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 Discovery Credentials

The Cisco APIC-EM supports two different types of discovery credentials: global and job specific (or discovery request-specific). Both types of discovery credentials can consist of CLI or SNMP credentials that are configured using the controller's GUI.

Global credentials can be configured in either the **Discovery** window or the **Discovery Credentials** windows (as described in this chapter). Job specific credentials are only configured in the **Discovery** window.

Note For information about the procedure to configure global and/or job specific credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Both CLI and SNMP credentials are required for a successful discovery. The SNMP credentials (either global or job specific) are used for *device* discovery. The CLI credentials (either global or job specific) are used for capturing or applying *device configurations* for the controller's inventory.

You should enter at least one set of SNMP credentials, either SNMPv2c or SNMPv3, for your device discovery. If you are going to configure SNMPv2 settings in your network, then SNMP Read Only (RO) community string values should be entered in the controller to assure a successful discovery and populated inventory. However, if an SNMP RO community string and SNMP Read Writer (RW) community string is not entered into the controller, as a *best effort*, discovery will run with the default SNMP RO community string "public." Additionally, if no SNMP RO community string is entered but a SNMP RW community string is entered, then the SNMP RW community string will be used as SNMP RO community string.

Note You can enter values for both SNMP versions (SNMPv2c and SNMPv3) for a single discovery. The controller supports multiple SNMP credential configurations. Altogether, you can enter a maximum of 5 global device credentials (SNMP or CLI) using the **Discovery Credentials** windows as described in this chapter, with an additional credentials set being created in the **Discovery** window. Therefore, for a single discovery scan request, you can configure a total of 6 credential sets of each type (CLI or SNMP).

Global Credentials

Global credentials are defined as preexisting credentials that are common to the devices in a network. Global credentials (CLI and SNMP) are configured on the devices using the GUI (**Discovery** window or **Discovery Credentials** window) and permit successful login to the devices. Global credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this device credential when performing network discoveries.

You can configure the global CLI credentials in the **CLI Credentials** window. You access this window by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane. You can also configure global CLI credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global CLI credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You configure the global SNMP credentials in the **SNMPv2c** or **SNMPv3** window . You access these windows by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen.

You then click the **Settings** link from the drop-down menu and then click one of the SNMP window links on the Setting Navigation pane. You can also configure global SNMP credentials in the **Credentials** field in the **Discovery** window. For information about the procedure to configure global SNMP credentials in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Note Multiple credentials can be configured in the **CLI Credentials** window.

Job Specific Credentials

Job specific credentials (request-specific credentials) are defined as preexisting *device* credentials for a specific network device or set of devices that do not share the global credentials.

You configure job specific credentials in the **Discovery** window prior to performing a discovery that is exclusive for that set of network devices. You access this window by clicking **Discovery** on the Navigation pane.

Discovery Credentials Example

Assume a network of 200 devices that form a CDP neighborship (neighboring devices discovered using Cisco Discovery Protocol (CDP)). In this network, 190 devices share a global credential (Credential-0) and the 10 remaining devices each have their own unique or job specific credentials (Credential 1- 5)

To properly authenticate and access the devices in this network by the Cisco APIC-EM, you perform the following tasks:

1. Configure the CLI global credentials as Credential-0 for the controller.

   You can configure the global credentials in the **CLI Credentials** window. You access this window, by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane.

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

   You can configure these global credentials in the two SNMP windows. You access these GUI windows by clicking the **Settings** button at the top right and then clicking **SNMPv2c** or **SNMPv3** on the Setting Navigation pane.

3. Run a **CDP** discovery using one of the 190 device IP addresses (190 devices that share the global credentials) and selecting the global credentials in the GUI. You run a **CDP** discovery in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

4. Run 10 separate **Range** discoveries for each of the remaining 10 devices using the appropriate job specific credentials and SNMP values (for example, Credential-1, Credential-2-5, etc.).

   You configure the job specific credentials in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.

5. Review the **Device Inventory** table in the **Device Inventory** window to check the discovery results

Discovery Credentials Rules

Discovery credentials (global and job specific) operate under the rules as described in the bullet list and table below.

Job Specific Credential Rules

- Job specific credentials can be provided when creating a new network discovery, but only a single set of job specific credentials is allowed per network discovery.
- Job specific credentials take precedence over any configured global credentials.
- If the job specific credentials are provided as part of a network discovery and cause an authentication failure, then discovery is attempted a second time with the configured global credentials (if explicitly selected in the **Discovery** window of the controller's GUI). If discovery fails with the global credentials then the device discovery status will result in an authentication failure.
- When using Cisco APIC-EM APIs for a network discovery and the job specific credentials (both CLI and SNMP) are *not* provided as part of the network discovery, then the global credentials (both CLI and SNMP provided by the user) are used to authenticate devices.

Global Credential Rules

Table 1: Global Credential Rules

Global Credentials	Job Specific Credentials	Result
Not configured	Not configured	If the network discovery is run from the controller's GUI, then the default SNMP read community string (public) is used for the discovery scan. A discovery failure will not occur in this case. If the network discovery is run using Cisco APIC-EM APIs, then a discovery failure will occur since both CLI and SNMP credentials must be configured for a successful device discovery using the Cisco APIC-EM APIs.
Not configured	Configured	The specified job specific credentials will be used for discovery.
Configured	Not configured	All the configured global credentials will be used.
Configured but not selected	Configured	Only the job specific credentials will be used.
Configured and selected	Not configured	Only selected global credential will be used.

Global Credentials	Job Specific Credentials	Result
Configured and selected	Configured	Both specified credentials (global and job specific) will be used for discovery.
Configured, but wrong global credential IDs are mentioned in the discovery POST REST API.	Correct job specific credentials configured	Discovery fails. **Note** This scenario is only possible by API not from the controller GUI.
Configured, but wrong global credential IDs are mentioned in the discovery POST REST API.	Not configured	Discovery fails. **Note** This scenario is only possible by API not from the controller GUI.

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.

Configuring Global Discovery Credentials

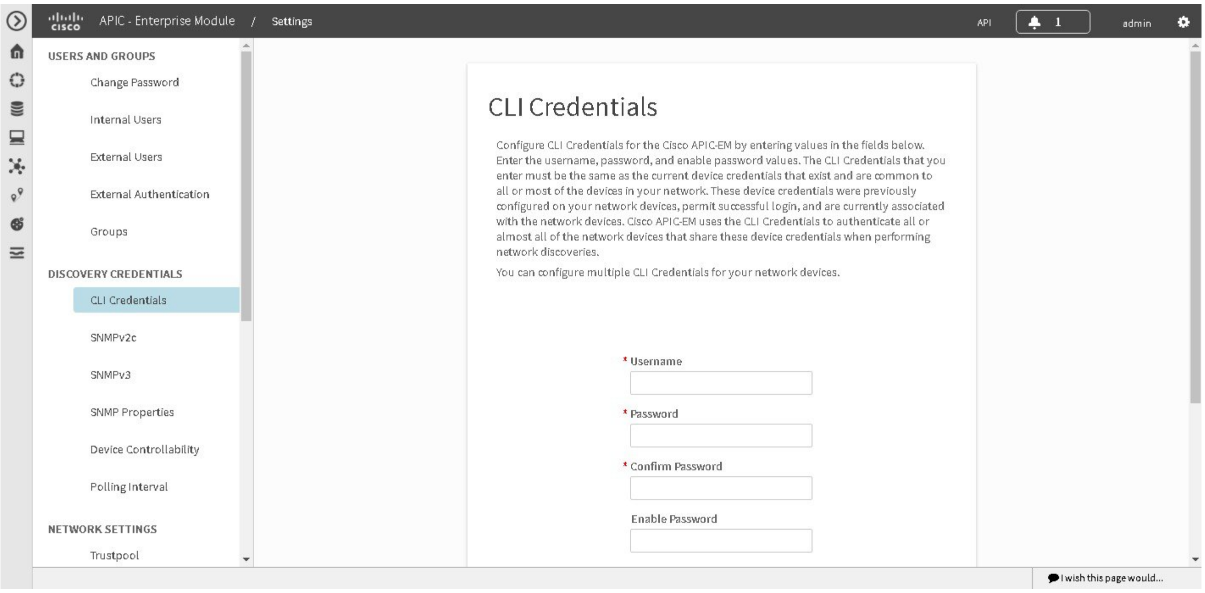
Configuring CLI Credentials

CLI credentials are defined as preexisting *device* credentials that are common to most of the devices in a network. CLI credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this CLI credential when performing devices discoveries.

You configure the CLI global credentials in the **CLI Credentials** window or the **Discovery** window. This procedure describes how to configure CLI global credentials in the **CLI Credentials** window.

Note You can configure up to five CLI credentials.

Figure 1: CLI Credentials Window



CLI Credentials

Configure CLI Credentials for the Cisco APIC-EM by entering values in the fields below. Enter the username, password, and enable password values. The CLI Credentials that you enter must be the same as the current device credentials that exist and are common to all or most of the devices in your network. These device credentials were previously configured on your network devices, permit successful login, and are currently associated with the network devices. Cisco APIC-EM uses the CLI Credentials to authenticate all or almost all of the network devices that share these device credentials when performing network discoveries.

You can configure multiple CLI Credentials for your network devices.

* Username

* Password

* Confirm Password

Enable Password

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **CLI Credentials** to view the **CLI Credentials** window.

In the **CLI Credentials** window, enter the appropriate CLI global credentials for the devices within your network or networks.

Step 4 Enter the CLI Credentials username in the **Username** field.

Step 5 Enter the CLI Credentials password in the **Password** field.

Step 6 Reenter the CLI Credentials password in the **Confirm Password** field to confirm the value that you just entered.

Step 7 If your network devices have been configured with an enable password, then enter the CLI Credentials for the enable password in the **Enable Password** field.

Note Both the CLI credentials password and enable password are saved in the controller in encrypted form. You cannot view these original passwords after you enter them.

Step 8 If you entered an enable password in the **Enable Password** field, reenter it in the **Confirm Enable Password** field to confirm the value that you just entered.

Step 9 In the **CLI Credentials** window, click **Add** to save the credentials to the Cisco APIC-EM database.

What to do next

Proceed to configure SNMP values for your network device discovery.

For a successful device discovery (with all the device information to be collected), CLI credentials (global and/or job specific) should be configured using the controller. The global credentials for CLI and SNMP (v2c or v3) can be configured in the **Discovery Credentials** windows (as described in this chapter) or the **Discovery** window, and are used in addition to any job specific credentials (for CLI and SNMP) that are also configured in the **Discovery** window.

Configuring SNMP

You configure SNMP for device discovery using the following **Discovery Credentials** windows in the Cisco APIC-EM GUI:

- **SNMPv2c**
- **SNMPv3**
- **SNMP Properties**

Note You can also configure SNMP for device discovery in the **Discovery** window of the controller's GUI. For information about the procedures to configure SNMP for device discovery in the **Discovery** window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

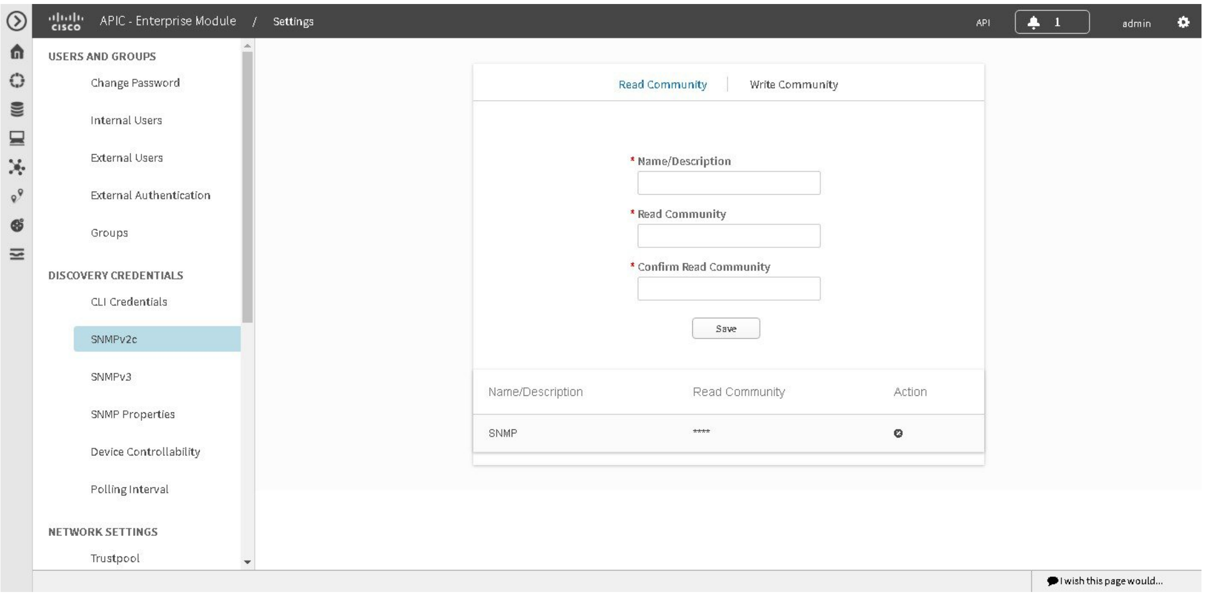
Important You can use SNMP and the existing security features in SNMP v3 to secure communications between the controller and the devices in your network. SNMP v3 provides both privacy (encryption) and authentication capabilities for these communications. If possible for your network, we recommend that you use SNMPv3 with both privacy and authentication enabled.

Configuring SNMPv2c

You configure SNMPv2c for device discovery in the **SNMPv2c** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv2c for the controller must match the SNMPv2c values that have been configured for your network devices.

Note You can configure up to five read community strings and five write community strings.

Figure 2: Configuring SNMPv2c



Name/Description	Read Community	Action
SNMP	****	⊗

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in clear text. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security).

Note In addition to configuring SNMPv2c for device discovery in the controller, a "best effort" Cisco APIC-EM discovery is in place, meaning that devices having SNMP with Read-Only (RO) community string set to "public" will be discovered all the time irrespective of the configured SNMP Read/Write community string.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMPv2c** to view the **SNMPv2c** window.

Step 4 In the **SNMPv2c** window, click **Read Community**.

Enter your **Read Community** values:

- **Name/Description**—Description of the Read-Only (RO) community string value and/or the device or devices that are configured with it.
- **Read Community**—Read-Only community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Read Community**—Reenter the Read-Only community string to confirm the value that you just entered.

Note If you are configuring SNMPv2c for your discovery, then configuring **Read Community** values is mandatory.

Step 5 Click **Save** to save your **Read Community** values.

The **Read Community** values will appear in the table below.

Step 6 (Optional) In the **SNMPv2c** window, click **Write Community**.

Enter your **Write Community** values:

- **Name/Description**—Description of the Write community string value and/or the device or devices that are configured with it.

- **Write Community**—Write community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Write Community**—Reenter the Write community string to confirm the value that you just entered.

Step 7 (Optional) Click **Save** to save your **Write Community** values.

The **Write Community** values will appear in the table below.

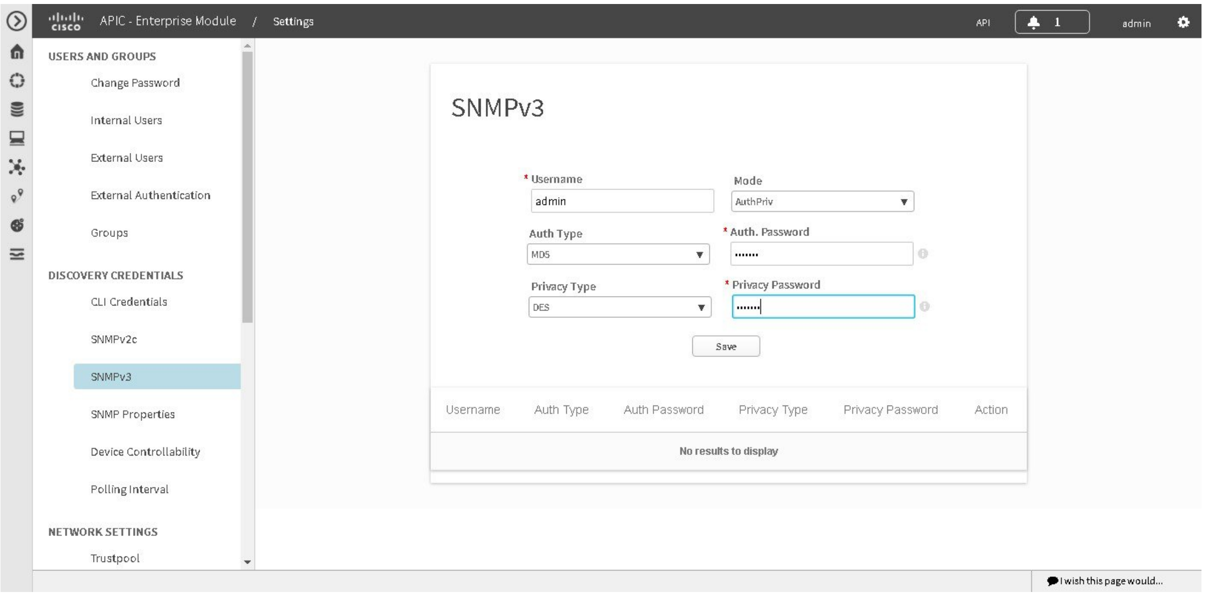
What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv3** or **SNMP Properties** using the GUI.

Configuring SNMPv3

You configure SNMPv3 for device discovery in the **SNMPv3** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv3 for the controller must match the SNMPv3 values that have been configured for your network devices. You can configure up to five SNMPv3 settings.

Figure 3: Configuring SNMPv3



SNMPv3

* Username: admin
Mode: AuthPriv
Auth Type: MD5
* Auth. Password: •••••••
Privacy Type: DES
* Privacy Password: •••••••

Save

Username	Auth Type	Auth Password	Privacy Type	Privacy Password	Action
No results to display					

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The following are supported SNMPv3 security models:

- Message integrity—Ensures that a packet has not been tampered with in-transit.

- Authentication—Determines the message is from a valid source
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- 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

The following table identifies what the combinations of security models and levels mean:

Table 2: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	User Name	No	Uses a username match for authentication.
v3	AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash algorithm (SHA)

Model	Level	Authentication	Encryption	What Happens
v3	AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • CBC-DES • CBC-AES-128	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Note With SNMPv3, passwords (or passphrases) must be at least 8 characters in length (minimum). Additionally, for several Cisco Wireless LAN controllers, passwords (or passphrases) must be at least 12 characters in length (minimum). Failure to ensure these required minimum character lengths for the passwords will result in devices not being discovered, monitored, and/or managed by the controller.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMPv3** to view the **SNMPv3** window.

If you use SNMPv3 in your network to monitor and manage devices, then configure the SNMPv3 values for discovery for your network.

Step 4 In the **SNMPv3** window, enter a **Username** value and choose a **Mode** from the drop down menu.

The following **Mode** options are available:

- **AuthPriv**
- **AuthNoPriv**
- **NoAuthNoPriv**

Note Subsequent **SNMPv3** configuration options might or might not be available depending upon your selection for this step.

Step 5 If you selected **AuthPriv** or **AuthNoPriv** as a **Mode** option, then choose an **Authentication** type from the drop down menu and enter an authentication password.

The following **Authentication** options are available:

- **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

Step 6 If you selected **AuthPriv** as a **Mode** option, then choose a **Privacy** type from the drop down menu and enter a SNMPv3 privacy password.

The SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

The following **Privacy** type options are available:

- **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.

Step 7 Click **Save** to save your SNMPv3 configuration values.

The **SNMPv3** configured values will appear in the table below.

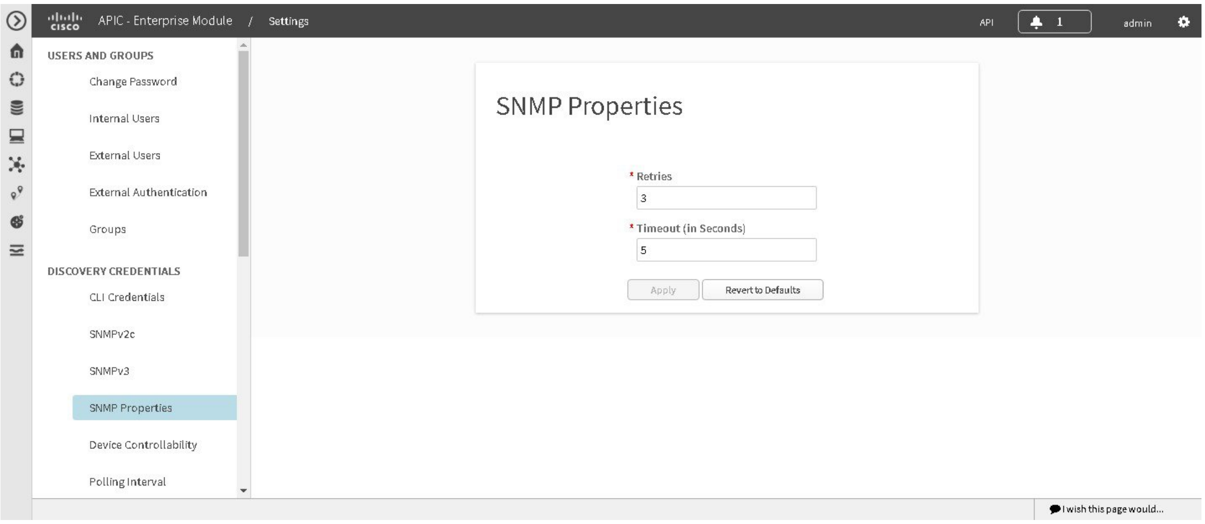
What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMP Properties** using the GUI.

Configuring SNMP Properties

You configure SNMP properties for device discovery in the **SNMP Properties** window in the Cisco APIC-EM GUI.

Figure 4: Configuring SNMP Properties



SNMP Properties

* Retries: 3

* Timeout (in Seconds): 5

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMP Properties** to view the **SNMP Properties** window.

Configure the SNMP property settings for discovery in your network.

Step 4 In the **SNMP Properties** window, enter a value in the **Retries** field.

The value entered in this field is the number of attempts the controller attempts to use SNMP to communicate with your network devices.

Step 5 In the **SNMP Properties** window, enter a value in the **Timeout** field.

The value entered in this field is the length of time in seconds the controller attempts to use SNMP to communicate with your network devices.

Step 6 Click **Apply** to save your SNMP configuration values.

You can also click **Revert to Defaults** to revert to the SNMP property default values. The following are the SNMP property default values:

- **Retries**—3

- **Timeout**—5

What to do next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMPv3** using the GUI.

Enabling Device Controllability

You can enable device controllability in the **Device Controllability** window of the Cisco APIC-EM GUI. When you enable device controllability, the controller performs two actions during a discovery:

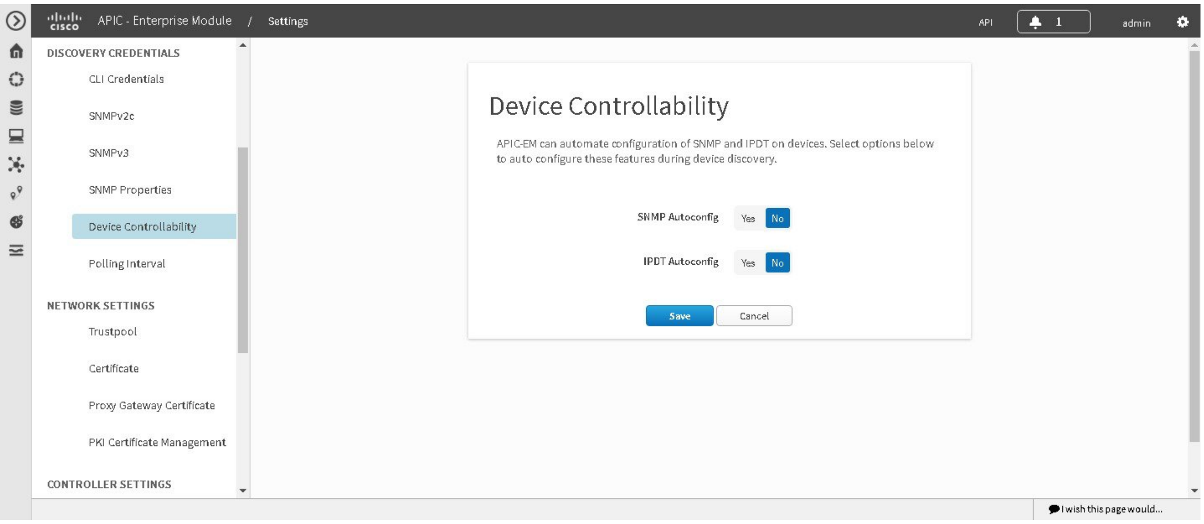
- The controller automatically configures (applies) the SNMP credentials that you entered using the controller's GUI on any network devices without SNMP credentials (SNMPv2c and/or SNMPv3).
- The controller automatically enables IP device tracking (IPDT) on any network devices where it is supported.

Note If you want to discover hosts through a trunk interface, you must manually enable IPDT on the trunk interface.

IPDT is enabled only on devices that are identified as Access role in **Device Inventory** window during the initial inventory collection. The device does not need to be in a **Managed** state to have IPDT enabled. The IPDT configuration is applied to devices as long as Device Inventory has the device's software version, role, and so on.

Note The device controllability functionality depends upon whether the CLI credentials provided by the user permits the controller to log into the device in enable mode (privilege level 15 for Cisco IOS devices).

Figure 5: Enabling Device Controllability



Device Controllability

APIC-EM can automate configuration of SNMP and IPDT on devices. Select options below to auto configure these features during device discovery.

SNMP Autoconfig Yes [✓ No]

IPDT Autoconfig Yes [✓ No]

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Device Controllability** to view the **Device Controllability** window.

Step 4 (Optional) Click **Yes** for **SNMP Autoconfig** to automatically to enable this feature.

Clicking **Yes** for **SNMP Autoconfig** automatically applies the SNMP credentials you configured using the controller's GUI to any devices in your network without an SNMP configuration.

Step 5 (Optional) Click **Yes** for **IPDT Autoconfig** to enable this feature.

Clicking **Yes** for **IPDT Autoconfig** automatically enables IP device tracking (IPDT) on any devices in your network where it is supported but not enabled.

Step 6 Click **Save** to save your configuration.

What to do next

If you have not already done so, configure SNMP in either the **Discovery** window or the appropriate **CLI Credentials** window for SNMP in **Settings**.

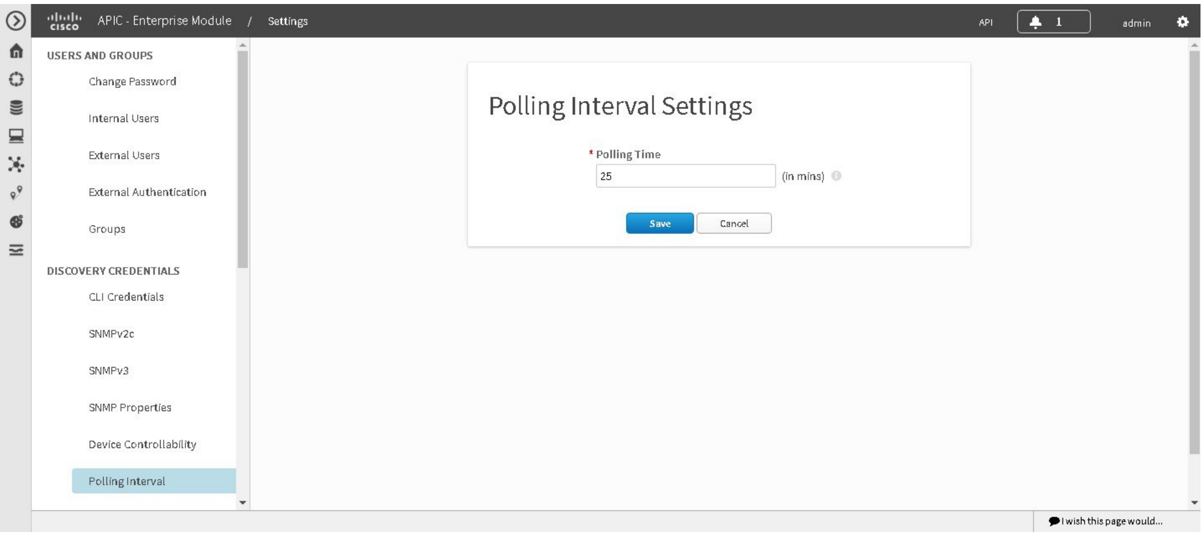
Configuring the Polling Interval

You can configure the polling interval for inventory data collection for devices managed by Cisco APIC-EM. This polling interval configuration will be used for all managed devices, unless the polling interval of a device is updated specifically in the **Inventory** page.

You configure the polling interval in the **Polling Interval Settings** window of the Cisco APIC-EM GUI.

Note The polling interval value that you configure is a global value used for performing periodic inventory data collection, it is not used for discovering the device.

Figure 6: Polling Interval Window



Polling Interval Settings

* Polling Time: 25 (in mins)

Save Cancel

Before you begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Polling Interval** to view the **Polling Interval** window.

Step 4 Enter a polling interval value in minutes in the **Polling Interval** field.

The default polling interval is 25 minutes for device discovery by the controller.

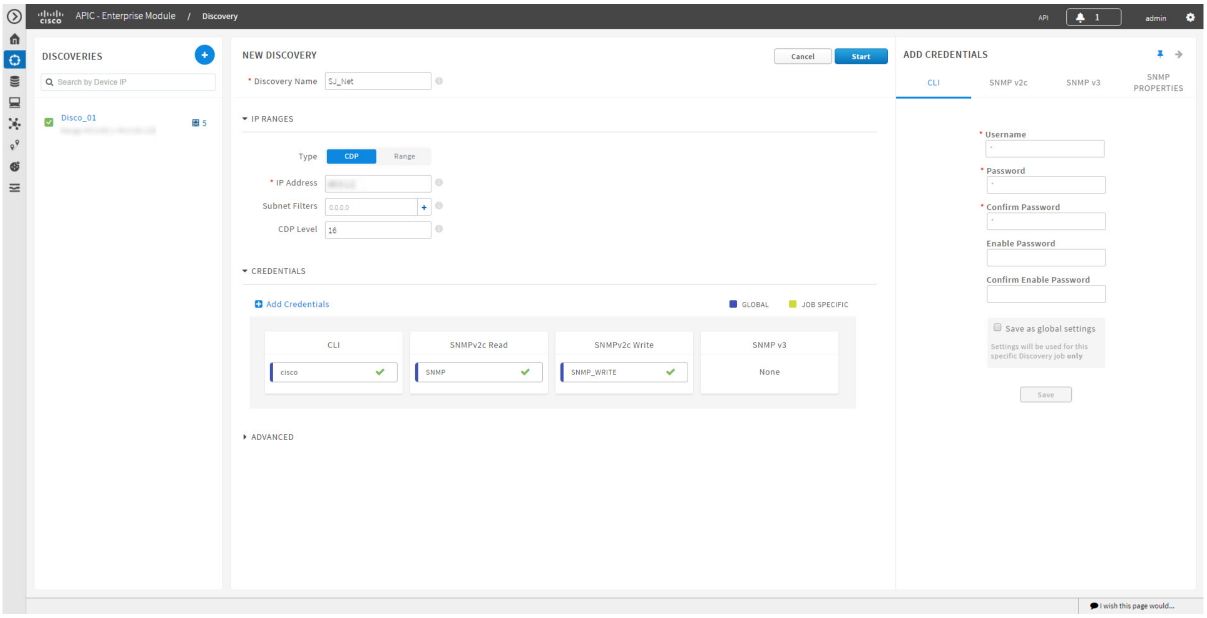
Step 5 Click **Save** to save your polling interval configuration.

Performing Discovery

Performing Discovery Using CDP

You can discover devices and hosts using CDP.

Figure 7: Discovery Using CDP



Disco_01 5

NEW DISCOVERY

* Discovery Name: SJ_Net

IP RANGES

Type: CDP | Range

* IP Address: [redacted]

Subnet Filters: 0.0.0.0

CDP Level: 16

CREDENTIALS

Add Credentials

CLI	SNMPv2c Read	SNMPv2c Write	SNMP v3
cisco ✓	SNMP ✓	SNMP_WRITE ✓	None

ADVANCED

* Username

* Password

* Confirm Password

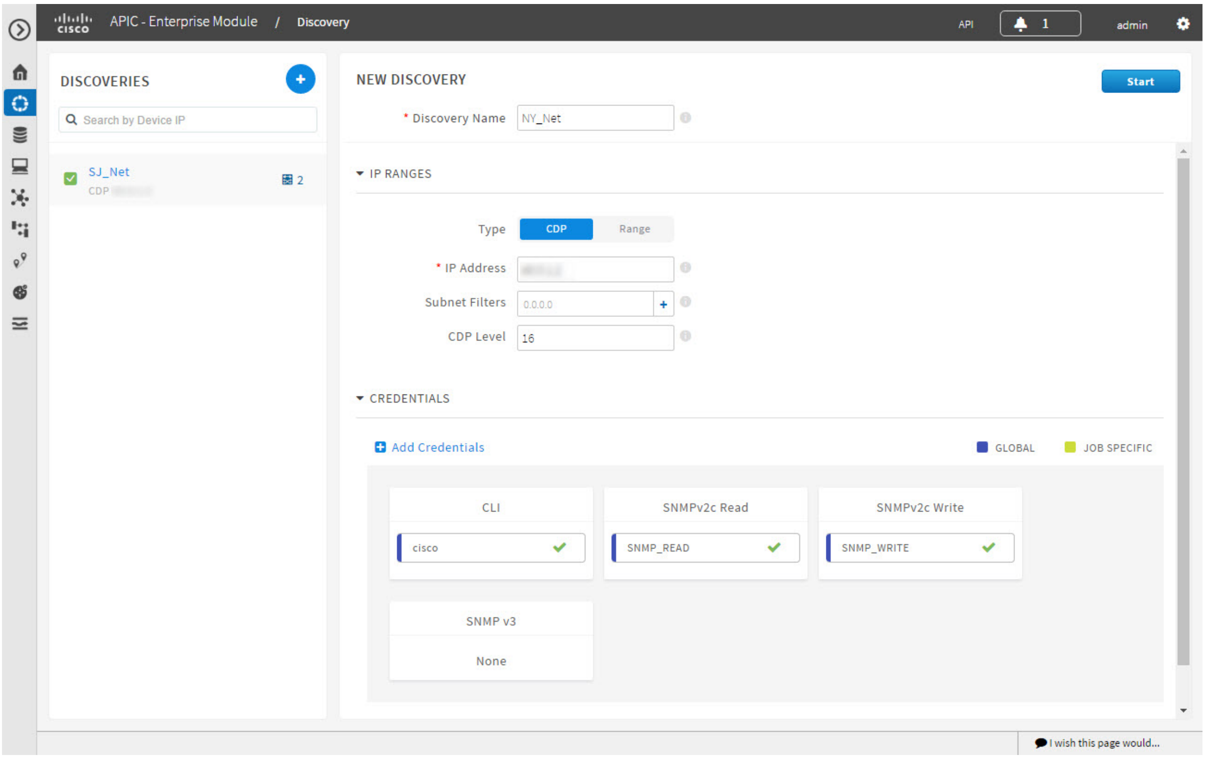
Enable Password

Confirm Enable Password

□ Save as global settings

Settings will be used for this specific Discovery job **only**

Figure 8: Discovery Using CDP



SJ_Net 2
CDP [redacted]

NEW DISCOVERY

* Discovery Name: NY_Net

IP RANGES

Type: CDP | Range

* IP Address: [redacted]

Subnet Filters: 0.0.0.0

CDP Level: 16

CREDENTIALS

Add Credentials

CLI	SNMPv2c Read	SNMPv2c Write	SNMP v3
cisco ✓	SNMP_READ ✓	SNMP_WRITE ✓	None

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.

Note CDP is required for the **hostname** column to be populated.

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

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 + the plus sign..

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 **SNMP Autoconfig** 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 3: 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.
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 4: 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 host IP address as the client IP address.

Table 5: 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. **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 6: 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**.

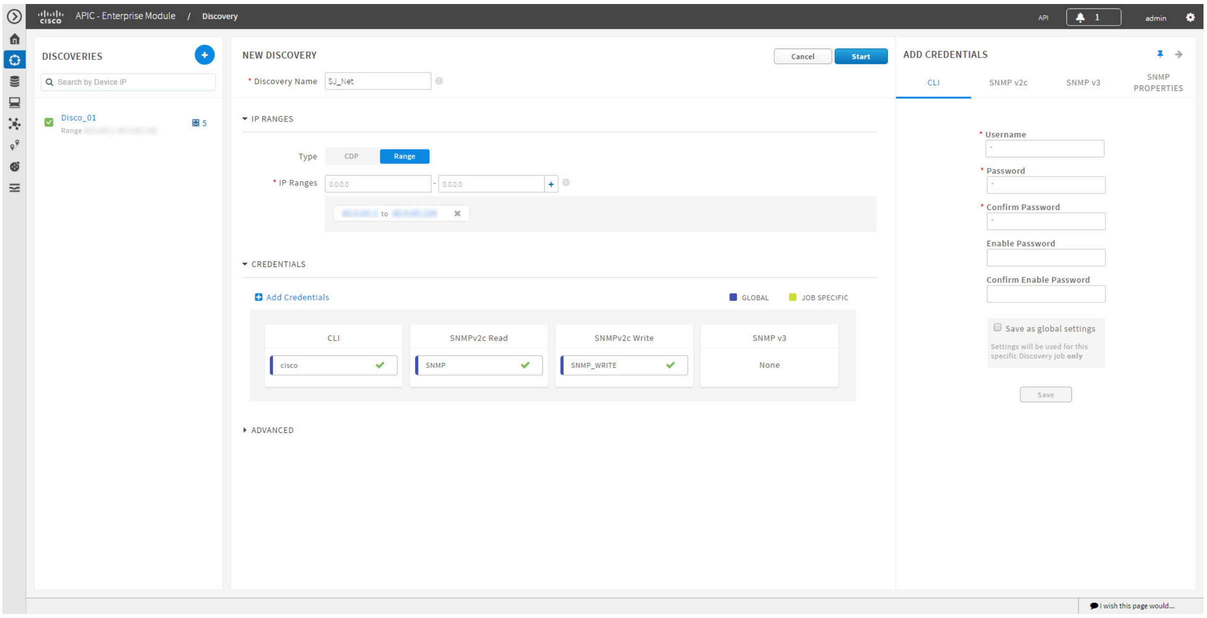
The **Discoveries** window displays the results of your scan.

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 9: Discovery Using IP Address Range



Disco_01 Range [redacted] 5

* Discovery Name: SJ_Net

Type: CDP [✓ Range]

* IP Ranges: 0.0.0.0 - 0.0.0.0 +

[redacted] to [redacted] ✖

CLI	SNMPv2c Read	SNMPv2c Write	SNMP v3
cisco ✓	SNMP ✓	SNMP_WRITE ✓	None

□ Save as global settings

Settings will be used for this specific Discovery job **only**

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.

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 + (the plus sign).

   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 **Save**.

   With the **SNMP Autoconfig** 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 7: 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.
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 8: 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 9: 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

Field	Description
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 10: 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.

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.

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.

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

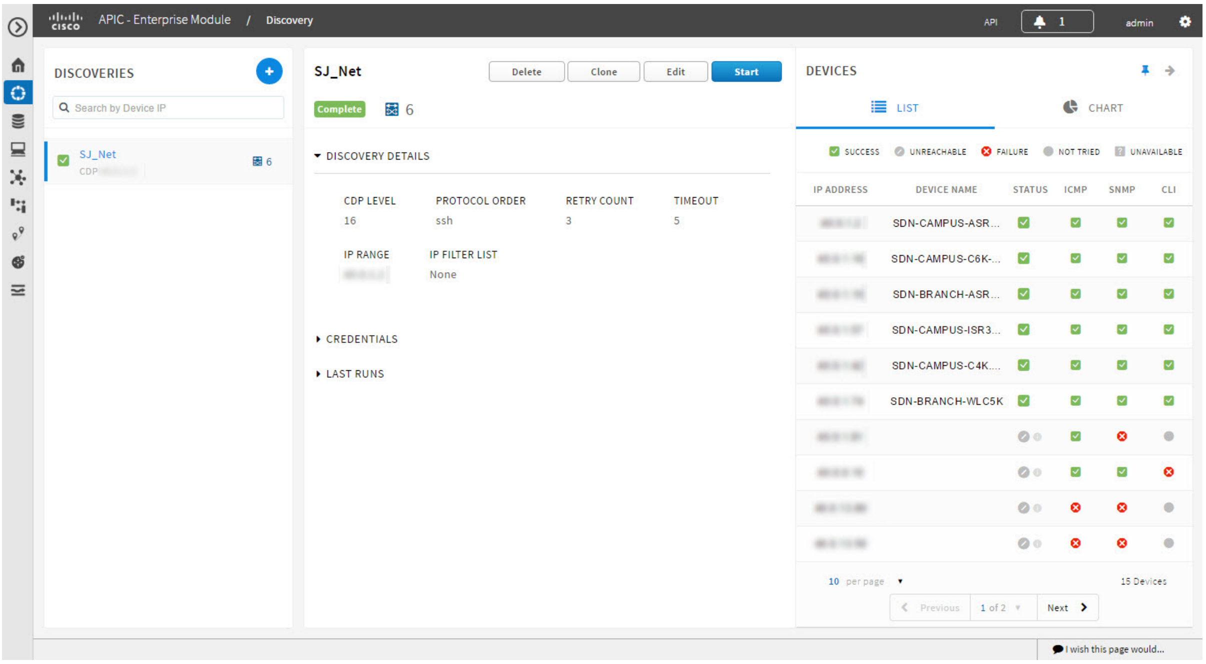
The **Discovery Results** pane provides information about the selected scan.

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 10: Discovery Results Window—List



DISCOVERY DETAILS

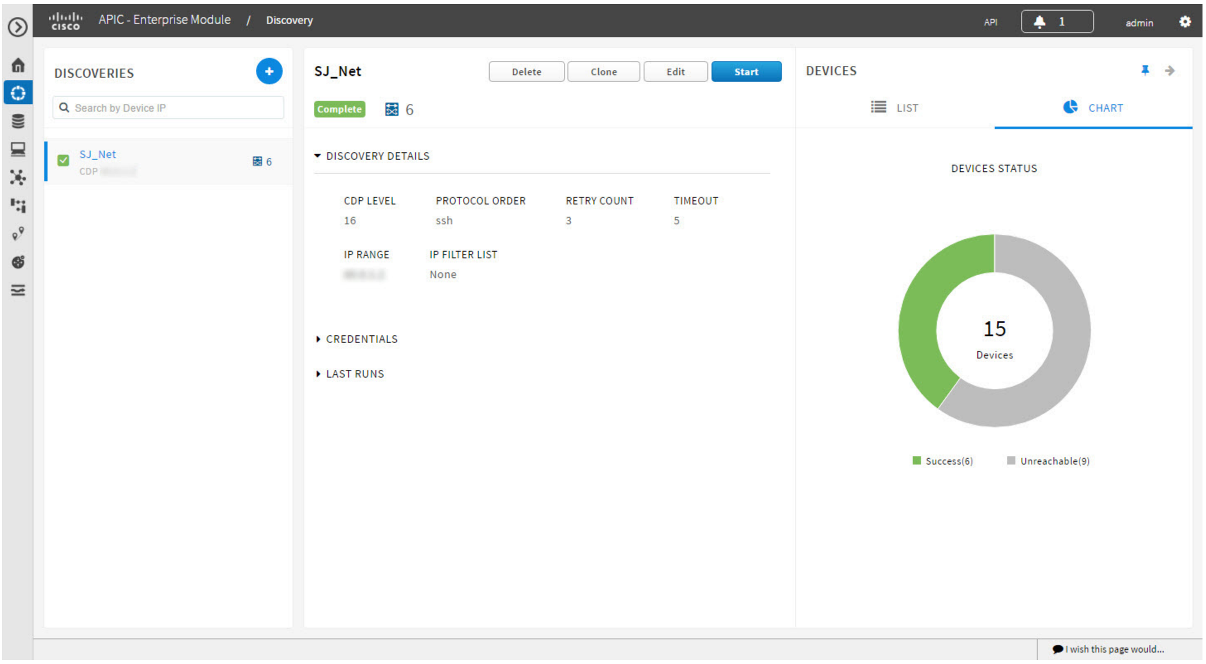
CDP LEVEL	PROTOCOL ORDER	RETRY COUNT	TIMEOUT
16	ssh	3	5

IP RANGE	IP FILTER LIST
[redacted]	None

✓ SUCCESS ⊘ UNREACHABLE ☒ FAILURE ● NOT TRIED ? UNAVAILABLE

IP ADDRESS	DEVICE NAME	STATUS	ICMP	SNMP	CLI
[redacted]	SDN-CAMPUS-ASR...	✓	✓	✓	✓
[redacted]	SDN-CAMPUS-C6K-...	✓	✓	✓	✓
[redacted]	SDN-BRANCH-ASR...	✓	✓	✓	✓
[redacted]	SDN-CAMPUS-ISR3...	✓	✓	✓	✓
[redacted]	SDN-CAMPUS-C4K....	✓	✓	✓	✓
[redacted]	SDN-BRANCH-WLC5K	✓	✓	✓	✓
[redacted]		⊘	✓	☒	●
[redacted]		⊘	✓	✓	☒
[redacted]		⊘	☒	☒	●
[redacted]		⊘	☒	☒	●

Figure 11: Discovery Results Window—Chart



DISCOVERY DETAILS

CDP LEVEL: 16

PROTOCOL ORDER: ssh

RETRY COUNT: 3

TIMEOUT: 5

IP RANGE: [redacted]

IP FILTER LIST: None

CREDENTIALS

LAST RUNS

Table 11: 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.

Name	Description
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.