CHAPTER 2

Managing 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 Prime Collaboration, you must create two separate credentials profiles.

Note Credentials are not required for the Cisco Unified IP Phone 8900 and 9900 series, Cisco Cius, and Cisco Jabber Video for TelePresence (Movi) endpoints. These endpoints are discovered with the discovery of the call processor with which they are registered.

You must enter CLI credentials for video endpoints and network devices before you start the troubleshooting workflow.

Adding and Copying Device Credentials

You must configure device credentials before discovering devices.

In your network, you may have configured the same SNMP credentials for all devices, but different CLI credentials. In such cases, first create a new profile and later clone the existing profile.

To add new credential profiles:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Work Center page, click **Manage Credentials**.

Step 3 In the Credentials Profile window, click **Add** enter the necessary information. See Table 2-1.

Step 4 Click **Add/Update**.

To copy an existing credential profiles:

Step 1 In the Credentials Profile window, select an existing profile and click **Clone**.

Step 2 Provide a new name for the profile and update existing fields, if necessary.

Step 3 Click **Add/Update**.

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

Table 2-1 describes the fields on the Credential Profiles page.

Table 2-1 Credential Profiles Field Descriptions

Field Name	Description	Additional Information
Profile Name	Name of the credential profiles.	• CTS_MAN • CUCM • router_switches
Device Type	(Optional) Type of the device for which you want to manage the device credentials. The credential fields (SNMP, CLI, and so on) are displayed, based on the device type that you have selected. Though optional, we recommend that you select the appropriate device type while creating credential profiles to reduce the time involved in discovery. 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 Codec. For MSE devices, select Cisco MCU as the device type.	You can enter any credentials (SNMP, HTTP, JTAPI, CLI, MSI) to create an Any credential profile. You must create an Any credential profile to run autodiscovery (Ping Sweep and CDP discovery). However, logical discovery can also be performed. If your network has multiple subnets, then create an Any profile for each subnet.

Table 2-1 Credential Profiles Field Descriptions (continued)

Field Name	Description	Additional Information
IP Address Pattern	IP address of the devices for which the credentials are provided. You must: • Enter only valid IPv4 addresses. • 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 CTS-Manager, Cisco Unified CM, and CTMS. • Enter the exact IP address for either CTS or network devices. • Do not use many wildcard expressions in the address patterns. If you are unable to find a common pattern for the devices, enter *.*.*.*. See SNMPv2C to understand how the patterns are used. Prime Collaboration supports only IPv4 configured endpoints. It does not support IPv6 configured endpoints. Also, Prime Collaboration does not support dual stack (IPv4 and IPv6 configured) endpoints.	• 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.
General SNMP Options	SNMP Timeout	The SNMP timeout is set for 10 seconds, by default.
	SNMP Retries	The retry value is 2, by default.
	SNMP Version	Selecting SNMP version is mandatory.

Table 2-1 Credential Profiles Field Descriptions (continued)

Field Name	Description	Additional Information
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. Prime Collaboration searches the credential profiles, based on the IP address pattern. 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, Prime Collaboration chooses the profile that matches first. **Note** Sometimes there may be multiple profiles that have the same SNMP credentials, but different CLI credentials. This might result in Prime Collaboration choosing a profile that contains the correct SNMP credentials, but incorrect CLI credentials for the device. If this occurs, the troubleshooting workflow may not work.
	SNMP Write Community String	—
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	This feature is not supported.
	SNMP Privacy Passphrase	This feature is not supported.
CLI Used to access the device through CLI to discover media path for troubleshooting.	CLI Login Username and Password	The CLI credentials are used during the troubleshooting workflow. If the credentials are not entered or if the entered credentials are incorrect, the troubleshooting workflow feature may not work.
HTTP Used to access the device through HTTP to poll system status and meeting information.	HTTP Username and Password	Prime Collaboration first checks the access for HTTP. If the access attempt fails, then Prime Collaboration checks the access for HTTPS.

Table 2-1 Credential Profiles Field Descriptions (continued)

Field Name	Description	Additional Information
JTAPI Used to retrieve the session status information from the Cisco Unified CM.	JTAPI Username and Password. **Note** Password must not contain a semicolon (;) or equals (=).	JTAPI is optional. It is required only for TelePresence session monitoring.
MSI Used to access the device through MSI to discover media path for troubleshooting.	MSI Username and Password	The MSI credentials are used during the troubleshooting workflow, to troubleshoot MSI enabled endpoints. MSI credentials remain the same as http credentials for TC 6.0 and TE 6.0 software versions. For TX 6.0 version, the default MSI username is **msiuser** and the password is **cisco**.

Note Minimize the use of wildcard character (*), while defining the IP address patterns in the credential profiles (**Operate > Device Work Center > Manage Credentials**). Use of wildcard character may increase the discovery time.

Updating Device Credentials

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

If the credentials are incorrect, a major event, `Device is not accessible from Prime Collaboration,` is triggered (**Operate > Alarms & Events > Events**).

To update a credential profiles:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Work Center page, click **Manage Credentials**.

Step 3 Select the Profile Name from the Credential Profiles window.

Step 4 Update the credentials and click **Add/Update**.

Prime Collaboration takes a few minutes to update its database with the updated credentials. After the credentials are updated, an informational event `Device is accessible from Collaboration Manager` is triggered. Prime Collaboration uses the updated credentials in the next polling job.

For details on monitoring events, see the *Cisco Prime Collaboration 9.0 Fault Management Guide*.

Verifying Device Credentials

If device discovery fails because of incorrect credentials, you can test the credentials for the failed devices and rediscover those devices. Choose **Operate > Device Work Center > Discovery Jobs** for a list of devices that were not discovered.

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

To verify defined credentials:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Device Work Center page, click **Manage Credentials**.

Step 3 From the Credential Profiles window, select the profile name to use for testing the credentials, and click **Verify**.

Step 4 Enter the 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. You must enter a valid IP address.

Step 5 Click **Test**.

If the verification fails, see the possible reasons listed in Table 2-2.

Table 2-2 Credentials Error Messages

Error Message	Conditions	Possible Solutions
SNMPv2		
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.

Table 2-2 Credentials Error Messages (continued)

Error Message	Conditions	Possible Solutions
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.
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.
JTAPI		
Failed to access JTAPI.	Incorrect JTAPI credentials entered in the credential profile.	Verify and reenter the device JTAPI credentials in the credential profile. **Note** Password must not contain a semicolon (;) or equals symbol (=).
MSI		
Failed to access MSI.	Incorrect MSI credentials entered in the credential profile.	Verify and reenter the device MSI credentials in the credential profile.

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 Prime Collaboration database in the Current Inventory table. For more information, see Viewing Inventory Details, page 6-1.

Deleting Device Credentials

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

To verify whether a profile is being used, go to the Inventory page and select a device. The profile details for the device are displayed in the Access Information pane, see Access Information, page 6-4.

To delete a credential profile:

Step 1 Choose **Operate > Device Work Center**.

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

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