Discover Your Network

- About Discovery, on page 1
- Discovery Dashboard, on page 2
- Discovery Prerequisites, on page 2
- Discovery Credentials, on page 3
- Preferred Management IP Address, on page 5
- Discovery Configuration Guidelines and Limitations, on page 5
- Perform Discovery, on page 6
- Manage Discovery Jobs, on page 21

About Discovery

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

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

There are three ways for you to discover devices:

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

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

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

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

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

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

Discovery Dashboard

In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery** to view the **Discovery Dashboard**. The **Discovery Dashboard** shows the inventory overview, latest discovery, discovery type, discovery status, and recent discoveries.

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the Supported Devices List.
- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential. For more information, see Discovery Credentials, on page 3.
- Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following criteria is met:
  - The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).
  - You configure the device’s enable password as part of the CLI credentials configured in the Discovery job. For more information, see Discovery Configuration Guidelines and Limitations, on page 5.

Discovery Credentials

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

- Network devices: CLI and SNMP credentials.

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

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

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

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

Discovery Credentials and Cisco ISE

If you are using Cisco ISE as an authentication server, the Discovery feature authenticates devices using Cisco ISE as part of the discovery process. To make sure that your devices are discovered properly, follow these guidelines:

- Do not use Discovery credentials that have fewer than 4 alphanumeric characters. Although devices may have credentials with fewer than 4 alphanumeric characters, Cisco ISE allows 4 alphanumeric characters as the minimum username and password length. If the device credentials have fewer than 4 characters, Cisco DNA Center cannot collect the device’s inventory data, and the device will go into a partial collection state.

- Do not use credentials that have the same username, but different passwords (cisco/cisco123 and cisco/pw123). While Cisco DNA Center allows the discovery of devices with the same username but different passwords, Cisco ISE does not allow this. If a duplicate username is used, Cisco DNA Center cannot authenticate the device and collect its inventory data, and the device will go into a partial collection state.

For information on how to define Cisco ISE as a AAA server, see Add Cisco ISE or Other AAA Servers.

Guidelines and Limitations for Discovery Credentials

The following are the guidelines and limitations for the Cisco DNA Center Discovery credentials:

- To change the device credentials used in a Discovery job, you need to edit the Discovery job and deselect the credentials that you no longer want to use. Then, you need to add the new credentials and start the discovery. For more information, see Change Credentials in a Discovery Job, on page 22.
- If you change a device's credential after successfully discovering the device, subsequent polling cycles for that device fail. To correct this situation, use one of the following options:
    - Use the Discovery tool to:
        - Run a new Discovery job with job-specific credentials that match the device's new credential.
        - Edit the existing Discovery job and re-run the Discovery job.
    - Use the Design tool to:
        - Create a new global credential and run a new Discovery job using the correct global credential.
        - Edit an existing global credential and use Copy & Edit to recreate the Discovery job. Alternately, create a new Discovery job.
- If an ongoing Discovery polling cycle fails because of a device authentication failure, you can correct the situation using one of following options:
    - Use the Discovery tool to:
        - Stop or delete the current Discovery job and run a new Discovery job with job-specific credentials that match the device's credential.
        - Stop or delete the current Discovery job, edit the existing Discovery job, and re-run the Discovery job.
    - Use the Design tool to:
        - Create a new global credential and run a new Discovery job using the correct global credential.
        - Edit an existing global credential and use Copy & Edit to recreate the Discovery job. Alternately, create a new Discovery job.
- Deleting a global credential does not affect previously discovered devices. The status of the previously discovered devices does not indicate an authentication failure. However, the next Discovery job that tries to use the deleted credential will fail. The Discovery job will fail **before** it tries to contact any devices.

Discovery Credentials Example

The devices that form a typical network can have widely varying Discovery requirements. Cisco DNA Center lets you create multiple Discovery jobs to support these varying requirements. For example, assume that a network of 200 devices form a Cisco Discovery Protocol (CDP) neighborhood. In this network, 190 devices share a global credential (Credential 0) and the remaining devices each have their own unique credential (Credential-1 through Credential-10).

To discover all the devices in this network using Cisco DNA Center, perform the following task:

Step 1 Configure the CLI global credentials as Credential-0.

Step 2 Configure the SNMP (v2c or v3) global credentials.

Step 3 Run a Discovery job using one of the 190 device IP addresses (190 devices that share the global credentials) and the global Credential-0.

Step 4 Run 10 separate Discovery jobs for each of the remaining 10 devices using the appropriate job-specific credentials, for example, Credential-1, Credential-2, Credential-3, and so on.

Step 5 Review the results in the **Inventory** window.

Preferred Management IP Address

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

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

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

After a device is discovered, you can update the management IP address from the **Inventory** window. For more information, see Update a Device's Management IP Address.

Discovery Configuration Guidelines and Limitations

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

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

Perform Discovery

Discover Your Network Using CDP

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see Discover Your Network Using an IP Address Range, on page 11 and Discover Your Network Using LLDP, on page 16.

Note

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

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 2.
- 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 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

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

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

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

a) For **Discovery Type**, click **CDP**.

b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.

c) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

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

d) Click +.

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

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

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

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

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

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

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

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

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

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) To configure CLI credentials, configure the following fields:

Table 1: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	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.

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

Table 2: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 3: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.

Field	Description
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 4: SNMP Properties

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

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

Table 5: HTTP(S) Credentials

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

Field	Description
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

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

Note You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller devices. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices. NETCONF will be disabled if you select Telnet in the **Advanced** area.

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

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

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

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

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

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

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

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

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

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other Discovery methods, see Discover Your Network Using CDP, on page 6 and Discover Your Network Using LLDP, on page 16.

Before you begin

Your devices must have the required device configurations, as described in Discovery Prerequisites, on page 2.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

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

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

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

a) For **Discovery Type**, click **IP Address/Range**.

b) In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Cisco DNA Center to scan, and click +.

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

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

c) (Optional) Repeat Step b to enter additional IP address ranges.

d) (Optional) In the **Subnet Filter** field, enter an IP address/range or subnet to exclude from the Discovery scan. You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x*/*y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

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

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

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

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

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

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) To configure CLI credentials, configure the following fields:

Table 6: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	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.

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

Table 7: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 8: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.

Field	Description
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 9: SNMP Properties

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

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

Table 10: HTTP(S) Credentials

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

Field	Description
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

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

Note You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller devices. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

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

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

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

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

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

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

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

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

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

Discover Your Network Using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see Discover Your Network Using CDP, on page 6 and Discover Your Network Using an IP Address Range, on page 11.

Note

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

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 2.
- 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 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

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

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

Step 4 Expand the **IP Address/Range** area and configure the following fields:

a) For **Discovery Type**, click **LLDP**.

b) In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.

c) (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

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

d) Click +.

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

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

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

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

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

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

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

Step 5 Expand the **Credentials** area and configure the credentials that you want to use for the Discovery job.

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

a) Make sure that the global credentials that you want to use are selected. If you do not want to use a credential, deselect it.

b) To add additional credentials, click **Add Credentials**.

c) For CLI credentials, configure the following fields:

Table 11: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	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.

Field	Description
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.

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

Table 12: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 13: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 14: SNMP Properties

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

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

Table 15: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.
Read	You can configure up to 10 HTTPS read credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).
Write	You can configure up to 10 HTTPS write credentials: • **Name/Description**: Name or description of the HTTPS credentials that you are adding. • **Username**: Name used to authenticate the HTTPS connection. • **Password**: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). The password must contain from 7 to 128 characters, including at least one: • Lowercase letter (a - z) • Uppercase letter (A - Z) • Number (0 - 9) • Special character: # _ * ? – The password cannot contain spaces or angle brackets (< >). Note that some Cisco IOS XE devices do not allow a question mark (?).

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

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

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

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

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

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

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

Manage Discovery Jobs

Stop and Start a Discovery Job

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

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

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

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

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

Edit a Discovery Job

You can edit an existing Discovery job and then rerun the Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

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

Step 4 Click **Edit**.

Step 5 Depending on the Discovery type, you can change the type of job, except for the following fields:

- **CDP**: Discovery name, Discovery type, IP address. For more information about the fields you can change, see Discover Your Network Using CDP, on page 6.
- **IP Range**: Discovery name, type, IP address range (although you can add additional IP address ranges). For more information about the fields you can change, see Discover Your Network Using an IP Address Range, on page 11.
- **LLDP**: Discovery name, type, IP address. For more information about the fields you can change, see Discover Your Network Using LLDP, on page 16.

Step 6 Click **Start**.

Change Credentials in a Discovery Job

You can change the credentials used in a Discovery job and then re-run the Discovery job.

Before you begin

You should have created at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

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

Step 4 Click **Edit**.

Step 5 Expand the **Credentials** area.

Step 6 Deselect the credentials that you do not want to use.

Step 7 Configure the credentials that you want to use:

a) Click **Add Credentials**.

b) To configure CLI credentials, configure the following fields:

Table 16: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	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.

Field	Description
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.

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

Table 17: SNMPv2c Credentials

Field	Description
Read	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **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. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

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

Table 18: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **noAuthNoPriv**: Does not provide authentication or encryption. • **AuthNoPriv**: Provides authentication, but does not provide encryption. • **AuthPriv**: Provides both authentication and encryption.

Field	Description
Auth Type	Authentication type to be used. (Enabled if you select **AuthPriv** or **AuthNoPriv** as the authentication mode.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **AuthPriv** as the authentication mode.) Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **None**: No privacy.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords (or passphrases) must be at least eight characters long. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Click **Start**.

Clone a Discovery Job

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

Before you begin

You should have run at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

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

Step 4 Click **Copy & Edit**.

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

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

Step 6 Define or update the parameters for the new Discovery job.

Delete a Discovery Job

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

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

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

Step 4 Click **Delete**.

Step 5 Click **OK** to confirm.

View Discovery Job Information

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

Before you begin

Run at least one Discovery job.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

Step 2 Click **View All Discoveries**.

Step 3 From the **Discoveries** pane, select the Discovery job. Alternatively, use the **Search** function to find a Discovery job by device IP address or name.

Step 4 Click the down arrow next to one of the following areas for more information:

- **Discovery Details**: Displays the parameters that were used to run the Discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.
- **Credentials**: Provides the names of the credentials that were used.

- **History**: Lists each Discovery job that was run, including the time when the job started, and whether any devices were discovered.

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

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