Manage Device Credentials

This section explains the following:

Manage Device Credentials

You need to configure device credentials for all devices that are managed using Cisco Prime Collaboration Assurance. 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 Assurance, you must create two separate credentials profiles. For more information, see the table on Credential Profiles Field Descriptions.

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

- HTTP and SNMP credentials are mandatory for the endpoints to get into Managed state.
- **For Cisco Prime Collaboration Release 11.1 and earlier**

  CLI credentials are required to troubleshoot sessions involving endpoints and network devices.
- **For Cisco Prime Collaboration Release 11.5 and later**

  CLI credentials are required to manage video test call and analyzing call signaling through SIP Call Flow Analyzer.
- JTAPI credentials are mandatory for Unified CM for conference monitoring. This credential is not required for endpoints.
- Create an Enterprise License Manager profile by selecting Enterprise License Manager as the device type for Prime License Manager.
- Define HTTP and SNMP credentials for Unified Contact Center devices such as Cisco Unified Intelligence Center (CUIC), Cisco Voice Portal (CVP), Cisco Finesse, Cisco SocialMiner, Cisco Unified Contact

Center Enterprise (Unified CCE), Cisco Unified Contact Center Express (Unified CCX), Cisco MediaSense.

For Cisco Prime Collaboration Release 11.5 and later

Define HTTP and SNMP credentials for Unified Contact Center devices such as Cisco Unified Intelligence Center (CUIC), Cisco Voice Portal (CVP), Cisco Finesse, Cisco SocialMiner, Cisco Unified Contact Center Enterprise (Unified CCE), Cisco Unified Contact Center Express (Unified CCX), Cisco Virtualized Voice Browser.

- Enter HTTP credentials for Contact Center Enterprise in the following format: domain\administrator. For example hcsdc2\administrator.
- Enter HTTP credentials for Cisco Unified Customer Voice Portal (CVP) which have the *ServiceabilityAdministrationUserRole* privileges. The default username *wsmadmin* has this privilege.
- Credentials are not required for the phones, Cisco Cius, Cisco Jabber, and Cisco Jabber Video for TelePresence (Movi) endpoints. These endpoints are discovered with the discovery of the call processor with which they are registered.
- Select VCS/ EXPRESSWAY in the Device type drop-down list to create credentials for Cisco Expressway-Core, Cisco Expressway-Edge or a Cisco VCS with Cisco Collaboration Edge or Core.

Note

- You must not enter * symbol with length of eight characters as SNMP Community String, SNMPv3, HTTP, JTAPI, and MSI password while creating credentials profiles in Credential Profile page or Add Device in Device Discovery.
- You must not enter % symbol with length of eight characters as password for CLI while creating credentials profiles in Credential Profile page or Add Device in Device Discovery.

Add a Device Credentials Profile

To add or clone a credential profile:

Step 1 In the **Cisco Prime Collaboration Assurance** page, choose **Device Inventory** > **Inventory Management** from the Toggle Navigation pane.

For Cisco Prime Collaboration Release 11.5 and later

In the **Cisco Prime Collaboration Assurance** 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 Table on Credential Profiles Field Descriptions, on page 3.

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 Assurance 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
Device Type	(Optional) The credential fields (such as SNMP, HTTP, CLI) 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. While managing coresident PLM, you should provide both CLI and HTTP credentials. • CLI credentials are used to access the license information. • HTTP credentials are used to manage Prime License Manager in Cisco Prime Collaboration Assurance.

Field Name	Description
Device Type	**For Cisco Prime Collaboration Release 12.1 and later** While managing co-resident PLM, you should provide both CLI and HTTP credentials. • CLI credentials are used to access the license information. • HTTP credentials are used to manage Prime License Manager in Cisco Prime Collaboration Assurance. Ensure the following conditions are met for the Router to be identified as a Cisco Unified Border Element (CUBE): **1.** CLI credentials (CLI Login Username and CLI Login Password) for the Device Type - Router is mandatory. **2.** Enabling SSH version 2 or later on Port 22 of the Router is mandatory. **3.** If Enable Password is set on the Router then provide the password in CLI Enable Password field. **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 Cisco MCU as the device type. **For Cisco Prime Collaboration Release 11.5 and later** For Cisco Virtualized Voice Browser devices, select Virtualized Voice Browser device type. You can enter any credentials (SNMP, HTTP, CLI, MSI) 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, and Cisco TMS. • Enter the exact IP address for either CTS or 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. **For Cisco Prime Collaboration Release 11.5 and later** **Inventory** > **Inventory management** > **Manage Credentials** Use of wildcard character may increase the discovery time. See SNMPv2C to understand how the patterns are used.

Field Name	Description
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 SNMPv1 or SNMPv2C credentials. We recommend that you use different SNMP credentials for Cisco TelePresence systems and network devices. Cisco Prime Collaboration Assurance searches the credential profiles, based on the IP address pattern. Cisco Prime Collaboration Assurance 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 Assurance chooses the profile that matches first. **For Cisco Prime Collaboration Release 11.1 and earlier** **Note** If multiple profiles have the same SNMP credentials but different CLI credentials, Cisco Prime Collaboration Assurance might chose a profile that contains the correct SNMP credentials but incorrect CLI credentials for the device. If this occurs, the troubleshooting workflow might 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 - You can choose either AES, AES128, or DES. **For Cisco Prime Collaboration Release 11.5 and later** SNMP Privacy Protocol - You can choose either AES128, or DES.

Field Name	Description
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. **For Cisco Prime Collaboration Release 11.5 and later** The CLI credentials are used to manage video test call and analyze call signaling through SIP Call Flow Analyzer. **For Cisco Prime Collaboration Release 12.1 and later** Ensure the following conditions are met for the Router to be identified as a Cisco Unified Border Element (CUBE): **1.** CLI credentials (CLI Login Username and CLI Login Password) for the Device Type - Router is mandatory. **2.** Enabling SSH version 2 or later on Port 22 of the Router is mandatory. **3.** If Enable Password is set on the Router then provide the password in CLI Enable Password field.
HTTP Used to access the device through HTTP to poll system status and meeting information.	HTTP Username and Password Cisco Prime Collaboration Assurance first checks the access for HTTP. If the access attempt fails, then Cisco Prime Collaboration Assurance 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.
JTAPI Used to retrieve the session status information from the Cisco Unified CM.	(Optional) JTAPI Username and Password. **Note** Password must not contain a semicolon (;) or equals (=).

Field Name	Description

Field Name	Description
	For Cisco Prime Collaboration Release 11.5 and later Used to retrieve the session status information from the Cisco Unified CM. **For Cisco Prime Collaboration Release 12.1 SP1** A new set of JTAPI specific parameters are introduced to secure the JTAPI (TLS v1.2) connection. **Note** 1. For more information on the method to secure the CTI, JTAPI, and TAPI applications and to know more about the certificate authority proxy function, see the Chapter on "Authentication and Encryption Setup for CTI, JTAPI, and TAPI" and "Certificate Authority Proxy Function" respectively in the "Security Guide for Cisco Unified Communications Manager". 2. Ensure that the CUCM is in Mixed mode. Following are a set of JTAPI specific parameters. 1. **Secure Connection** check box a. **Check the check box** - Checking this option enables you to have a secure TLS connection to Cisco Unified Communications Manager. A warning message appears indicating you to "Ensure that "Standard CTI Secure Connection" role is associated with this JTAPI user, along with other required roles". Click OK to return to Cisco Prime Collaboration Assurance. b. **Uncheck the check box** - If the check box is not checked, JTAPI cannot make a secure connection. A warning message appears indicating you to "Ensure that "Standard CTI Secure Connection" role associated with this JTAPI user is removed. To continue to Monitor Conferences, ensure that the required roles are configured". Click OK to return to Cisco Prime Collaboration Assurance. For more information, see Setting up Devices for

Field Name	Description
	Cisco Prime Collaboration Assurance. The check box enables you to enter the parameters in (enable or disable) the new Secure JTAPI fields.

Field Name	Description

Field Name	Description
	2. TFTP Server IP Address - Specify the IP address of the TFTP Server. **Note** The value must be one of the nodes on the CUCM cluster. Make sure that the TFTP service is running on that node. **3. TFTP Server Port** - The TFTP Server Port defaults to 69. **Note** Do not change the default value unless the System Administrator recommends. **4. CAPF Server IP Address** - Specify the IP address of the CAPF Server. **Note** 1. For more information on the certificate authority proxy function, see the Chapter on "Certificate Authority Proxy Function" in the "Security Guide for Cisco Unified Communications Manager". 2. Ensure to select **RSA Only** from the **Key Order** drop-down list while creating the CAPF profile on CUCM. 3. You must always provide the CUCM Publisher IP Address. **5. CAPF Server Port** - The CAPF Server Port number defaults to 3804. **Note** Ensure that the value entered matches with the value that is configured in Cisco Unified Communication Manager. **7. Instance ID for Publisher** - This field specifies the application instance identifier configured in CAPF Settings section of Application or End User CAPF profile configuration page in the Cisco Unified Communication Manager cluster. **8. Secure Authentication String** – Enter the Authentication String configured in CAPF Settings section of Application or End User CAPF profile configuration page in the respective Communication Manager Publisher. **Note** The section on Troubleshooting Secure JTAPI Connections lists the details of troubleshooting the possible errors and recommended actions "with setup of

Field Name	Description
	CUCM for Secure JTAPI and Sessions not coming up on Conference Diagnostics" respectively.

For Cisco Prime Collaboration Release 11.5 and later

The following devices are renamed in Credential Profiles Page:

- CISCO INTERACTION MANAGER is renamed as WEB/EMAIL INTERACTION MANAGER
- CUIC is renamed as INTELLIGENCE CENTER
- CTS is renamed as CTS/IX ENDPOINT
- CISCO UNIFIED COMMUNICATIONS MANAGER is renamed as COMMUNICATIONS MANAGER
- C_SERIES CODEC is renamed as TC/CE ENDPOINT
- E20 is renamed as E20 ENDPOINT
- ISDN is renamed as ISDN GATEWAY
- MCU is renamed as MULTIPOINT CONTROLLER
- MXP is renamed as MXP ENDPOINT
- ROUTER is renamed as ROUTER/VOICEGATEWAY
- TPS is renamed as TELEPRESENCE SERVER
- TELEPRESENCE CONDUCTOR is renamed as TELEPRESENCE CONDUCTOR

Note You do not need to add credentials for Cisco Device, Cisco Unified Communications Manager Express (Cisco Unified CME), and UC500 Series devices in Credential Profiles page.

SSL Certificate Authentication for Device Discovery

For Cisco Prime Collaboration Release 11.1 and earlier

In Cisco Prime Collaboration Assurance, when a device is added, the SSL certificates are exchanged for credential validation by accessing a protected resource using HTTPS. During exchange, the SSL certificate is not stored in Cisco Prime Collaboration Assurance trust-store and communication with the device fails, at a later point of time. It is recommended that you manually import the SSL certificate to Cisco Prime Collaboration Assurance trust-store to access the device.

Cisco Prime Collaboration Assurance enables you to check the authenticity of the SSL certificate during its communication with the devices or applications over HTTPS. However, this is not mandatory as you can still continue to discover the devices without authenticating the certificate.

Cisco Prime Collaboration Assurance does not validate the certificates from the devices or applications it communicates by default.

To enable the SSL certificate authentication:

Step 1 Choose **System Administration** > **Certificate Management**.
The **Certificate Management** page is displayed.

Step 2 In the **Device Certificate Management** tab, check the **Enable SSL certificate authentication for device discovery** check box.

Step 3 Click the **Import Certificates** button.

Step 4 Restart the Cisco Prime Collaboration Assurance server for the changes in trust manager to take effect.

```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```

Modify Device Credentials

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

If the credentials are incorrect, a major event — Device is inaccessible is triggered from Cisco Prime Collaboration Assurance (**Monitor** > **Alarms & Events** > **Events**).

To edit a credential profile:

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

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**

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

Step 3 Update the credentials as described in the Table on Credential Profiles Field Descriptions, on page 3.

Step 4 Click **Rediscover**.

Cisco Prime Collaboration Assurance 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 Assurance uses the updated credentials in the next polling job.

Verify Device Credentials

For Cisco Prime Collaboration Release 11.5 and later

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** > **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 device credentials:

Step 1 **For Cisco Prime Collaboration Release 11.5 and later**

Choose **Inventory** > **Inventory Management**.

The **Inventory Management** 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 Assurance 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		
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.

Error Message	Conditions	Possible Solutions
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.
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.

Error Message	Conditions	Possible Solutions
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.
For Cisco Prime Collaboration Release 11.1 and earlier MSI		
Failed to access MSI.	Incorrect MSI credentials entered in the credential profile.	Verify and reenter the device MSI 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 Assurance application.

To delete a credential profile:

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

For Cisco Prime Collaboration Release 11.5 and later

Choose **Inventory** > **Inventory Management**

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

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