Discovering Devices and Hosts

About 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 do this, you need to provide the controller with information about your network 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 network 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) (You must manually enable IPDT on devices and interfaces for this protocol to be used to collect host information.)
- LLDP Media Endpoint Discovery (LLDP-MED) (IP phones and some servers are discovered using LLDP-MED).

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

Name	Description
Discoveries pane	Lists the names of the discovery scans 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 in a box to the right of the discovery name. An unsuccessful scan shows no box or number of devices discovered. From the **Discoveries** pane, clicking on a discovery name displays the information in the **Discovery Details** and **Device Details** panes.
Discovery Details pane	Provides detailed information about the discovery parameters that were used to perform the discovery, the state of the discovery, and the number of devices that were discovered. The buttons on this pane allow you to **Start**, **Stop**, and **Delete** discoveries.
In-tool guide	Provides guidance about how to configure discovery.

Understanding Device and Host Discovery

The Cisco APIC-EM controller scans network devices and attempts to log in to newly found devices by presenting credentials that this guide refers to as discovery credentials.

The Cisco APIC-EM controller discovers network devices automatically by conducting a network scan that attempts to authenticate each network element that it finds. The process of finding network devices is known as discovery. The discovery scanner attempts to log in to a newly found network element by presenting credentials that this guide refers to as discovery credentials. To enable automated discovery of devices made by a variety of manufacturers, the Cisco APIC-EM supports several kinds of discovery credentials.

The Cisco APIC-EM discovers devices and hosts and populates the device and host inventory database with the results of the discovery.

Wireless LAN Controllers (WLCs) have additional setup requirements in order to be discovered. For more information, see Understanding Wireless LAN Controller Discovery, on page 2.

Understanding Wireless LAN Controller Discovery

The Cisco APIC-EM accepts SNMP traps from several Cisco Wireless LAN Controllers (WLCs). The SNMP traps are used to update the host inventory database. You need to configure the WLCs so that the Cisco APIC-EM is the trap receiver, and the WLCs send the enhanced traps to the Cisco APIC-EM.

The following WLCs require SNMP traps to be enabled:

- Cisco Series 2504 Wireless LAN Controller
- Cisco Series 5508 Wireless LAN Controller
- Cisco Series 8510 Wireless LAN Controller

The following table specifies the SNMP traps and object identifiers that must be set on the WLCs.

Trap Name	OID
ciscoLwappDot11ClientAssocTrap	1.3.6.1.4.1.9.9.599.0.9
ciscoLwappDot11ClientDeAuthenticatedTrap	1.3.6.1.4.1.9.9.599.0.10
ciscoLwappDot11ClientMovedToRunStateNewTrap	1.3.6.1.4.1.9.9.599.0.11
ciscoLwappDot11ClientMobilityTrap	1.3.6.1.4.1.9.9.599.0.12

The following configurations must be set to enable the above SNMP traps:

- config trapflags client enhanced-802.11-associate enable
- config trapflags client enhanced-802.11-deauthenticate enable
- config trapflags client enhanced-authentication enable
- config trapflags client enhanced-802.11-stats enable

Note When setting the SNMP traps on the WLCs, ensure you configure the IP address of the Cisco APIC-EM as the SNMP trap destination IP address. You set the Cisco APIC-EM IP address using the configuration wizard during the deployment process. For information about this process and the controller IP address, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information.

Understanding the Discovery Results

The Discovery window provides information about the selected scan. To access the **Discovery** window, from the **Navigation** pane, click **Discovery**. The **Discovery Results** window has three main panes.

Note You must have created at least one discovery scan for the **Discovery Results** window to display.

Name	Description
Discoveries pane	Lists the names of the discovery scans 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 in a box to the right of the discovery name. An unsuccessful scan shows no box or number of devices discovered. From the **Discoveries** pane, clicking on a discovery name displays the information in the **Discovery Details** and **Device Details** panes.

Name	Description
Discovery Details pane	Provides detailed information about the discovery parameters that were used to perform the discovery, the state of the discovery, and the number of devices that were discovered. The buttons on this pane allow you to **Start**, **Stop**, and **Delete** discoveries.
Devices pane	Displays the host name, IP address, and status of the devices found during the scan. Discovery displays devices as discarded if the IP address belongs to an access point (associated with a wireless controller) or the device was filtered based on input given in the **Subnet Filter** field.

Discovery Credentials Rules

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

Discovery request-specific credentials rules:

- These credentials can be provided when creating a new network discovery, but only a single set of these credentials is allowed per network discovery.
- These credentials take precedence over any configured global credentials.
- If the discovery request-specific credentials cause an authentication failure, then discovery is attempted a second time with the configured global credentials (if explicitly selected in the **Discovery** window). If discovery fails with the global credentials then the device discovery status will result in an authentication failure.
- If the discovery request-specific credentials (both CLI and SNMP) are not provided as part of network discovery, then the global credentials (both CLI and SNMP) are used to authenticate devices.

Global credentials rules:

Table 1: Global Credentials Rules

Global Credentials	Discovery Request-Specific Credentials	Result
Not configured	Not configured	The default SNMP read community string (public) is used for the discovery scan, but the device discovery will fail since both CLI and SNMP credentials must be configured for a successful device discovery.

Global Credentials	Discovery Request-Specific Credentials	Result
Not configured	Configured	The specified discovery request-specific credentials will be used for discovery.
Configured	Not configured	Configured global credentials will be used for discovery if selected in **Discovery**.
Configured but not selected	Configured	Only the request-specific credentials will be used.
Configured and selected	Not configured	Only selected global credential will be used.
Configured and selected	Configured	Both specified credentials (global and discovery request-specific) will be used for discovery.
Configured, but wrong global credential IDs are mentioned in the discovery POST REST API.	Correct request-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:
    - Update the global credentials with the new device credential. Execute a new discovery scan with the new global credentials.
    - Start a new discovery scan with changed discovery request-specific credentials that matches the new device credential.
- 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 discovery request-specific credential that matches the device credential.
    - Create a new global credential or modify one of the global credentials, and execute a new discovery selecting the correct global credential.

- 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, including certain administrative credentials (SNMP community strings and CLI usernames). 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. Any user account with a ROLE_ADMIN has access to this API.

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

Using Discovery

Performing Discovery Using CDP

You can perform a discovery using CDP.

Note that while a discovery is in progress, you can do any of the following actions:

- Create a new discovery by clicking **Add New** from the **Discoveries** pane.
- Stop an active discovery by selecting the discovery name in the **Discoveries** pane and clicking **Stop** in the **Discovery Details** pane.
- Start an inactive discovery by selecting the discovery name in the **Discoveries** pane and clicking **Start** in the **Discovery Details** pane.
- Delete a discovery by selecting the discovery name in the **Discoveries** pane and clicking **Delete** in the **Discovery Details** pane.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

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

Procedure

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

The **Discovery** window appears.

Step 2 (Optional) In the **Discovery Name** field, enter a unique name for this discovery.

Step 3 In the **IP Ranges** area, do the following:

a) From the **Discovery Type** field, choose **CDP**.

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

Step 4 In the **SNMP** area, choose one of the previously configured SNMP settings from the **Saved SNMP** drop-down list. If the settings that you need are not available in the list, you can configure SNMP settings for the current discovery.
Use the following guidelines and the information in the tables to help you enter the correct values in the fields:

- The controller supports multiple SNMP credential configurations, but if you configure more than six credential sets (global and/or exception, SNMPv2c and/or SNMPv3 credentials), you will receive an error message.
- An SNMP Read Only (RO) community string is required to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, as a *best effort*, discovery will run with the default SNMP RO community string "public."

Table 2: SNMPv2c

Field	**Description**
Read Community	SNMP read-only (RO) or read/write (RW) community string. The SNMP community string that you configure in this field is used only for this specific discovery. **Note** To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write Community	SNMP read-only (RO) or read/write (RW) community string.

Note Certain **SNMPv3** configuration options are or are not available depending upon your selections.

Table 3: SNMPv3

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

Field	Description
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
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
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
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.

Table 4: SNMP Properties

Field	Description
Connection 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.
Retry Count	Number of attempts to connect to the device. Valid values are from 0 to 4 attempts.

Step 5 In the **CLI Credentials** area, enter the username, password, and enable password in the fields for the devices that you want the Cisco APIC-EM to discover.
Both the password and enable password are encrypted for security reasons and cannot be seen when viewing the configuration.

Discovery credentials are preexisting device credentials used by the Cisco APIC-EM to authenticate and discover the Cisco devices in your network. For host discovery, credentials are not required as hosts are discovered through the devices.

Note Cisco APIC-EM uses both the exception discovery credentials and the global discovery credentials (set in the **Settings > Discovery Credentials** window) to help you discover all of the Cisco devices within your network.

Step 6 (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. By default, the Cisco APIC-EM uses the following protocols:

- SSH
- Telnet

To remove a protocol from the scan, click the protocol name. The checkmark next to the protocol disappears and the protocol fades from the display.

To customize the order that protocols are used to connect to devices, drag and drop a selected protocol to the desired location in the list.

Step 7 (Optional) To save these settings, select the **Save theses settings to be used again tin the future** check box.

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.

Performing a Discovery Using an IP Address Range

You can discover devices using an IP address range.
Note that while a discovery is in progress, you can do any of the following actions:

- Create a new discovery by clicking **Add New** from the **Discoveries** pane.
- Stop an active discovery by selecting the discovery name in the **Discoveries** pane and clicking **Stop** in the **Discovery Details** pane.
- Start an inactive discovery by selecting the discovery name in the **Discoveries** pane and clicking **Start** in the **Discovery Details** pane.
- Delete a discovery by selecting the discovery name in the **Discoveries** pane and clicking **Delete** in the **Discovery Details** pane.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

Step 1 From the **Navigation** pane, click **Discovery**.
The **Discovery** window appears.

Step 2 (Optional) In the **Discovery Name** field, enter a unique name for this discovery.

Step 3 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) Enter any additional IP addresses in the IP address fields and click **Add**.

Step 4 In the **SNMP** area, choose one of the previously configured SNMP settings from the **Saved SNMP** drop-down list. If the settings that you need are not available in the list, you can configure SNMP settings for the current discovery.
Use the following guidelines and the information in the tables to help you enter the correct values in the fields:

- The controller supports multiple SNMP credential configurations, but if you configure more than 5 credential sets (global and/or exception, SNMPv2c and/or SNMPv3 credentials), you will receive an error message.
- An SNMP Read Only (RO) community string is required to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, as a *best effort*, discovery will run with the default SNMP RO community string "public."

Table 5: SNMPv2c

Field	Description
Read Community	SNMP read-only (RO) or read/write (RW) community string. The SNMP community string that you configure in this field is used only for this specific discovery. **Note** To enable discovery on the network devices, configure the network device's IP host address as the client address.
Write Community	SNMP read-only (RO) or read/write (RW) community string.

Note Certain **SNMPv3** configuration options are or are not available depending upon your selections.

Table 6: SNMPv3

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

Field	Description
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
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3.
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
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.

Table 7: SNMP Properties

Field	Description
Connection 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.
Retry Count	Number of attempts to connect to the device. Valid values are from 0 to 4 attempts.

Step 5 In the **CLI Credentials** area, enter the username, password, and enable password in the fields for the devices that you want the Cisco APIC-EM to discover.
Both the password and enable password are encrypted for security reasons and cannot be seen when viewing the configuration.

Discovery credentials are preexisting device credentials used by the Cisco APIC-EM to authenticate and discover the Cisco devices in your network. For host discovery, credentials are not required as hosts are discovered through the devices.

Note Although you are limited to only one set of discovery credentials per discovery scan, you can run several different discovery scans with different credentials to authenticate and discover all of the Cisco devices within your network.

Step 6 (Optional) In the **Advanced** area, configure the protocols that the Cisco APIC-EM uses to connect to devices. By default, the Cisco APIC-EM uses the following protocols:

- SSH
- Telnet

To remove a protocol from the scan, click the protocol name. The checkmark next to the protocol disappears and the protocol fades from the display.

To customize the order that protocols are used to connect to devices, drag and drop a selected protocol to the desired location in the list.

Step 7 (Optional) To save these settings, select the **Save theses settings to be used again in the future** check box.

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.

Stopping and Starting a Discovery

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

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

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

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

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

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

Deleting a Discovery

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

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

Procedure

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

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