



# Discover Your Network

---

- [Discovery Overview, 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 24](#)

## Discovery Overview

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

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

There are three ways for you to discover devices:

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

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

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



---

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

---

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



---

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

---

## Discovery Dashboard

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 [Cisco DNA Center Compatibility Matrix](#).
- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure that at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential. 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 25](#).
- 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). These credentials are the same CLI username and password that you configure in Cisco DNA Center for the Discovery function. Cisco DNA Center requires the highest access level to the device.
- Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
- Do not change the default login method for a device's console port and the VTY lines. If a device is already configured with a AAA (TACACS) login, make sure that the CLI credential defined in the Cisco DNA Center is the same as the TACACS credential defined in the TACACS server.
- Cisco wireless controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.

# Perform Discovery

The following sections provide information about how to 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.

**Note**

- The Discovery function requires the correct SNMP read-only community string. If an SNMP read-only community string is not provided, as a *best effort*, the Discovery function uses the default SNMP read-only 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 host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

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

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

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

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

- **Discovery Type:** Enable CDP by clicking the **CDP** radio button.
- **IP Address:** Enter a seed IP address for Cisco DNA Center to start the Discovery scan.
- **Subnet Filters:** Exclude an IP address or subnet from the Discovery scan. To exclude an IP address, enter an individual IP address ( $x.x.x.x$ ). To exclude a subnet, enter a classless inter-domain routing (CIDR) address ( $x.x.x.x/y$ ), where  $x.x.x.x$  is the IP address and  $y$  is the subnet mask. The subnet mask can be a value from 0 to 32.

To exclude more IP addresses and subnets, click the add icon (+).

- **CDP Level:** 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.

- **Preferred Management IP Address:** Click one of the following radio buttons:

- **None:** Allow the device to use any of its IP addresses.

- **Use Loopback IP:** Specify the device 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 IP address of the CDP neighbor is reachable from Cisco DNA Center.

**Step 5** Expand the **Credentials** area and choose the credentials that you want to use.

Choose any of the global credentials that have already been created or configure your own Discovery credentials.

**Step 6** To use existing credentials, select the global credentials that you want to use and proceed to Step 14. If you do not want to use a credential, deselect it.

**Step 7** To configure new credentials, click **Add Credentials**.

**Note** If you configure your own credentials, you can save them future Discovery jobs by checking the **Save as global settings** check box.

**Step 8** For CLI credentials, do the following:

a) Configure the following fields:

*Table 1: CLI Credentials*

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

b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.

c) Click **Save**.

**Step 9** For SNMP v2c credentials, click **SNMP v2c** and do the following:

a) Configure the following fields:

Table 2: SNMPv2c Credentials

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

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

**Step 10**

(Optional) For SNMP v3 credentials, click **SNMP v3** and do the following:

- a) Configure the following fields:

Table 3: SNMPv3 Credentials

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



Field	Description
<b>Auth Password</b>	<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><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
<b>Privacy Type</b>	<p>Privacy type. (Enabled if you select <b>AuthPriv</b> as <b>Mode</b>.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> <li>• <b>AES128</b>: 128-bit CBC mode AES for encryption.</li> <li>• <b>AES192</b>: 192-bit CBC mode AES for encryption.</li> <li>• <b>AES256</b>: 256-bit CBC mode AES for encryption.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Discovery and Inventory features support only AES192 and AES256 privacy types.</li> <li>• Cisco DNA Assurance does not support any of these privacy types.</li> </ul>
<b>Privacy Password</b>	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

**Step 11**

(Optional) To configure SNMP properties, click **SNMP PROPERTIES** and do the following:

- a) Configure the following fields:

Table 4: SNMP Properties

Field	Description
<b>Retries</b>	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
<b>Timeout</b>	Amount of time, in seconds, between retries.

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

**Step 12**

(Optional) To configure HTTP(S) credentials, click **HTTP(S)** and do the following:

- a) Configure the following fields:

Table 5: HTTP(S) Credentials

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

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

- b) (Optional) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

### Step 13

(Optional) If you have network devices with NETCONF enabled and want Cisco DNA Center to use NETCONF to install, manipulate, and delete the configurations of these devices, click **NETCONF** and do the following:

- a) In the **Port** field, enter a port number. You can use one of the following ports:
- Port 830 (default)
  - Any other port that is available on the device
  - A custom port that Cisco DNA Center configures (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the [Cisco DNA Center Administrator Guide](#).)
- )

**Note** NETCONF is disabled if you choose the **Telnet** protocol in the **Advanced** area of the **Add Discovery** window.

**Note** To discover Cisco Catalyst 9800 Series Wireless Controller devices, you must enable NETCONF.

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

- Step 14** (Optional) To configure the protocols that are used to connect with devices, expand the **Advanced** area and do the following:
- Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.
  - Drag and drop the protocols in the order that you want them to be used.

**Note** NETCONF is disabled if you choose the **Telnet** protocol in the **Advanced** area of the **Add Discovery** window.

**Step 15** Click **Discover**.

**Step 16** To run Discovery now, click the **Now** radio button in the **Discover Devices** slide-in pane and click **Start**. Otherwise, proceed to the next step.

If you want to discover only new devices, click the **Discover only new devices** toggle button.

**Step 17** To schedule Discovery for a later time, do the following:

- Click the **Later** radio button.
- Define the start date and time.
- From the **Time Zone** drop-down list, choose a time zone.
- In the **Recurrence** area, click **None**, **Daily**, or **Weekly**.
  - **None**: Discovery will not recur.
  - **Daily**: Enter the interval in days in the **Run at Interval (Days)** field.
  - **Weekly**: Enter the interval in weeks in the **Run at Interval (Weeks)** field.
- If you have chosen **Daily** or **Weekly** for recurrence, check the **Set Schedule End** check box to define the end date and time.
 

**Note** You can discover only new devices in recurrence. The **Discover only new devices** toggle button at the top is enabled by default.
- Click **End Date** or **End After**.
  - **End Date**: Enter month, date, and year for recurrence to end.
  - **End After**: Enter the number of occurrences after you want recurrence to end.
- Click **Start**.

Click the notifications icon to view the scheduled Discovery. Before Discovery starts, you can click **Edit** to edit it, or **Cancel** to cancel it.

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.

### Before you begin

Your devices must have the required device configurations, as described in [Discovery Prerequisites, on page 2](#).

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

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

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

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

- **Discovery Type:** Discover devices using an IP address or address range by clicking the **IP Address/Range** radio button.
- **From** and **To** fields: Enter the beginning IP address in the **From** field and the ending IP address in the **To** field.

Click the add icon (+) to add more IP address ranges.

**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.

- **Subnet Filters:** Exclude an IP address or subnet from the Discovery scan. To exclude an IP address, enter an individual IP address ( $x.x.x.x$ ). To exclude a subnet, enter a classless inter-domain routing (CIDR) address ( $x.x.x.x/y$ ), where  $x.x.x.x$  is the IP address and  $y$  is the subnet mask. The subnet mask can be a value from 0 to 32.

To exclude more IP addresses and subnets, click the add icon (+).

- **Preferred Management IP Address:** Click one of the following radio buttons:

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

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

**Step 5** Expand the **Credentials** area and choose the credentials that you want to use.

Choose any of the global credentials that have already been created or configure your own Discovery credentials.

**Step 6** To use existing credentials, select the global credentials that you want to use and proceed to Step 14. If you do not want to use a credential, deselect it.

**Step 7** To configure new credentials, click **Add Credentials**.

**Note** If you configure your own credentials, you can save them future Discovery jobs by checking the **Save as global settings** check box.

**Step 8** For CLI credentials, do the following:

- a) Configure the following fields:

**Table 6: CLI Credentials**

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

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

## Step 9

For SNMP v2c credentials, click **SNMP v2c** and do the following:

- a) Configure the following fields:

**Table 7: SNMPv2c Credentials**

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

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.

c) Click **Save**.

### Step 10

(Optional) For SNMP v3 credentials, click **SNMP v3** and do the following:

a) Configure the following fields:

*Table 8: SNMPv3 Credentials*

Field	Description
<b>Name/Description</b>	Name or description of the SNMPv3 settings that you are adding.
<b>Username</b>	Name associated with the SNMPv3 settings.
<b>Mode</b>	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> <li>• <b>noAuthNoPriv</b>: Does not provide authentication or encryption.</li> <li>• <b>AuthNoPriv</b>: Provides authentication, but does not provide encryption.</li> <li>• <b>AuthPriv</b>: Provides both authentication and encryption.</li> </ul>
<b>Auth Type</b>	Authentication type to be used. (Enabled if you select <b>AuthPriv</b> or <b>AuthNoPriv</b> as <b>Mode</b> .) Choose one of the following authentication types: <ul style="list-style-type: none"> <li>• <b>SHA</b>: Authentication based on HMAC-SHA.</li> <li>• <b>MD5</b>: Authentication based on HMAC-MD5.</li> </ul>
<b>Auth Password</b>	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><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
<b>Privacy Type</b>	Privacy type. (Enabled if you select <b>AuthPriv</b> as <b>Mode</b> .) Choose one of the following privacy types: <ul style="list-style-type: none"> <li>• <b>AES128</b>: 128-bit CBC mode AES for encryption.</li> <li>• <b>AES192</b>: 192-bit CBC mode AES for encryption.</li> <li>• <b>AES256</b>: 256-bit CBC mode AES for encryption.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Discovery and Inventory features support only AES192 and AES256 privacy types.</li> <li>• Cisco DNA Assurance does not support any of these privacy types.</li> </ul>

Field	Description
<b>Privacy Password</b>	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

**Step 11**

(Optional) To configure SNMP properties, click **SNMP PROPERTIES** and do the following:

- a) Configure the following fields:

*Table 9: SNMP Properties*

Field	Description
<b>Retries</b>	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
<b>Timeout</b>	Amount of time, in seconds, between retries.

- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

**Step 12**

(Optional) To configure HTTP(s) credentials, click **HTTP(S)** and do the following:

- a) Configure the following fields:

*Table 10: HTTP(S) Credentials*

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



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

- b) (Optional) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
- c) Click **Save**.

- Step 13** (Optional) If you have network devices with NETCONF enabled and want Cisco DNA Center to use NETCONF to install, manipulate, and delete the configurations of these devices, click **NETCONF** and do the following:
- a) In the **Port** field, enter a port number. You can use one of the following ports:
    - Port 830 (default)
    - Any other port that is available on the device
    - A custom port that Cisco DNA Center configures (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the [Cisco DNA Center Administrator Guide](#).)
- )
- Note** NETCONF is disabled if you choose the **Telnet** protocol in the **Advanced** area of the **Add Discovery** window.
- Note** To discover Cisco Catalyst 9800 Series Wireless Controller devices, you must enable NETCONF.
- b) If you want to save these credentials for future use, click the **Save as global settings** check box. If you don't click this checkbox, the credentials can be used only for the current Discovery job.
  - c) Click **Save**.
- Step 14** (Optional) To configure the protocols that are used to connect with devices, expand the **Advanced** area and do the following:
- 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.
- Note** NETCONF is disabled if you choose the **Telnet** protocol in the **Advanced** area of the **Add Discovery** window.
- Step 15** Click **Discover**.
- Step 16** To run the discovery now, click the **Now** radio button and click **Start**. Otherwise, proceed to the next step. If you want to discover only new devices, click the **Discover only new devices** toggle button.
- Step 17** To schedule the discovery for a later time, do the following:
- a. Click the **Later** radio button.
  - b. Define the start date and time.
  - c. From the **Time Zone** drop-down list, choose a time zone.
  - d. In the **Recurrence** area, click **None**, **Daily**, or **Weekly**.
    - **None**: Discovery will not recur.
    - **Daily**: Enter the interval in days in the **Run at Interval (Days)** field.
    - **Weekly**: Enter the interval in weeks in the **Run at Interval (Weeks)** field.
  - e. If you have chosen **Daily** or **Weekly** for recurrence, check the **Set Schedule End** check box to define the end date and time.

**Note** You can discover only new devices in recurrence. The **Discover only new devices** toggle button at the top is enabled by default.

f. Click **End Date** or **End After**.

- **End Date:** Enter month, date, and year for recurrence to end.
- **End After:** Enter the number of occurrences after you want recurrence to end.

g. Click **Start**.

Click the notifications icon to view the scheduled Discovery. Before Discovery starts, you can click **Edit** to edit it, or **Cancel** to cancel it.

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.



- Note**
- Discovery requires the correct SNMP read-only community string. If one is not provided, Discovery uses the default SNMP read-only community string, public, as a *best effort*.
  - 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** Click the menu icon (☰) and choose **Tools > Discovery**.


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

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

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

- **Discovery Type:** Enable LLDP by clicking the **LLDP** radio button.
- **IP Address:** Enter a seed IP address for Cisco DNA Center to start the Discovery scan.

- **Subnet Filters:** Exclude an IP address or subnet from the Discovery scan. To exclude an IP address, enter an individual IP address ( $x.x.x.x$ ). To exclude a subnet, enter a classless inter-domain routing (CIDR) address ( $x.x.x.x/y$ ), where  $x.x.x.x$  is the IP address and  $y$  is the subnet mask. The subnet mask can be a value from 0 to 32.

To exclude more IP addresses and subnets, click the add icon (  ).

- **LLDP Level:** 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.

- **Preferred Management IP Address:** Click one of the following radio buttons:

- **None:** Allow the device to use any of its IP addresses.

- **Use Loopback IP:** Specify the device 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 IP address of the LLDP neighbor 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.

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

**Table 11: CLI Credentials**

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

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

**Table 12: SNMPv2c Credentials**

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

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

**Table 13: SNMPv3 Credentials**

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

Field	Description
<b>Auth Password</b>	<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><b>Note</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
<b>Privacy Type</b>	<p>Privacy type. (Enabled if you select <b>AuthPriv</b> as <b>Mode</b>.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> <li><b>AES128</b>: 128-bit CBC mode AES for encryption.</li> <li><b>AES192</b>: 192-bit CBC mode AES for encryption.</li> <li><b>AES256</b>: 256-bit CBC mode AES for encryption.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Discovery and Inventory features support only AES192 and AES256 privacy types.</li> <li>Cisco DNA Assurance does not support any of these privacy types.</li> </ul>
<b>Privacy Password</b>	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>

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

**Table 14: SNMP Properties**

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

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

Table 15: HTTP(S) Credentials

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

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

- 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**.

The **Discover Devices** slide-in pane appears.

**Step 8** To run the discovery now, click the **Now** radio button and click **Start**.

If you want to discover only new devices, click the **Discover only new devices** toggle button.

**Step 9** To schedule the discovery for a later time, do the following:

- a. Click the **Later** radio button.
- b. Define the start date and time.
- c. From the **Time Zone** drop-down list, choose a time zone.
- d. In the **Recurrence** area, click **None**, **Daily**, or **Weekly**.
  - **None**: Discovery will not recur.
  - **Daily**: Enter the interval in days in the **Run at Interval (Days)** field.
  - **Weekly**: Enter the interval in weeks in the **Run at Interval (Weeks)** field.
- e. If you have chosen **Daily** or **Weekly** for recurrence, check the **Set Schedule End** check box to define the end date and time.

**Note** You can discover only new devices in recurrence. The **Discover only new devices** toggle button at the top is enabled by default.
- f. Click **End Date** or **End After**.
  - **End Date**: Enter month, date, and year for recurrence to end.
  - **End After**: Enter the number of occurrences after you want recurrence to end.
- g. Click **Start**.

Click the notifications icon to view the scheduled Discovery. Before Discovery starts, you can click **Edit** to edit it, or **Cancel** to cancel it.

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

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

---

## Manage Discovery Jobs

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



## Stop and Start a Discovery Job

---

- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** In the **Discovery** window, click **View All Discoveries**.
- Step 3** To stop an active Discovery job, perform these steps:
- In the left **Discoveries** pane, click a Discovery job.
  - In the bottom pane, on the right side, click **Stop**.
- Step 4** To restart an inactive Discovery job, perform these steps:
- In the left **Discoveries** pane, click a Discovery job.
  - In the bottom pane, on the right side, click **Re-discover**.
- 

## Edit a Discovery Job

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

---

- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** In the **Discovery** window, 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 13](#).
  - **LLDP**: Discovery name, type, IP address. For more information about the fields you can change, see [Discover Your Network Using LLDP, on page 19](#).
- Step 6** Click **Start**.
- 

## Change Credentials in a Discovery Job

You can change the credentials used in a Discovery job and then rerun the Discovery job.

### Before you begin

You should have created at least one Discovery job.

---

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

- Step 2** In the **Discovery** window, click **View All Discoveries**.
- Step 3** 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:
- Click **Add Credentials**.
  - To configure CLI credentials, configure the following fields:

Table 16: CLI Credentials

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

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

Table 17: SNMPv2c Credentials

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

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

**Table 18: SNMPv3 Credentials**

Field	Description
<b>Name/Description</b>	Name or description of the SNMPv3 settings that you are adding.
<b>Username</b>	Name associated with the SNMPv3 settings.
<b>Mode</b>	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> <li>• <b>noAuthNoPriv</b>: Does not provide authentication or encryption.</li> <li>• <b>AuthNoPriv</b>: Provides authentication, but does not provide encryption.</li> <li>• <b>AuthPriv</b>: Provides both authentication and encryption.</li> </ul>
<b>Auth Type</b>	Authentication type to be used. (Enabled if you select <b>AuthPriv</b> or <b>AuthNoPriv</b> as <b>Mode</b> .) Choose one of the following authentication types: <ul style="list-style-type: none"> <li>• <b>SHA</b>: Authentication based on HMAC-SHA.</li> <li>• <b>MD5</b>: Authentication based on HMAC-MD5.</li> </ul>
<b>Auth Password</b>	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><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>
<b>Privacy Type</b>	Privacy type. (Enabled if you select <b>AuthPriv</b> as <b>Mode</b> .) Choose one of the following privacy types: <ul style="list-style-type: none"> <li>• <b>AES128</b>: 128-bit CBC mode AES for encryption.</li> <li>• <b>AES192</b>: 192-bit CBC mode AES for encryption.</li> <li>• <b>AES256</b>: 256-bit CBC mode AES for encryption.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Discovery and Inventory features support only AES192 and AES256 privacy types.</li> <li>• Cisco DNA Assurance does not support any of these privacy types.</li> </ul>

Field	Description
<b>Privacy Password</b>	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Passwords are encrypted for security reasons and are not displayed in the configuration.</li> </ul>

**Step 8** Click **Start**.

---

## Clone a Discovery Job

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

### Before you begin

You should have run at least one Discovery job.

---

- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** In the **Discovery** window, click **View All Discoveries**.
- Step 3** In the left **Discoveries** pane, click a Discovery job.
- Step 4** In the bottom pane, on the right side, click **Copy & Edit**.  
Cisco DNA Center creates a copy of the Discovery job, named Clone of *Discovery\_Job*.
- Step 5** (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.
- Step 6** Define or update the parameters for the new Discovery job.
- 

## Delete a Discovery Job

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

---

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

**Step 5** Click **OK** to confirm.

---

## View Discovery Job Information

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

### Before you begin

Run at least one Discovery job.

---

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

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

**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.

---

