Manage Device Credentials

Manage Device Credentials

You need to configure device credentials for all devices that are managed using Cisco Prime Collaboration. Device credentials are required for discovering devices and updating inventory. If the credentials vary for different devices, create separate credentials profiles; that is, if you want to manage two Cisco Unified Communications Managers with different credentials in Cisco Prime Collaboration, you must create two separate credentials profiles.

The following are some of the requirements while creating credentials profiles:

- HTTP and SNMP credentials are mandatory for the TelePresence endpoints to get into Managed state.
- Create an Enterprise License Manager profile by selecting Enterprise License Manager as the device type for Prime License Manager.
- Credentials are not required for the phones, and Cisco Jabber. These endpoints are discovered with the discovery of the call processor with which they are registered.

You must review the Configure Devices for Cisco Prime Collaboration document to understand the required protocols to manage devices in Cisco Prime Collaboration.

Add a Device Credential Profile

To add or clone a credential profile:

Step 1 In the **Cisco Prime Collaboration** page, choose **Inventory** > **Inventory Management** from the Toggle Navigation pane.
The **Inventory Management** page is displayed.

Step 2 In the Credentials Profile page, click **Add** and enter the necessary information described in the Credential Profiles Field Descriptions table.

Step 3 Click **Save**.
In your network, you may have configured the same SNMP credentials for all devices. In such cases, first create a new profile and later clone the existing profile. To clone, in the Credentials Profile page, select an existing profile and click **Clone** and after the required updates click **Add/Update**.

Credential Profiles Field Descriptions

After the devices are discovered, you can check the current Inventory table to verify that the credentials have been updated in the Cisco Prime Collaboration database.

The following table describes the fields on the Credential Profiles page.

Table 1: Credential Profiles Field Descriptions

Field Name	Description
Profile Name	Name of the credential profiles. For example: • CUCM • router_switches

Field Name	Description
Device Type	(Optional) The credential fields (such as SNMP, HTTP) are displayed, based on the device type that you have selected. To reduce rediscovery time, we recommend that you select the device type when you create the credential profiles. The default device type is “Any”, if you do not select a device type while creating a credential profile. See cisco.com for the list of device types. For EX series, MX series, SX series, bare Codec devices, and all profiles with Codec, select the device type as TC_CE. **For Cisco Prime Collaboration Release 11.6 and later** For EX series, MX series, SX series, DX series with CE image, bare Codec devices, and all profiles with Codec, select the device type as Codec. For MSE devices, select as the device type. You can enter any credentials (SNMP, HTTP) to create an “Any” credential profile. You must create an “Any” credential profile to run auto-discovery (Ping Sweep and CDP discovery). However, you can run logical discovery also. If your network has multiple subnets, then create an “Any” profile for each subnet.
IP Version	The IP address is version 4 or version 6.

Field Name	Description
IP Address Pattern	IP address of the devices for which the credentials are provided. You must: • Separate multiple IP addresses by the delimiter pipe (|). • Not use 0.0.0.0 or 255.255.255.255. • Not use question mark (?). We recommend that you: • Enter the exact IP address for Cisco Unified CM. • Enter the exact IP address for network devices. • Do not use many wildcard expressions in the address patterns. For example: • 100.5.10.*|100.5.11.*|100.5.20.*|100.5.21.* • 200.5.1*.*|200.5.2*.*|200.5.3*.* • 172.23.223.14 • 150.5.*.* Avoid using patterns such as 150.*.*.*, 192.78.22.1?, 150.5.*.*/24. If you are unable to find a common pattern for the devices, enter *.*.*.*. Minimize the use of wildcard character (*), while defining the IP address patterns in the credential profiles (**Inventory** > **Inventory Management** > **Manage Credentials**). Use of wildcard character may increase the discovery time. See SNMPv2C to understand how the patterns are used.
General SNMP Options	SNMP Timeout - The default is 10 seconds.
	SNMP Retries - The default is 2.
	SNMP Version - Selecting an SNMP version is mandatory.
SNMPv2C Used to discover and manage the device.	SNMP Read Community String You can provide either SNMPv2C or SNMPv3 credentials. We recommend that you use different SNMP credentials for Cisco TelePresence systems and network devices. Cisco Prime Collaboration searches the credential profiles, based on the IP address pattern. Cisco Prime Collaboration then chooses a profile for which the SNMP credentials match. There can be multiple matching profiles, that is, profiles with the same SNMP credentials. In such cases, Cisco Prime Collaboration chooses the profile that matches first.
	SNMP Write Community String

Field Name	Description
SNMPv3 Used to discover and manage the device.	SNMP Security Name - Enter a security name.
	SNMP Authentication Protocol - You can choose either MD5 or SHA.
	SNMP Authentication Passphrase - Enter a passphrase.
	SNMP Privacy Protocol - You can choose either AES128, or DES.
HTTP Used to access the device through HTTP to poll system status and meeting information.	HTTP Username and Password Cisco Prime Collaboration first checks the access for HTTP. If the access attempt fails, then Cisco Prime Collaboration checks the access for HTTPS. If you log in to Cisco TMS using the <domain/username> format, then ensure that you add the same <domain/username> value in the **HTTPS Username** field.

Clone a Device Credentials Profile

To copy an existing credential profile:

Step 1 In the page, select an existing profile and click **Clone**.

Step 2 Click **Add/Update**.

Modify Device Credentials

If you have modified credentials for the devices that you are currently managing in the Cisco Prime Collaboration application, you must modify the relevant credential profiles in the Cisco Prime Collaboration database.

If the credentials are incorrect, a major event— Device is inaccessible is triggered from Cisco Prime Collaboration ().

To edit a credential profile:

Step 1 Choose **Inventory** > **Inventory Management**.

Step 2 From the **Inventory Management** page, select a device and click **Modify Credentials**.

Step 3 Update the credentials and click **Rediscover**.
Cisco Prime Collaboration takes a few minutes to update its database with the modified credentials. After the credentials are updated, an informational event, Device is accessible from Collaboration Manager, is triggered. Cisco Prime Collaboration uses the updated credentials in the next polling job.

Verify Device Credentials

If device discovery fails because of incorrect credentials, you can test the credentials for the failed devices and rediscover those devices. Choose **Inventory** > **Inventory Management** for a list of devices that were not discovered.

Note Do not run this task when a discovery job is in progress.

To verify device credentials:

Step 1 In the Inventory Management page, choose **Manage Credentials**
The Manage Credential page is displayed.

Step 2 From the Credential Profiles page, select the profile name to use for testing the credentials, and click **Verify**.

Step 3 Enter a valid device IP address to test the credentials. You can verify only one device at a time, and you cannot enter expressions such as *.*.*.*, 192.2.*.*, and so on.

Step 4 Click **Test**. You can see an inprogress moving icon next to the test button till the task completes. The test results are displayed under the Test Credential Result pane.
If the verification fails, see the possible reasons listed in Credential Verification Error Messages.

Note All the nodes in the cluster may not be running all the protocols. For example, JTAPI may not be running on all the nodes. As a result, the credential validation test may fail for some of your nodes. After fixing the credentials issue, test the device credentials again and run the discovery for that device. After the devices are discovered, you can verify if the access information is updated in the Cisco Prime Collaboration database in the current Inventory table.

Credential Verification Error Messages

The credential verification error messages are tabulated below.

Table 2: Credential Verification Error Messages

Error Message	Conditions	Possible Solutions
SNMPv2		

Error Message	Conditions	Possible Solutions
SNMP Request: Received no response from *IP Address*.	Failed for one of the following reasons: • Device response time is slow. • Device is unreachable. • Incorrect community string entered in the credential profile.	• Verify the device connectivity. • Update the credential profile with the correct community strings.
SNMP timeout.	Either the device response time is slow or the device is unreachable.	• Verify the device connectivity. • Increase the SNMP Timeout and Retries values in the credential profile.
Failed to fetch table due to: Request timed out.	Either the device response time is slow or the device is unreachable.	Increase the SNMP Timeout and Retries values in the credential profile.
SNMPv3		
The configured SNMPv3 security level is not supported on the device.	Device does not support the configured SNMPv3 security level.	Change the SNMPv3 security level to the supported security level in the credential profile.
The SNMPv3 response was not received within the stipulated time.	Either the device response time is slow or the device is unreachable.	Verify the device connectivity.
SNMPv3 Engine ID is wrong.	Incorrect engine ID entered in the credential profile.	Enter the correct SNMPv3 engine ID in the credential profile.
SNMPv3 message digest is wrong.	Failed for one of the following reasons: • Either the SNMPv3 authentication algorithm or the device password is incorrect. • Network errors.	• Verify that the correct SNMPv3 authentication algorithm and device password are set in the credential profile. • Check for network errors.
SNMPv3 message decryption error.	Cannot decrypt the SNMPv3 message.	Verify that the correct SNMPv3 authentication algorithm is entered in the credential profile.
Unknown SNMPv3 Context.	The configured SNMPv3 context in the credential profile does not exist on the device.	Verify that the configured SNMPv3 context is correct in the credential profile.

Error Message	Conditions	Possible Solutions
Unknown SNMPv3 security name.	Either the SNMPv3 username is incorrect in the credential profile or the SNMPv3 username is not configured on the device.	Verify that the correct SNMPv3 username is set in the credential profile and on the device.
CLI		
Login authentication failed.	Incorrect credentials entered in the credential profile.	Verify and reenter the device CLI credentials in the credential profile.
Connection refused.	Either SSH or Telnet service may not be running on the device.	1 Verify the device connectivity for the supported CLI (port). 2 Verify whether the SSH or Telnet service is running on the device.
HTTP		
Server returned HTTP response code: 401 for URL.	Either the HTTP service is not running or the URL is invalid.	• Verify whether the HTTP or HTTPS service is running on the device. • Verify whether the URL is valid on the server.
Connection refused.	The HTTP or HTTPS service is not running.	Verify whether the HTTP or HTTPS service is running on the device.
HTTP check failed.	Incorrect HTTP credentials entered in the credential profile.	Verify and reenter the device HTTP credentials in the credential profile.

Delete a Device Credential Profile

You can delete only unused credential profiles. We recommend that you do not delete the credential profile of a device that is being managed in the Cisco Prime Collaboration application.

To delete a credential profile:

Step 1 Choose **Inventory** > **Inventory Management**.

Step 2 In the page, click **Manage Credentials**. By default, the credentials for a device that appears first on the list are displayed.

Step 3 Select the profile name and click **Delete**.