Discovering Devices and Hosts

About Discovery

The process of finding network devices and hosts is known as discovery. The Discovery function scans the devices and hosts in your network and populates the Cisco APIC-EM database with the information that it retrieves. To discover devices and hosts, you need to provide the controller with information about the devices so that the Discovery function can reach as many of the devices in your network as possible and gather as much information as it can.

The Discovery function uses the following protocols and methods to retrieve device information, such as hosts IP addresses, MAC addresses, and network attachment points:

- Cisco Discovery Protocol (CDP)
- Community-based Simple Network Management Protocol Version 2 (SNMPv2c)
- Simple Network Management Protocol version 3 (SNMPv3)
- Link Layer Discovery Protocol (LLDP)
- IP Device Tracking (IPDT) (For Discovery to collect host information, you must manually enable IPDT on devices. After IPDT is enabled, Discovery collects host information on a best-effort basis, because in addition to IPDT, Discovery relies on ARP entries for host information.)
- LLDP Media Endpoint Discovery (LLDP-MED) (IP phones and some servers are discovered using LLDP-MED).

For information about the required protocol configuration for your devices, see Device Configuration Prerequisites.

Understanding Device and Host Discovery

The process of finding network devices and hosts is known as discovery. You populate the Cisco APIC-EM database by discovering the devices and hosts in your network. To discover network devices, you need to provide the Cisco APIC-EM with discovery credentials for the devices in your network in the form of SNMP settings and CLI credentials. When you perform a discovery, the Cisco APIC-EM scans the network and attempts to log in to newly found devices by presenting these credentials.

The Cisco APIC-EM uses the CDP, LLDP and wireless controller databases on the network devices to discover hosts, such as wireless laptops, handheld devices, printers, and IP phones. To discover wired laptops, the Cisco APIC-EM uses the IP Device Tracking database, which needs to be enabled on some switches. (This feature is enabled by default on some switches.)

Wireless LAN Controllers (WLCs) have additional setup requirements in order to be discovered. For more information, see Wireless LAN Controller Configuration.

Discovery Credentials Caveats

The following are caveats for the Cisco APIC-EM discovery credentials:

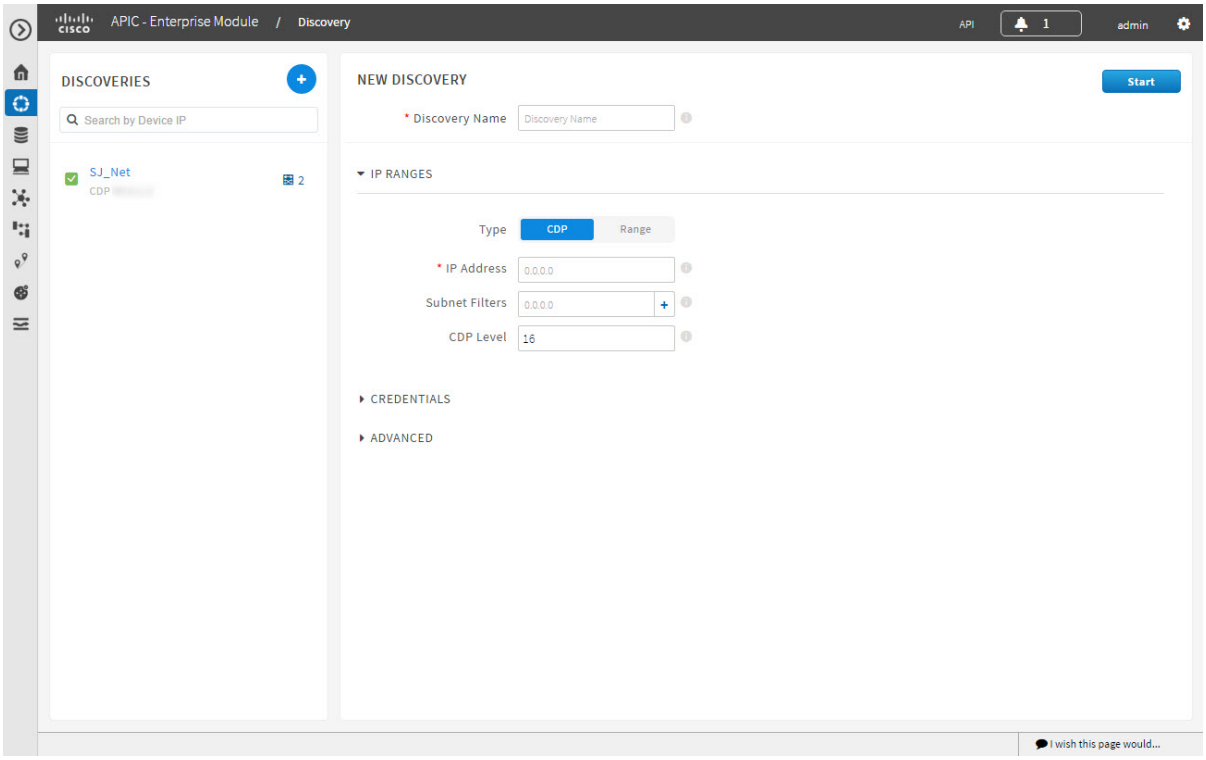
- If a device credential changes in a network device or devices after Cisco APIC-EM discovery is completed for that device or devices, any subsequent polling cycles for that device or devices will fail. To correct this situation, an administrator has following options:
  - Start a new discovery scan with changed job specific credentials that matches the new device credential.
  - Edit the existing discovery by updating or modifying the global credentials, and then rerun the discovery scan.
- If the ongoing discovery fails due to a device authentication failure (for example, the provided discovery credential is not valid for the devices discovered by current discovery), then the administrator has following options:
  - Stop or delete the current discovery. Create one or more new network discovery jobs (either a **CDP** or **Range** discovery type) with a job specific credential that matches the device credential.
  - Create a new global credential and execute a new discovery selecting the correct global credential.
  - Edit an existing global credential and re-run the discovery.
- Deleting a global credential does not affect already discovered devices. These already discovered devices will not report an authentication failure.
- The Cisco APIC-EM provides a REST API which allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory. The purpose of this API is to allow an external application to synchronize its own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios, Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution.

Note Only the username is provided in clear text. SNMP community strings and passwords are not provided in cleartext for security reasons.

Understanding the Discovery Window

To access the Discovery function, from the **Navigation** pane, click **Discovery**.

Figure 1: Discovery Window



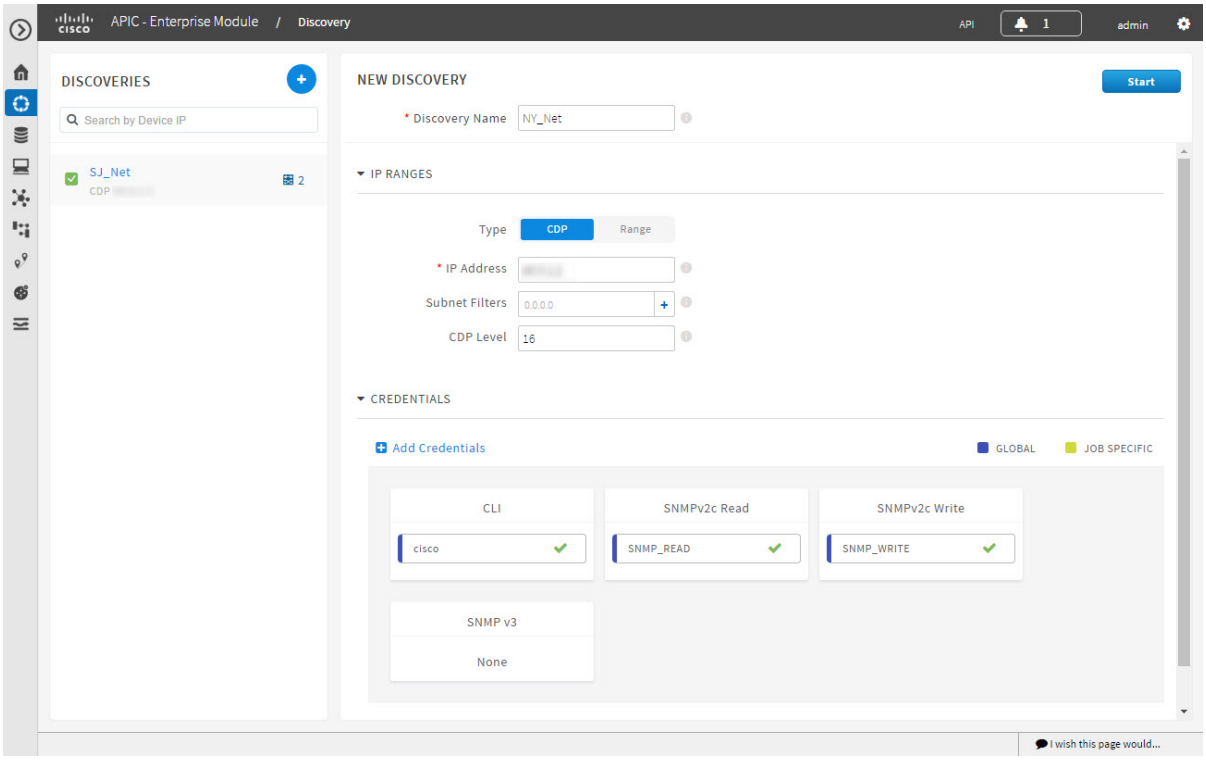
Name	Description
Discoveries pane	Lists the names of the discovery jobs that have been created, along with the method and IP addresses used for discovery. The list is divided between active and inactive discoveries. A successful scan (one with discovered and authenticated devices) has the number of discovered devices indicated to the right of the discovery name. An unsuccessful scan shows no box or number of devices discovered. From the **Discoveries** pane, clicking a discovery name displays information about the discovery in the **Discovery Results** pane. For information about the **Discovery Results** pane, see Understanding the Discovery Results, on page 14. If you cannot find the discovery job that you want, enter an IP address used in the discovery job in the **Search by Device IP** field that is above the list of discovery jobs.
New Discovery	Displays a pane for configuring and starting new discovery jobs. For information, see Performing Discovery Using CDP, on page 5 and Performing Discovery Using an IP Address Range, on page 9.

Performing Discovery

Performing Discovery Using CDP

You can discover devices and hosts using CDP.

Figure 2: Discovery Using CDP



Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

CDP must be enabled on the devices in order for them to be discovered.

Your devices must have the required device configurations, as described in Device Configuration Prerequisites.

Procedure

Step 1 From the **Navigation** pane, click **Discovery**.

Step 2 From the **Discovery** window, click **+ New Discovery**.
The **New Discovery** pane appears.

Step 3 In the **Discovery Name** field, enter a unique name for the discovery job.

Step 4 In the **IP Ranges** area, configure the following settings:

a) In the **Type** field, choose **CDP**.

b) In the **IP Address** field, enter a seed IP address for the Cisco APIC-EM to use to start the discovery scan.

c) (Optional) In the **Subnet Filter** field, enter the IP address or subnet and click **Add**.
You can enter the address 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.

Repeat this step to exclude multiple subnets from the discovery job.

d) (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.

Step 5 Open the **Credentials** area and configure the credentials that you want to use for the discovery job.
You can configure credentials to be used for the current discovery job, or you can check the **Save as global settings** checkbox to save the credentials for future discovery jobs.

a) Make sure that any global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.

b) To add additional credentials, click **+ Add Credentials**, complete the fields in the following tables for the credentials that you want to use, and click **Add**.
With the **Enable Device Control** option enabled under **Settings > Device Controllability**, APIC-EM configures devices that do not have SNMP credentials with the SNMP credentials set in Global Settings or in the specific discovery job, whichever one takes priority.

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

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

Table 1: CLI Credentials

Field	Description
Username	Username that is used to log into the command line interface (CLI) of the devices in your network.
Password **Confirm Password**	Password that is used to log into the CLI of the devices in your network. For security reasons, you must enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Enable Password **Confirm Enable Password**	Password used to move to a higher privilege level in the CLI. For security reasons, you must enter the enable password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 2: SNMP v2c Credentials

Field	Description
Read	SNMP read-only (RO) community string configuration, which comprises the following fields: • **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Read Community** and **Confirm 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. **Note** To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write	SNMP read-write (RW) community string configuration, which comprises the following fields: • **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Write Community** and **Confirm Write Community—**Read/Write community string password used to view and make changes to SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration. **Note** To enable discovery on the network devices, configure the network device's IP host address as the client address.

Table 3: SNMP v3 Credentials

Field	Description
Username	Username associated with the SNMPv3 settings.

Field	Description
Mode	Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes: • noAuthNoPriv—Security level that does not provide authentication or encryption • AuthNoPriv—Security level that provides authentication but does not provide encryption • AuthPriv—Security level that provides both authentication and encryption
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Auth Type	Specifies the authentication type to be used. • **SHA—**Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm • **MD5—**Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm • **None—**No authentication
Privacy Password	SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Specifies the privacy type: • **DES—**Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. • **AES128—**Cipher Block Chaining (CBC) mode AES for encryption. • **None—**No privacy

Table 4: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0 to 4 attempts.
Timeout (in Seconds)	Number of seconds the controller waits when trying to establish a connection with a device before timing out. Valid values are from 5 to 120 seconds in intervals of 5 seconds.

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

a) Click the protocols that you want to use. A green checkmark 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.

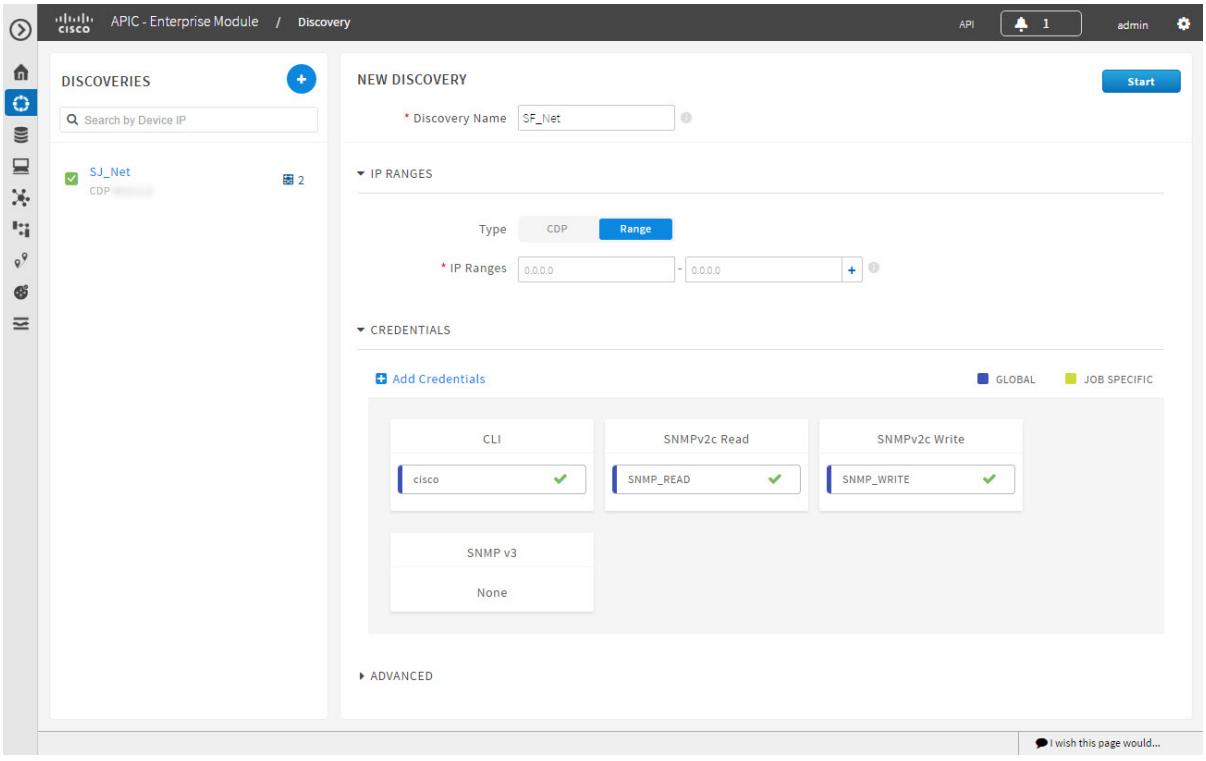
Step 7 Click **Start Discovery**.
The **Discoveries** window displays the results of your scan.

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 for the selected discovery.

Performing Discovery Using an IP Address Range

You can discover devices using an IP address range.

Figure 3: Discovery Using IP Address Range



Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Your devices must have the required device configurations, as described in Device Configuration Prerequisites.

Procedure

Step 1 From the **Navigation** pane, click **Discovery**.

Step 2 From the **Discovery** window, click **+ New Discovery**.
The **New Discovery** pane appears.

Step 3 In the **Discovery Name** field, enter a unique name for the discovery job.

Step 4 If the **Discovery Details** pane does not appear, click **Add New**.

Step 5 In the **Discovery Name** field, enter a unique name for this discovery.

Step 6 In the **IP Ranges** area, do the following:

a) From the **Discovery Type** field, choose **Range** for the discovery scan type.

b) In the **IP Address** field, enter the beginning and ending IP addresses (IP range) for the devices being discovered and click **Add**.
You can enter a single IP address range or multiple IP addresses for the discovery scan.

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

Step 7 Open the **Credentials** area and configure the credentials that you want to use for the discovery job.
You can configure credentials to be used for the current discovery job, or you can check the **Save as global settings** checkbox to save the credentials for future discovery jobs.

a) Make sure that any global credentials that you want to use are checked. If you do not want to use a credential, remove it by clicking the check mark.

b) To add additional credentials, click **+ Add Credentials**, complete the fields in the following tables for the credentials that you want to use, and click **Add**.
With the **Enable Device Control** option enabled under **Settings > Device Controllability**, Cisco APIC-EM configures devices that do not have SNMP credentials with the SNMP credentials set in Global Settings or in the specific discovery job, whichever one takes priority.

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

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

Table 5: CLI Credentials

Field	Description
Username	Username that is used to log into the command line interface (CLI) of the devices in your network.

Field	Description
Password **Confirm Password**	Password that is used to log into the CLI of the devices in your network. For security reasons, you must enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password **Confirm Enable Password**	Password used to move to a higher privilege level in the CLI. For security reasons, you must enter the enable password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 6: SNMP v2c Credentials

Field	Description
Read	SNMP read-only (RO) community string configuration, which comprises the following fields: • **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Read Community** and **Confirm Read Community—**Read-only community string used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration. **Note** To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write	SNMP read-write (RW) community string configuration, which comprises the following fields: • **Name/Description—**Name or description of the SNMP v2c settings that you are adding. • **Write Community** and **Confirm Write Community—**Read/Write community string used to view and make changes to SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration. **Note** To enable discovery on the network devices, configure the network device's IP host address as the client address.

Table 7: SNMP v3 Credentials

Field	Description
Username	Username associated with the SNMPv3 settings.
Mode	Specifies the security level that an SNMP message requires and whether the message needs to be authenticated. Choose one of the following modes: • noAuthNoPriv—Security level that does not provide authentication or encryption • AuthNoPriv—Security level that provides authentication but does not provide encryption • AuthPriv—Security level that provides both authentication and encryption
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
Auth Type	Specifies the authentication type to be used. • **SHA—**Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm • **MD5—**Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm • **None—**No authentication
Privacy Password	SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.
Privacy Type	Specifies the privacy type: • **DES—**Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. • **AES128—**Cipher Block Chaining (CBC) mode AES for encryption. • **None—**No privacy

Table 8: SNMP Properties

Field	Description
Retries	Number of attempts to connect to the device. Valid values are from 0 to 4 attempts.
Timeout (in Seconds)	Number of seconds the controller waits when trying to establish a connection with a device before timing out. Valid values are from 5 to 120 seconds in intervals of 5 seconds.

Step 8 Click **Start Discovery**.
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 for the selected discovery.

Step 9 (Optional) To configure the protocols to be used to connect with devices, open the **Advanced** area and do the following:

a) Click the protocols that you want to use. A green checkmark 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.

Copying a Discovery Job

You can copy a discovery job and retain all of the information defined for the job, except the SNMP and CLI credentials. The SNMP and CLI credentials are included in the copy only if you used global credentials (saved in **Settings**) for the original job. If you defined specific (one-time only) SNMP and CLI credentials for the original job, the credentials are not copied.

Before You Begin

You have created at least one discovery scan.

Procedure

Step 1 From the **Navigation** pane, click **Discovery**.

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

Step 3 From the **Discovery Details** pane, click **Copy**.
The discovery job is copied, and the new job is named Copy of *Discovery_Job*.

Step 4 (Optional) Change the name of the discovery job.

Step 5 Define or update the SNMP and CLI credentials and any other parameters for the discovery job.

Stopping and Starting a Discovery Job

You can stop a discovery job that is in progress, and restart it.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Procedure

Step 1 From the **Navigation** pane, click **Discovery**.

Step 2 To stop an active discovery job, do the following:

a) From the **Discoveries** pane, select the discovery job.
b) From the **Discovery Details** pane, click **Stop**.
c) Click **OK** to confirm that you want to stop the discovery job.

Step 3 To restart an inactive discovery, do the following:

a) From the **Discoveries** pane, select the discovery job.
b) From the **Discovery Details** pane, click **Start**.

Deleting a Discovery Job

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Procedure

Step 1 From the **Navigation** pane, click **Discovery**.

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

Step 3 From the **Discovery Details** pane, click **Delete**.

Step 4 Click **OK** to confirm that you want to delete the discovery.

Understanding the Discovery Results

The **Discovery Results** pane provides information about the selected scan.

To access the **Discovery Results** pane, do the following:

1 From the **Navigation** pane, click **Discovery**.

2 From the **Discoveries** pane, select the discovery job that you want to display.

The **Discovery Results** pane appears. See the following figures and table for information.

Figure 4: Discovery Results Window—List

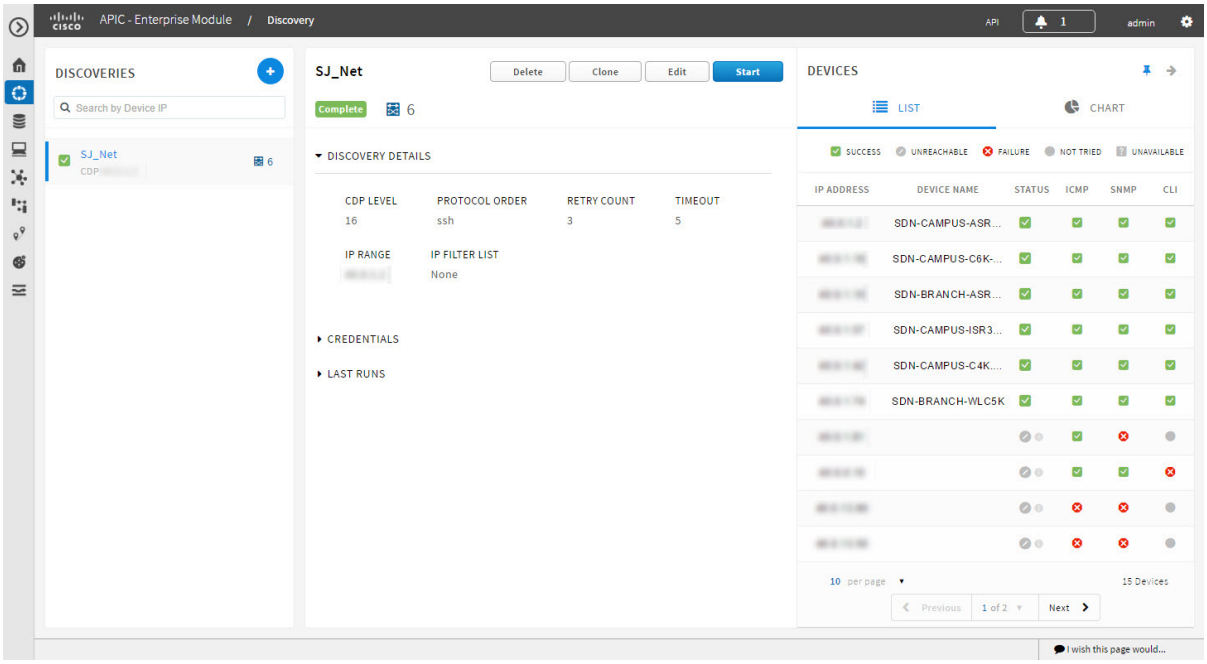


Figure 5: Discovery Results Window—Chart

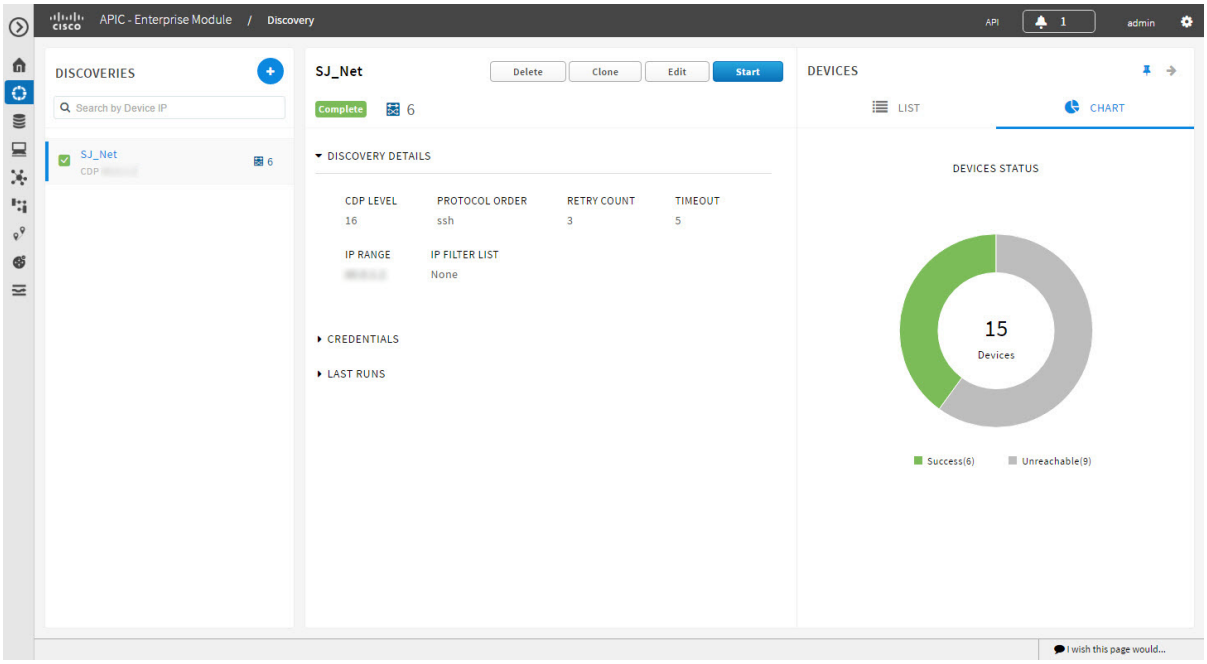


Table 9: Discovery Pane

Name	Description
Discovery Identification and Action Area	Displays the following information: • Name of the discovery job. • Status of the discovery job. • Number of devices discovered. From this area, you can delete, clone, edit, or start a discovery job.
Discovery Details area	Open this area to display detailed information about the parameters that were used to perform the discovery, including the CDP level (if used), protocol order, retry count, timeout value, IP address (seed) or range of IP addresses used, and IP address filter list.
Credentials area	Open this area to display the credentials used in the discovery job and identifies them as either global or job-specific.
Last Runs area	Open this area to display a table showing information about each iteration of the discovery job, including the job number, its status, an option to view the devices discovered, and the duration of the job. Clicking the **View** link in the **Devices** column opens the **Devices** pane.
Devices pane	(Shown when you open the **Last Runs** area and click the **View** link in the **Devices** column.) The devices pane displays the results of the device discovery in two forms: • **List—**For each device, provides the following information: ◦ **IP address—**IP addresses of the devices that Cisco APIC-EM discovered or attempted to discover. ◦ **Device name—**Name of the device, if available. ◦ **Status—**Status of the discovery for the device. Possible states are success, unreachable, failure, not tried, or unavailable. ◦ **Internet Control Message Protocol (ICMP)—**Status of the ICMP for the device. ◦ **SNMP—**Status of theCisco APIC-EM's use of the SNMP settings to gather SNMP information from the device. ◦ **CLI—**Status of theCisco APIC-EM's use of the CLI username and passwords to gather information from the device. • **Chart—**Displays a circle graph showing the proportional representation of successful versus failed discovered devices.