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 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](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](#).
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>Deprecated: 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&lt;br&gt;API access = Yes&lt;br&gt;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&lt;br&gt;• Standard CCM Admin Users&lt;br&gt;• Standard CCMADMIN Read Only&lt;br&gt;• 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&lt;br&gt;API access = Yes&lt;br&gt;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>
### 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>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>
<td></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.

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/xbcr37/).
• 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 Ports

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</td>
<td>30000-35999</td>
<td>TLS</td>
<td>Cisco Webex hosts&lt;br&gt;&lt;small&gt;See External Connections made by the Serviceability Connector (<a href="https://help.webex.com/article/xbc37">https://help.webex.com/article/xbc37</a>)&lt;/small&gt;</td>
<td>443</td>
</tr>
<tr>
<td>Log data upload</td>
<td>Connector host</td>
<td>30000-35999</td>
<td>TLS</td>
<td>Cisco TAC SR datastore&lt;br&gt;&lt;small&gt;See External Connections made by the Serviceability Connector (<a href="https://help.webex.com/article/xbc37">https://help.webex.com/article/xbc37</a>)&lt;/small&gt;</td>
<td>443</td>
</tr>
<tr>
<td>AXL (Administrative XML Layer) for log collection</td>
<td>Connector host</td>
<td>30000-35999</td>
<td>TLS</td>
<td>VOS devices (Unified CM, IM and Presence, UCCX)</td>
<td>8443</td>
</tr>
<tr>
<td>SSH access</td>
<td>Connector host</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</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</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</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</td>
<td>30000-35999</td>
<td>TLS</td>
<td>DMZ Expressway-E (or VCS Expressway)</td>
<td>443</td>
</tr>
</tbody>
</table>