
- Step 3** In the left **Discoveries** pane, select the Discovery job. Alternatively, use the **Search** function to find a Discovery job by device IP address or name.
- Step 4** Click the down arrow next to one of the following areas for more information:
- **Discovery Details:** Displays the parameters that were used to run the Discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.
 - **Credentials:** Provides the names of the credentials that were used.
 - **History:** Lists each Discovery job that was run, including the time the job started, and whether any devices were discovered.

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

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

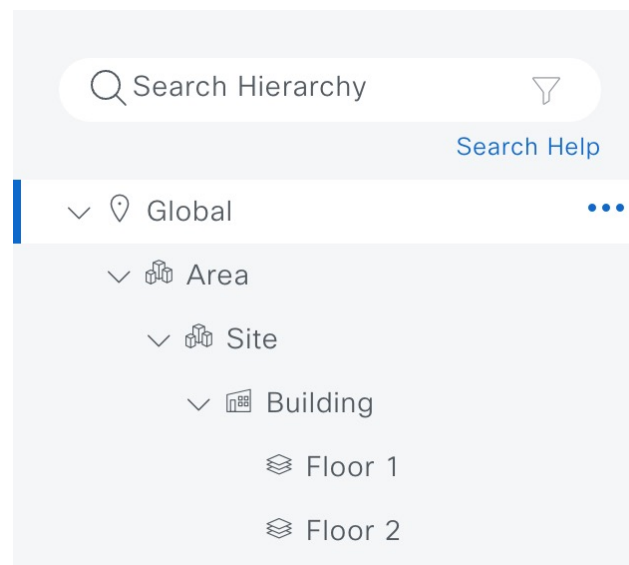
Design Network Hierarchy



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


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

The hierarchical elements that you can create have rules that dictate under which elements they can reside and which elements can reside under them. See the following figure and descriptions:

Figure 2: Network Hierarchy



- **Global:** Default element under which all other hierarchical elements reside. Areas or sites are the only elements that can reside directly under **Global**.
- **Areas and Sites** (): Areas and sites reside under **Global** or under other areas or sites. They do not have a physical address. As the largest element, they identify a geographic region. They provide a way to group areas or sites.
- **Buildings** (): Buildings reside under areas or sites. When you create a building, specify a physical address or latitude and longitude coordinates. Buildings can't contain areas. However, they can contain floors.

- **Floors** (): Floors reside under buildings. You can add floors to buildings with or without maps that contain various building components, like walls and windows. If you decide to use floor maps, you can manually create them or import them from files, such as DXF, DWG, JPG, GIF, PNG, or PDF file types. Then you can position your wireless devices on the floor maps to visualize your wireless network coverage.

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

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

- Create a new network hierarchy. For more information, see [Create a New Network Hierarchy, on page 20](#).
- Import an existing network hierarchy from Cisco Prime Infrastructure or Ekahau Pro. For more information, see [Use an Existing Cisco Network Hierarchy, on page 23](#) or [Use an Existing Ekahau Network Hierarchy, on page 26](#).

Create a New Network Hierarchy

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

Create, Edit and Delete a Site

Catalyst 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 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

A world map appears in the right pane.

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

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

Add, Edit, and Delete a Building

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

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

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

Add, Edit, and Delete a Floor

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

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

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

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

| Action | Steps |
|-------------------|---|
| Add a basic floor | <ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the desired building and choose Add Floor. b. In the Floor Name field, enter a name for the floor. The Floor Name field has the following restrictions: <ul style="list-style-type: none"> • The floor name cannot exceed 40 characters. • Special characters & > < ? ' " / [] aren't allowed. c. In the Global Unit System area, select Feet or Meters. When the floor is added, all the floors across all the sites sync to display all measurements in your chosen unit system. To update the global unit system, see "2D Map View Options" in the <i>Cisco Catalyst Center User Guide</i>. d. If you have wireless devices, for the Type (RF Model) drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated when computing 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. e. Configure the Floor Number, Floor Type and Thickness fields. The floor type and thickness are used when calculating a heatmap for wireless devices. f. Skip uploading a floor map image in Floor Image area. g. Configure map dimensions in the Width, Length, and Height fields. h. Click Add. |
| Edit a floor | <ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the floor and choose Edit Floor. b. In the Edit Floor dialog box, make the necessary changes. c. Click Update to save the changes. |
| Delete a floor | <ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the floor and choose Delete Floor. b. Click Ok. |

Use an Existing Cisco Network Hierarchy

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

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

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

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

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



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

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

If FIPS mode is *enabled*:

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

If FIPS mode is *disabled*:

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

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

Export Your Site Hierarchy from Cisco Prime Infrastructure

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

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

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

Export Your Map Archive from Cisco Prime Infrastructure

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

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

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

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

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

Step 4 Select at least one of the following options:

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

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

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

Step 5 Click **Generate Map Archive**.

The following message shows the progress of the operation:

```
Exporting data is in progress
```

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

Step 6 Click **Done**.

Import Your Site Hierarchy to Catalyst Center

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

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your Catalyst Center inventory. If not, discover them using the **Discovery** feature.
- Add and position APs on a floor map.
- If you manually created sites in Catalyst Center that are present in Cisco Prime Infrastructure, you must remove them from Catalyst Center before you can import them.

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
- Step 2** From the map toolbar, click **Import** and choose **Import Sites**.
- Step 3** In the dialog box, click one of the following radio buttons:
- **Merge with Existing Sites:** The downloaded site information is combined with the existing site information.
 - **Overwrite Existing Sites:** If the same site already exists in Catalyst Center, the existing site information is overwritten with the downloaded site information.
- Step 4** In the dialog box, drag and drop your CSV file into the download area. Alternatively, you can click **Choose a file**, navigate to where your CSV file is located, and then click **Import**.
- Note** If you do not have a CSV file, click **CSV template** to download a CSV file that you can edit and upload.
-

Import Your Map Archive to Catalyst Center

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



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

For information about exporting site hierarchy, see [Export Your Map Archive from Cisco Prime Infrastructure, on page 25](#).

- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
- Step 2** From the map toolbar, click **Import** and choose **Import Floor Maps**.
- Step 3** In the **Import Floor Maps** dialog box, drag and drop the map archive file.
- Step 4** Click **Import**.
- The map archive file is imported.
-

Use an Existing Ekahau Network Hierarchy

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

Export the Ekahau Project from Catalyst Center

To augment the preconfigured working floors, the Catalyst Center allows you to export the working floors from Catalyst Center as an Ekahau project and import the project into the Ekahau Pro Tool.

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
A world map displays in the right pane.
- Step 2** In the left pane, select the desired site, building, or floor.
- Step 3** To export a complete network map as an Ekahau project, from the **Export** drop-down list, choose **Export Floor Maps**.
To export an Ekahau project of a site, building, or floor map, from the left pane, hover your cursor over the ellipsis **...** next to the desired site, building, or floor and choose **Export Floor Maps**.
The **Export Floor Maps** dialog box is displayed.
- Step 4** In the **Export Floor Maps** dialog box, select the **Ekahau Project** export format.
- Step 5** Click **Export**.
An ESX file is created and saved to your local machine.
- Step 6** Import the ESX file into the Ekahau Pro tool, augment the floor, and save the file.
- Step 7** Import the Ekahau project into the Catalyst Center under the site. For more information, see [Import an Ekahau Project to Catalyst Center, on page 27](#).
-

Import an Ekahau Project to Catalyst Center

Before you begin

Importing an Ekahau Cloud project can fail if the project has local changes (such as removing an AP or wall), that are out-of-sync with the Ekahau Cloud project. To avoid this situation, make sure to synchronize any local changes to the Ekahau Cloud before importing the Ekahau Cloud project to Catalyst Center.

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
- Step 2** Design your network hierarchy by adding sites, buildings, and floors.
Note For more information, see [Create, Edit and Delete a Site, on page 20](#), [Add, Edit, and Delete a Building, on page 21](#), and [Add, Edit, and Delete a Floor, on page 22](#).
While adding floors, make sure that you create floors with the same name given in the Ekahau project.
- Step 3** In the left pane, hover your cursor over the ellipsis **...** icon next to the site where you want to import the Ekahau project and choose **Import Ekahau Project**.
The **Import Ekahau Project** dialog box appears.
- Step 4** Drag and drop the ESX file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the ESX file.

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

Step 5 If an AP is not found in the inventory and remains unmapped, the planned AP is retained on the floor. To see the reason for the mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.

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

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

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

The **Assign Planned APs** panel appears.

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

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

Step 9 Click **Save**.

Import an Ekahau Site Survey to Catalyst Center

To create your network hierarchy, you can upload an Ekahau site survey file and an AP mapping file (in CSV format).

The Ekahau site survey only contains the floor map with the APs known by name and position on the map. By default the AP model might not be set in the Ekahau site survey. A pre-requisite of importing to Catalyst Center is to open the project in Ekahau and configure the AP models using Ekahau-allowed model names, for example, *Cisco C9130i* for the Catalyst Center 9130 AP.

Because the Ekahau site survey doesn't provide Catalyst Center with any information about the radios of each AP, the AP mapping file augments the Ekahau site survey with this information. The AP mapping file is limited in that you can only provide the desired AP mapping by AP model, not by AP name. So, if you have multiple APs of the same type but different antenna configurations, only one antenna configuration can be applied to all APs of that type within the project.

For each AP in the AP mapping file, you define the model number followed by the configuration of each antenna:

```
model, antennaName0, antennaAzimuth0, antennaElevation0, antennaName1, antennaAzimuth1, antennaElevation1
```

For example, the following AP mapping file defines the configuration of a Catalyst 9130I with two antennas:

```
AP9130I, Internal-9130-2.4GHz, 90d, 0d, Internal-9130-5GHz, 90d, 0d
```

The model attribute must be the same as the equivalent planned AP model in the Catalyst Center GUI, for example, AP9130I for the Catalyst Center 9130 AP. Similarly, the *antennaName* attributes must also be the same names found and supported in the Catalyst Center GUI. If the AP has three or more radios, you can

continue the n -based numbering pattern of the *antennaName*, *antennaAzimuth*, and *antennaElevation* parameters to define the antenna information for each radio by slot number supported by that AP model.

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

Figure 3: The CSV template file contains the following fields and defaults:

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

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

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

Before you begin

- Open the project in Ekahau and configure the AP models using Ekahau-allowed model names, for example, *Cisco C9130i* for the Catalyst Center 9130 AP.
- Create an AP mapping file (CSV format) to provide Catalyst Center with information about the radios of each AP model that is being used.

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

Alternatively, you can hover your cursor over the ellipsis **...** next to the parent site or **Global** in the left pane, and choose **Add Area**. For more information, see [Create, Edit and Delete a Site, on page 20](#).

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

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

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

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

Step 6 Click **Import**.

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

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

Configure 2D Floor Map Devices and Overlay Objects

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

Devices

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

Overlay Objects

- **Coverage Areas:** By default, any area defined as part of a floor map is considered as a wireless coverage area. However, if you have a building that is nonrectangular or you want to mark a nonrectangular or polygon-shaped area on a floor, you can use the **Coverage Areas** drawing tool to create a coverage area.
- **Openings:** An opening, also called an atrium, is an open-air or skylight-covered area within a building. An opening can extend through multiple floors and can affect wireless signal coverage areas.
- **Location Regions:** Location regions define areas that are included in or excluded from the computation of heatmaps. Inclusion areas are included in the calculations, and exclusion areas are not included. For example, you might want to exclude areas such as openings, atriums, or stairwells within a building, but include a work area, such as cubicles, labs, or manufacturing floors.
- **Walls:** Walls define any exterior or interior vertical structures in a building, such as windows, cubicles, and doors. Because they can be made of different materials and have different densities, they can significantly impact RF signal attenuation and heatmap calculation. For example, the more walls you include in a floor map, the longer it can take to compute a heatmap. Although, even if you have a high number of walls on your floormap, you can adjust the number used to compute the heatmap. For information, see "2D Map View Options" and "3D Map View Options" in the [Cisco Catalyst Center User Guide](#).
- **Shelving Units:** Shelving units are obstacles that can significantly impact RF signal attenuation and heatmap calculation. A high-ceiling warehouse is an example of a location with shelving units.
- **Markers:** A marker identifies a location on a map. When you create a marker, you can name it and position it to help you identify it later.
- **GPS Markers:** When integrated with Catalyst Center, location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), use GPS markers to calculate the approximate geographical location of clients.

- **Align Points:** Align points are markers that are used to position multiple floors that have different physical shapes. In 3D maps, floors are aligned at the top-left corner of the map (point 0,0). If you manage each floor independently, the misalignment is not a problem. However, to use some of the features of 3D maps, the floors need to be aligned as they are in reality. To compensate this misalignment, you can insert one or more align points on two or more floors, so that the floors align properly one on top of the other in a 3D map.

Add, Position, Edit, and Remove APs

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

Step 3 From the map toolbar, click **2D > Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 From this window, you can add, position, edit, and remove APs. See the following table for details.

| Action | Steps |
|-----------------|---|
| Add APs. | <ol style="list-style-type: none"> a. In the left pane of the map, click Add Access Points. b. In the Add Access Points slide-in pane, do one of the following in the table: <ul style="list-style-type: none"> • To add a single AP: Locate the AP that you want to add, and scroll to the right and click Add. • To add multiple APs: Check the check boxes next to the APs you want to add and click Add Selected. <p>Newly added APs appear in the Unpositioned category in the left pane of the map.</p> c. From the Unpositioned category, click an AP. d. Click the location on the map where you want to position the AP. e. In the map toolbar, click Save. |

| Action | Steps |
|-------------------------|---|
| Add planned APs. | <p>a. From the left pane of the map, in the Planned AP Models area, click the AP model of the planned AP that you want to add.</p> <p>If the AP model isn't listed, click Add Model and choose the AP model to add to the list.</p> <p>b. On the floor map, click the location where you want to place the planned AP.</p> <p>c. In the Edit Planned AP slide-in pane, click the gear icon and add a unique name pattern.</p> <p>d. Define the antenna type and the azimuth and elevation, if necessary.</p> <p>e. To continue adding planned APs with the same properties, click locations on the map.</p> <p>f. To stop adding planned APs, press Esc or right-click the floor map.</p> <p>g. In the map toolbar, click Save.</p> |
| Edit an AP. | <p>a. In the map, right-click the AP and choose Edit.</p> <p>b. Change any of the editable AP settings. Note the information about the following fields:</p> <ul style="list-style-type: none"> • Antenna: For external APs, you must choose an antenna. If an antenna isn't chosen, the AP will not be present in the map. • Azimuth: The azimuth is the angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is 0 to 360. In Catalyst Center, pointing right is 0 or 360 degrees; pointing down is 90 degrees. <p>You can manually enter the value or use the blue arrow under the field to change the value.</p> <p>For omnidirectional antennas, the azimuth is not relevant if the elevation is 0.</p> <ul style="list-style-type: none"> • Elevation: You can manually enter the elevation in degrees or use the blue arrow under the field to change the value. <p>For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values mean pointing down.</p> <p>c. In the map toolbar, click Save.</p> |

| Action | Steps |
|----------------------|--|
| Remove an AP. | <ol style="list-style-type: none"> Click the AP, or to select multiple APs, click the first AP and while pressing the Shift key, click the rest of the APs. In the Edit pane, click Remove. In the map toolbar, click Save. |

Add, Position, and Remove Sensors

Before you begin

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

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

| Action | Steps |
|------------------------|--|
| Add sensors. | <ol style="list-style-type: none"> From the Add Sensors slide-in pane, click Add next to the sensor that you want to add, or to add multiple sensors, check the check boxes next to sensors you want to add and click Add Selected. Newly added sensors appear in the Unpositioned category in the map left pane. From the Unpositioned category in the map left pane, click a sensor. Click the location on the map where you want to position the sensor. Click Save. |
| Remove sensors. | <ol style="list-style-type: none"> Click the sensor, or to select multiple sensors, click the first sensor and while pressing the Shift key, click the rest of the sensors. In the Edit pane, click Remove. From the map toolbar, click Save. |

Add, Edit, and Remove Coverage Areas

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

For more information about coverage areas, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Coverage Areas**.
- Step 4** To add a coverage area, do the following:
- In the **Coverage Area** dialog box, enter a name for the coverage area in the field.
 - Click **Add Coverage**.
 - Click on the map to create a point and initiate the drawing tool.
 - Continue creating points to define the coverage area shape.
- Note** The coverage area shape must have at least three points. Click and drag a point to redefine the coverage area shape.
- Double-click to exit the drawing tool and finalize the coverage area shape.
- Step 5** To edit a coverage area, do the following:
- In the map toolbar, click **Add/Edit > Coverage Areas**.
 - To redefine the shape of a coverage area, click and drag a point.
 - To edit a coverage area name, right-click the coverage area and choose **Edit**.
- Step 6** To delete a coverage area, do the following:
- In the map toolbar, click **Add/Edit > Coverage Areas**.
 - Right-click the coverage area and choose **Remove**.
- Step 7** In the map toolbar, click **Save**.
-

Add, Edit, Copy, and Remove Openings

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

For more information about openings, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Openings**.
- Step 4** To add an opening, do the following:
- From the left pane of the map, click **Opening**.
 - Click on the map to create a point and initiate the drawing tool.
 - Continue creating points to define the opening shape.
- Note** The opening shape must have at least three points. Click and drag a point to redefine the opening shape.

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

Step 5 To edit an opening, do the following:

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

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

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

Step 7 To remove an opening, do the following:

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

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

Add, Edit, and Remove Location Regions

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

Add, Edit, and Remove an Inclusion Region

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

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

For more information about inclusion regions, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 In the left pane of the map, click the **Inclusion** icon.

Step 5 To create an inclusion region, use the drawing tool:

- a) Click the map to create a point where you want the inclusion region to begin.
- b) Move the cursor to the next point and click again.
- c) Continue creating points to define the inclusion region shape.
- d) To finalize the shape, double-click the map.

Alternatively, from the left pane of the map, click the **Inclusion** icon.

e) To exit the drawing tool, double-click the map again.

Step 6 To edit the location of an inclusion region, drag and drop the shape to the new location.

Step 7 To remove an inclusion region, right-click the shape and choose **Remove**.

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

Add, Edit, and Remove an Exclusion Region

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

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

For more information about exclusion regions, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 From the left pane of the map, click the **Exclusion** icon.

Step 5 To create an exclusion region, use the drawing tool:

- a) Click the map to create a point where you want the exclusion region to begin.
- b) Move the cursor to the next point and click again.
- c) Continue creating points to define the exclusion region shape.
- d) To finalize the shape, double-click the map.

Alternatively, from the map left pane, click the **Exclusion** icon.

e) To exit the drawing tool, double-click the map again.

Step 6 To edit the location of an exclusion region, drag and drop the shape to the new location.

Step 7 To remove an exclusion region, right-click the shape and choose **Remove**.

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

Add, Edit, and Remove Walls

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

For information about how walls impact RF signal attenuation and heatmap calculation, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 To add walls, do the following:

- a) In the left pane of the map, click a wall type from the **Others** or **On this floor** category.

Note If a wall type isn't listed, click **Add Wall Type** to create a custom wall type.

- b) Click the map to create a point where you want the wall to begin.
- c) Move the cursor to the next point, where you want to end the wall or where you want to create a corner and click again.
- d) Continue creating points to define the wall shape.
- e) To end a wall, double-click the map.

Alternatively, from the left pane, click the wall type.

- f) To exit the drawing tool, double-click the map again.

Step 5 To change a wall type, and depending on the wall type also configure its parameters, do the following:

- a) Click the wall that you want to change.

The **Wall Type** dialog box opens.

- b) From the **Wall Type** drop-down list, choose the type of wall.
- c) Configure any other parameters that are appropriate for the new wall type.
- d) Click **Update**.

Step 6 To move a wall, do the following:

- a) Hover your cursor over the wall that you want to move.

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

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

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

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

Add, Copy, Edit, and Remove Shelving Units

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

For information about shelving units, see [Configure 2D Floor Map Devices and Overlay Objects](#), on page 30.

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 To add shelving units, do the following:

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

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

c) Click **Add Shelving**.

The shelving unit is displayed on the map.

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

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

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

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

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

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

Add, Edit, and Remove Markers

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

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 In the left pane of the map, click the **Markers** icon.

Step 5 In the **Place Markers** dialog box, enter the name for the marker, and click **Add Marker**.

Step 6 To place the marker, click the map where you want to place the marker.

Step 7 To move a marker, hover your cursor over the marker until it turns blue. Then drag and drop it in the new location.

Step 8 To edit a marker, right-click the marker and choose **Edit**.

Step 9 To remove a marker, right-click the marker and choose **Remove**.

Step 10 In the map toolbar, click **Save**.

Add, Edit, and Remove GPS Markers

This procedure shows you how to add, edit, and remove GPS markers. For more information about GPS markers, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).



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

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 To add a GPS marker, do the following:

- a) In the left pane of the map, click the **GPS Markers** icon.
- b) On the map, click the location where you want to place the GPS marker.

GPS markers must be positioned inside the outer-perimeter walls, typically at the building corners.

- c) In the **Place Markers** dialog box, enter the name, latitude, longitude, and the x and y coordinates in the appropriate fields.

The latitude and longitude coordinates of the GPS marker located in the northwest corner of a floor must match the building coordinates.

- d) Click **Add GPS Marker**.

Step 5 To edit a GPS marker, right-click the GPS marker and choose **Edit**.

Step 6 To remove a GPS marker, right-click the GPS marker and choose **Remove**.

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

Add, Edit, and Remove Align Points

This procedure shows you how to add, edit, and remove align points. For more information about align points, see [Configure 2D Floor Map Devices and Overlay Objects, on page 30](#).

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

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

Step 4 To add an alignment point, do the following:

- a) In the left pane of the map, click the **Align Points** icon.
- b) On the map, click the location where you want to place the alignment point.

Step 5 To edit the name of an alignment point, do the following:

- a) Right-click the alignment point and choose **Edit**.
- b) Change the name and click **Edit Marker**.

Step 6 To change the location of an alignment point, do the following:

- a) Right-click the alignment point and choose **Edit**.
- b) Click **Edit Marker**.
- c) Drag and drop the alignment point to the new location.

Step 7 To remove an alignment point, right-click the alignment point and choose **Remove**.

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

Manage Inventory

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

About Inventory

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

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

Inventory uses the following protocols, as required:

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

After the initial discovery, Catalyst Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see [Update the Device Polling Interval, on page 40](#). 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. A configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Device resynchronization is also triggered after the inventory service restart under the following circumstances:

- If there is an upgrade (Catalyst Center upgrade) after the inventory service restart.
- If the device's synchronization is in terminated or delayed state after the service restart.
- If the **Last Sync** time for the device is more than 75 percent of the periodic resync interval configured on the device. For example, after the inventory service restart, if the **Last Sync** time for a device has crossed 18 hours and the configured periodic resync interval is 24 hours, the device will be resynchronized before the periodic resync interval. The percentage for the resync interval cutoff time may vary based on the value configured on the device.

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 From the top-left corner, click the menu icon and choose **Provision > Inventory**.

Step 2 Select the devices that you want to update.

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

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

Step 5 Select the resync type.

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

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

Step 7 Click **Update**.

Display Information About Your Inventory

You can display and filter for information about discovered devices in your inventory. You can also customize or change the information displayed in the **Devices** table.


Before you begin

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

Step 1 From the top-left corner, click the menu icon and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Note For the devices that are added as Fully Qualified Domain Name (FQDN), hover your cursor over the **i** icon next to the device name in the **IP address** column to view the **Resolved IP Address**.

Step 2 (Optional) To change the Inventory view, use the toggle button () in the top-right corner. You can change your default view (the list layout) to other layouts, such as the topology or map layout.

Step 3 (Optional) To change the **Devices** table's focus views, from the **Focus** drop-down list, choose a view, such as **Default**, **Inventory**, or **Software Images**.

- Note**
- The displayed columns change depending on the chosen focus view.
 - Selected devices persist in each new focus view.

Step 4 (Optional) To filter for specific device details in the **Devices** table, you can do the following:

- To filter for a device family, choose one or more of the device family buttons at the top of the **Inventory** window.

For example, you can click **Routers** to display only routers in the table.

- To filter for device work items, in the left pane, check the check box of one or more work items. The table is immediately filtered for the work item.

For example, you can check the **Unreachable** check box to display only unreachable devices in the table.

- To filter for specific device details, click **Filter devices** and choose from the filter options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Then click **Apply**.

Step 5 (Optional) To take a guided tour of the **Inventory** window, click **Take a tour** in the top-right corner.

Step 6 (Optional) To export all the data in the **Devices** table, click **Export** in the top-right corner.

Step 7 (Optional) To customize the **Devices** table, click the settings icon (⚙️) in the top-right corner, choose from the following options in the **Table Settings** slide-in pane, and then click **Apply**.


- **Table Appearance:** Choose if you want the default or compact table view and table striping.
- **Edit Table Columns:** Choose if you want to create a custom view and if you want to hide or display columns. Note that the column selection does not persist across sessions.

The following table provides key information relevant to certain table columns.

| Column | Description |
|--------------------|--|
| Device Name | <p>Name of the device.</p> <p>Click the device name for more information about that device.</p> <p>Note A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.</p> |

| Column | Description |
|---------------------|---|
| Support Type | <p>Shows the device support level:</p> <ul style="list-style-type: none"> • Supported: The device profile is tested for all applications on Catalyst Center. You can open a service request if any of the Catalyst Center functionalities for these devices do not work. • Limited: The device profile for legacy devices is tested only for the following features and tested only on a best-effort basis on Catalyst Center. <ul style="list-style-type: none"> • Discovery • Topology • Device Reachability • Config Change Audit • Inventory • Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.) • Template Provisioning (Applicable only for switches.) <p>For more information, see the Legacy Device Compatibility Matrix.</p> <ul style="list-style-type: none"> • Third Party: The device profile has been tested on Catalyst Center for third-party devices that are capable of populating SNMP MIB 2 values. Catalyst Center support limited base automation and assurance capabilities, such as Inventory and Topology as a best effort basis. <p>For more information, see the Cisco Catalyst Center Compatibility Matrix.</p> <ul style="list-style-type: none"> • Unsupported: All remaining Cisco and third-party devices that are not tested and certified on Catalyst Center. You can try out various functionalities on Catalyst Center for these devices, as a best effort. However, you cannot raise a service request or a bug if Catalyst Center features do not work as expected. |
| Reachability | <p>The following is a list of the various statuses:</p> <ul style="list-style-type: none"> • Reachable: The device is reachable by Catalyst Center using SNMP, HTTP(S), and NETCONF polling. • Ping Reachable: The device is reachable by Catalyst 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. |

| Column | Description |
|----------------------|---|
| EoX Status | <p>Shows the EoX scan status:</p> <ul style="list-style-type: none"> • Success: The device is scanned for EoX alerts successfully. • Not Scanned: The device is not scanned for EoX alerts. • Scan Failed: Catalyst Center is not able to scan the device for EoX alerts. • Scanning: Catalyst Center is scanning the device for EoX alerts. <p>Hover your cursor over the i icon next to EoX Status, and click Click here to accept to initiate an EoX scan.</p> <p>For the devices that are scanned successfully, the EoX Status column shows the number of alerts, if any. Click the number of alerts to view the alerts in detail.</p> <p>In the slide-in pane, click the Hardware, Software, and Module tabs to view the hardware, software, and module EoX alerts.</p> |
| Manageability | <p>Shows the device status:</p> <ul style="list-style-type: none"> • Managed with green tick icon: Device is reachable and is fully managed. • Managed with orange error icon: Device is managed with some error, such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. Hover your cursor over the error message to view more details about the error and the impacted applications. • Unmanaged: Device cannot be reached and no inventory information was collected because of device connectivity issues. <p>Note Click Last Sync Details to view the Last Sync Start Time and Reason(s) for Last Sync.</p> |
| Platform | Cisco product part number. |
| 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 Catalyst 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. Catalyst Center does not update the device role even if it detects a change during a subsequent device resynchronization.</p> <p>If required, you can use the drop-down list in this column to change the assigned device role.</p> |
| Site | <p>The site to which the device is assigned. Click Assign if the device is not assigned to any site. Click Choose a Site, select a site from the hierarchy, and click Save. For more information, see Design Network Hierarchy, on page 19.</p> |
| Last Updated | <p>Most recent date and time on which Catalyst Center scanned the device and updated the database with new information about the device.</p> <p>Note Click Last Sync Details to view the Last Sync Start Time and Reason(s) for Last Sync.</p> |

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

- **Edit Custom Views**: First you must create a custom view in the **Edit Table Columns** tab, and then you can edit the custom view.
- **Reset All Settings**: Reset the table settings to the default settings.

Step 8 (Optional) To manage your devices from the **Devices** table, you can use the following options:

| Name | Description |
|-------------------------------|---|
| Tag | You can click Tag to tag devices, edit and delete tags, or create port groups. |
| Add Device | You can click Add Device to add a network or compute device, or integrate a Meraki dashboard or Firepower Management Center (FMC) with Catalyst Center. |
| Actions drop-down list | <p>You can use the Actions drop-down list to manage your devices, software images, telemetry, and more.</p> <p>To view more details about each action option, click the right-adjacent information icon (ⓘ).</p> |

Step 9 (Optional) In the **Devices** table, you can do the following:

- To sort the columns in either ascending or descending order, click the column header.
- To view more details about a device, click the device name and then click **View Device Details**.
- To view a device's compliance details, click either **Non-Compliant** or **Compliant** under the **Compliance** column.
- To assign a site to a device, click **Assign** under the **Site** column.
- To change a device role, click the edit icon under the **Device Role** column and then choose from the options, such as **ACCESS** or **CORE**.
- To mark an image as Golden or view its needed updates, click **Mark Golden** or **Needs Update** under the **Software Image** column.
- To change the number of entries, scroll down to the bottom of the window, and from the **Show Records** drop-down list, choose the number of entries that you want displayed.

Note that if there are more than 25 entries in the table and you choose a different focus view, the same number of entries is displayed in each new view.

Note Each focus view displays different columns, and you can customize a table view to include columns, such as **Compliance**, **Site**, **Device Role**, and **Software Image**.

Delete a Network Device

You can delete devices from the Catalyst 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** From the top-left corner, click the menu icon and choose **Provision > 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**.
- Note** When you delete devices integrated with ISE, those deleted devices are moved to new NDG group in Cisco ISE.
- 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 Catalyst Center as the syslog and SNMP trap server, which enables Syslog Level 2 and configures global telemetry settings.



Note Third-party devices can be assigned to a site, but the devices are not managed by Catalyst Center, it is only for visibility.

-
- Step 1** From the top-left corner, 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.
- Note** You cannot assign Firepower Threat Defense (FTD) high availability (HA) paired devices to different sites. Both the paired devices must be assigned to the same site.
- Step 3** From the **Actions** menu, choose **Provision > Assign Device to Site**.
- Step 4** In the **Assign Device to Site** slide-in pane, click the link next to the Site icon () for the device.
- Step 5** In the **Choose a floor** slide-in pane, select the floor to assign to the device and click **Save**.
- Step 6** (Optional) If you select multiple devices to add to the same location, check the **Apply to All** check box for the first device to assign its location to the rest of the devices and click **Next**.
- Step 7** Review summary settings and click **Next**.

Note Application Telemetry and Controller-Based Application Recognition (CBAR) is enabled on the applicable network devices by default, if you enable Application Telemetry and CBAR on **Design > Network Settings > Telemetry** window. For more information, see [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 58](#).

Application and Endpoint Visibility enablement is skipped by default for the devices that does not support Controller-Based Application Recognition (CBAR) enablement or undeployed Application Visibility Service (AVS).

Step 8 Based on the Visibility and Control of Configurations settings, choose an available option. For more information, see "Visibility and Control of Configurations Workflow" in the [Catalyst Center User Guide](#).

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Configurations Workflow" in the [Catalyst Center User Guide](#).

Step 9 In the **Task Name** field, enter a task name.

Step 10 Do the following:

- If you chose **Now** or **Later**, click **Assign**.
- If you chose **Generate configuration preview**, click **Preview**.

Step 11 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.
If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 12 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

- a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.
- b. On the **Preview Configuration** window, review the device configurations.
For more information, see "Visibility and Control of Configurations Workflow" in the [Catalyst Center User Guide](#).
- c. Do one of the following:
 - When you're ready, click **Deploy** or **Submit for Approval**.

- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

- In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.
- Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

Note If only MD5 authentication type is configured on the device, the site assignment will be blocked for devices with software image version or golden tagged image version 17.14.1 and later.

To continue the site assignment, you must configure SHA authentication as well. For information on how to configure SHA as the authentication type for SNMP credentials, see "Edit Global Device Credentials" in the *Catalyst Center User Guide*.

Step 13

When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.

From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled Device Controllability.

What to do next

You can view the status of the task on the **Tasks** window. To navigate to the **Tasks** window, click the menu icon and choose **Activities > Tasks**.

Add APs to a Map

This procedure describes how to add APs to a map.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover them using the Discovery feature. See [Discovery Overview, on page 4](#).

Step 1 From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.

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

Step 3 From the map toolbar, click **2D > Add/Edit**.

By default, the **Devices** and **Access Points** toggle buttons are chosen.

Step 4 In the left pane of the map, click **Add Access Points**.

Step 5 In the **Add Access Points** slide-in pane, do one of the following in the table:

- **To add a single AP:** Locate the AP that you want to add, and scroll to the right and click **Add**.
- **To add multiple APs:** Check the check boxes next to the APs you want to add, and click **Add Selected**.

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

In edit mode, newly added APs are displayed in the **Unpositioned** category in the map left pane. For more information, see [Position an AP on a Map, on page 50](#).

Step 6 After adding the APs to a floor, close the **Add Access Points** slide-in pane.

What to do next

When you add an AP to a map, the wireless map automatically stores the following data even after the AP is deleted from the inventory:

- AP name
- AP MAC address
- Current site of the AP
- Current position of the AP on the map



Note If you delete the corresponding site from the network hierarchy, the stored AP data is also removed.

When you delete the wireless controller with all its managed APs from the inventory, Catalyst Center displays a planned AP icon for the corresponding APs on the map. For more information, see "About the AP Icon and Planned AP Icon" in the [Cisco Catalyst Center User Guide](#).

If the same AP is rediscovered in the inventory later, Catalyst Center automatically places it back on the map at the same site and position even if a different wireless controller manages it.

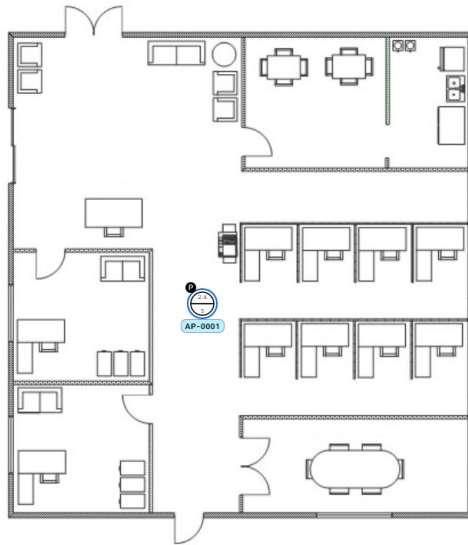
To remove the AP data from the map when the AP is deleted from the inventory, you can do one of the following:

- Before deleting the wireless controller from the inventory, assign the corresponding APs to the **Global** site. For more information, see [Add a Device to a Site, on page 47](#).
- After deleting the wireless controller from the inventory, remove the corresponding planned APs from the map. For more information, see "Remove APs from a Map" in the [Cisco Catalyst Center User Guide](#).

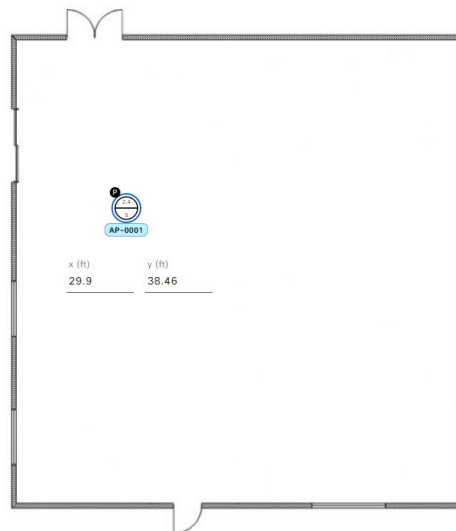
Position an AP on a Map

After adding an AP to a floor, you must position it on the map using one of the following methods:

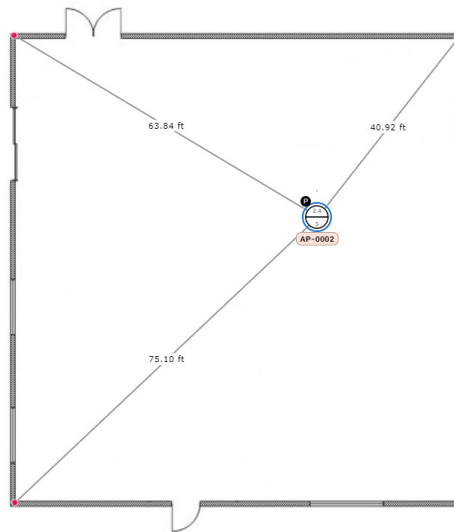
- Manually position it on the map. Use this method if you can approximate the location of the AP using reference points in the building that you can correlate to the detail on the floor map.



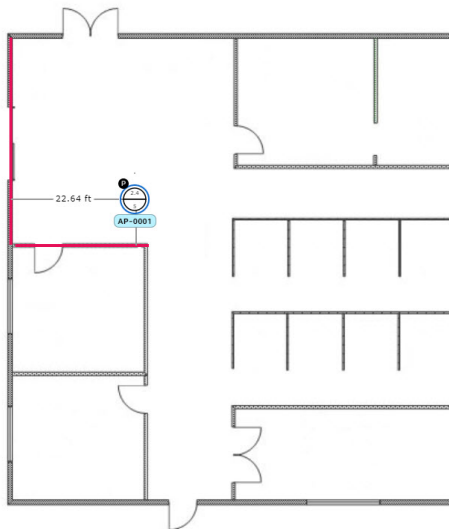
- Define its **x** and **y** coordinates. Use this method if you have the exact coordinates of the AP and you want its position on the map to be as accurate as possible.



- Triangulate it using 3 points. Use this method if you have large open space with only a few points from which to measure the distance to the AP. For example, you might measure from the AP to each corner of the room.



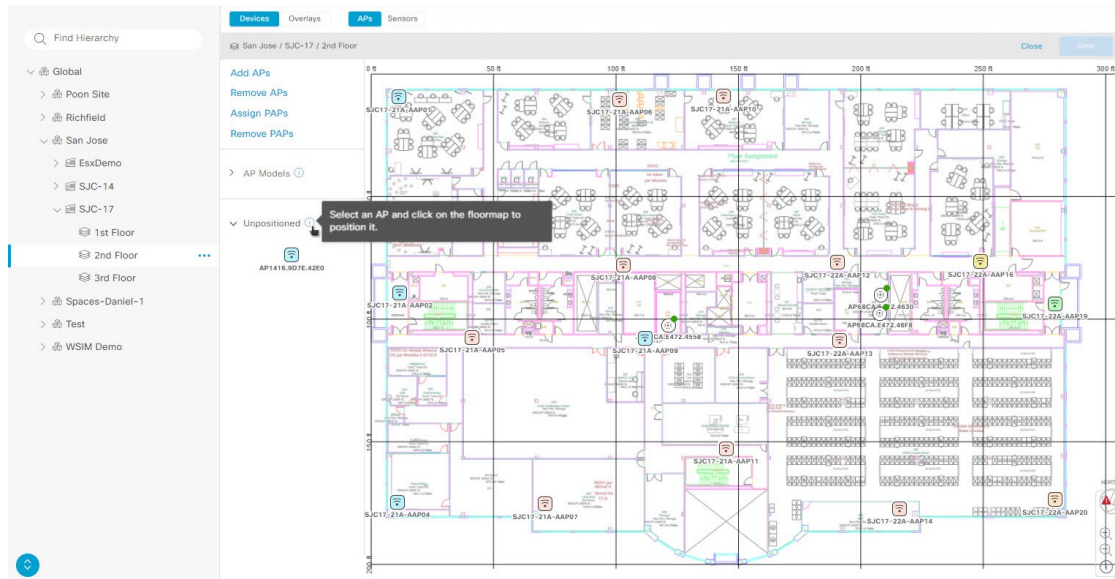
- Intersect it based on its distance from two walls. Use this method if the AP is located in a space where you have two walls that intersect, even if they aren't perpendicular to one another.



For all but the first method (manual positioning), you need to have your measurements on hand, and make sure the unit of measure is specified correctly in the **Global Map Properties** settings. For information, see in [2D Map View Options](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit**.
By default, the **Devices** and **Access Points** toggle buttons are chosen.
- Step 4** From the left pane of the map, in the **Unpositioned** area, click an AP.

Figure 4: Unpositioned APs



Step 5 To position the AP, use one of the following methods:

- Click the location on the floor map where you want to position the AP.
- Define its **x** and **y** coordinates in the **Edit AP** slide-in pane.
- Triangulate its location:
 - a. In the **Edit AP** slide-in pane, click **3 points**.
 - b. Click on floor map to draw the first point.
 - c. In the dialog box, set the distance from the AP to the first point and click **Set Distance**.
 - d. Define the second and third points similarly, and click **Save**.
- Define two walls on the floor map and position the APs between the defined walls:
 - a. In the **Edit AP** slide-in pane, click **2 walls**.
 - b. To define the first wall, click the floor map to start drawing the line. Click again to finish drawing the line. A dialog box is displayed to set the distance from the AP to the first wall.
 - c. Enter the distance in meters, and click **Set Distance**.
 - d. Define the second wall similarly, making sure that the distance to the AP from the first and second walls create an intersecting point.
 - e. Click **Save**.
The AP is placed based on the defined distance between the walls.

Step 6 In the map toolbar, click **Save**.

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

About Cisco ISE Configuration for Catalyst Center

If your network uses Cisco ISE for user authentication, you can configure Catalyst 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. From the top-left corner, 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

Catalyst 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 Catalyst 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 Catalyst Center with the AAA server, including defining the shared secret on both the AAA server and Catalyst Center.
- Define an attribute name for Catalyst Center on the AAA server.
- For a Catalyst Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.

Before you configure Cisco ISE, confirm that:

- You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the [Cisco Catalyst Center Compatibility Matrix](#). For information on installing Cisco ISE, see the [Cisco Identity Services Engine Install and Upgrade guides](#).
- If you have a standalone Cisco ISE deployment, you must integrate Catalyst Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.

- If you have a distributed Cisco ISE deployment:

You must integrate Catalyst 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 Policy Service Nodes (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 Protected Access Credentials (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 Catalyst 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 Catalyst 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 the fully qualified domain name (FQDN) in either the certificate subject name or the Subject Alternative Name (SAN).
- The Catalyst Center system certificate must list both the Catalyst 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 doesn't occur in Cisco ISE 3.0 and later. For more information, see the [Cisco ISE Release Notes](#).

Step 1 From the top-left corner, 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 must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).

Note Make sure that you do not configure a PSN that is part of an existing Cisco ISE cluster as a primary AAA server.

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

- **Server IP Address:** IP address of the Cisco ISE server.
- **Shared Secret:** Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).
- **Username:** Username that is used to log in to Cisco ISE via HTTPS.
- **Password:** Password for the Cisco ISE HTTPS username.

Note The username and password must be an ISE admin account that belongs to the Super Admin.

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

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

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

hostname.domainname.com

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

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

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

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

If you want to use the Catalyst Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Catalyst Center system as a pxGrid client), check the **Use Catalyst 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 Certificate Authority (CA). If this option is disabled, Catalyst 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 Catalyst Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
 - The Certificate Extended Key Use (EKU) field includes "Client Authentication."
- **Protocol:** **TACACS** and **RADIUS** (the default). You can select both protocols.

Attention If you do not enable TACACS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design > Network Settings > Servers** when configuring a AAA server for network device authentication.

- **Authentication Port:** UDP port used to relay authentication messages to the AAA server. The default UDP port used for authentication is 1812.
- **Accounting Port:** UDP port used to relay important events to the AAA server. The default is UDP port 1812.
- **Port:** TCP port used to communicate with the TACACS server. The default TCP port used for TACACS is 49.
- **Retries:** Number of times that Catalyst 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 Catalyst Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window.

Cisco ISE server registration phase:

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

pxGrid subscriptions registration phase:

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

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

Step 6 Click **Add**.

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

Step 8 To view the Cisco ISE integration status of a device, do the following:

- a. From the top-left corner, click the menu icon and choose **Provision > Inventory**.
The **Inventory** window displays the device information.
 - b. From the **Focus** drop-down menu, choose **Provision**.
 - c. In the **Devices** table, the **Provisioning Status** column displays information about the provisioning status of your device (**Success**, **Failed**, or **Not Provisioned**).
Click **See Details** to open a slide-in pane with additional information.
 - d. In the slide-in pane that is displayed, click **See Details**.
 - e. Scroll down to the **ISE Device Integration** tile to view detailed information about the integration status of the device.
-

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

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

Before you begin

Create a site and assign a device to the site. See [Create, Edit and Delete a Site, on page 20](#).

-
- Step 1** From the top-left corner, click the menu icon and choose **Design > Network Settings > Telemetry**.
- Step 2** In the **SNMP Traps** area, do one of the following:
- Check the **Use Catalyst Center as SNMP trap server** check box.
 - Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server. The selected server collects SNMP traps and messages from the network devices.
- Step 3** In the **Syslogs** area, do one of the following:
- Check the **Use Catalyst Center as syslog server** check box.
 - Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.
- Step 4** In the **Application Visibility** area, check the **Enable by default on wired access devices** check box to enable Application Telemetry and Controller-Based Application Recognition (CBAR) by default upon the network device site assignment.
- Do one of the following:
- Click the **Use Catalyst Center as NetFlow collector** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.
 - Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.
- Note** Catalyst Center must be configured as a destination in Cisco Telemetry Broker to receive NetFlow records. If Catalyst Center is not configured as a destination, the Application Experience does not work.
- Step 5** In the **Wired Endpoint Data Collection** area, click the **Enable Catalyst Center Wired Endpoint Data Collection At This Site** radio button to turn on IP Device Tracking (IPDT) on the access devices of the site.
- If you don't want to enable IPDT for the site, click the **Disable Catalyst Center Wired Endpoint Data Collection At This Site** radio button (the default).
- Note** You must enable IPDT to preview the CLI configuration. When provisioning a device, you can preview the CLI configuration before deploying it on the device.
- Step 6** In the **Wireless Controller, Access Point and Wireless Clients Health** area, check the **Enable Wireless Telemetry** check box to monitor the health of the wireless controllers, APs, and wireless clients in your network.

Step 7 Click **Save**.

Configure Cisco AI Network Analytics

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

Before you begin

- Make sure that you have the Advantage software license for Catalyst Center. The **AI Network Analytics** application is part of the Advantage software license.
- Make sure that the latest version of the AI Network Analytics application is installed. See the "Download and Install Packages and Updates" topic in the *Cisco Catalyst 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 From the top-left corner, 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 opens.

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.

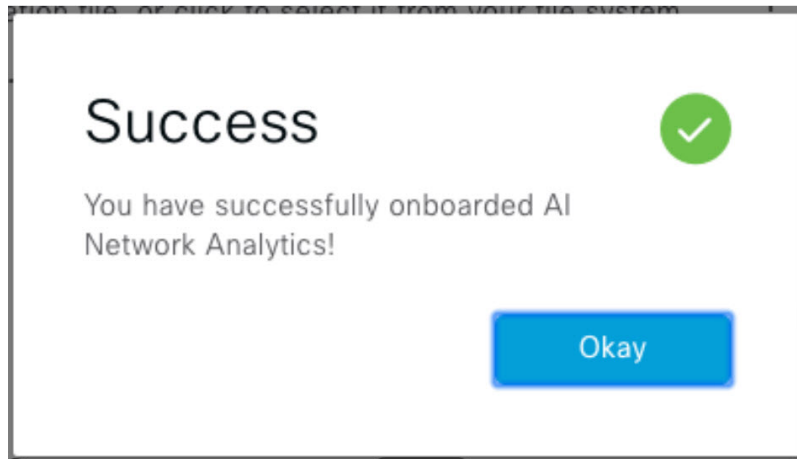
[Configure](#)

[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 opens.
 - 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 opens.



- For the first-time configuration of 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)**.

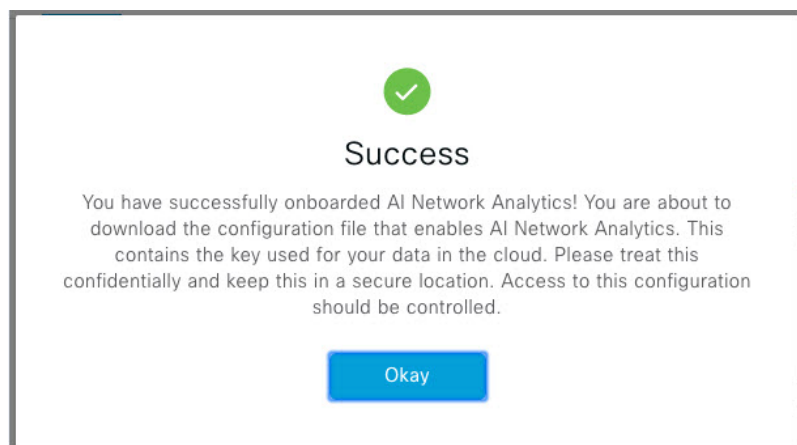
The system starts testing cloud connectivity as indicated by the **Testing cloud connectivity...** tab. After cloud connectivity testing completes, the **Testing cloud connectivity...** tab changes to **Cloud connection verified**.

- c. Click **Next**.

The terms and conditions window opens.

- 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 opens.



Step 4 In the **Success** dialog box, click **Okay**.

The **AI Network Analytics** window opens, and the **Enable AI Network Analytics** toggle button displays .

Step 5 (Recommended) In the **AI Network Analytics** window, click **Download Configuration file**.

Disable Cisco AI Network Analytics

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

Step 1 From the top-left corner, click the menu icon and choose **System > Settings**.

Step 2 Scroll down to **External Services** and choose **Cisco AI Analytics**.

For each feature, a check mark () indicates that the feature is enabled. If the check box is unchecked (), the feature is disabled.

Step 3 In the **AI Network Analytics** area, click the **Enable AI Network Analytics** toggle button so that it's unchecked ().

Step 4 Click **Update**.

Step 5 To delete your network data from the Cisco AI Network Analytics cloud, contact the Cisco Technical Response Center (TAC) and open a support request.

Step 6 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 Catalyst Center to automatically update the Machine Reasoning Knowledge Base daily, or you can perform a manual update.

Step 1 From the top-left corner, 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's a new update to the Machine Reasoning Knowledge Base, the **AVAILABLE UPDATE** area is displayed 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 Catalyst Center daily.
- **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER, SECURITY ADVISORY, FIELD NOTICES AND EOX:** Integrates Catalyst Center with CX Cloud that allows you to perform an automated config. This integration provides enhanced vulnerability detection on devices directly from the security advisories tool on Catalyst Center.

- Step 3** (Recommended) Check the **AUTO UPDATE** check box to automatically update the Machine Reasoning Knowledge Base.
The **Next Attempt** area shows the date and time of the next update.
You can perform an automatic update only if Catalyst Center is successfully connected to the Machine Reasoning Engine in the cloud.
- Step 4** To manually update the Machine Reasoning Knowledge Base in Catalyst 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 Catalyst 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 Catalyst Center.
- Step 5** Check the **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY** check box to enable Cisco CX Cloud connection with network bug identifier and security advisory.
- Step 6** In the **Security Advisories Settings** area click the **RECURRING SCAN** toggle button to enable or disable the weekly recurring scan.
- Step 7** Click the **CISCO CX CLOUD** toggle button to enable or disable the Cisco CX cloud.
-

Enable Localization

You can view the Catalyst Center GUI windows in English (the default), Chinese, Japanese, or Korean.

To change the default language, perform the following task:

- Step 1** In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.
- From Google Chrome, do the following:
 - a. Click the  icon in the top-right corner, and then choose **Settings**.
 - b. Click **Languages**.
 - c. Click **Add languages**.
 - d. In the **Add languages** dialog box, choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
 - From Mozilla Firefox, do the following:
 - a. Click the  icon in the top-right corner, and then choose **Settings**.
 - b. From the **Language and Appearance > Language** area, click **Choose**.

- c. From the **Select a language to add** drop-down list, choose **Chinese, Japanese, or Korean**.
- d. Click **OK**.

Step 2

Log in to Catalyst Center.

The GUI is shown in the selected language.
