Deploy Serviceability Service

Serviceability Connector Deployment Task Flow

Procedure

	Command or Action	Purpose
Step 1	(Recommended) If you deploy the Serviceability Connector on ECP, Register the ECP Connector Host to Cisco Webex, on page 3.	After you complete the registration steps, the connector software automatically deploys on your on-premises connector host.
Step 2	(Alternate) If you deploy the Serviceability Connector on Expressway, Register the Expressway Connector Host to Cisco Webex, on page 4.	After you complete the registration steps, the connector software automatically deploys on your on-premises connector host.
Step 3	Configure the Serviceability Connector on ECP, on page 6 or Configure the	Name your Serviceability Connector.

	Command or Action	Purpose
	Serviceability Connector on Expressway, on page 6, as appropriate.	
Step 4	Create Accounts on Managed Devices, on page 8	Configure accounts on each product that the Connector can manage. The connector uses these accounts to authenticate data requests to the managed devices. **Note** If you import all your managed devices and clusters from HCM-F, you don't need to do this task. You must do it if the Connector manages devices that aren't in the HCM-F database.
Step 5	(Optional) Configure an ECP Connector Host with Locally Managed Unified CMs , on page 9 or (Optional) Configure Serviceability Connector with Locally Managed Devices, on page 11	If you import all your managed devices and clusters from HCM-F, you don't need to do this task. You must do it if the Connector manages devices that aren't in the HCM-F database. If your connector host is an Expressway, we strongly recommend that you configure the connector host as a locally managed device for the TAC use case. But, an ECP connector host has no logs that TAC would request through the Serviceability Service.
Step 6	(Optional) Configure an ECP Connector Host with Locally Managed Unified CM Clusters, on page 13 or (Optional) Configure Serviceability Connector with Locally Managed Clusters, on page 14	You can associate locally managed devices of the same type as a managed cluster on the Connector configuration. Clusters enable data collection from multiple devices with one request.
Step 7	(Optional) Import Devices from Hosted Collaboration Mediation Fulfillment, on page 7	We recommend importing from the Connector to automatically maintain a list of customer devices and clusters from HCM-F. You could manually add the devices, but integrating with HCM-F saves you time.
Step 8	Configure Upload Settings, on page 15.	**Note** This task is only needed for the TAC case. Customer eXperience Drive (CXD) is the default and only option.
Step 9	Start the Serviceability Connector, on page 16	Expressway only task
Step 10	Validate the Serviceability Connector Configuration, on page 17	Expressway only task. Use this procedure to test the data collection and transfer to your service request.

Register the ECP Connector Host to Cisco Webex

Hybrid Services use software connectors to securely connect your organization's environment to Webex. Use this procedure to register your ECP connector host.

After you complete the registration steps, the connector software automatically deploys on your on-premises connector host.

Before you begin

- You must be on the enterprise network where you installed the Serviceability Connector node when you run the registration wizard. That network requires access to the Connector and to the `admin.webex.com` cloud. (See Prepare Your Environment for links to the relevant addresses and ports). You're opening browser windows to both sides to establish a more permanent connection between them.
- If your deployment proxies outbound traffic, enter the details of your proxy. See (Optional) Configure ECP Node for Proxy Integration.
- If the registration process times out or fails for some reason, you can restart registration in Control Hub.

Procedure

Step 1 In Control Hub (https://admin.webex.com), select **Customers** > **My Organization**.

Step 2 Choose **Services** > **Hybrid**.

Step 3 Click **View All** on the **Serviceability Service** card.

Note If you haven't deployed a Serviceability Connector before, scroll to the bottom of the page to find the card. Click **Set Up** to launch the wizard.

Step 4 Click **Add Resource**.

Step 5 Select **Enterprise Compute Platform** and click **Next**.

The wizard shows the **Register Serviceability Service on ECP Node** page.

If you haven’t installed and configured the VM, you can download the software from this page. You must install and configure the ECP VM before continuing with this wizard. (See Create a VM for the ECP Connector Host.)

Step 6 Enter a cluster name (arbitrary, and only used by Webex) and the FQDN or IP Address of the ECP node, then click **Next**.

- If you use an FQDN, enter a domain that the DNS can resolve. To be useable, an FQDN must resolve directly to the IP address. We validate the FQDN to rule out any typo or configuration mismatch.
- If you use an IP address, enter the same internal IP address that you configured for the Serviceability Connector from the console.

Step 7 Define an upgrade schedule.

When we release an upgrade to the Serviceability Connector software, your node waits until the defined time before it upgrades. To avoid interrupting TAC’s work on your issues, choose a day and time when TAC is

unlikely to use the connector. When an upgrade is available, you can intervene to **Upgrade Now** or **Postpone** (defers until the next scheduled time).

Step 8 Select a release channel and click **Next**.

Choose the stable release channel unless you're working with the Cisco trials team.

Step 9 Review the node details and click **Go to Node** to register the node to the Cisco Webex cloud.

Your browser tries to open the node in a new tab; add the IP address for the node to your organization's allow list.

Step 10 Review the notice about allowing access to this node.

Step 11 Check the box that allows Webex to access this node, then click **Continue**.

The Registration Complete window appears when the node finishes registering.

Step 12 Go back to the Control Hub window.

Step 13 Click **View All** on the **Serviceability Services** page.

You should see your new cluster in the list of Enterprise Compute Platform Clusters. The **Service Status** is "Not Operational" because the node needs to upgrade itself.

Step 14 Click **Open nodes list**.

You should see the available upgrade for your node.

Step 15 Click **Install now...**.

Step 16 Review the release notes and click **Upgrade Now**.

The upgrade can take a few minutes. The cluster status switches to operational after the upgrade completes.

Register the Expressway Connector Host to Cisco Webex

Hybrid Services use software connectors to securely connect your organization's environment to Webex. Use this procedure to register your connector host Expressway.

After you complete the registration steps, the connector software automatically deploys on your on-premises Expressway connector host.

Before you begin

- Sign out of any other connections to this Expressway.
- If your on-premises environment proxies the outbound traffic, enter the details of the proxy server on **Applications > Hybrid Services > Connector Proxy** before completing this procedure. For a TLS proxy, add the root CA certificate that is signed by the proxy server certificate to the CA trust store on the Expressway. Doing so is necessary for successful registration.
- Webex rejects any attempt at registration from the Expressway web interface. Register your Expressway through Control Hub.
- If the registration process times out or fails for some reason, you can restart registration in Control Hub.

Procedure

Step 1 In Control Hub (https://admin.webex.com), select **Customers** > **My Organization**.

Step 2 Choose **Services** > **Hybrid**.

Step 3 Click **View All** on the **Serviceability Service** card.

Note If you haven't deployed a Serviceability Connector before, scroll to the bottom of the page to find the card. Click **Set Up** to launch the wizard.

Step 4 For new registrations, choose the first radio button and click **Next**.

Step 5 Enter your connector host's IP address or FQDN.

Webex creates a record of that Expressway and establishes trust.

Step 6 Enter a meaningful display name for the connector host and click **Next**.

Step 7 Click the link to open your Expressway web interface.

This link uses the FQDN from Control Hub. Make sure that the PC that you use for the registration can access the Expressway interface using that FQDN.

Step 8 Sign in to the Expressway web interface, which opens the **Connector Management** page.

Step 9 Decide how you want to update the Expressway trust list:

- Check the box if you want Webex to add the required CA certificates to the Expressway trust list.

  When you register, the root certificates for the authorities that signed the Webex certificates are installed automatically on the Expressway. This method means that the Expressway should automatically trust the certificates and can set up the secure connection.

  Note If you change your mind, you can use the **Connector Management** window to remove the Webex CA root certificates and manually install root certificates.

- Uncheck the box if you want to update the Expressway trust list manually. See the Expressway online help for the procedure.

Step 10 Click **Register**.

Control Hub launches. Read the on-screen text to verify that Webex identified the correct Expressway.

Step 11 Click **Allow** to register the Expressway for Hybrid Services.

- After the Expressway registers successfully, the Hybrid Services window on the Expressway shows the connectors downloading and installing. If there's a newer version available, the management connector automatically upgrades. It then installs any other connectors that you selected for this Expressway connector host.
- The connectors install their interface pages on the Expressway connector host. Use these new pages to configure and activate the connectors. The new pages are in the **Applications > Hybrid Services** menu on your Expressway connector host.

Troubleshooting Tips

If registration fails and your on-premises environment proxies the outbound traffic, review the prerequisites of this procedure.

Configure the Serviceability Connector on ECP

Before you begin

You must register the ECP node to Cisco Webex before you can configure the Serviceability Connector.

Note When you first sign in to a new ECP node, use the default credentials. The username is "admin" and the password is "cisco". Change the credentials after signing on for the first time.

Procedure

Step 1 Sign in to the connector host and go to **Config Settings**.

Step 2 Enter a name for this connector.

Choose a meaningful name for the connector that helps you discuss it.

Step 3 Click **Save**.

Configure the Serviceability Connector on Expressway

Before you begin

You must register the Expressway to Cisco Webex before you can configure the Serviceability Connector.

Procedure

Step 1 Sign in to the Expressway connector host and go to **Applications** > **Hybrid Services** > **Connector Management**.

Step 2 Check that Serviceability Connector is listed, it should not be running. Do not start it yet.

Step 3 Go to **Applications** > **Hybrid Services** > **Serviceability** > **Serviceability Configuration**.

Step 4 Enter a name for this connector.

Choose a name that is meaningful to you and represents the Expressway's purpose.

Step 5 Click **Save**.

(Optional) Import Devices from Hosted Collaboration Mediation Fulfillment

If you use the Serviceability Service with Cisco Hosted Collaboration Solution (HCS), we recommend importing the devices from HCM-F. Then, you can avoid manually adding all those customers, clusters, and devices from the HCM-F inventory.

If your deployment isn't an HCS environment, you can ignore this task.

Note Integrate each Serviceability Connector with one HCM-F inventory. If you have multiple inventories, you need multiple connectors.

Before you begin

Create an administrative account on Hosted Collaboration Mediation Fulfillment (HCM-F) to use with Serviceability Service. You need the address of HCM-F and it must be reachable from the Serviceability host.

Procedure

Step 1 Sign into your connector host and go to **Managed Devices**, as follows:

- On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Managed Devices**.
- On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Serviceability** > **Managed Devices**.

Step 2 Click **New**.

Step 3 Select **Hosted Collaboration Mediation Fulfillment** from the **Type** dropdown.

The interface generates a unique Device Name, based on the selected Type.

Step 4 Edit the **Device Name**.

The default name identifies the device type and gives it a unique number. Modify the name to make it meaningful during conversations about this device.

Step 5 Enter the **Address**, FQDN or IP address, of the HCM-F northbound API interface (NBI).

Step 6 Enter the **Username** and **Password** of the HCM-F administrative account.

Step 7 Choose a **Polling Frequency**, between 1 hour and 24 hours.

This setting governs how often the service checks your inventory for changes to the imported devices. We recommend one day unless you make frequent changes to your inventory.

You can choose *Never* to disable the import from HCM-F. The setting takes effect when you save the page. This setting removes from the serviceability connector the data that was previously imported from HCM-F.

Step 8 Click **Verify** to test that the account can authenticate itself with HCM-F.

Step 9 Click **Add** to save your changes.

The Serviceability connector connects to HCM-F, and populates the **Customers**, **Managed Devices**, and **Managed Clusters** pages with read-only copies of that information.

You can click **Update Now** to force an immediate refresh of the data from HCM-F.

What to do next

Note The **Customers** page is always visible in the connector UI, even in non-HCM-F deployments. The page is empty unless you import data from HCM-F.

Create Accounts on Managed Devices

Configure an account on each device so that Serviceability Connector can authenticate itself to the devices when requesting data.

Procedure

Step 1 **For Cisco Unified Communications Manager, IM and Presence Service, UCCX, and other VOS (Voice Operating System) products**:

a) From Cisco Unified CM Administration on your publisher node, go to **User Managment** > **User Settings** > **Access Control Group**, click **Add New**, enter a name (for example, Serviceability Connector Group), and then click **Save**.

b) From the **Related Links**, click **Assign Role to Access Control Group**, and then click **Go**. Click **Assign Role to Group**, choose the following roles, and then click **Add Selected**:

- **Standard AXL API Access**
- **Standard CCM Admin Users**
- **Standard CCMADMIN Read Only**
- **Standard ServiceAbility**

c) Configure an application user by going to **User Management** > **Application User** and then clicking **Add New**.

d) Enter a username and password for the new account.

e) Click **Add to Access Control Group**, choose your new Access Control Group, click **Add Selected**, and then click **Save**.

Step 2 **For Cisco TelePresence Video Communication Server, or Cisco Expressway Series**:

a) Go to **Users** > **Administrator Accounts**, and then click **New**.

b) In the Configuration section, configure these settings:

- **Name**—Enter a name for the account.

- **Emergency Account**—Set to **No**.
- **Access Level**—Set to **Read-write**.
- Enter a **Password** and re-enter it in **Confirm password**.
- **Web Access**—Set to **Yes**.
- **API Access**—Set to **Yes**.
- **Force password reset**—Set to **No**.
- **State**—Set to **Enabled**.

c) Under Authorize, enter **Your current password** (of the account that you used to access the Expressway interface) to authorize creation of this account.
d) Click **Save**.

Step 3 **For Cisco Unified Border Element**:

a) From the CUBE CLI, configure a user with privilege level 15:

```
username <myuser> privilege 15 secret 0 <mypassword>
```

Step 4 **For Cisco BroadWorks Application Server, Profile Server, Messaging Server, Xtended Services Platform, and Execution Server**:

Use the system administrator account that you created when you installed the server.

(Optional) Configure an ECP Connector Host with Locally Managed Unified CMs

If your connector host is an Expressway, you add each Unified CM publisher and subscriber separately. But, the ECP connector host automates adding the subscribers for each Unified CM publisher.

Note Remember to enable appropriate logging on all devices. The Serviceability Connector only collects logs, it doesn't enable the actual logging.

Before you begin

This task doesn't apply if you:

- Run the connector host on an Expressway.
- Use the HCM-F inventory to add devices to an ECP connector host.

Procedure

Step 1 On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Managed Devices**.

Note After you install the Serviceability Connector, it prompts you to change your password when you first sign in. Change the default password, **cisco**, to a secure value.

Step 2 Click **New**.

Step 3 Select the Unified CM **Type**.

You can only add a Unified CM publisher.

The interface generates a unique Device Name using the selected type.

Step 4 Edit the **Device Name**.

The default name identifies the device type and gives it a unique number. Modify the name to make it meaningful during conversations about this device.

Step 5 Enter the following information for the Unified CM publisher:

Property	Value
Address	The FQDN or IP address of the publisher
Role	(Optional) Roles help you differentiate devices from each other when viewing the list or arranging a cluster.
TLS verify mode	If you leave this mode **On** (default), then the connector requires a valid certificate from this managed device. The certificate must contain the address that you entered earlier as subject alternative name (SAN). The certificate must be valid and trusted by this connector host. If you're using self-signed certificates on the managed devices, copy them to the connector host CA trust store.
Username	For the Unified CM account
Password	For the Unified CM account
Do SSH Credentials differ from those of Application User	If your managed device has a separate account for SSH access, change the value to **Yes**, and then enter the SSH account credentials.

Step 6 Click **Verify** to test that the account can authenticate itself to the managed device.

Step 7 Click **Add**.

Step 8 Repeat this task to add other Unified CM publishers to the Serviceability Connector configuration.

You can now create a managed cluster for the publisher. That cluster automatically populates with the subscribers for the publisher. You can then add any of the subscribers from the cluster.

Important If you previously configured Unified CM subscribers on the connector, the **Managed Devices** page still lists them. But, the **Alarms** displays an alarm for each subscriber. Delete the old subscriber entries and then add the subscribers back through the managed cluster.

What to do next

- (Optional) Configure Serviceability Connector with Locally Managed Devices, on page 11
- (Optional) Configure an ECP Connector Host with Locally Managed Unified CM Clusters, on page 13

(Optional) Configure Serviceability Connector with Locally Managed Devices

To get logs from your managed devices, you first specify the devices in the Serviceability Connector.

If your connector host is an Expressway, we strongly recommend that you configure the connector host as a locally managed device in the TAC use case. Then, TAC can help if your Serviceability Connector isn't working as expected. But, an ECP connector host has no logs that TAC would request through the Serviceability Service.

Note When you add devices, include both the publisher and all subscribers for each Unified CM cluster.

Remember to enable appropriate logging on all devices. The Serviceability Connector only collects logs, it doesn't enable the actual logging.

Before you begin

- Complete Managed Device Prerequisites
- Create Accounts on Managed Devices, on page 8

Procedure

Step 1 Sign into your connector host and go to **Managed Devices**, as follows:

- On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Managed Devices**.
- On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Serviceability** > **Managed Devices**.

Note After you install the Serviceability Connector, it prompts you to change your password when you first sign in. Change the default password, **cisco**, to a secure value.

Step 2 Click **New**.

Step 3 Select the device **Type**.

The interface generates a unique Device Name, based on the selected Type.

Step 4 Edit the **Device Name**.

The default name identifies the device type and gives it a unique number. Modify the name to make it meaningful during conversations about this device.

Step 5 Enter the **Address**, FQDN or IP address, of the managed device.

The remaining fields on the configuration page change depending on the type of device. Skip to the step that is relevant for your device, as follows:

- Cisco Unified Communications Manager (Step 6)
- Cisco Unified CM IM and Presence (Step 6)
- Cisco Unified Contact Center Express (Step 6)
- Cisco Expressway or VCS (Step 7)
- Cisco Unified Border Element (Step 8)
- Cisco BroadWorks server types (Step 9)

Step 6 [VOS devices] Enter the details of the VOS device:

a) (Optional) Select a **Role** for this device.

The roles depend on the **Type**. Roles help you differentiate devices from each other when viewing the list or arranging a cluster. For example, you could select the *Publisher* role for a particular IM and Presence Service node.

b) Change the **TLS verify mode** if necessary.

If you leave this mode **On** (default), then the connector requires a valid certificate from this managed device.

The certificate must contain the address that you entered above as subject alternative name (SAN). The certificate must be valid and trusted by this connector host.

If you're using self-signed certificates on the managed devices, copy them to the connector host CA trust store.

c) Enter the **Username** and **Password** of the application account for this device.

d) If your managed device has a separate account for SSH access, change **Do SSH Credentials differ from those of Application User** to **Yes**, and then enter the SSH account credentials.

e) Go to Step 10.

Step 7 [Expressway/VCS] Enter the details of an Expressway or VCS:

a) (Optional) Select a **Role** for this Expressway, either **C** (Expressway-C) or **E** (Expressway-E).

b) Change the **TLS verify mode** if necessary.

If you leave this mode **On** (default), then the connector requires a valid certificate from this managed device.

The certificate must contain the address that you entered above as subject alternative name (SAN). The certificate must be valid and trusted by this connector host.

c) Enter the **Username** and **Password** of the account for this device.

d) Go to Step 10.

Step 8 [CUBE] Enter the details of a CUBE:

a) (Optional) Select a **Role** for this CUBE, either **Active** or **Standby**.
b) Enter the **Username** and **Password** of the SSH account for the CUBE.
c) Go to Step 10.

Step 9 [BroadWorks] Enter the details of a BroadWorks Server:

a) Enter the **Username** and **Password** of the BWCLI account for the BroadWorks server.
b) Go to Step 10.

Step 10 Click **Verify** to test that the account can authenticate itself to the managed device.

Step 11 Click **Add**.

Step 12 Repeat this task to add other devices to the Serviceability Connector configuration.

What to do next

- (Optional) Configure Serviceability Connector with Locally Managed Clusters, on page 14.
- Configure Upload Settings, on page 15.

(Optional) Configure an ECP Connector Host with Locally Managed Unified CM Clusters

Locally managed *clusters* in the connector configuration are groups of locally managed devices of the same type. When you configure a cluster on the Serviceability Connector, it doesn't create connections between the devices. The clusters only aid in sending a single command to a group of similar devices.

If your connector host is an Expressway, you create a cluster and add each Unified CM publisher and subscriber to it separately. But, the ECP connector host automates adding the subscribers to the cluster for each Unified CM publisher.

Note Remember to enable appropriate logging on all devices. The Serviceability Connector only collects logs, it doesn't enable the actual logging.

Before you begin

This task doesn't apply if you:

- Run the connector host on an Expressway.
- Use the HCM-F inventory to add devices to an ECP connector host.

Procedure

Step 1 On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Managed Clusters**.

Step 2 Create a cluster for each Unified CM publisher:

a) Click **New**.
b) Enter a cluster **Name**.

Use a name that distinguishes this cluster from other clusters. You can change the name later, if necessary.

c) Choose the Unified CM **Product type**, and then click **Add**.
d) Choose the publisher.
e) Click **Save**.

The connector polls the publisher and populates a list of its subscribers in the cluster.

Step 3 Toggle the check box for each subscriber to add or remove it in the **Managed Devices**.

Important For security reasons, the connector can't retrieve the sign-in credentials for the subscribers when it polls the publisher. When it creates the record for each subscriber, it defaults to the username and password for the publisher instead. If your subscribers have different sign-in credentials from your publisher, you must update the subscriber records.

Note Unchecking the subscriber in the cluster automatically removes its record from the **Managed Devices** page.

Step 4 If necessary, change the default username and password for each subscriber on the **Managed Devices** page.

Step 5 Repeat this procedure for each managed cluster that you want to add.

(Optional) Configure Serviceability Connector with Locally Managed Clusters

Locally managed *clusters* in the connector configuration are groups of locally managed devices of the same type. When you configure a cluster on the Serviceability Connector, it doesn't create connections between the devices. The clusters only aid in sending a single command to a group of similar devices.

You don't need to arrange locally managed devices into clusters.

If you're importing clusters from HCM-F, the Clusters page shows read-only information about those clusters.

Before you begin

(Optional) Configure Serviceability Connector with Locally Managed Devices, on page 11

Procedure

Step 1 Sign into your connector host and go to **Managed Clusters**, as follows:

- On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Managed Clusters**.
- On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Serviceability** > **Managed Clusters**.

Step 2 For each cluster of managed devices:

a) Click **New**.
b) Enter a cluster **Name**.

Use a name that distinguishes this cluster from other clusters. You can change the name later, if necessary.

c) Choose a **Product type**, and then click **Add**.
d) Choose the managed devices to include in this cluster.
e) Click **Save**.

The page shows the list of clusters, including your new cluster.

Step 3 Repeat this procedure for each managed cluster that you want to add.

(Optional) Configure local logging and problem report collection

This is how you enable local logging and problem report collection. When these settings are on, the data is kept locally on the service connector host. You can read about managing this data in *Manage local logs* and *Collect problem reports*.

Procedure

Step 1 Sign in to the Serviceability node and click **Config Settings**.

Step 2 (Optional) Set **Keep a copy of collected logs locally** to **Allow** and select the number of files to save.

This allows the node to keep local copies of the logs that were remotely collected through it.

Step 3 (Optional) Change **Enable endpoint prt log collection** to **Allow** and select the number of files to save.

Step 4 (Optional) Change **Restrict prt log collection from configured subnets** to True if you want to restrict the networks this connector can see for collecting problem reports.

You must enter the subnets you want to use. Use commas to separate multiple ranges.

Step 5 Click **Save**.

Configure Upload Settings

To upload files to a case, use "Customer eXperience Drive" (CXD). This setting is the default when you configure **Upload Settings** for the first time.

If you need further assistance, call the Cisco Technical Assistance Center.

Note This task is only for the TAC use case.

In Cloud-Connected UC, the destination is preset. See the Cisco TAC Delivery Services Privacy Data Sheet for information on where this feature processes and stores data.

Procedure

Step 1 Sign into your connector host and go to **Upload Settings**, as follows:

- On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Upload Settings**.
- On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Serviceability** > **Upload Settings**.

Step 2 For the TAC use case, check that the connector's **Upload authentication method** is **Customer eXperience Drive**. This setting is the default selection for new installations.

Step 3 Click **Save**.

Configure remote collections on this Connector

The Service Connector allows remote collections by default. You can check to ensure that TAC has your permission to collect logs from your managed devices:

Procedure

Step 1 Sign into your connector host and go to **Configuration**, as follows:

- On an ECP connector host, go to the web interface of your Serviceability Connector at `https://<FQDN or IP address>:8443/home`. Sign in and click **Configuration**.
- On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Serviceability** > **Configuration**.

Step 2 For the TAC use case, change **Collect data to store with Service Requests** to **Allow**.

This switch is set to **Allow** by default. If you change it to **Deny**, then you no longer receive the benefits of the Serviceability Connector.

Step 3 For the Cloud-Connected UC use case, ensure that **Collect data for CCUC troubleshooting** is **Allow** (the default).

Step 4 Click **Save**.

What to do next

Start the Serviceability Connector, on page 16

Start the Serviceability Connector

If your Connector Host is an Expressway, this task turns on the Serviceability Connector to enable sending log collection requests to your managed devices. You should only need to do this task once, then the Serviceability Connector is active and waiting for a request.

Before you begin

- (Optional) Configure Serviceability Connector with Locally Managed Devices, on page 11
- Configure Upload Settings, on page 15

Procedure

Step 1 On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Connector Management** and click **Serviceability**.

Step 2 Click **Serviceability Connector**.

Step 3 Change the **Active** field to **Enabled**.

Step 4 Click **Save**.

The connector starts and the status changes to **Running** on the Connector Management page.

What to do next

- Validate the Serviceability Connector Configuration, on page 17

Validate the Serviceability Connector Configuration

If your Connector Host is an Expressway, this task validates the configuration of your connector.

Procedure

Step 1 On an Expressway connector host, sign in and go to **Applications** > **Hybrid Services** > **Connector Management** and click **Serviceability**.

Step 2 Check that Serviceability Connector is *Running* with *No alarms*.

Step 3 Check that managed device accounts can connect:

a) Go to the **Managed Devices** page.
b) For each of the devices listed, click **View/Edit**.
c) On the device configuration page, click **Verify** to test the account against the device. You should see a Success banner.