Prepare your environment for Hybrid Calling for Webex Devices

Requirements for Hybrid Calling for Webex Devices

Hybrid Calling is a service that you enable for your Webex Control Hub-managed organization, and then you can add this service to Webex cloud-registered devices. Before you configure these devices for the service, ensure that you meet all the prerequisites:

- Review the overview and benefits of Hybrid Calling for Webex Devices. (See Hybrid Calling for Webex Devices)
- Supported devices as covered in Device requirements, on page 2.
- The Unified CM user account that'll represent the Workspace account must have a minimum Enhanced UCL license. (See Cisco Spark Remote Device overview and license requirements, on page 12 for more information.)
- Hybrid Calling for Webex Devices requires a version of Cisco Unified Communications Manager that supports the Cisco Spark Remote Device (Cisco Spark-RD). (See Requirements for Hybrid Calling, on page 3 for more information.) These devices are associated with Unified CM accounts that represent Webex Workspaces.
- A supported Expressway traversal pair release. (See Requirements for Hybrid Calling, on page 3 for more information.)

Device requirements

The following Room, Desk, and Board devices are fully supported on the Webex platform. In shared mode, these devices can get PSTN calling functionality from the Unified CM after they're enabled for Hybrid Calling. PSTN for Personal Mode devices (registered to the cloud and associated with users) is also supported.

See more information about these devices. For licensing requirements for Hybrid Calling, see the Cisco Spark-RD information in this chapter.

- Cisco DX70
- Webex DX80
- Webex Desk Pro
- Webex Board 55
- Webex Board 55S
- Webex Board 70
- Webex Board 70S
- Webex Board 85
- Webex Room 55
- Webex Room 55 Dual
- Webex Room 70
- Webex Room 70G2
- Webex Room Kit
- Webex Room Kit Mini
- Webex Room Kit Plus
- Webex Room Kit Plus Precision 60
- Webex Room Kit Pro
- Webex Room Phone
- TelePresence SX10 Quick Set
- TelePresence SX20 Quick Set
- TelePresence SX80 Codec
- TelePresence MX200 G2
- TelePresence MX300 G2
- TelePresence MX700
- TelePresence MX800
- Webex Share

To activate your Room, Desk, or Board device on Webex, the device must run software version CE8.3.4 or later.

You must use a TRC6 remote control with the SX20. The TRC5 is not supported.

Requirements for Hybrid Calling

Cisco call control solution requirements

To enable Hybrid Calling, you must use one of the supported Unified CM-based Cisco call control solutions, and ensure that you're on the minimum supported version or later.

Table 1: Cisco call control solution requirements

Unified-CM Based Call Control Solution	Version
Cisco Unified Communications Manager	Supported Cisco Spark Remote Device (Cisco Spark-RD) releases are required for Hybrid Calling deployments. **Releases with Cisco Spark Remote Device Support** • 11.5(1)SU3 and later; we recommend the latest SU release. **Releases with Session Management Edition (SME) support** • 12.0(1) and later; we recommend the latest release. **Note** The leaf clusters that are connected to the SME cluster do not have to be on release 12.0(1)
Cisco Business Edition	Check the software load summary documentation for BE6K and BE7K to ensure the solution is running a supported version of Unified CM.
Cisco Hosted Collaboration Solution (check to see if your provider is offering Hybrid Services)	11.5 and later

Cisco Expressway requirements

Table 2: Cisco Expressway requirements

Requirements	Version

Cisco Expressway E and C Traversal Pair (for hybrid call traffic)	X8.11.4 or later is required for Hybrid Calling. See the “Important Information” section in the Expressway Release Notes for more information. This release provides added security and toll fraud mitigation. Hybrid Calling calls are classified the same as Mobile Remote Access (MRA) calls. Hybrid Calling traverses existing Expressway C and E pairs and doesn't consume licenses. • Calls that include *.webex.com in the route path do not count towards the traversal license cost. • Any B2B calls for a Webex device after anchoring on the Cisco Spark-RD and then then routing back out through the Expressways will consume traversal licenses. Hybrid Calling follows existing MRA and B2B preferred architecture planning recommendations. • Determine the total number of concurrent MRA, B2B, and Call Service Connect calls • Deploy the appropriate number of Expressway E/C pairs • There is no dedicated Expressway C or E required for Hybrid Calling traversal.

Webex Device Connector requirements

- The Webex Device Connector is a lightweight piece of software that you can install on these supported operating systems:
  - Microsoft Windows 10
  - MacOS Mojave (10.14) or High Sierra (10.13)
- You sign into the software by using your full administrator or device administrator credentials that you use to manage your organization in Control Hub.
- To configure Hybrid Calling for Webex Devices, the system where the software is installed requires network access to the Unified CM that contains configuration that you want to synchronize to Webex cloud-registered devices in Workspaces.
- 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. Webex Device Connector cannot use other methods to authenticate with the proxy.
  - We tested and verified Squid 3.1.19 on Ubuntu 12.04.5.
  - We have not tested auth-based proxies.

Network requirements

- Port access for HTTPS or secure web sockets outbound from the system with the Webex Device Connector to *.wbx2.com, *.webex.com, *.ciscospark.com, and *.cisco.com: TCP port 443 (secure)
- For AXL queries from the system with the Webex Device Connector to Unified CM, TCP port 8443.
- Open the following ports for media traversal between phones, Expressways in the traversl pair, and the Webex cloud:

Table 3: Media traversal port requirements for Hybrid Calling

Client	Destination	Ports	Protocol	Function
Expressway traversal pair	Any	36000–59999	UDP	SIP media between phones and Expressways. Open these ports on the Expressways themselves.

Other network requirements

We recommend that you implement network requirements that are covered in the following documents:

- Network requirements for Webex services
- How do I allow Webex Meetings traffic on my network?

Important items for Hybrid Services deployments

This section provides added context about key configuration items that relate to Hybrid Services.

These points are crucial if you want to successfully deploy Hybrid Calling for Webex devices. We've highlighted these items in particular for the following reasons:

- We want to explain them, so that you understand their role in a hybrid deployment and feel reassured.
- They are mandatory prerequisites that ensure a secure deployment between our cloud and your on-premises environment.
- They should be treated as pre-day zero activities: they can take a bit longer to complete than typical configuration in a user interface, so allow a timeframe to get these items sorted.
- After these items are addressed in your environment, the rest of your Hybrid Services configuration will go smoothly.

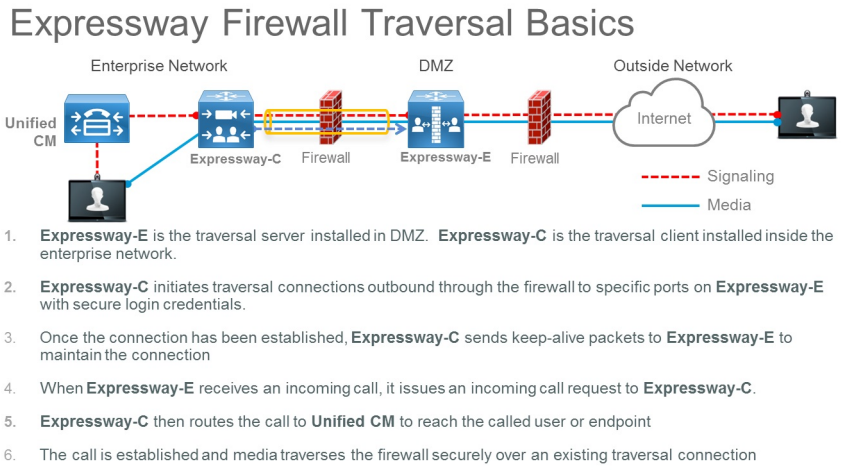
TCP port 5062 on the internet firewall

The Expressway-C and Expressway-E pair deployment allows calls to and from the Internet using firewall traversal technologies. This deployment is what securely takes your on-premises call control and ties it in to Webex.

The Expressway-C and Expressway-E don't require any inbound port to be opened in the demilitarized zone (DMZ) firewall because of the firewall traversal architecture. But TCP SIP signaling ports and UDP media

ports must be opened inbound on the Internet firewall to let incoming calls come through. You must allow time to have the appropriate port opened on your enterprise firewall.

The firewall traversal architecture is shown in the following diagram:



For example, for inbound business-to-business (B2B) calls using SIP protocol, TCP ports 5060 and 5061 (5061 is used for SIP TLS) must be opened on the external firewall, together with UDP media ports used for services such as voice, video, content sharing, dual video, and so on. Which media ports to open depends on the number of concurrent calls and the number of services.

You can configure the SIP listening port on Expressway to be any value between 1024 to 65534. At the same time, this value and the protocol type must be advertised in the public DNS SRV records, and that same value must be opened on the Internet firewall.

Though the standard for SIP TCP is 5060 and for SIP TLS 5061, nothing prevents use of different ports, as the following example shows.

Example

In this example, we assume that port 5062 is used for inbound SIP TLS calls.

The DNS SRV record for a cluster of two Expressway servers looks like this:

_sips._tcp.example.com SRV service location:

priority = 10

weight = 10

port = 5062

svr hostname = us-expe1.example.com

_sips._tcp.example.com SRV service location:

priority = 10

weight = 10

port = 5062

svr hostname = us-expe2.example.com

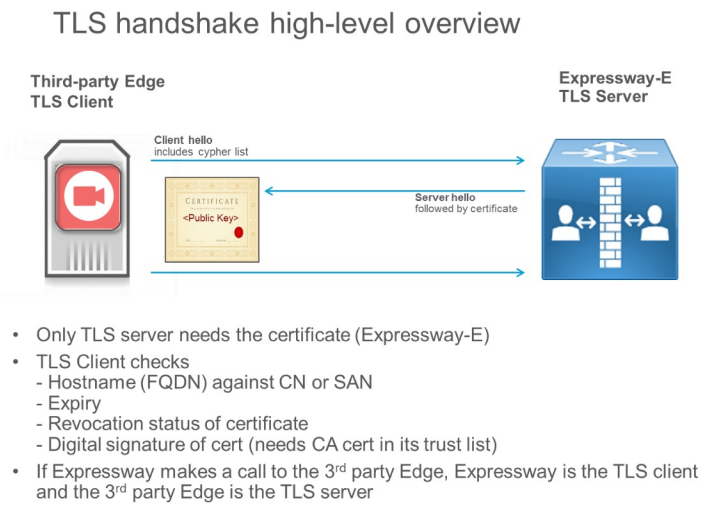
These records mean that calls are directed to **us-expe1.example.com** and **us-expe2.example.com** with equal load sharing (priority and weight) using TLS as the transport type and 5062 as the listening port number.

A device that is external to the network (on the Internet) and that makes a SIP call to a user of the corporate domain (user1@example.com) must query the DNS to understand which transport type to use, the port number, how to load-share the traffic, and which SIP servers to send the call to.

If the DNS entry includes *_sips._tcp*, the entry specifies SIP TLS.

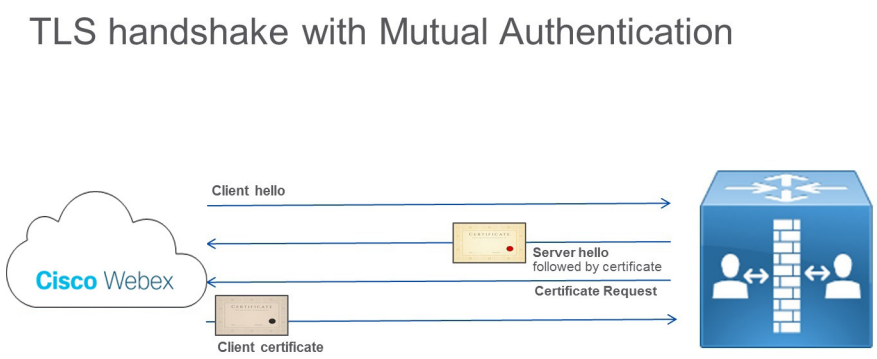
TLS is a client-server protocol and, in the most common implementations, uses certificates for authentication. In a business-to-business call scenario, the TLS client is the calling device, and the TLS server is the called device. With TLS, the client checks the certificate of the server, and if the certificate check fails, it disconnects the call. The client doesn't need a certificate.

TLS handshake is shown in the following diagram:



However, the TLS specification states that the server can also check the client certificate by sending a Certificate Request message to the client during TLS handshake protocol. This message is helpful on a server-to-server connection, such as on call that is established between Expressway-E and the Webex cloud. This concept is called TLS with mutual authentication and is required when integrating with Webex.

Both the calling and called parties check the certificate of the other peer, as the following diagram shows:



Both TLS client and TLS server check the certificate of the other peer

The cloud checks the Expressway identity, and Expressway checks the cloud identity. For example, if the cloud identity in the certificate (CN or SAN) doesn't match what's configured on Expressway, the connection is dropped.

If mutual authentication is turned on, Expressway-E always requests the client certificate. As a result, Mobile and Remote Access (MRA) won't work, because in most cases certificates are not deployed on Jabber clients. In a business-to-business scenario, if the calling entity is not able to provide a certificate, the call is disconnected.

We recommend that you use a value other than 5061 for TLS with mutual authentication, such as port 5062. Webex Hybrid Services use the same SIP TLS record used for B2B. In the case of port 5061, some other services that cannot provide a TLS client certificate won't work.

If an existing record is already used for business-to-business communications, we recommend specifying a subdomain of the corporate domain as the SIP destination in Control Hub, and consequently a public DNS SRV record, as follows:

```
 Service and protocol: _sips._tcp.mtls.example.com
Priority: 1
Weight: 10
Port number: 5062
Target: us-expe1.example.com
```

Business-to-Business, Mobile and Remote Access and Webex traffic on the same Expressway pair

Business-to-business (B2B) and Mobile and Remote Access (MRA) calls use port 5061 for SIP TLS, and Webex traffic uses port 5062 for SIP TLS with mutual authentication.

Why the cloud checks domain ownership

The domain ownership check is part of identity verification. Domain verification is a security measure and identity check that the Webex cloud implements to prove that you are who you say you are.

The identity check is performed in two stages:

1. Domain ownership check. This step involves three types of domains and is a one-time verification check:
    - Email domain
    - Expressway-E DNS domain

- Directory URI domain

2. Expressway-E DNS name ownership check. This step is performed through the implementation of TLS with mutual authentication and involves the use of public certificates on both the cloud and the Expressway. Unlike the domain identity check, this step is performed during any call made to and received from the cloud.

The importance of the domain ownership check

The Webex cloud performs the domain ownership check to enforce security. Identity theft is one possible threat if this check is not performed.

The following story details what might happen if a domain ownership check is not performed.

A company with DNS domain set to "hacker.com" buys Webex Hybrid Services. Another company, with its own domain set to "example.com", is also using hybrid services. One of the general managers of the company Example.com is named Jane Roe and has the directory URI jane.roe@example.com.

The administrator of Hacker.com company sets one of her directory URIs to jane.roe@example.com and the email address to jane.roe@hacker.com. She can do that because the cloud doesn't check the SIP URI domain in this example.

Next, she signs in to Webex App with jane.roe@hacker.com. Because she owns the domain, the verification email is read and answered, and she can sign in. Finally, she makes a call to a colleague, John Doe, by dialing john.doe@example.com from her Webex App. John is sitting in his office and sees a call on his video device coming from jane.roe@example.com; that is the directory URI associated with that email account.

"She's abroad," he thinks. "She might need something important." He answers the phone, and the fake Jane Roe asks for important documents. She explains that her device is broken, and because she is travelling, she asks him to send the documents to her private email address, jane.roe@hacker.com. This way, the company realizes only after Jane Roe gets back to the office that important information was leaked outside of the company.

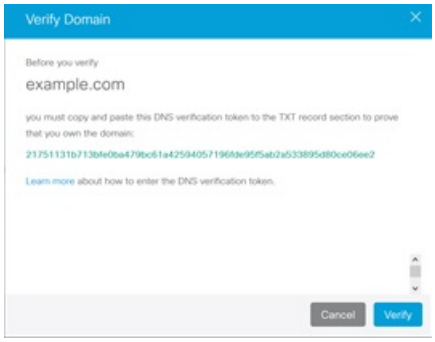
The company Example.com has many ways to protect against fraudulent calls coming from the Internet, but one of the responsibilities of the Webex cloud is to make sure that the identity of anyone calling from Webex is correct and not falsified.

To check the identity, Webex requires that the company proves that it owns the domains used in Hybrid Calling. If it doesn't, Hybrid Services won't work.

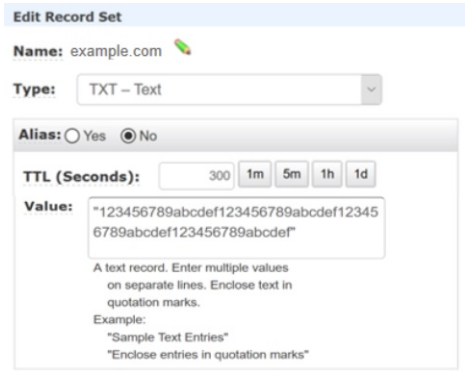
To ensure this ownership, the two domain verification steps are required:

1. Prove that the company owns the email domain, Expressway-E domain, Directory URI domain.
    - All those domains must be routable and known by public DNS servers.
    - To prove the ownership, the DNS administrator must enter a DNS Text record (TXT). A TXT record is a type of resource record in the DNS used to provide the ability to associate some arbitrary and unformatted text with a host or other name.
    - The DNS administrator must enter that TXT record in the zone whose ownership must be proved. After that step, the Webex cloud performs a TXT record query for that domain.
    - If the TXT query is successful and the result matches the token that was generated from the Webex cloud, the domain is verified.

- As an example, the administrator must prove that she owns the domain "example.com", if she wants Webex Hybrid Services to work on her domain.
- Through https://admin.webex.com, she starts the verification process by creating a TXT record to match the token that the Webex cloud generated:



- The DNS administrator then creates a TXT record for this domain with the value set to *123456789abcdef123456789abcdef123456789abcdef123456789abcdef*, as in the following example:



- At this point, the cloud can verify that the TXT record for the domain example.com matches the token.
- The cloud performs a TXT DNS lookup:

```
> set type=txt
> example.com
Server:  dns-ams.cisco.com
Address:  144.254.71.184

Non-authoritative answer:
example.com    text =

       "123456789abcdef123456789abcdef123456789abcdef123456789abcdef"
```

- Because the TXT value matches the token value, this match proves that the administrator added the TXT record for her own domain to the public DNS, and that she owns the domain.

2. Expressway-E DNS Name ownership check.
   - The cloud must check that the Expressway-E has a confirmed identity from one of the certificate authorities that the cloud trusts. The Expressway-E administrator must request a public certificate for his Expressway-E to one of those certificate authorities. To issue the certificate, the certificate

authority performs an identity verification process, based on a domain validation check (for domain validated certificates) or organization validation check (for organization validated certificates).

- Calls to and from the cloud depend on the certificate that was issued to the Expressway-E. If the certificate is not valid, the call is dropped.

Supported certificate authorities

The Webex Device Connector must communicate with Webex in order for Hybrid Calling to work.

Webex Device Connector is deployed in the internal network, and the way it communicates with the cloud is through an outbound HTTPS connection—the same type that is used for any browser that connects to a web server.

Communication to the Webex cloud uses TLS. Webex Device Connector is the TLS client, and the Webex cloud is the TLS server. As such, Webex Device Connector checks the server certificate.

The certificate authority signs a server certificate using its own private key. Anyone with the public key can decode that signature and prove that the same certificate authority signed that certificate.

If Webex Device Connector has to validate the certificate provided by the cloud, it must use the public key of the certificate authority that signed that certificate to decode the signature. A public key is contained in the certificate of the certificate authority. To establish trust with the certificate authorities used by the cloud, the list of certificates of these trusted certificate authorities must be in the Webex Device Connector trust store.

When communicating with devices, the tool uses trusted certificates that you provide. Currently the way to do that is by placing them in `[home folder]/.devicestool/certs`.

A list of certificate authority certificates is also required for the Expressway-E in the traversal pair. Expressway-E communicates with the Webex cloud using SIP with TLS, enforced by mutual authentication. Expressway-E trusts calls coming from and going to the cloud, only if the CN or SAN of the certificate presented by the cloud during TLS connection setup matches the subject name configured for the DNS zone on Expressway ("callservice.webex.com"). The certificate authority releases a certificate only after an identity check. The ownership of the callservice.webex.com domain must be proved to get a certificate signed. Because we (Cisco) own that domain, the DNS name "callservice.webex.com" is direct proof that the remote peer is truly Webex.

Related Topics

Supported certificate authorities for Webex

Custom certificates for mutual TLS authentication between Expressway-E and the cloud

For extra security, you might want your Expressway to communicate with the cloud through certificates that were signed by a certificate authority (CA).

If your Expressway-E SIP TLS certificate was signed by a private certificate authority (or a certificate authority that is not trusted by the Webex default trust list—see the links below), then you can upload the certificate authority's root certificate to your organization's custom trust list on the **Services** > **Hybrid** > **Hybrid Calling for Webex Devices** > **Settings** page.

- To use a custom certificate, you must verify any domain that is used in your organization. Any verified domains must be present on the Expressway-E certificate as a subject alternate name (SAN).
- When a SIP-TLS transaction takes place between the Webex cloud and your Expressway-E, the cloud analyzes the domains that are listed in your Expressway-E SAN list. The cloud then checks if the domain in the SAN has been verified by the organization. If the check fails, the TLS connection will terminate.
- If the Expressway-E certificate does not contain your domain as a SAN, or if you did not verify the domain, the cloud cannot identify which certificate store to use. The result is that TLS negotiations fail, even if you have supplied the correct certificates on the **Services** > **Hybrid** > **Hybrid Calling for Webex Devices** > **Settings** page.

Certificate Revocation Lists

If your private certificate authority inserts a certificate revocation list (CRL), ensure that the CRL locations are reachable from the public internet. If a CRL is present but not reachable, the Webex cloud cannot verify whether the certificate was revoked.

In this case, the certificate must not try to access a CRL.

Related Topics

Manage Domains

Supported Certificate Authorities for Cisco Webex

Cisco Spark Remote Device overview and license requirements

To configure Webex Hybrid Calling for Webex devices (Room, Desk, and Board) in a Workspace, you must create a Cisco Spark Remote Device for each Workspace. The virtual device's settings tie in with the Webex device remote destination so that Unified CM-based calls can be made from the Webex device.

The Cisco Spark Remote Device (Cisco Spark-RD) is a dedicated and fully compatible virtual device for Hybrid Calling's functional requirements and behaviors. Cisco Spark-RD provides the following features:

- Remote Destination (Webex SIP address) length can be greater than 48 characters
- Does not require an MTP for calls
- Does not require IOS-MTP passthrough for video or screen share capability

Use this table to understand the license requirements for Cisco Spark-RD for Unified CM or HCS.

Table 4: License requirements for Cisco Spark-RD

Device	License requirement for Unified CM or HCS
Cisco Spark-RD plus Hybrid Call for Webex (Room, Desk, and Board) Devices in a Workspace	Enhanced UCL—For a newly deployed system, this license must be provided. For a Webex device that is converted from Unified CM-registered to Webex-registered, its existing Unified CM license is sufficient.

Recommendations for global Hybrid Calling deployments

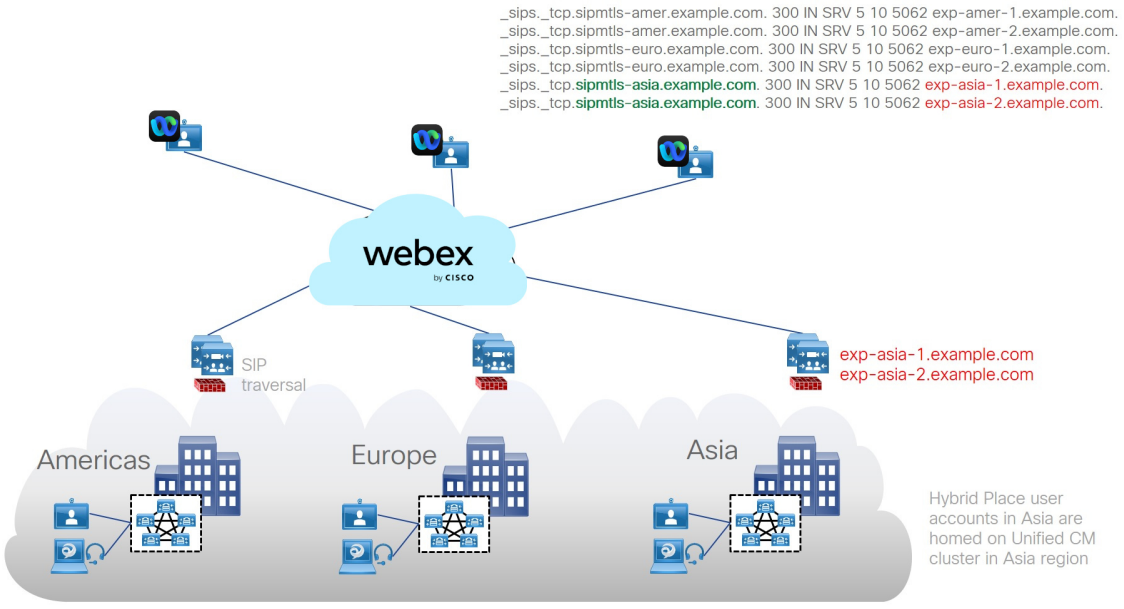
Distributed Unified CM call control

See the following diagram for an example of a global deployment with SIP destinations in Workspaces for Hybrid Calling and geographically distributed Unified CM clusters.

Recommended deployment for distributed Unified CM

- An Expressway-C/E cluster is required for each location (US, EMEA, and so on). Create a SIP mutual TLS SRV pointing at each cluster.

Figure 1: Cloud and on-premises components for multiple SIP destinations and distributed Unified CM call control for a Hybrid Calling deployment

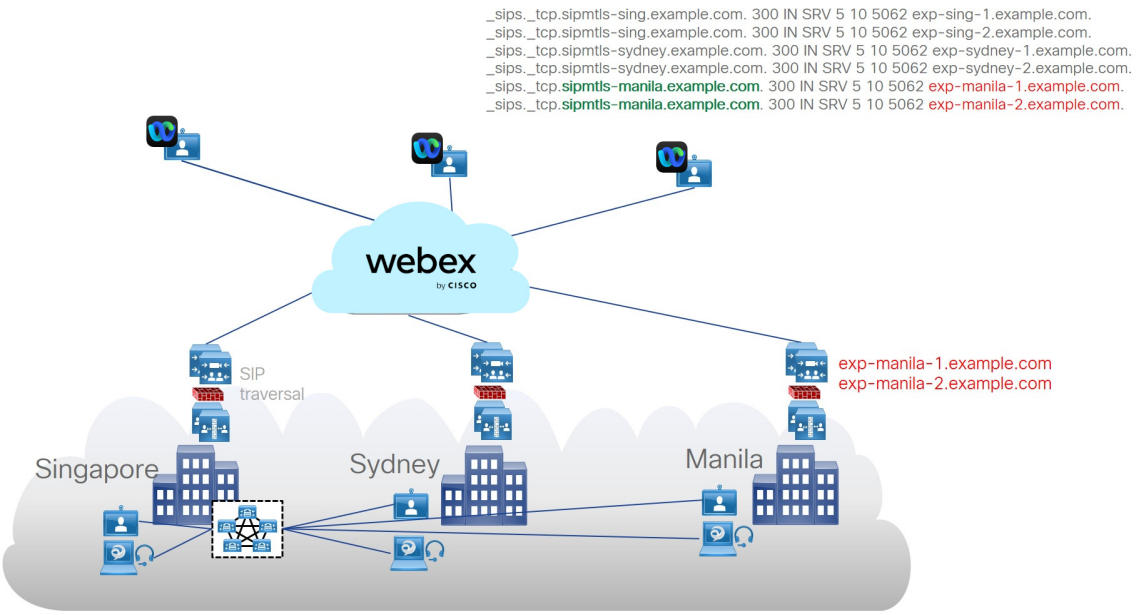


Centralized Unified CM call control

Recommended deployment for centralized Unified CM

- An Expressway-C/E cluster is required for each location (US, EMEA, and so on). Create a SIP mutual TLS SRV pointing at each cluster.

Figure 2: Cloud and on-premises components for multiple SIP destinations and centralized Unified CM call control for a Hybrid Calling deployment



Complete the prerequisites for Hybrid Calling

Use this checklist to prepare your call control environment for Hybrid Calling. Address these items in advance to ensure a smooth deployment of Hybrid Calling for Webex devices.

Step 1 Allow extra time to prepare these items:

- Determine your certificate trust method. You can use manual or automatic upload; see Supported Certificate Authorities for Webex for more information.

  Note If you plan to use the manual method, you must trust IdenTrust as a public certificate authority (CA). See Webex Root CA Certificate Update. Upload the IdenTrust certificate to your Expressway devices as soon as possible. Otherwise, calls from the Expressway-E to the cloud may fail.

- Verify your identity by registering all the domains that are used to form your users' directory URIs and email addresses. Ensure that the subject alternative names (SANs) belong to the domains that are registered on your Webex organization.

  See Why the cloud checks domain ownership, on page 8 to understand why domain checks are an important security measure.

- Install or upgrade to a supported version of Unified Communications Manager, as described in Requirements for Hybrid Calling, on page 3
- Prepare your Expressway-Es (default SIP Destination and Workspace-specific SIP destination overrides) for the secure mutual TLS connection between Webex and your call control environment:

- For the SIP destination in Control Hub, create `_sips._tcp.sipmtls.example.com` in your external DNS:

```
 Service and protocol: _sips._tcp.mtls.example.com
Priority: 1
Weight: 10
Port number: 5062
Target: us-expe1.example.com
```

- An SRV record (multiple Expressway-Es for redundancy) is recommended for large deployments:
  - You cannot reuse an existing SRV; allow the time to request a dedicated SRV for Hybrid Calling and use port 5062. The SRV record resolves into Expressway-E A-records; the hostname is the A-record for Expressway-E.
  - Request that port 5062 be open on the enterprise firewall. This port is required to establish a mutual TLS connection between the premises and cloud.
  - Make sure that the port is open to and from the Internet.
  - Verify that the mutual TLS port is reachable by using a ping utility—for example, *telnet [domainname or ip] [port]* in a command prompt.
- If you don't have time to request a dedicated SRV domain or have a small deployment, you can use *FQDN:port* or *IP address:port* to avoid blocking the rest of setup. Later, you can change to an SRV-based SIP destination if you prefer.

See TCP port 5062 on the internet firewall, on page 5 for more information.

- Follow these Expressway pair requirements:
  - If you don't have an existing Expressway pair that is deployed, read the following documents (Release X8.11.4 and later) to design your new Expressway pair to work together:
    - Cisco Expressway Installation Guides
    - Cisco Expressway Basic Configuration Deployment Guide
    - Cisco Expressway and CUCM via SIP Trunk Deployment Guide
    - Cisco Expressway IP Port Usage for Firewall Traversal Deployment Guide
  - Install or upgrade your Expressway pair that handles SIP traffic to a supported version, as described in Requirements for Hybrid Calling, on page 3. Use the recommended version for all Expressways that are handling SIP calls to take full advantage of Hybrid Calling.

You can use an Expressway pair that's already configured for B2B or MRA deployments. You cannot use a Jabber Guest Expressway pair to handle Hybrid Calling calls.

Step 2 Follow these Unified Communications Manager requirements:

- Install or upgrade your Unified Communications Manager to the minimum version that supports Cisco Spark-RD, as described in Requirements for Hybrid Calling, on page 3.
- Prepare your licensing. (See Cisco Spark Remote Device overview and license requirements, on page 12)
- On the Unified CM, configure Directory URIs in one or both of the following ways, depending on your deployment:
  - Intracluster routing for intracluster routing in single cluster and multicluster deployments.
  - Intercluster lookup service (ILS) routing for multicluster and business-to-business deployments.

- Check your codec configuration.

  Webex supports the following codecs:

  - Audio—G.711, G.722, AAC-LD
  - Video—H.264

  Note We support G.729 when users join a Webex meeting, Personal Room meeting, or Webex meeting from a SIP device. We do not support G.729 when a user dials 1:1 from Webex to a SIP device or bridge.

- Configure the following settings to be used for Cisco Spark-RD creation:
  - Device pools
  - Locations
  - Calling search spaces

    Note The calling search space must be able to route to partition of the PSTN gateway or trunk, and any other destinations that you want Webex devices to be able to reach (conference bridges, enterprise-to-enterprise trunks, and so on).

  - Note these values. You will use them when you create each Cisco Spark-RD.

Step 3 Provide port access (for media traversal between phones, Expressways, and the Webex cloud), as covered in the Network requirements, on page 5.

Step 4 For all existing SIP trunks between Unified Communications Manager clusters, go to **Device > Trunk**, open the trunk settings, and set the **Calling and Connected Party Info Format** to **Deliver URI and DN in connected party**.

Step 5 Enable the AXL Web Service on at least one node in the cluster (the bootstrap server, which can be the publisher or subscriber node of a cluster).

We recommend that you enable AXL Web Service on at least two nodes in the cluster.

Step 6 Ensure that Cisco CallManager Serviceability is enabled on at least one node in the cluster. This service is enabled by default and is used to discover nodes where the AXL Web Service is enabled.