Deployment Guide for Cisco Webex Serviceability Connector

First Published: 2017-11-17
Last Modified: 2020-05-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
   800 553-NETS (6387)
Fax: 408 527-0883
CONTENTS

CHAPTER 1

Serviceability Connector Overview 1

Serviceability Connector Overview 1
Benefits of Using Serviceability Service 1
Differences to Other Hybrid Services 2
Short Description of How it Works 2
Deployment Architecture 3
Limitations 4
People and Roles 5
Data Movement 8
Security 9
Serviceability Connections 12
Serviceability Connector Ports 14

CHAPTER 2

Prepare Your Environment 15

Requirements for Serviceability Connector 15
Complete Managed Device Prerequisites 16
Complete the Expressway Connector Host Prerequisites for Serviceability Connector 17

CHAPTER 3

Deploy Cisco Webex Serviceability Service 21

Serviceability Connector Deployment Task Flow 21
Register the Expressway Connector Host to Cisco Webex 22
Configure the Serviceability Connector 23
Create Accounts on Managed Devices 24
Configure Serviceability Connector with Managed Devices 25
(Optional) Configure Serviceability Connector with Managed Clusters 27
Configure Upload Settings 27
Ensure the Connector Allows Collections  28
Start the Serviceability Connector  28
Validate the Serviceability Connector Configuration  29
Serviceability Connector Overview

This offering increases the speed with which Cisco technical assistance staff can diagnose issues with your infrastructure. It automates the tasks of finding, retrieving and storing diagnostic logs and information into an SR case, and triggering analysis against diagnostic signatures so that TAC can more efficiently identify and resolve issues with your on-premises equipment.

This capability uses Serviceability Connector deployed on your premises. Serviceability Connector is a piece of software that resides on a dedicated Expressway in your network (‘connector host’). It connects to Cisco Webex to receive requests to collect data, and uses the APIs of your on-premises equipment to collect the requested data. The requested data is securely uploaded to Customer eXperience Drive and associated with your SR case.

Benefits of Using Serviceability Service

• Speeds up the collection of logs by allowing TAC engineers to request relevant logs as they perform the diagnosis of the problem – avoiding the delays of requesting additional logs and manual collection and delivery steps. This can take days off your problem resolution time.

• In conjunction with TAC’s Collaboration Solution Analyser and its database of diagnostic signatures, the logs are automatically analysed, known issues identified and known fixes or workarounds recommended.
Differences to Other Hybrid Services

You deploy and manage Serviceability Connectors through Control Hub in a similar way to other Expressway-based Hybrid Services such as Hybrid Calendar Service and Hybrid Call Service, but there are several important differences.

The main difference is that Serviceability Service does not have features for users. The TAC is the predominant user of this service, so, while it would benefit organizations that are using Hybrid Services, it is more commonly used for organizations that don’t use other Hybrid Services.

If you already have your organization configured in Control Hub, you can enable the service through your existing organization administrator login.

The Serviceability Connector has a different load profile to those other connectors that provide features directly to users. It is always available, so that TAC can collect data when necessary, but it does not have a steady load over time. The TAC representatives manually initiate data collection, and they negotiate an appropriate time to do it, so as to minimize the impact on other services provided by the same infrastructure.

Short Description of How it Works

1. Your administrators work with Cisco TAC to deploy Serviceability service - see Deployment Architecture, on page 3.
2. TAC learns of a problem with one of your Cisco devices (when you open a case).
3. TAC representative uses the Collaborations Solution Analyzer (CSA) web interface to request Serviceability Connector to collect data from relevant devices.
4. Your Serviceability Connector translates the request into API commands that the device(s) understand in order to collect the requested data from the managed devices.
5. Your Serviceability Connector collects, encrypts, and uploads that data over an encrypted link to Customer eXperience Drive (CXD), and associates the data with your Service Request.
6. The data can be analyzed against the TAC database of more than 1000 diagnostic signatures.
7. The TAC representative reviews the results, checking the original logs if necessary.
**Deployment Architecture**

*Description of the components*

(from left top to bottom right)

**Managed devices** - includes any devices you want to be able to query for logs using Serviceability Service. You can configure up to 150 managed devices with one Serviceability connector.

The service currently works with the following devices:

- Cisco Unified Communications Manager
- Cisco Unified CM IM and Presence Service
- Cisco Expressway Series
- Cisco TelePresence Video Communication Server (VCS)
- Cisco Unified Contact Center Express (UCCX)
- Cisco Unified Border Element (CUBE)
- Cisco BroadWorks Application Server (AS)
- Cisco BroadWorks Profile Server (PS)
- Cisco BroadWorks Messaging Server (UMS)
- Cisco BroadWorks Execution Server (XS)
Your administrator - Uses Cisco Webex Control Hub to register a connector host and enable Serviceability Service. The URL is https://admin.webex.com and you need your “organization administrator” credentials.

Expressway connector host - An Expressway that hosts the Management connector and the Serviceability Connector.

• Management Connector (on Expressway) and the corresponding Management Service (in Cisco Webex) are the components that manage your Expressway’s registration, persisting the connection, updating connectors when required, and reporting status and alarms.

• Serviceability Connector - a small piece of software that the connector host Expressway downloads from Cisco Webex after your organization is enabled for Serviceability service.

Proxy - optional. If you change the proxy configuration after starting Serviceability Connector, then you must restart the Serviceability Connector.

Cisco Webex cloud - is where Webex Teams, Webex Calling, Webex Meetings, and Webex Hybrid Services are hosted.

Technical Assistance Center, which contains:

• TAC representative using CSA to communicate with your Serviceability Connector(s) via Cisco Webex cloud.

• TAC case management system with your case and associated logs collected by Serviceability Connector and uploaded to Customer eXperience Drive.

Limitations

Limitations are added and removed as we continue to develop the Serviceability Service. You can read the current list in Known Issues with Serviceability Service.
People and Roles

Figure 1: Accounts required for Serviceability Service

The diagram shows all the accounts required to deliver Serviceability Service. Many of these accounts are not for users; there are several devices that the Serviceability Connector needs permission to access so that it can retrieve data from your devices before associating it with your TAC case.
The following tables lists people and accounts, and their roles in deploying and using the service:

### Table 1: People and Roles

<table>
<thead>
<tr>
<th>Person / Device</th>
<th>Roles in delivering Serviceability Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your network administrator</td>
<td>• (Once) Configure HTTP proxy if required</td>
</tr>
<tr>
<td></td>
<td>• (Once) Open required firewall ports to allow HTTPS access from the connector host Expressway to Customer eXperience Drive.</td>
</tr>
<tr>
<td>Cisco Technical Assistance Centre representative/s</td>
<td>• (Ongoing) Initiate requests, when necessary, for data from the managed devices</td>
</tr>
<tr>
<td></td>
<td>• (Ongoing) Onward analysis of log data, when necessary, towards case resolution (outside scope of this document)</td>
</tr>
<tr>
<td>Your administrator of managed devices, eg Unified CM, IM &amp; P, BW Application Server</td>
<td>Create accounts on all devices to be monitored, so that the Serviceability Connector can securely connect to them and retrieve data.</td>
</tr>
<tr>
<td>Your Expressway administrator</td>
<td>• (Once) Prepare Expressway for Hybrid Services</td>
</tr>
<tr>
<td></td>
<td>• (Periodically) Configure Serviceability Connector with managed device addresses and credentials (login to Expressway)</td>
</tr>
<tr>
<td></td>
<td>• (Once) Start the connector and authorize it to collect data</td>
</tr>
<tr>
<td>“Organization administrator”</td>
<td>• (Once) Create your organization and account in Cisco Webex (if not done already)</td>
</tr>
<tr>
<td>This could be your Expressway Connector Host administrator or network admin, or a Cisco partner; either way, a person uses this account to log in to Control Hub and manage your organization’s cloud configuration.</td>
<td>• (Once) Register your Expressway to Cisco Collaboration Cloud</td>
</tr>
<tr>
<td></td>
<td>• (Once) Onboard the Serviceability connector to the Expressway host</td>
</tr>
<tr>
<td>Serviceability Connector</td>
<td>• Access managed devices using pre-configured API or SSH accounts</td>
</tr>
<tr>
<td></td>
<td>• Access CXD to save diagnostic data to the associated service request (no credentials required on Expressway)</td>
</tr>
</tbody>
</table>
### Table 2: Accounts and Scope Required for Each

<table>
<thead>
<tr>
<th>Account type</th>
<th>Scope / specific privileges</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deprecated:</strong> Cisco Account</td>
<td>The Serviceability Connector does not need explicit upload credentials. This method of authenticating uploads is deprecated and must not be used.</td>
<td>The Serviceability Connector integrates with the Customer eXperience Drive (CXD). The Customer eXperience Drive (CXD) is a multi-protocol file upload service. It allows the Serviceability Connector to upload data directly to the active Service Request using a unique set of credentials created for that Service Request. After choosing CXD on the the Upload Settings page, it does not require any additional configuration.</td>
</tr>
<tr>
<td>Cisco Expressway (Connector Host) Administrator</td>
<td>Access level = Read-write API access = Yes Web access = Yes</td>
<td>This account is on the Connector Host, used to read configuration about the Serviceability Connector itself.</td>
</tr>
<tr>
<td>Managed device API and/or SSH accounts (all of the following rows)</td>
<td>Send API calls to, or perform SSH commands on, the managed device. For example to collect logs.</td>
<td>These accounts reside on the managed devices, and their credentials are entered in the Serviceability Connector configuration on Expressway Connector Host.</td>
</tr>
<tr>
<td>Application User for Voice Operating System (VOS) Products</td>
<td>• Standard AXL API Access • Standard CCM Admin Users • Standard CCMADMIN Read Only • Standard Serviceability</td>
<td>VOS products include Unified CM, IM and Presence, and UCCX. If the SSH account is different to the Application User account, you must enter credentials for both accounts in the Serviceability Connector UI.</td>
</tr>
<tr>
<td>SSH user for Voice Operating System (VOS) Products</td>
<td></td>
<td>If the Application User account is different to the SSH account, you must enter credentials for both accounts in the Serviceability Connector UI.</td>
</tr>
<tr>
<td>Cisco Expressway or VCS Administrator</td>
<td>Access level = Read-write API access = Yes Web access = Yes</td>
<td>This account is on the managed VCS or Expressway, unrelated to the connector host.</td>
</tr>
<tr>
<td>CUBE SSH user account</td>
<td>Privilege Level 15</td>
<td></td>
</tr>
</tbody>
</table>
The CLI account must be privileged to run commands on the managed BroadWorks device; that is, Application Server, Profile Server, Execution Server, or Messaging Server.

### Data Movement

<table>
<thead>
<tr>
<th>Account type</th>
<th>Scope / specific privileges</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BroadWorks CLI user account</td>
<td></td>
<td>The CLI account must be privileged to run commands on the managed BroadWorks device; that is, Application Server, Profile Server, Execution Server, or Messaging Server.</td>
</tr>
</tbody>
</table>

#### Table 3: Data Transfer Summary

<table>
<thead>
<tr>
<th>Data Operation</th>
<th>Transport Mechanism</th>
<th>Account Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read data from managed devices</td>
<td>HTTPS</td>
<td>API access or SSH account on the managed device</td>
</tr>
<tr>
<td>Write to case management system</td>
<td>HTTPS</td>
<td>Service Request number and associated unique token</td>
</tr>
</tbody>
</table>

TAC representatives use their own accounts to access Collaboration Solutions Analyzer (CSA), a web application that interacts with Cisco Webex to communicate requests to Serviceability Connector.

In CSA, the TAC person selects a particular Serviceability Connector from those that are in your organization, and then scopes the command with the following:

- The ID of the TAC case where the logs are going to be stored (service request number).
- The target device (known by an alias that Serviceability Connector created when the device was first added as a managed device) or a cluster of devices.
• A data collection command and any parameters required for that command.

CSA determines the type of device from the Serviceability Connector and is aware of the capabilities of each type of managed device. For example, it knows that to collect service logs from Unified CM, start and end date/times may be required from the TAC user.

When the TAC representative executes the command on CSA, Cisco Webex sends the request to the Serviceability Connector, which acts on it to collect the required data.

Note

This request has no directly identifiable data about the managed device. It has a device ID or cluster ID, so it knows which device(s) to get the data from. This device / cluster ID is translated by the Serviceability Connector and cannot by itself identify your infrastructure. Also, the connection between the cloud and the connector uses HTTPS transport.

The Serviceability Connector translates the request it gets as follows:

• It finds the device(s) for the device ID / cluster ID in its list of managed devices / managed clusters and obtains the address(es)

• The request and parameters are re-created as an API or SSH call towards the address(es), using the appropriate API or command for that device

• To authorize the commands, the connector uses the pre-configured device credentials for the target device

The connector temporarily stores the resulting data file/s on the connector host (Expressway).

The connector chunks the temporary file, encrypts the chunks and transmits them over HTTPS to the Customer eXperience Drive.

The TAC case file store reassembles the log data and stores it against your Service Request.

Serviceability Connector writes the following data about the transaction to the command history on the Expressway connector host:

• Unique identifiers for the command issued and the issuer of the command. The ID of the issuer can be traced back to the person who issued the command, but not on the connector host.

• The command and parameters that were issued (not the resulting data).

• The connector-generated alias of the device(s) to which the command was issued (not the address or hostname).

• The status of the requested command (eg. success/failure).

Security

Managed devices:

• You keep the data at rest on your managed devices secure by using the measures available on those devices and your own policies.

• You create and maintain the API or SSH access accounts on those devices. You enter the credentials on the connector host; Cisco personnel and third parties do not need to and cannot access those credentials.
• The accounts may not need to be full administrative accounts but do need to be authorized for typical logging APIs (See People and Roles, on page 5). The Serviceability Service uses the minimum permissions required to retrieve log information.

**Connector host Expressway:**

• Management Connector creates a TLS connection with Cisco Webex when you first register the Connector Host Expressway. To do this, it needs to trust the certificates presented by Cisco Webex. You can opt to manage the Expressway trust list yourself, or allow Expressway to download and install the required root CA list from Cisco.

• The Management Connector maintains a connection to Cisco Webex, for reporting and alarms; the Serviceability Connector uses a similar persistent connection for receiving serviceability requests.

• Only your administrator(s) need to access the Expressway to configure the Serviceability Connector. Cisco personnel do not need to access the Expressway.

**Serviceability Connector (on connector host Expressway):**

• Makes HTTPS or SSH connections to your managed devices, to execute API commands.

• You can configure the Serviceability Connector to request and verify server certificates from the managed devices.

• Makes outbound HTTPS connections to the Cisco TAC case management system storage.

• Does not log any of your personally identifiable information (PII).

---

**Note**

The connector itself does not log any PII. However, the connector does not inspect or clean the data that it transfers from the managed devices.

• Does not permanently store any of your diagnostic data.

• Keeps a record of the transactions that it makes in the connector’s command history (Applications > Hybrid Services > Serviceability > Command History); the records do not directly identify any of your devices.

• Only stores the addresses of devices and the credentials to their API accounts in the Connector configuration store.

• Encrypts data for transfer to the TAC case management system using a dynamically generated 128 bit AES key.

**Proxy:**

• If you use a proxy to go out to the internet, the Serviceability Connector needs credentials to use the proxy. The Expressway supports basic authentication.

• If you deploy a TLS inspecting device, then it must present a certificate that is trusted by the Connector Host Expressway. You may need to add a CA certificate to the Expressway trust list.

**Firewall/s:**

• Open TCP port 443 outbound from the connector host Expressway to a number of Cisco service URLs. See External Connections Made by the Serviceability Connector (https://help.webex.com/article/xbcrt?/ ).
• Open the required ports into protected networks that contain devices you want to manage (see Serviceability Connector Ports, on page 14 which lists ports required by managed devices). For example, you would need to open TCP 443 into your DMZ to collect logs via an Expressway-E's inward facing address.

• Do not open any additional ports inbound to the connector host Expressway.

**Cisco Webex:**

• Does not make unsolicited inbound calls to your on-premises equipment. The TLS connection is persisted by the Management Connector (on connector host Expressway).

• All traffic between your connector host Expressway and Cisco Webex is HTTPS or secure web sockets.

**Technical Assistance Center:**

• Collects and analyzes device data in response to more than 1.8 million service requests a year.

• Has developed comprehensive and secure data storage tools and protocols to safeguard customer device data.

• Employees are bound by Code of Business Conduct to not share customer data unnecessarily.

• Stores diagnostic data in encrypted form in the TAC case management system.

• Only the personnel who are working on the resolution of your case may access that data.

• You can access your own cases and see what data has been collected.
Serviceability Connections

Figure 2: Serviceability Connections
Serviceability Connector Overview

Serviceability Connections

Deployment Guide for Cisco Webex Serviceability Connector
This table lists the ports used between the Serviceability Connector and managed devices. If there are firewalls protecting your managed devices, open the listed ports towards those devices (internal firewalls are not required for successful deployment and are not shown in the preceding diagram).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent HTTPS registration</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TLS</td>
<td>Cisco Webex hosts</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See External Connections made by the Serviceability Connector (<a href="https://help.webex.com/article/xbr37">https://help.webex.com/article/xbr37</a>)</td>
<td></td>
</tr>
<tr>
<td>Log data upload</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TLS</td>
<td>Cisco TAC SR datastore</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>See External Connections made by the Serviceability Connector (<a href="https://help.webex.com/article/xbr37">https://help.webex.com/article/xbr37</a>)</td>
<td></td>
</tr>
<tr>
<td>AXL (Administrative XML Layer) for log collection</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TLS</td>
<td>VOS devices (Unified CM, IM and Presence, UCCX)</td>
<td>8443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH access</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TCP</td>
<td>VOS devices (Unified CM, IM and Presence, UCCX)</td>
<td>22</td>
</tr>
<tr>
<td>SSH access, log collection</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TCP</td>
<td>CUBE</td>
<td>22</td>
</tr>
<tr>
<td>SSH access, log collection</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TCP</td>
<td>BroadWorks Servers (AS, PS, UMS, XS)</td>
<td>22</td>
</tr>
<tr>
<td>Log collection</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TLS</td>
<td>Expressway or VCS</td>
<td>443</td>
</tr>
<tr>
<td>Log collection</td>
<td>Connector host Expressway</td>
<td>30000-35999</td>
<td>TLS</td>
<td>DMZ Expressway-E (or VCS Expressway)</td>
<td>443</td>
</tr>
</tbody>
</table>
## Prepare Your Environment

- Requirements for Serviceability Connector, on page 15
- Complete Managed Device Prerequisites, on page 16
- Complete the Expressway Connector Host Prerequisites for Serviceability Connector, on page 17

### Requirements for Serviceability Connector

**Table 4: Supported Product Integrations**

<table>
<thead>
<tr>
<th>On-Premises Servers</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>10.x and later</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager IM and Presence Service</td>
<td>10.x and later</td>
</tr>
<tr>
<td>Cisco Unified Border Element</td>
<td>15.x and later</td>
</tr>
<tr>
<td>Cisco TelePresence Video Communication Server / Cisco Expressway series</td>
<td>X8.9 and later</td>
</tr>
<tr>
<td>Cisco Unified Contact Center Express (UCCX)</td>
<td>10.x and later</td>
</tr>
<tr>
<td>Cisco BroadWorks Application Server (AS)</td>
<td>Latest release and two major versions before that. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.</td>
</tr>
<tr>
<td>Cisco BroadWorks Profile Server (PS)</td>
<td>Latest release and two major versions before that. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.</td>
</tr>
<tr>
<td>Cisco BroadWorks Messaging Server (UMS)</td>
<td>Latest release and two major versions before that. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.</td>
</tr>
</tbody>
</table>
Cisco BroadWorks Execution Server (XS) | Latest release and two major versions before that. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.

Table 5: Cisco Expressway Connector Host Details

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway Connector Host</td>
<td>We recommend using a virtual Expressway to host the Serviceability Connector. You must specify the virtual machine to have enough resources to support at least the Medium Expressway. Do not use a Small Expressway. See the Cisco Expressway on Virtual Machine Installation Guide at <a href="https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html</a>. You can download the software image from <a href="https://software.cisco.com/download/home/286255326/type/280886992">https://software.cisco.com/download/home/286255326/type/280886992</a> at no charge. We recommend the latest released version of Expressway for connector host purposes. See Expressway Connector Host Support for Cisco Webex Hybrid Services for more information.</td>
</tr>
</tbody>
</table>

Complete Managed Device Prerequisites

The devices listed here are not prerequisites for the Serviceability Service. These configuration steps are only required if you want Serviceability Connector to manage these devices.

Procedure

Step 1  
**Voice Operating System (VOS) products**: These services must be running to enable Serviceability Connector to manage VOS products like Unified CM, IM and Presence Service, and UCCX:

- SOAP - Log Collection APIs
- SOAP - Performance Monitoring APIs
- SOAP - Real-Time Service APIs
- SOAP - Diagnostic Portal Database Service
- Cisco AXL Web Service

These services are enabled by default. If you stopped any of them, restart the services by using Cisco Unified Serviceability.

Step 2  
**CUBE**: These configurations are required to enable Serviceability Connector to manage CUBE:

- Enable Secure Shell (SSH), as covered in this document.
- Enable Secure Copy (SCP), as covered in this document.
• Enable Smart Call Home (call-home reporting contact-email-addr <email addr>); use the Integrated Services Router guide or the Cloud Services Router guide.

(You must enable Smart Call Home if you want to enable Diagnostic Signatures on CUBE.)

SSH is a protocol which provides a secure remote access connection to network devices. SCP provides a secure and authenticated method for copying router configuration or router image files.

Complete the Expressway Connector Host Prerequisites for Serviceability Connector

Use this checklist to prepare an Expressway for hosting connectors, before you register it to the Cisco Webex.

Before you begin

We require that the Expressway is dedicated to hosting the Serviceability Connector.

Note

As an administrator of hybrid services, you retain control over the software running on your on-premises equipment. You are responsible for all necessary security measures to protect your servers from physical and electronic attacks.

Procedure

Step 1

Obtain full organization administrator rights before you register any Expressways, and use these credentials when you access the customer view in Cisco Webex Control Hub (https://admin.webex.com).

Step 2

Follow these requirements for the Expressway-C connector host.

• Install the minimum supported Expressway software version. See the version support statement for more information.
• Install the virtual Expressway OVA file according to the Cisco Expressway Virtual Machine Installation Guide, after which you can access the user interface by browsing to its IP address. You can find the document in the list of Cisco Expressway Install and Upgrade Guides on cisco.com.

Note

• The Expressway install wizard asks you to change the default root and admin passwords. You should use different, strong passwords for these accounts.

• The serial number of a virtual Expressway is based on the virtual machine's MAC address. The serial number is used to validate Expressway licenses and to identify Expressways that are registered to the Cisco Webex cloud. Do not change the MAC address of the Expressway virtual machine when using VMware tools, or you risk losing service.

• You do not require a release key, or an Expressway series key, or any other licence, to use the virtual Expressway-C for Cisco Webex Hybrid Services. You may see an alarm about the release key. You can acknowledge it to remove it from the interface.
You do not need to enable SIP or H.323 services on the Expressway. They are disabled by default on new installs, and you should leave them disabled. You may see an alarm warning you about misconfiguration, because most Expressway applications require SIP and/or H.323, but you can safely acknowledge the alarm to clear it.

**Step 3**
If this is your first time running Expressway, you get a first-time setup wizard to help you configure it for Cisco Webex Hybrid Services. If you previously skipped the wizard, you can run it from the Status > Overview page.

a) Select **Expressway series**.
b) Select **Expressway-C**.
c) Select **Cisco Webex Hybrid Services**.
   This ensures that you will not require a release key.
   Do not select any other services. The Serviceability Connector requires a dedicated Expressway.
d) Click **Continue**.
   The wizard does not show the licensing page, which it would do at this point for other Expressway deployment types. This is because the Expressway does not need any keys or licenses for hosting connectors (the wizard skips to the configuration review page).
e) Review the Expressway configuration (IP, DNS, NTP) and reconfigure if necessary.
   You would have entered these details, and changed the relevant passwords, when you installed the virtual Expressway.
f) Click **Finish**.

**Step 4**
If you have not checked already, check the following configuration of the Expressway-C connector host. You would normally do this during installation, and you also get a chance to confirm when you use Service Setup wizard.

- Basic IP configuration ([System > Network interfaces > IP](#)
- System name ([System > Administration settings](#)
- DNS settings ([System > DNS](#)) especially the **System host name** and the **Domain**, as these form the FQDN that you need to register the Expressway to Cisco Webex.
- NTP settings ([System > Time](#))

**Note** You must synchronize the Expressway with an NTP server. You should use the same NTP server as the virtual machine's host.

- Desired password for admin account ([Users > Administrator accounts](#), click **Admin** user then **Change password** link)
- Desired password for root account, **which should be different to the Admin account password**, (Log on to CLI as root and run the passwd command)

**Note** Expressway-C connector hosts do not support dual NIC deployments.

Your Expressway is now ready to register to Cisco Webex. The remaining steps in this task are about the network conditions and items to be aware of before you attempt to register the Expressway.

**Step 5**
If you have not already done so, open required ports on your firewall.

- All traffic between Expressway and the Cisco Webex cloud is HTTPS or secure web sockets.
- TCP port 443 must be open outbound from the Expressway-C. See [https://help.webex.com/article/WBX000028782/](https://help.webex.com/article/WBX000028782/) for details of the cloud domains that are requested by the Expressway-C.
• The Serviceability Connector also makes the outbound connections listed in https://help.webex.com/article/xbcr37/.

Step 6  Get the details of your HTTP proxy (address, port) if your organization uses one to access the internet. You’ll also need a username and password for the proxy if it requires basic authentication. The Expressway cannot use other methods to authenticate with the proxy.

Note  If your organization uses a TLS proxy, the Expressway-C must trust the TLS proxy. The proxy’s CA root certificate must be in the trust store of the Expressway. You can check if you need to add it at Maintenance > Security > Trusted CA certificate.

Step 7  Review these points about certificate trust. You can choose the type of secure connection when you begin the main setup steps.

• Cisco Webex Hybrid Services requires a secure connection between the connector host Expressway and Cisco Webex.

You can let Cisco Webex manage the root CA certificates for you. However, if you choose to manage them yourself, be aware of certificate authorities and trust chains; you must also be authorized to make changes to the Expressway-C trust list.
Complete the Expressway Connector Host Prerequisites for Serviceability Connector

Prepare Your Environment
CHAPTER 3

Deploy Cisco Webex Serviceability Service

- Serviceability Connector Deployment Task Flow, on page 21
- Register the Expressway Connector Host to Cisco Webex, on page 22
- Configure the Serviceability Connector, on page 23
- Create Accounts on Managed Devices, on page 24
- Configure Serviceability Connector with Managed Devices, on page 25
- (Optional) Configure Serviceability Connector with Managed Clusters, on page 27
- Configure Upload Settings, on page 27
- Ensure the Connector Allows Collections, on page 28
- Start the Serviceability Connector, on page 28
- Validate the Serviceability Connector Configuration, on page 29

Serviceability Connector Deployment Task Flow

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Register the Expressway Connector Host to Cisco Webex, on page 22</td>
<td>After you complete the registration steps, the connector software is automatically deployed on your on-premises Expressway connector host.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create Accounts on Managed Devices, on page 24</td>
<td>Configure accounts on each product that the Serviceability Connector integrates with. Serviceability Connector uses these accounts to authenticate data requests to the managed devices.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Serviceability Connector with Managed Devices, on page 25 on the Expressway which is hosting the connector.</td>
<td>Add the on-premises devices from which Serviceability Connector can collect data.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Configure Serviceability Connector with Managed Clusters, on page 27</td>
<td>If managed devices are of the same type, you can associate them as a managed cluster on the Serviceability Connector configuration. This</td>
</tr>
</tbody>
</table>
Register the Expressway Connector Host to Cisco Webex

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

After you complete the registration steps, the connector software is automatically deployed 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, you must first enter the details of the proxy server on Applications > Hybrid Services > Connector Proxy and then complete this procedure. For a proxy acting as a TLS proxy, you must add the root CA certificate signed by the proxy server certificate to the CA trust store on the Expressway. Doing so is necessary for successful registration.
- CISCO Webex rejects any attempt at registration from the Expressway web interface. You must register your Expressway through Cisco Webex Control Hub.
- If the registration process times out, or fails for another reason (for example, you must fix certificate errors or enter proxy details), you can restart registration in Cisco Webex Control Hub.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Upload Settings, on page 27</td>
<td>We are deprecating the option to use cisco.com credentials to authenticate uploads to Customer Service Central. You must choose Customer eXperience Drive.</td>
</tr>
<tr>
<td>Start the Serviceability Connector, on page 28</td>
<td></td>
</tr>
<tr>
<td>Validate the Serviceability Connector Configuration, on page 29</td>
<td>Use this procedure to test the data collection and transfer to your service request.</td>
</tr>
</tbody>
</table>
A check box on the Expressway's connector management page determines whether you must manually append the required CA certificates to the Expressway-C trust list, or whether you allow Cisco Webex to add those certificates for you.

Choose one of the following options:

- Check the box if you want Cisco Webex to add the required CA certificates to the Expressway trust list. When you register, the root certificates for the authorities that signed the Cisco Webex certificates are installed automatically on the Expressway. This means that the Expressway should automatically trust the certificates and be able to set up the secure connection.

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

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

**Step 6** Click **Register**. You're redirected to Cisco Webex Control Hub. Read the on-screen text to verify that Cisco Webex identified the correct Expressway.

**Step 7** Click **Allow** to register the Expressway for Cisco Webex Hybrid Services.

  - After the Expressway registers successfully, the Cisco Webex Hybrid Services window on the Expressway shows the connectors downloading and installing. The management connector automatically upgrades itself if there is a newer version available, and then installs 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 Before You Begin section of this procedure.

---

**Configure the Serviceability Connector**

**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.

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 Management > 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 the Access Control Group that you created above (for
      example, “Serviceability Connector 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) Enter the Name, and the configure these settings:
      • Emergency Account—Set to No
      • Access Level—Set to Read-write
      • Enter a Password and re-enter it in Confirm password.
      • Web Access and API Access—Set to Yes
      • Force password reset—Set to No.
      • State—Set to Enabled
• Authorize creation of this user, by re-entering **Your current password** (of the account you used to access the Expressway interface).

c) 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, and Execution Server:**

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

---

**Configure Serviceability Connector with Managed Devices**

This is how you make it possible for TAC to use Serviceability Connector to get logs from your managed devices. As a first step, we recommend using this procedure to add your Expressway connector host as a managed device - so that TAC can help if your Serviceability Connector is not working as expected.

**Before you begin**

- Complete Managed Device Prerequisites, on page 16
- Create Accounts on Managed Devices, on page 24

**Procedure**

**Step 1**  
Sign on to the Expressway connector host, and go to **Applications > Hybrid Services > Serviceability > Managed devices**.

**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 in future conversations you may have with TAC 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 you are adding. Skip to the step that is relevant to the type you selected, 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)
Step 6  [VOS devices] Enter the details of the VOS device that you want to manage with Serviceability Connector:

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

The roles depend on the Type, and are intended to 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 you entered above as subject alternative name (SAN); the certificate must be valid, and it must be trusted by this Expressway.

If you are using self-signed certificates on the managed devices, you must copy them to the Expressway CA trust store.

c) Enter the Username and Password of the application account you created on 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 that you want to manage with the Serviceability Connector:

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 you entered above as subject alternative name (SAN); the certificate must be valid, and it must be trusted by the connector host.

c) Enter the Username and Password of the account you created on this device.

d) Go to Step 10.

Step 8  [CUBE] Enter the details of a CUBE that you want to manage with the Serviceability Connector.

a) (Optional) Select a Role for this CUBE, either Active or Standby.

b) Enter the Username and Password of the SSH account you created on the CUBE.

c) Go to Step 10.

Step 9  [BroadWorks] Enter the details of a BroadWorks Server that you want to manage with the Serviceability Connector.

a) Enter the Username and Password of the BWCLI account you created on 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 this Serviceability Connector's configuration.
What to do next

- (Optional) Configure Serviceability Connector with Managed Clusters, on page 27.
- Configure Upload Settings, on page 27.

(Optional) Configure Serviceability Connector with Managed Clusters

'Clusters' in the connector configuration are simply groups of devices of the same type. If you configure a cluster on the Serviceability Connector, there is no implied clustering of the devices themselves. The purpose of these 'clusters' is to enable TAC to send a single command to a group of the same type of device.

There is no need to arrange your managed devices into clusters but, if you do have real clusters of devices, you can group them using this feature to make it easier to collect logs for a whole cluster in one request.

Before you begin

Configure Serviceability Connector with Managed Devices, on page 25

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Sign into the Expressway connector host and go to Applications &gt; Hybrid Services &gt; Serviceability &gt; Managed Clusters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>For each cluster of managed devices:</td>
</tr>
</tbody>
</table>

  a) Click New.  
  b) Enter a cluster Name. Use a name that distinguishes this cluster from other clusters. You can also change the name later if necessary (click Edit cluster on an existing cluster).  
  c) Choose a Product type, and then click Add.  
  d) Choose the managed devices to be included for this cluster.  
  e) Click Save.  

The page shows the list of clusters, including the one you just created.

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

Configure Upload Settings

To upload files to a case, you must use "Customer eXperience Drive" (CXD). This is the default if you are configuring your Upload Settings for the first time.

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

Step 1  Sign in to the Expressway connector host, and go to Applications > Hybrid Services > Serviceability > Upload Settings

Step 2  Check that the connector’s Upload authentication method is Customer eXperience Drive. This is the default selection for new installations.

You must not select cisco.com user credentials or try to enter account credentials. If you were previously using this method, you must change this setting to Customer eXperience Drive.

Step 3  Click Save.

Ensure the Connector Allows Collections

You should not need to do this task because collections are allowed, by default, when you install the Serviceability Connector.

To ensure that TAC has your permission to collect logs from your managed devices:

Procedure

Step 1  Sign in to the Expressway connector host, and go to Applications > Hybrid Services > Serviceability > Configuration.

Step 2  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 will no longer be able to receive the benefit of quicker problem analysis.

Step 3  Click Save.

What to do next

Start the Serviceability Connector, on page 28

Start the Serviceability Connector

This task turns on the Serviceability Connector, which makes it possible for TAC engineers to use CSA to send log collection requests to your managed devices. You should only need to do this once, after which the Serviceability Connector is active and waiting until you need assistance from TAC.

Before you begin

• Configure Serviceability Connector with Managed Devices, on page 25

• Configure Upload Settings, on page 27
Procedure

Step 1  Sign in to the Expressway connector host, and go to Applications > Hybrid Services > Connector Management.
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 29

Validate the Serviceability Connector Configuration

Procedure

Step 1  Check that Serviceability Connector is Running with No alarms (Applications > Hybrid Services > Connector Management).
Step 2  Check that managed device accounts can connect:
  a) Go to Applications > Hybrid Services > Serviceability > Managed Devices.
  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.
Step 3  Check that your Cisco Account can connect:
  a) Go to Applications > Hybrid Services > Serviceability > Upload Settings.
  b) For the listed account, click View/Edit.
  c) On the account configuration page, click Verify to test the account against the Service Request file repository. You should see a Success banner.
Deploy Cisco Webex Serviceability Service

Validate the Serviceability Connector Configuration