Discover Your Network

• About Discovery, on page 1
• Discovery Prerequisites, on page 2
• Discovery Credentials, on page 2
• Preferred Management IP Address, on page 4
• Discovery Configuration Guidelines and Limitations, on page 5
• Perform Discovery, on page 5
• Manage Discovery Jobs, on page 20

About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory. The Discovery feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

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.
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.

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

**Discovery Prerequisites**

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the Supported Devices List.
- Understand that the maximum network latency between Cisco DNA Center and devices is 50 ms.
- 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 2.
- 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 two criteria are 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:

- Standard Cisco devices: CLI and SNMP credentials.
- NFVIS devices: HTTP(S) credentials.
• Both standard and NFVIS devices: 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 define up to five saved 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 20.

• 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 rerun 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 re-run the 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 rerun 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 re-run the 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. For example, 25 minutes after you delete the credential, Discovery jobs that use it will fail.

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 logs one of the device's IP addresses as the preferred management IP address for the device. The IP address can be that of a built-in management interface of the device, or another physical interface, or a logical interface like Loopback0. You can configure Cisco DNA Center to log the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.
If you choose to use a device's loopback IP address 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. Cisco DNA Center cannot discover devices that enforce the AAA login method.
- 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 10 and Discover Your Network Using LLDP, on page 15.
Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a best effort, the Discovery function uses the default SNMP RO community string, public.

- CLI credentials are not required to discover hosts; hosts are discovered through the network devices that they are connected to.

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
From the Cisco DNA Center home page, click Discovery.

Step 2
In the Discovery Name field, enter a name.

Step 3
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 4.

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 4  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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

d) Click SNMP v2c and configure the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td><strong>• Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td><strong>• Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write</td>
<td><strong>• Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td><strong>• Write Community</strong>—Write community string used to make changes to the SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
e) (Optional) Click **SNMP v3** and configure the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select <strong>AuthPriv</strong> or <strong>AuthNoPriv</strong> as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td>Auth Password</td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
<tr>
<td>Privacy Type</td>
<td>Privacy type. (Enabled if you select <strong>AuthPriv</strong> as the authentication mode.) Choose one of the following privacy types:</td>
</tr>
</tbody>
</table>

**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.

- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **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 DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>

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

**Table 5: HTTP(S) Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
</tbody>
</table>
| Read    | You can configure up to 5 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.
  - **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

  Note: The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `< > @ : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration. |
You can configure up to 5 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.
- **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 at least one lower case, one upper case, one digit, and a special character and must not contain < > @ ' , : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

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 5**

(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 6**

Click **Start**.

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 5 and Discover Your Network Using LLDP, on page 15.

**Before you begin**

Your devices must have the required device configurations, as described in Discover Prerequisites, on page 2.
Step 1  From the Cisco DNA Center home page, click Discovery.
Step 2  In the Discovery Name field, enter a name.
Step 3  Expand the IP Address/Ranges area, if it is not already visible, and configure the following fields:
   a) For Discovery Type, click 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) 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 4.

Step 4  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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation.</td>
</tr>
</tbody>
</table>

   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, enter the enable password again.

Note: Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 7: SNMPv2c Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td>Read Community</td>
<td>Read-only community string password used only to view SNMP information on the device.</td>
</tr>
</tbody>
</table>

Note: Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 8: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• noAuthNoPriv: Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthNoPriv: Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• AuthPriv: Provides both authentication and encryption.</td>
</tr>
</tbody>
</table>
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 8 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 a the authentication mode.) Choose one of the following privacy types:

- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **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 DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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.

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

**Table 9: SNMP Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retries</strong></td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>
g) (Optional) Click **HTTP(S)** and configure the following fields:

**Table 10: HTTP(S) Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
</tbody>
</table>
| **Read** | You can configure up to 5 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.  
  - **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).  
  **Note**  
  The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `<` `>` `@` `;` `:` `!` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration. |

| **Write** | You can configure up to 5 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.  
  - **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).  
  **Note**  
  The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain `<` `>` `@` `;` `:` `!` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration. |

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 5**  
(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 6**  
Click **Start**.
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 5 and Discover Your Network Using an IP Address Range, on page 10.

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 that they are connected to.

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

From the Cisco DNA Center home page, click Discovery.

Step 2

In the Discovery Name field, enter a name.

Step 3

Expand the IP Address/Range area if it is not already visible, 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 to 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 4.

  **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 4** 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation. <strong>Note</strong>: Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>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, enter the enable password again. <strong>Note</strong>: Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

---

d) Click **SNMP v2c** and configure the following fields:
Table 12: SNMPv2c Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |

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

Table 13: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
</tbody>
</table>
| 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. |
SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 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. (Enabled if you select AuthPriv as a the authentication mode.) Choose one of the following privacy types:

- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **AES128**: CBC mode AES for encryption.
- **None**: No privacy.

SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retries</td>
<td>Number of times Cisco DNA Center tries to communicate with network devices using SNMP.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds between retries.</td>
</tr>
</tbody>
</table>

g) (Optional) Click **HTTP(S)** and configure the following fields:
Table 15: HTTP(S) Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write.</td>
</tr>
</tbody>
</table>

For Read:

- **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.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**

The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain < > @ ’ , : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

For Write:

- **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.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**

The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain < > @ ’ , : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

---

**Step 5** (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 6**

Click Start.

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  From the Cisco DNA Center home page, click Discovery.

Step 2  To stop an active Discovery job, perform these steps:
   a)  From the Discoveries pane, select the corresponding Discovery job.
   b)  Click Stop.

Step 3  To restart an inactive Discovery job, perform these steps:
   a)  From the Discoveries pane, select the corresponding Discovery job.
   b)  Click Start.

Edit a Discovery Job

You can edit a Discovery job and then rerun the Discovery job.

Before you begin

You should have created at least one Discovery job.

Step 1  From the Cisco DNA Center home page, click Discovery.

Step 2  From the Discoveries pane, select the Discovery job.

Step 3  Click Edit.

Step 4  Depending on the Discovery type, you can change the type of Discovery 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 5.
   •  IP Range—Discovery name, Discovery 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 10.
   •  LLDP—Discovery name, Discovery type, IP address. For more information about the fields you can change, see Discover Your Network Using LLDP, on page 15.

Step 5  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**  
From the Cisco DNA Center home page, click **Discovery**.

**Step 2**  
From the **Discoveries** pane, select the Discovery job.

**Step 3**  
Click **Edit**.

**Step 4**  
Expand the **Credentials** area.

**Step 5**  
Deselect the credentials that you do not want to use.

**Step 6**  
Configure the credentials that you want to use:

a) Click **Add Credentials**.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td>Username</td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
</tbody>
</table>
|                | **Note**  
|                | Passwords are encrypted for security reasons and are not displayed in the configuration. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
</tbody>
</table>
|               | **Note**  
|               | Passwords are encrypted for security reasons and are not displayed in the configuration. |

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td><strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td>Read Community</td>
<td><strong>Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
</tbody>
</table>
|                    | **Note**  
<p>|                    | Passwords are encrypted for security reasons and are not displayed in the configuration. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
</tbody>
</table>
| 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.                                  |
| Auth Password| SNMPv3 password used for gaining access to information from devices that use SNMPv3.  
|              | These passwords (or passphrases) must be at least 8 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  | Description
--- | ---
Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Choose one of the following privacy types:
- **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **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 DES or AES128 encryption. Passwords (or passphrases) must be at least 8 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 7**  Click Start.

**Clone a Discovery Job**

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

**Before you begin**

You should have run at least one Discovery job.

**Step 1**  From the Cisco DNA Center home page, click Discovery.
**Step 2**  From the Discoveries pane, select the Discovery job.
**Step 3**  Click Clone.
Cisco DNA Center creates a copy of the Discovery job, named Copy of *Discovery_Job*.

**Step 4**  (Optional) Change the name of the Discovery job.
**Step 5**  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.
**View Discovery Job Information**

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

Before you begin

Run at least one Discovery job.

---

**Step 1**  
From the Cisco DNA Center home page, click Discovery.

**Step 2**  
From the Discoveries pane, select the Discovery job that you want to delete.

**Step 3**  
Click Delete.

**Step 4**  
Click OK to confirm.

---

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.