Discovering Devices and Hosts

About Discovery

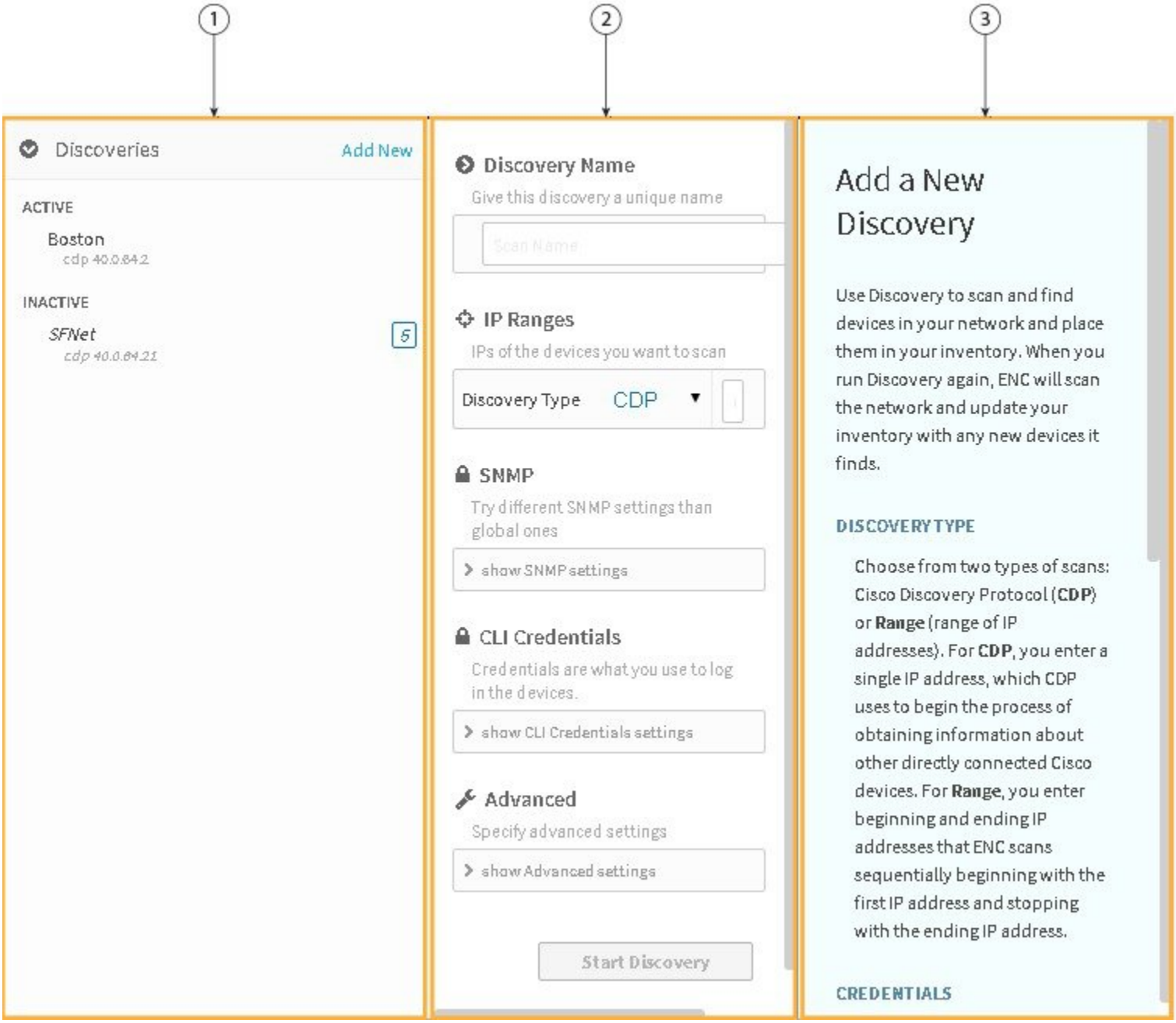
The Discovery function scans the devices and hosts in your network and populates the Cisco APIC-EM database with the information that it retrieves. To do this, you need to tell the controller some information about your network so that the Discovery function can reach as many of the devices in your network as possible and gather as much information as it can.

The Discovery function uses the following protocols and methods to retrieve the information about your network:

- 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)—IPDT is enabled automatically for all devices by the controller. For this configuration, privileges must be given to the controller during discovery.
- LLDP-MED—IP phones and possibly some servers are discovered using LLDP Media Endpoint Discovery

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

Figure 1: Discovery Window



Numbered Callout	Name	Description
1	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.
2	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.
3	In-tool guide	Provides guidance about how to configure discovery.

Understanding Device and Host Discovery

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

To discover devices and hosts, you must configure SNMPv2c credentials or SNMPv3 credentials or both SNMPv2c and SNMPv3 credentials (depending on your network). For SNMPv2, only the SNMP read community credentials are mandatory.

CLI credentials are also mandatory. Configure CLI credentials to access to the configuration files on the devices.

These credentials can be configured in two different places in the Cisco APIC-EM GUI:

- **Settings > Discovery Credentials** window—You configure SNMP and CLI credentials in this window when they are common to all or most of the devices in your network. These credentials are referred to as *global* credentials.
- **Discovery** window—You configure SNMP and CLI credentials in this window when you want to discover devices on the fly or when you need to devices that do not have the typical SNMP and CLI credentials that the majority of the devices have in your network and that were configured in the **Settings > Discovery Credentials** window. These credentials are referred to as *exception* credentials.

Wireless LAN Controllers (WLCs) have additional setup requirements in order to be discovered. For more information, see Understanding Wireless LAN Controller Discovery, on page 4.

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
- Cisco Wireless Service Module 2 (WiSM2)

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.

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 **Stop** 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 permissions. For information about user permissions, see Managing Users and Roles.

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

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 starting point for the discovery scan.

Step 4 In the **SNMP** area, configure one or both of the SNMP versions that are being used by the devices that you want to discover.
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 1: 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. To set up default SNMP community strings that can be saved and used for all discoveries, go to **Settings > Discovery Credentials**. **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 2: 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
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 3: 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. The Cisco APIC-EM supports two types of discovery credentials: common discovery credentials and exception discovery credentials.

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 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 permissions. For information about the user permissions, see Managing Users and Roles.

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, configure one or both of the SNMP versions that are being used by the devices in your network. Use the following guidelines and the information in the following tables to help you enter the correct values in the fields:

- The controller supports up to five SNMP credential configurations.
- 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, discovery runs with the default SNMP RO community string "public" as a *best effort* discovery scan.

Table 4: 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 only. To set up default SNMP community strings that can be saved and used for all discoveries, go to **Settings > Discovery Credentials**. **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 Depending on your selections, certain **SNMPv3** configuration options are or are not available.

Table 5: SNMPv3

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 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 6: 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 *exception* username, password, and enable password for the devices that you want to discover. You can add up to five CLI credentials.

Note Both the password and enable password are encrypted for security reasons and cannot be seen when viewing the configuration.

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 attempts to connect to devices using 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 view.

To customize the order that protocols are used to connect, drag and drop a selected protocol to the top of the list.

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.

Stopping and Starting a Discovery

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

Before You Begin

You must have administrator permissions. For information about the user permissions, see Managing Users and Roles.

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

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 permissions. For information about the user permissions, see Managing Users and Roles.

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

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

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

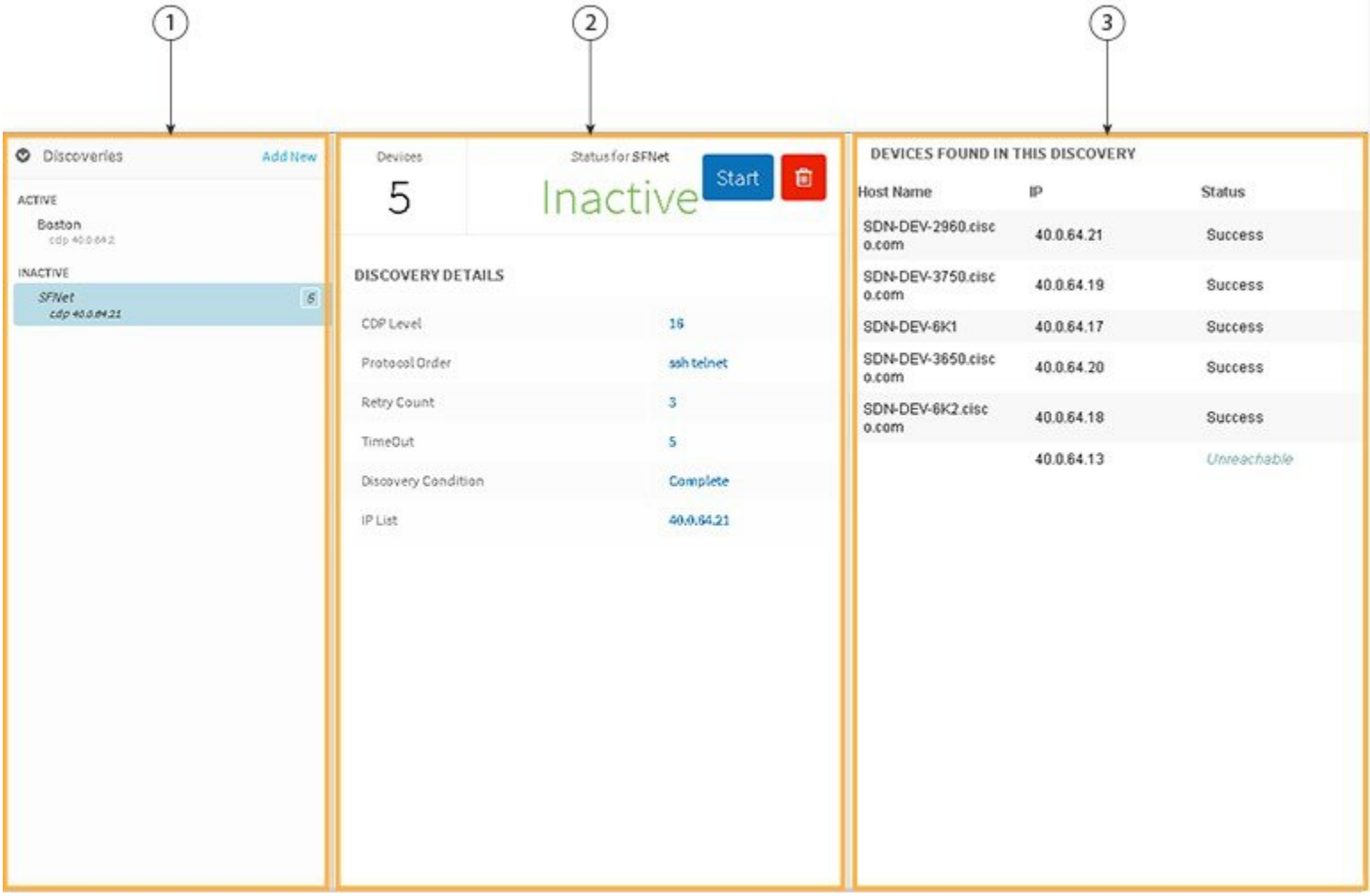
Step 4 Click **OK** to confirm that you want to delete the discovery.

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.

Figure 2: Discovery Results Window



Callout Number	Name	Description
1	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.
2	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.
3	Devices pane	Displays the host name, IP address, and status of the devices found during the scan.