Prepare Your Environment

Requirements for Serviceability Connector

Table 1: Supported Product Integrations

On-Premises Servers	Version
Cisco Hosted Collaboration Media Fulfillment (HCM-F)	HCM-F 10.6(3) and later
Cisco Unified Communications Manager	10.x and later
Cisco Unified Communications Manager IM and Presence Service	10.x and later
Cisco Unified Border Element	15.x and later
Cisco TelePresence Video Communication Server or Cisco Expressway Series	X8.9 and later
Cisco Unified Contact Center Express (UCCX)	10.x and later
Cisco BroadWorks Application Server (AS)	Latest release and the two earlier major versions. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.
Cisco BroadWorks Profile Server (PS)	Latest release and the two earlier major versions. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.

On-Premises Servers	Version
Cisco BroadWorks Messaging Server (UMS)	Latest release and the two earlier major versions. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.
Cisco BroadWorks Execution Server (XS)	Latest release and the two earlier major versions. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.
Cisco BroadWorks Xtended Services Platform (XSP)	Latest release and the two earlier major versions. For example, R23 is current at the time of writing, so we support managed devices running R21 and later.

Note Unified CM is the only server that you can monitor in the Cloud-Connected UC case.

Table 2: Connector Host Details

Requirements	Version
Enterprise Compute Platform (ECP)	Use VMware vSphere client 6.0 or later to host the ECP VM. Deploy ECP on a dedicated virtual machine of either specification: • 4 CPU, 8GB RAM, 20GB HDD • 2 CPU, 4GB RAM, 20GB HDD You can download the software image from https://binaries.webex.com/serabecpaws/serab_ecp.ova. If you don't install and configure the VM first, the registration wizard prompts you to do so. **Note** Always download a fresh copy of the OVA to install or reinstall the Serviceability Connector VM. An outdated OVA can lead to problems. **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.

Requirements	Version
Cisco Expressway Connector Host	If you host the Connector on Expressway, use a virtual Expressway. Provide the virtual machine with enough resources to support at least the Medium Expressway. Don't use a Small Expressway. See the *Cisco Expressway on Virtual Machine Installation Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html. You can download the software image from https://software.cisco.com/download/home/286255326/type/280886992 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. **Note** For Cloud-Connect UC, you can deploy the Serviceability Connector on an Expressway. But, you can't monitor the Expressway through the connector.

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 Ensure that these services are running to enable the connector to manage Voice Operating System (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 Make these configurations to enable Serviceability Connector to manage CUBE:

Note You don't need to do this for the Cloud-Connected UC case.

- Enable Secure Shell (SSH) to provide a secure remote access connection for network devices, as covered in Configuring Secure Shell on Routers and Switches Running Cisco IOS.
- Enable Secure Copy (SCP) to provide a secure and authenticated method for copying router configuration or router image files, as covered in Secure Shell Configuration Guide.

- Enable Smart Call Home (**call-home reporting contact-email-addr <email addr>**). You can find instructions in either 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.)

Complete the ECP Connector Host Prerequisites

Complete these tasks before you deploy the Serviceability service:

Before you begin

If you choose to use ECP for the Connector host, we require that you deploy the Serviceability Connector on a dedicated ECP.

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.

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

Procedure

Step 1 Obtain full organization administrator rights to access the customer view in Control Hub (https://admin.webex.com).

Step 2 Create a VM for the new ECP node. See Create a VM for the ECP Connector Host, on page 5.

Step 3 Open the required ports on your firewall. See Serviceability Connections and Serviceability Connector Ports.

The Serviceability Connector on ECP uses port 8443 outbound to the Cisco Webex cloud. See https://help.webex.com/article/WBX000028782/ for details of the cloud domains that ECP requests. The Serviceability Connector also makes the outbound connections listed in https://help.webex.com/article/xbcr37/ .

Step 4 If your deployment uses a proxy to access the internet, get the address and port for the proxy. If the proxy uses basic authentication, you also need those credentials.

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

Step 5 Review these points about certificate trust. You can choose the type of secure connection when you begin the main setup steps.

- Hybrid Services requires a secure connection between the connector host and Webex.

  You can let Webex manage the root CA certificates for you. If you choose to manage them yourself, be aware of certificate authorities and trust chains. You must have authorization to change to the trust list.

Create a VM for the ECP Connector Host

Create a VM for the ECP node.

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

Procedure

Step 1 Download the OVA from https://binaries.webex.com/serabecpaws/serab_ecp.ova to your local computer.

Step 2 Choose **Actions** > **Deploy OVF Template** in the VMware vCenter.

Step 3 On the **Select template** page, choose **Local File**, select your `serab_ecp.ova`, and click **Next**.

Step 4 On the **Select name and location** page, enter a name for your VM, such as, **`Webex-Serviceability-Connector-1`**.

Step 5 Select the datacenter or folder to host the VM and click **Next**.

Step 6 (Optional) You might need to select a resource, such as a host, that the VM can use and click **Next**.
The VM installer runs a validation check and displays the template details.

Step 7 Review the template details and make any necessary changes, then click **Next**.

Step 8 Choose which configuration to use for the VM and click **Next**.

We recommend the larger option with 4 CPU, 8GB RAM, and 20GB HDD. If you have limited resources, you can choose the smaller option.

Step 9 On the **Select storage** page, choose these settings:

VM Property	Value
Select virtual disk format	Thick provision lazy zeroed
VM storage policy	Datastore default

Step 10 On the **Select networks** page, choose the target network for the VM and click **Next**.

Note The connector needs to make outbound connections to Webex. For these connections, the VM requires a static IPv4 address.

Step 11 On the **Customize template** page, edit the network properties for the VM, as follows:

VM Property	Recommendation
Hostname	Enter the FQDN (hostname and domain) or a single word hostname for the node. Don't use capitals in the hostname or FQDN. FQDN is 64 characters maximum.
Domain	Required. Must be valid and resolvable. Don't use capitals.
IP Address	A static IPv4 address. DHCP isn’t supported.
Mask	Use dot-decimal notation, for example, `255.255.255.0`
Gateway	The IP address of the network gateway for this VM.
DNS Servers	Comma-separated list of up to four DNS servers, accessible from this network.
NTP Servers	Comma-separated list of NTP servers, accessible from this network. The Serviceability Connector must be time synchronized.

Step 12 Click **Next**.
The **Ready to Complete** page displays the details of the OVF template.

Step 13 Review the configuration and click **Finish**.
The VM installs and then appears in your list of VMs.

Step 14 Power on your new VM.
The ECP software installs as a guest on the VM host. Expect a delay of a few minutes while the containers start on the node.

What to do next

If your site proxies outbound traffic, integrate the ECP node with the proxy.

Note After you configure the network settings and you can reach the node, you can access it through secure shell (SSH).

(Optional) Configure ECP Node for Proxy Integration

If your deployment proxies outbound traffic, use this procedure to specify the type of proxy to integrate with your ECP node. For a transparent inspecting proxy or an explicit proxy, you can use the node interface to do the following:

- Upload and install the root certificate.
- Check the proxy connection.

- Troubleshoot issues.

Procedure

Step 1 Go to the web interface of your Serviceability Connector at `https://<IP or FQDN>:443/setup` and sign in.

Step 2 Go to **Trust Store & Proxy**, and then choose an option:

- **No Proxy**—The default option before you integrate a proxy. Requires no certificate update.
- **Transparent Non-Inspecting Proxy**—ECP nodes don't use a specific proxy server address and don't require any changes to work with a non-inspecting proxy. This option requires no certificate update.
- **Transparent Inspecting Proxy**—ECP nodes don't use a specific proxy server address. No http(s) configuration changes are necessary on ECP. However, the ECP nodes need a root certificate to trust the proxy. Typically, IT uses inspecting proxies to enforce policies on allowing visits to websites and permitting types of content. This type of proxy decrypts all your traffic (even https).
- **Explicit Proxy**—With explicit proxy, you tell the client (ECP nodes) which proxy server to use. This option supports several authentication types. After you choose this option, enter the following information:

  a. **Proxy IP/FQDN**—Address to reach the proxy machine.

  b. **Proxy Port**—A port number that the proxy uses to listen for proxied traffic.

  c. **Proxy Protocol**—Choose **http** (ECP tunnels its https traffic through the http proxy) or **https** (traffic from the ECP node to the proxy uses the https protocol). Choose an option based on what your proxy server supports.

  d. Choose from among the following authentication types, depending on your proxy environment:

Option	Usage
None	Choose for HTTP or HTTPS explicit proxies where there's no authentication method.
Basic	Available for HTTP or HTTPS explicit proxies Used for an HTTP user agent to provide a username and password when making a request, and uses Base64 encoding.
Digest	Available for HTTPS explicit proxies only Used to confirm the account before sending sensitive information. This type applies a hash function on the user name and password before sending it over the network.

Step 3 For a transparent inspecting or explicit proxy, click **Upload a Root Certificate or End Entity Certificate**. Then, choose the root certificate for the explicit or transparent inspecting proxy.

The client uploads the certificate but doesn't install it yet. The node installs the certificate after its next reboot. Click the arrow by the certificate issuer name to get more details. Click **Delete** if you want to reupload the file.

Step 4 For a transparent inspecting or explicit proxy, click **Check Proxy Connection** to test the network connectivity between the ECP node and the proxy.

If the connection test fails, you see an error message with the reason and how to correct the issue.

Step 5 For an explicit proxy, after the connection test passes, select **Route all port 443/444 https requests from this node through the explicit proxy**. This setting requires 15 seconds to take effect.

Step 6 Click **Install All Certificates Into the Trust Store** (appears whenever the proxy setup adds a root certificate) or **Reboot** (appears if the setup doesn't add a root certificate). Read the prompt and then click **Install** if you're ready.

The node reboots within a few minutes.

Step 7 After the node reboots, sign in again if needed and open the **Overview** page. Review the connectivity checks to ensure that they are all in green status.

The proxy connection check only tests a subdomain of webex.com. If there are connectivity problems, a common issue is that the proxy blocks some of the cloud domains listed in the install instructions.

Complete the Expressway Connector Host Prerequisites

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

Before you begin

If you choose to use Expressway to host the Serviceability Connector, we require that you use a dedicated Expressway for the host.

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.

Note As an administrator of hybrid services, you retain control over the software running on your on-premises equipment. You’re 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 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. You can then access the user interface by browsing to its IP address.

  Note
  - The Expressway install wizard asks you to change the default root and admin passwords. Use different, strong passwords for these accounts.
  - The serial number of a virtual Expressway is based on the MAC address of the VM. We use the serial number to identify Expressways that are registered to the Cisco Webex cloud. **Don't change the MAC address of the Expressway VM when using VMware tools, or you risk losing service.**

- You don't require a release key, or an Expressway series key, or any other license, to use the virtual Expressway-C for Hybrid Services. You may see an alarm about the release key. You can acknowledge it to remove it from the interface.
- Although most Expressway applications require SIP or H.232, you don't need to enable SIP or H.323 services on this Expressway. They are disabled by default on new installs. Leave them disabled. If you see an alarm warning you about misconfiguration, you can safely 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 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**.

   Selecting this service ensures that you don't require a release key.

   Don't select any other services. The Serviceability Connector requires a dedicated Expressway.

d) Click **Continue**.
   The wizard doesn't show the licensing page, as for other Expressway deployment types. This Expressway doesn't 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 haven't checked already, check the following configuration of the Expressway-C connector host. You normally check during installation. You can also confirm the configuration 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 properties form the FQDN that you need to register the Expressway to Cisco Webex.
- NTP settings (**System** > **Time**)

  Note Synchronize the Expressway with an NTP server. Use the same NTP server as the VM'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 don’t 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 haven’t already done so, open required ports on your firewall.

- All traffic between Expressway and the 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/ 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 also need a username and password for the proxy if it requires basic authentication. The Expressway can’t 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.

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

  You can let Webex manage the root CA certificates for you. 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.