Serviceability Connector Overview and Preparation

Serviceability Connector Overview

You can ease the collection of logs with the Webex Serviceability service. The service automates the tasks of finding, retrieving, and storing diagnostic logs and information.

This capability uses the *Serviceability Connector* deployed on your premises. Serviceability Connector runs on a dedicated host in your network ('connector host'). You can install the connector on either of these components:

- Enterprise Compute Platform (ECP)—Recommended

  ECP uses Docker containers to isolate, secure, and manage its services. The host and the Serviceability Connector application install from the cloud. You don’t need to manually upgrade them to stay current and secure.

Important We recommend use of ECP. Our future development will focus on this platform. Some new features won't be available if you install the Serviceability Connector on an Expressway.

- Cisco Expressway

You can use the Servicability Connector for these purposes:

- Automated log and system information retrieval for service requests
- Log collection of your Unified CM clusters in a Cloud-Connected UC deployment

You can use the same Serviceability Connector for both use cases.

Use in Service Request Cases

You can use the Webex Serviceability service to aid Cisco technical assistance staff in diagnosing issues with your infrastructure. The service automates the tasks of finding, retrieving, and storing diagnostic logs and information into an SR case. The service also triggers analysis against diagnostic signatures so that TAC can identify problems and resolve cases faster.

When you open a case with TAC, TAC engineers can retrieve relevant logs as they perform the diagnosis of the problem. We can collect the needed logs without coming back to you each time. The engineer sends requests to the Serviceability Connector. The connector collects the information and securely transfers it to the Customer eXperience Drive (CXD). The sytem then appends the information to your SR.

When we have the information, we can use the Collaboration Solution Analyzer and its database of diagnostic signatures. The system automatically analyses logs, identifies known issues, and recommends known fixes or workarounds.

You deploy and manage Serviceability Connectors through Control Hub like other Hybrid Services, such as Hybrid Calendar Service and Hybrid Call Service. You can use it along with other Hybrid Services, but they aren't required.

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

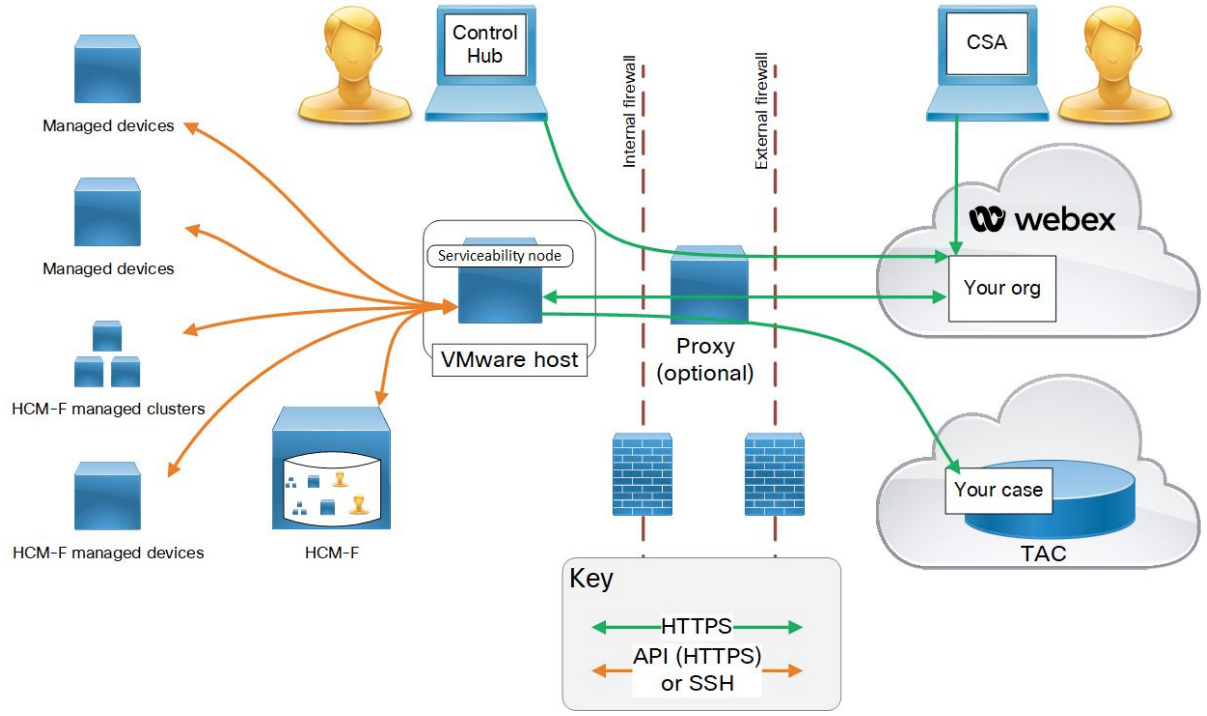
In this deployment, the Serviceability Connector is always available, so that TAC can collect data when necessary. But, it doesn’t have a steady load over time. The TAC engineers manually initiate data collection. They negotiate an appropriate time for the collection to minimize the impact on other services provided by the same infrastructure.

How it works

1. You work with Cisco TAC to deploy the Serviceability service. See Deployment Architecture for TAC Case, on page 3.
2. You open a case to alert TAC to a problem with one of your Cisco devices.
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 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). CXD then associates the data with your Service Request.
6. The system analyes the data 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 for TAC Case

Figure 1: Deployment with Service Connector on Expressway



Element	Description
Managed devices	Includes any devices that you want to supply logs from to Serviceability Service. You can add up to 150 locally managed devices with one Serviceability connector. You can import information from HCM-F (Hosted Collaboration Mediation Fulfillment) about HCS customers' managed devices and clusters (with larger numbers of devices, see https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service). The service currently works with the following devices: • Hosted Collaboration Mediation Fulfillment (HCM-F) • 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) • Cisco Broadworks Xtended Services Platform (XSP)
Your administrator	Uses 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.
Connector host	An Enterprise Compute Platform (ECP) or Expressway that hosts the Management connector and the Serviceability Connector. • **Management Connector** (on ECP or Expressway) and the corresponding Management Service (in Webex) manage your registration. They persist the connection, update connectors when required, and report status and alarms. • **Serviceability Connector**—A small application that the connector host (ECP or Expressway) downloads from Webex after you enable your organization for Serviceability service.
Proxy	(Optional) If you change the proxy configuration after starting Serviceability Connector, then also restart the Serviceability Connector.
Webex cloud	Hosts Webex, Webex calling, Webex meetings, and Webex Hybrid Services.

Element	Description
Technical Assistance Center	Contains: • TAC representative using CSA to communicate with your Serviceability Connectors through Webex cloud. • TAC case management system with your case and associated logs that Serviceability Connector collected and uploaded to Customer eXperience Drive.

Use in Cloud-Connected UC Deployments

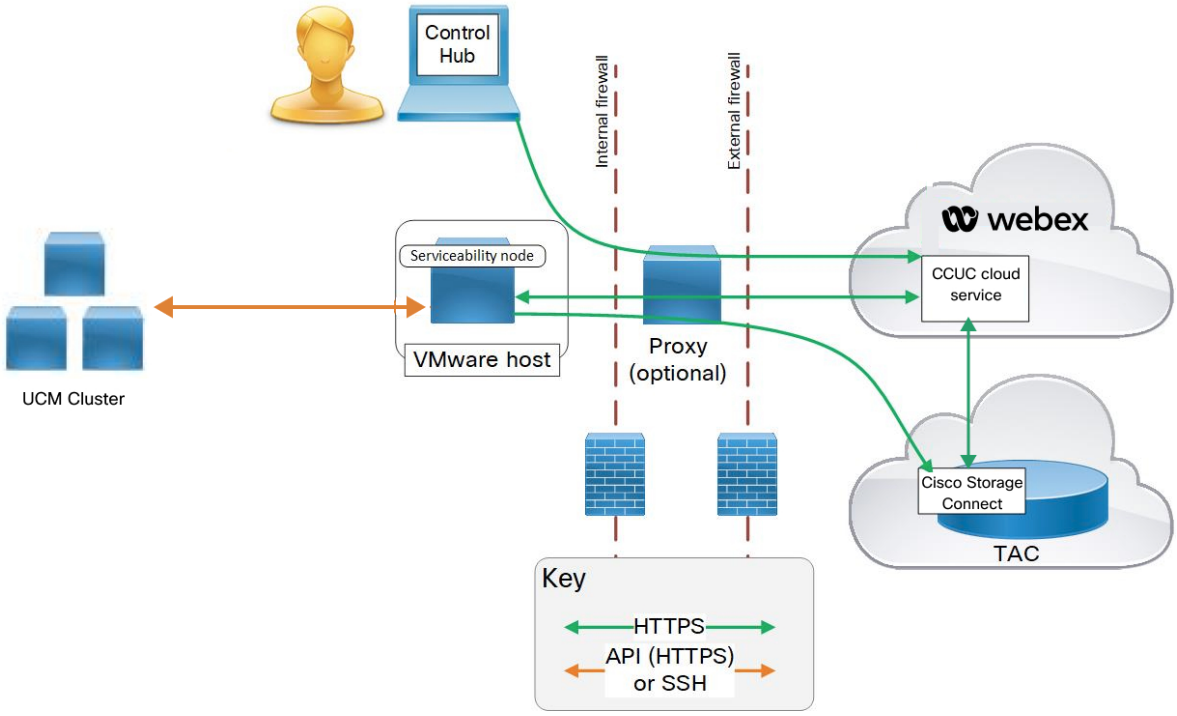
You can use the Serviceability service through Control Hub to monitor your Unified CM clusters in a Cloud-Connected UC deployment.

How it works

1. You deploy a Serviceability Connector instance for your Unified CM clusters.
2. To troubleshoot a Unified CM call signalling issue, you trigger a data collection request in Control Hub.
3. Your Serviceability Connector translates the request into API commands to collect the requested data from the managed devices.
4. Your Serviceability Connector collects, encrypts, and uploads that data over an encrypted link to Customer eXperience Drive (CXD).

Deployment Architecture for Cloud-Connected UC

Figure 2: Deployment with Service Connector



Element	Description
Managed devices	Includes any devices from which you want to supply logs to Serviceability Service. You can add up to 150 locally managed devices with one Serviceability connector. You can import information from HCM-F (Hosted Collaboration Mediation Fulfillment) about HCS customers' managed devices and clusters (with larger numbers of devices, see https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service). With Cloud-Connected UC, the service works with the following devices: • Cisco Unified Communications Manager
Your administrator	Uses 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.

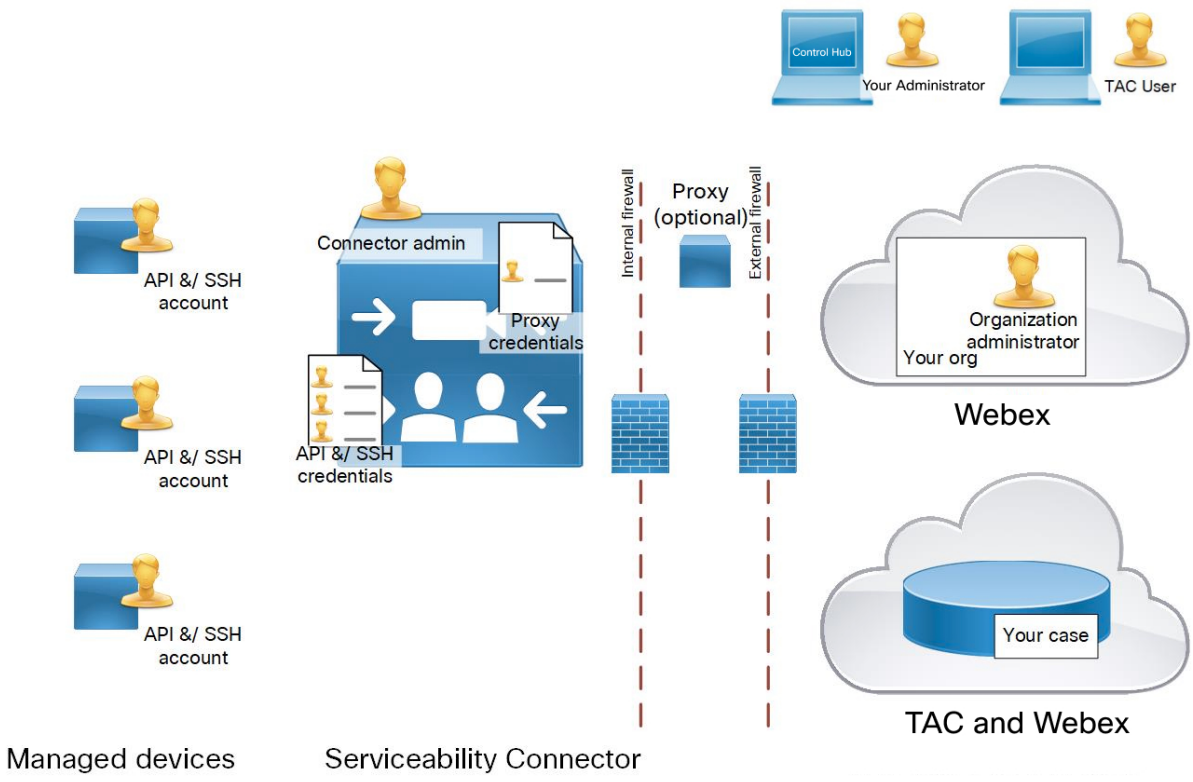
Element	Description
Connector host	An Enterprise Compute Platform (ECP) or Expressway that hosts the Management connector and the Serviceability Connector. • **Management Connector** (on ECP or Expressway) and the corresponding Management Service (in Webex) manage your registration. They persist the connection, update connectors when required, and report status and alarms. • **Serviceability Connector**—A small application that the connector host (ECP or Expressway) downloads from Webex after you enable your organization for Serviceability service.
Proxy	(Optional) If you change the proxy configuration after starting Serviceability Connector, then also restart the Serviceability Connector.
Webex cloud	Hosts Webex, Webex calling, Webex meetings, and Webex Hybrid Services.

Serviceability Connector Limitations

For a current list of limitations, see the Known Issues with Serviceability Service article.

People and Roles

Figure 3: Accounts Required for Serviceability Service



The diagram shows the required accounts to deliver Serviceability Service. Many of these accounts aren't for users. The Serviceability Connector needs permission to retrieve data from several devices.

The following tables lists people and accounts, and their roles in deploying and using the service:

Table 1: People and Roles

Person / Device	Roles in delivering Serviceability Service
Your network administrator	• (Once) Configure HTTP proxy if required • (Once) Open required firewall ports to allow HTTPS access from the connector host (ECP or Expressway) to Customer eXperience Drive.

Person / Device	Roles in delivering Serviceability Service
Cisco Technical Assistance Center representatives	Only for the TAC use case. • (Ongoing) Initiate requests, when necessary, for data from the managed devices • (Ongoing) Analysis of log data, when necessary, towards case resolution (outside scope of this document)
Your administrator of managed devices, such as Unified CM, IM & Presence Service, and BW Application Server	• (Once) Create accounts on all monitored devices, so that the service can securely connect to them and retrieve data.
Your Connector host administrator	• (Once) Prepare ECP or Expressway for Hybrid Services • (Periodically) Configure Serviceability Connector with managed device addresses and credentials • (Once) Start the connector and authorize it to collect data.
"Organization administrator" This account could be your Connector host administrator or network admin, or a Cisco partner. That person uses this account to sign in to Control Hub and manage your organization's cloud configuration.	• (Once) Create your organization and account in Cisco Webex (if not done already) • (Once) Register your Connector host to Cisco Collaboration Cloud • (Once) Onboard the Serviceability connector to the Connector host
Serviceability Connector	• Access-managed devices using pre-configured API or SSH accounts • Access CXD to save diagnostic data to the associated service request (no credentials required on Connector host)

Table 2: Accounts and Scope Required for Each

Account type	Scope / specific privileges	Notes
Cisco Connector Host Administrator	Access level = Read-write API access = Yes (Expressway only) Web access = Yes (Expressway only)	This account on the Connector Host reads the Serviceability Connector configuration.

Account type	Scope / specific privileges	Notes
Managed device API and SSH accounts (all of the following rows)	Send API calls to, or perform SSH commands on, the managed device. For example, to collect logs.	These accounts reside on the managed devices. You enter their credentials in the Serviceability Connector configuration on the Connector host.
API account for HCM-F API	Read	This account authenticates the connector when it polls HCM-F for information about customers, their clusters and devices, and credentials to access them.
Application User for Voice Operating System (VOS) Products	• Standard AXL API Access • Standard CCM Admin Users • Standard CCMADMIN Read Only • Standard Serviceability	VOS products include Unified CM, IM and Presence, and UCCX. If the SSH account is different to the Application User account, enter credentials for both accounts in the Serviceability Connector UI.
SSH user for Voice Operating System (VOS) Products		If the Application User account is different to the SSH account, enter credentials for both accounts in the Serviceability Connector UI.
Cisco Expressway or VCS Administrator	Access level = Read-write API access = Yes Web access = Yes	Only for TAC use case. This account for the managed VCS or Expressway, rather than for the connector host.
CUBE SSH user account	Privilege Level 15	Only for TAC use case.
BroadWorks CLI user account		Only for TAC use case. Ensure that the CLI account has privileges to run commands on the managed BroadWorks device; that is, Xtended Services Platform, Application Server, Profile Server, Execution Server, or Messaging Server.

Data Movement

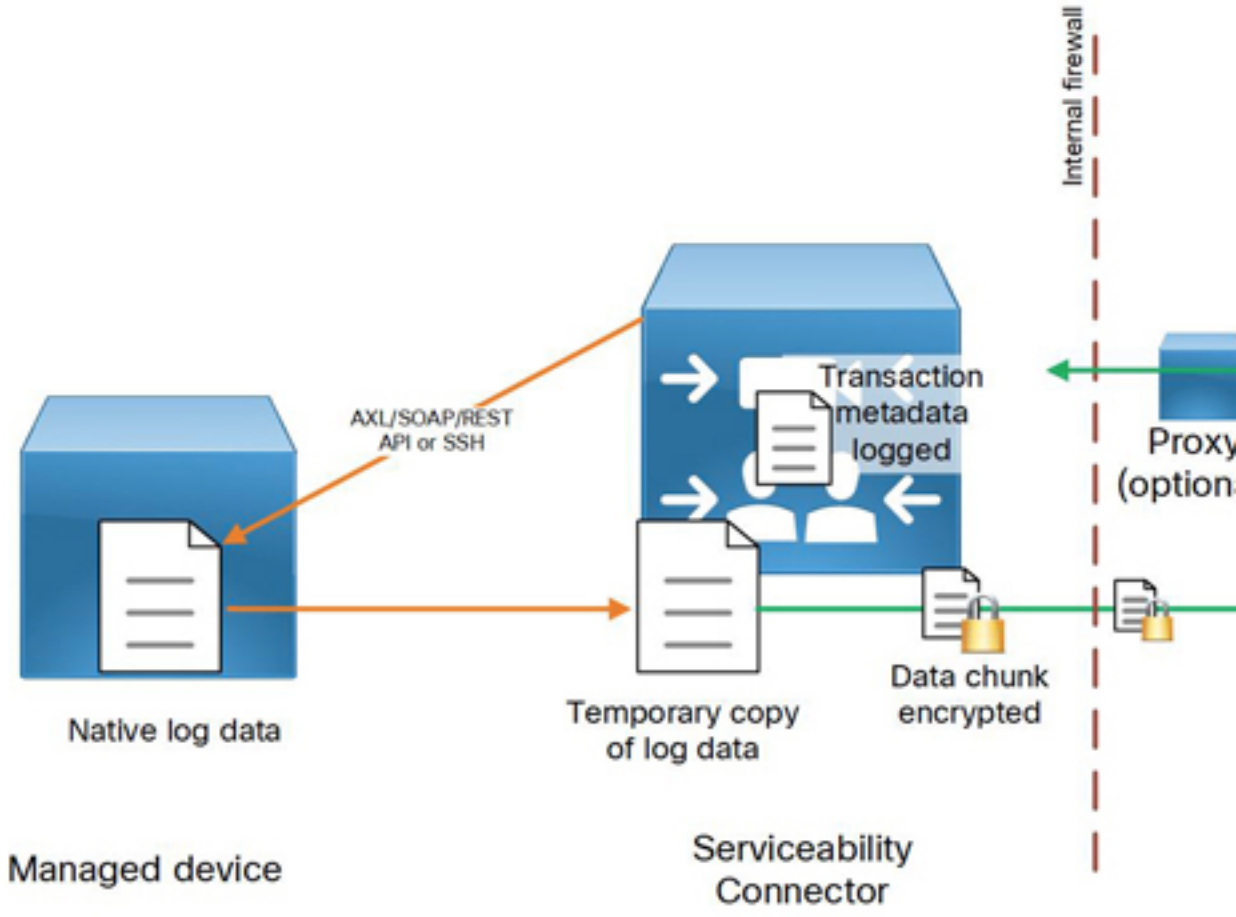


Table 3: Data Transfer Summary

Data Operation	Transport Mechanism	Account Used
Read data from managed devices	HTTPS	API access or SSH account on the managed device
Write to case management system	HTTPS	Service Request number and associated unique token

When a command is entered, 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 from which devices to get the data. The Serviceability Connector translates this device/cluster ID. The ID can't by itself identify your infrastructure. Also, the connection between the cloud and the connector uses HTTPS transport.

The Serviceability Connector translates the request as follows:

- It finds the devices for the device/cluster ID in its list of managed devices and clusters and obtains the addresses.
- It recreates the request and parameters as API or SSH calls to the addresses, using the appropriate API or command for the devices.
- To authorize the commands, the connector uses the pre-configured device credentials for the target devices.

The connector temporarily stores the resulting data files on the connector host (Expressway or ECP).

The connector chunks the temporary file, encrypts the chunks, and transmits them over HTTPS to the Customer eXperience Drive. If the request came from TAC, 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 Connector host:

- Unique identifiers for the command issued and the issuer of the command. You can trace the ID of the issuer back to the person who issued the command, but not on the connector host.
- The issued command and parameters (not the resulting data).
- The connector-generated alias of the devices to which the command was issued (not the address or hostname).
- The status of the requested command (success/failure).

TAC case

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 in which to store the logs(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 necessary parameters.

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, the TAC user should provide start and end date/times.

Cloud-Connected UC case

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

- 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 necessary parameters.

  LogAdvisor prompts for the appropriate parameters.

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 don't need to and can't access those credentials.
- The accounts might not need full administrative privileges, but do need authorization for typical logging APIs (See People and Roles, on page 8). The Serviceability Service uses the minimum permissions required to retrieve log information.

Connector host:

- Management Connector creates a TLS connection with Webex when you first register the Connector host (ECP or Expressway). To do this, the Management Connector needs to trust the certificates that Webex presents. You can opt to manage the host trust list yourself, or allow the host to download and install the required root CA list from Cisco.
- The Management Connector maintains a connection to Webex, for reporting and alarms. The Serviceability Connector uses a similar persistent connection for receiving serviceability requests.
- Only your administrators need to access the host to configure the Serviceability Connector. Cisco personnel don't need to access the host.

Serviceability Connector (on connector host):

- 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.
- Doesn't log any of your personally identifiable information (PII).

Note The connector itself doesn't log any PII. However, the connector doesn't inspect or clean the data that it transfers from the managed devices.

- Doesn't 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 don't 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 Customer eXprerience Drive 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 Connector host supports basic authentication.
- If you deploy a TLS inspecting device, then it must present a certificate that the Connector host trusts. You may need to add a CA certificate to the host trust list.

Firewalls:

- Open TCP port 443 outbound from the connector host 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 the managed devices. See Serviceability Connector Ports, on page 16 which lists ports required by the managed devices. For example, open TCP 443 into your DMZ to collect logs through an Expressway-E's inward facing address.
- Don't open any additional ports inbound to the connector host.

Webex:

- Doesn't make unsolicited inbound calls to your on-premises equipment. The Management Connector on the connector host persists the TLS connection.
- All traffic between your connector host and Webex is HTTPS or secure web sockets.

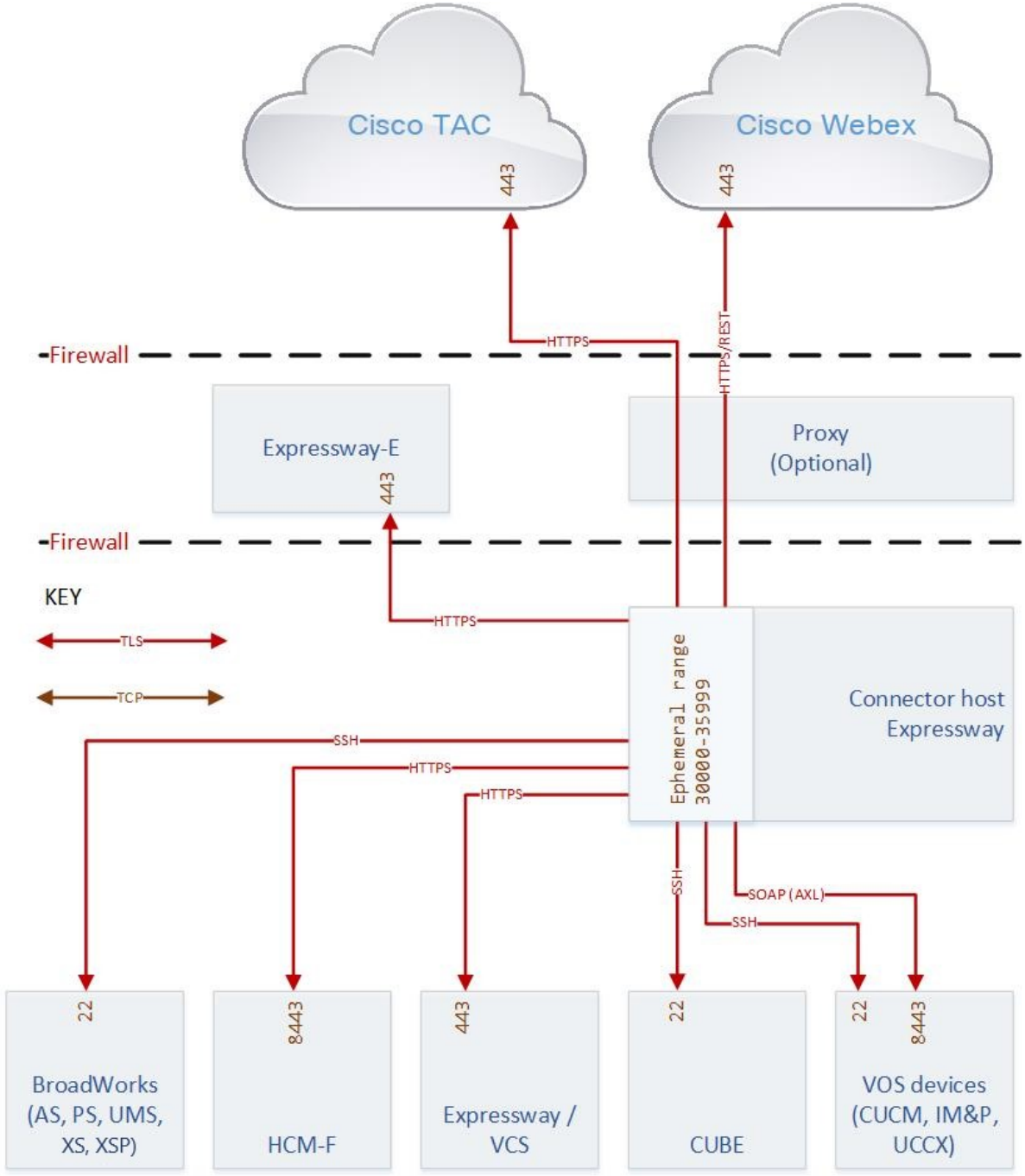
Technical Assistance Center:

When you enable the Serviceability Service for the TAC use case:

- Has developed comprehensive and secure data storage tools and protocols to safeguard customer device data.
- Employees are bound by Code of Business Conduct not to 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 was collected.

Serviceability Connections

Figure 4: Serviceability Connections



Serviceability Connector Ports

Note This table includes the ports that are 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 aren't required for successful deployment and aren't shown in the preceding diagram.

Purpose	Src. IP	Src. Ports	Protocol	Dst. IP	Dst. Ports
Persistent HTTPS registration	VMware host	30000-35999	TLS	Webex hosts See *External Connections made by the Serviceability Connector* (https://help.webex.com/article/xbcr37)	443
Log data upload	VMware host	30000-35999	TLS	Cisco TAC SR datastore See *External Connections made by the Serviceability Connector* (https://help.webex.com/article/xbcr37)	443
API requests to HCM-F	VMware host	30000-35999	TLS	HCM-F Northbound interface (NBI)	8443
AXL (Administrative XML Layer) for log collection	VMware host	30000-35999	TLS	VOS devices (Unified CM, IM and Presence, UCCX)	8443
SSH access	VMware host	30000-35999	TCP	VOS devices (Unified CM, IM and Presence, UCCX)	22
SSH access, log collection	VMware host	30000-35999	TCP	CUBE	22
SSH access, log collection	VMware host	30000-35999	TCP	BroadWorks Servers (AS, PS, UMS, XS, XSP)	22
Log collection	VMware host	30000-35999	TLS	ECP or Expressway or VCS	443
Log collection	VMware host	30000-35999	TLS	DMZ Expressway-E (or VCS Expressway)	443