



Deployment guide for Hybrid Calling for Webex Devices (Device Connector)

First Published: 2019-09-19

Last Modified: 2023-10-12

Americas Headquarters

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



CONTENTS

Full Cisco Trademarks with Software License vii

PREFACE

New and changed information viii

CHAPTER 1

Overview of Hybrid Calling for Webex Devices 1

Hybrid Calling for Webex Devices 1

Calling functionality for users 2

Hybrid Calling for Webex Devices architecture 2

Global Hybrid Calling architecture 3

CHAPTER 2

Prepare your environment for Hybrid Calling for Webex Devices 5

Requirements for Hybrid Calling for Webex Devices 5

Device requirements 6

Requirements for Hybrid Calling 7

Cisco call control solution requirements 7

Cisco Expressway requirements 7

Webex Device Connector requirements 8

Network requirements 9

Important items for Hybrid Services deployments 9

TCP port 5062 on the internet firewall 9

Why the cloud checks domain ownership 12

Supported certificate authorities 15

Custom certificates for mutual TLS authentication between Expressway-E and the cloud 15

Cisco Spark Remote Device overview and license requirements 16

Recommendations for global Hybrid Calling deployments 17

Complete the prerequisites for Hybrid Calling 18

CHAPTER 3**Deploy Hybrid Calling for Webex Devices 21**

- Hybrid Calling for Webex Devices deployment task flow 21
- Configure Unified Communications Manager settings for Hybrid Calling 24
- Configure the Expressway-E for Hybrid Calling 28
 - Update the Expressway-E trust list with Webex cloud certificates 29
 - Configure call processing language (CPL) rules on Expressway-E 29
 - Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud 30
 - Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud 33
 - Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud) 34
 - Configure a secure traversal server zone from Expressway-E to Expressway-C 34
 - Create inbound and outbound search rules on Expressway-E 36
- Configure the Expressway-C for Hybrid Calling 38
 - Configure a secure traversal client zone from Expressway-C to Expressway-E 39
 - Create an Expressway-C neighbor zone for each Unified CM cluster 40
 - Configure search rules on Expressway-C (to Unified CM) 43
- Activate Hybrid Calling for your organization 45
- Configure Workspace settings 47
 - Create a directory number and directory URI for Webex devices with Hybrid Calling 47
 - Create a Unified CM account for Webex devices with Hybrid Calling 48
 - Create a Cisco Spark-RD for Webex devices with Hybrid Calling 49
- Enable Hybrid Calling for Webex devices 50
 - Enable Hybrid Calling for a New or Existing Workspace With Webex Devices 51
 - Enable Hybrid Calling for Personal Mode Devices 52
- Install Webex Device Connector 53
- Synchronize device configuration changes with Webex Device Connector 54
- Known issues and limitations with Hybrid Calling for Webex devices 55

CHAPTER 4**Manage and troubleshoot Hybrid Calling for Webex Devices 57**

- Rename a Workspace enabled for Hybrid Calling 57
- Override the default SIP destination for a Workspace 58
- Remove Hybrid Calling from Webex device 59

Deactivate Hybrid Calling for Webex Devices	60
Troubleshooting sources for Hybrid Calling	60
Hybrid connectivity test tool (Control Hub)	61
Webex status page	62
Mutual TLS and SIP destination	62
Expressway pair configuration	63
Unified CM configuration	63

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



New and changed information

Date	Changes Made
October 12, 2023	Added a note to <i>Overview</i> that <i>Webex Calling Dedicated Instance</i> does not require the Device Connector.
December 3, 2021	<ul style="list-style-type: none"> • Added the following note to the mutual TLS authentication configuration steps: If you Expressway-E is clustered, you can't disable H.323 box-wide because clustering relies on H.323. For this reason, we recommend setting up firewall rules on Expressway or the Internet firewall to block H.323 inbound. • In the Unified CM SIP trunk security profile configuration, added a step to set the Device Security Mode to Encrypted. • Added the following note to the “Complete the prerequisites” section: 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. • In accordance with style guidelines, changed section titles from title case to sentence case.
July 9, 2021	<ul style="list-style-type: none"> • Updated naming and diagrams to reflect the new Webex Suite branding. • Moved non-deployment tasks (such as Rename Workspace, Remove Calling, and so on) to the Manage and Troubleshoot chapter.

Date	Changes Made
May 21, 2021	<ul style="list-style-type: none"> • Corrected references to various parts of the Control Hub web interface. • In the Known Issues section, added a link to the Preferred Architecture guide which contains more information about loop detection and avoidance. • Retitled "Configure Directory Number" to "Configure Directory Number and Directory URI", and added a statement to clarify the workaround for Directory URI dialing between a user and a device.
January 20, 2021	<ul style="list-style-type: none"> • Added new section "Enable Hybrid Calling for Personal Mode Devices" in the deployment chapter. • Combined the personal mode and shared mode enablement steps under a single workflow table.
December 9, 2020	<ul style="list-style-type: none"> • References to "Webex Teams" are changed to "Webex." • Clarified that Hybrid Calling calls don't consume traversal licenses. • Added known issues about extension dialing, directory URI dialing, and calling from one organization to another.
August 19, 2020	<ul style="list-style-type: none"> • Removed incorrect content about the automatic creation of Cisco Spark-RD. • Rearranged deployment chapter; now, the directory number, Cisco Spark-RD, end user, and Workspaces steps are tied together in a mini task flow.
June 16, 2020	References to "Places" have been changed to "Workspaces."
April 23, 2020	Added "Migrate Hybrid Calling Organization Using Webex Device Connector" section to the Prepare Your Environment chapter.
February 28, 2020	Initial version of the document.



CHAPTER 1

Overview of Hybrid Calling for Webex Devices

- [Hybrid Calling for Webex Devices](#), on page 1
- [Calling functionality for users](#), on page 2
- [Hybrid Calling for Webex Devices architecture](#), on page 2
- [Global Hybrid Calling architecture](#), on page 3

Hybrid Calling for Webex Devices



Note Hybrid Calling for Devices (device connector) is not supported within the Dedicated Instance (DI) for Webex Calling.

There is no requirement for an Expressway-based solution (device connector) because you can use the pre-configured inter-op SIP trunk between Webex Calling Multi-Tenant and Dedicated Instance. Devices registered to Unified CM in your DI use the trunk to connect with Webex-registered devices.

You can use [Webex Edge for Devices](#) for devices registered in your dedicated instance, or you can register your devices to Webex Calling.

Hybrid Calling for devices in Workspaces

You can use Hybrid Calling for Webex Devices to provide hybrid call functionality for Room, Desk, and Cisco Webex Board devices that are added to Workspaces in Control Hub. Webex devices are registered to the cloud, and when they are enabled with Hybrid Calling, they also connect to the enterprise. Webex devices in the Workspace become a part of your existing on-premises dial plan, allowing these devices to call user extensions or the PSTN, and receive incoming calls.

Call directly from the device—Although the devices in a Workspace are registered to the cloud, you can provide them with a line and PSTN service that is served through your Unified CM deployment. People can call these devices to join a meeting; people can also use these devices to dial other extensions or numbers.

Call from Webex App while connected to the device—From Webex App, users can also call phone numbers while connected to a cloud-registered Webex device that is enabled for Hybrid Calling. They can call someone's mobile phone number or the local pizza place directly from Webex App and have the call take place on the Webex device.

Webex Device Connector is a lightweight piece of software that connects your Unified CM configuration with cloud configuration and Webex devices registered to the cloud. You can use the software automate

synchronizing Unified CM configuration to device in your Control Hub-managed organization. You get the software from Control Hub and install it on a Windows or Mac device or virtual machine in your network that can access your premises environment and the devices themselves.

Hybrid Calling for devices associated with users (Personal Mode)

You can also add Hybrid Calling to Room, Desk, and Board devices that are associated with a user in personal mode. These devices don't need to be added to Workspaces. Webex devices in Personal Mode become a part of your existing on-premises dial plan, allowing these devices to call user extensions or the PSTN, and receive incoming calls.

They appear in Control Hub under devices and are associated with users in your organization. They register to the cloud and share the same directory number that is tied to a user's Webex App account if they're already enabled for Unified CM calling (<https://www.cisco.com/go/webex-teams-ucm-calling>).



Note On a personal mode device enabled for Hybrid Calling, if a user dials a number on the device, the call goes through the enterprise like a typical PSTN call. However, a SIP call always goes through the Webex cloud rather than the enterprise.

Calling functionality for users

Calling for Webex App users is outside of the scope of this document. The Webex Device Connector-based architecture for Hybrid Calling only supports Webex devices registered to the cloud. If you want to provide calling features to users in your organization, see [this deployment guide](#) to set up Webex App users with Unified CM calling; this deployment model uses a Webex App client-based integration into your Unified CM environment.



Note [Hybrid Calling with the Call Connector architecture is end of life \(EOL\) and no longer supported.](#)

Hybrid Calling for Webex Devices architecture

Figure 1: On-premises and cloud components for Hybrid Calling for Webex Devices

This diagram shows the on-premises and cloud components that comprise the Hybrid Calling for Webex Devices architecture. This architecture provides call connectivity to Webex cloud-registered devices in a Workspace (created in Control Hub), so that these devices can use the Unified CM dial plan. You manually synchronize configuration between premises and cloud by running a sync in the Webex Device Connector software.



CHAPTER 2

Prepare your environment for Hybrid Calling for Webex Devices

- [Requirements for Hybrid Calling for Webex Devices](#) , on page 5
- [Requirements for Hybrid Calling](#), on page 7
- [Important items for Hybrid Services deployments](#), on page 9
- [Custom certificates for mutual TLS authentication between Expressway-E and the cloud](#), on page 15
- [Cisco Spark Remote Device overview and license requirements](#), on page 16
- [Recommendations for global Hybrid Calling deployments](#), on page 17
- [Complete the prerequisites for Hybrid Calling](#), on page 18

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](#), on page 1)
- Supported devices as covered in [Device requirements](#), on page 6.
- 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 16 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 7 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 7 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	<p>Supported Cisco Spark Remote Device (Cisco Spark-RD) releases are required for Hybrid Calling deployments.</p> <p>Releases with Cisco Spark Remote Device Support</p> <ul style="list-style-type: none"> • 11.5(1)SU3 and later; we recommend the latest SU release. <p>Releases with Session Management Edition (SME) support</p> <ul style="list-style-type: none"> • 12.0(1) and later; we recommend the latest release. <p>Note The leaf clusters that are connected to the SME cluster do not have to be on release 12.0(1)</p>
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
--------------	---------

<p>Cisco Expressway E and C Traversal Pair (for hybrid call traffic)</p>	<p>X8.11.4 or later is required for Hybrid Calling. See the “Important Information” section in the Expressway Release Notes for more information.</p> <p>This release provides added security and toll fraud mitigation.</p> <p>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.</p> <ul style="list-style-type: none"> • 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. <p>Hybrid Calling follows existing MRA and B2B preferred architecture planning recommendations.</p> <ul style="list-style-type: none"> • 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 traversal 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

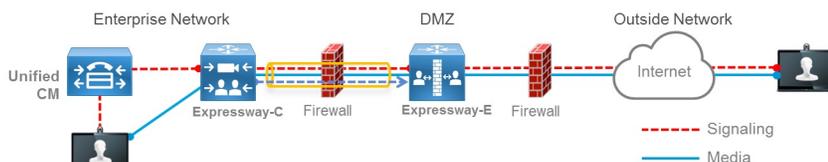
The [Expressway-C and Expressway-E pair deployment](#) allows calls to and from the Internet using [firewall traversal technologies](#). This deployment is what securely takes your on-premises call control and ties it in to Webex.

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:

Expressway Firewall Traversal Basics



1. **Expressway-E** is the traversal server installed in DMZ. **Expressway-C** is the traversal client installed inside the enterprise network.
2. **Expressway-C** initiates traversal connections outbound through the firewall to specific ports on **Expressway-E** with secure login credentials.
3. Once the connection has been established, **Expressway-C** sends keep-alive packets to **Expressway-E** to maintain the connection.
4. When **Expressway-E** receives an incoming call, it issues an incoming call request to **Expressway-C**.
5. **Expressway-C** then routes the call to **Unified CM** to reach the called user or endpoint.
6. The call is established and media traverses the firewall securely over an existing traversal connection.

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-expel.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.

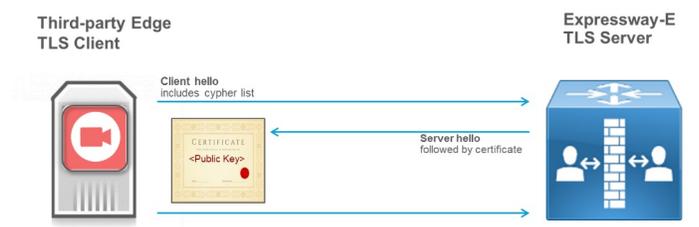
A device that is external to the network (on the Internet) and that makes a SIP call to a user of the corporate domain (user1@example.com) must query the DNS to understand which transport type to use, the port number, how to load-share the traffic, and which SIP servers to send the call to.

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:

TLS handshake high-level overview

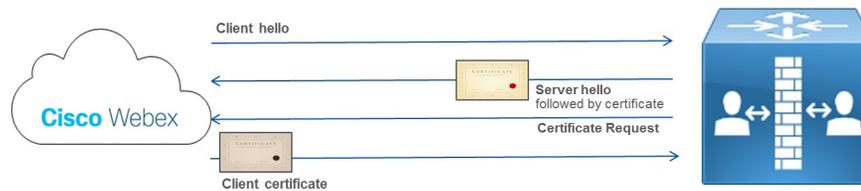


- Only TLS server needs the certificate (Expressway-E)
- TLS Client checks
 - Hostname (FQDN) against CN or SAN
 - Expiry
 - Revocation status of certificate
 - Digital signature of cert (needs CA cert in its trust list)
- If Expressway makes a call to the 3rd party Edge, Expressway is the TLS client and the 3rd party Edge is the TLS server

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:

TLS handshake with Mutual Authentication



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-expel.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

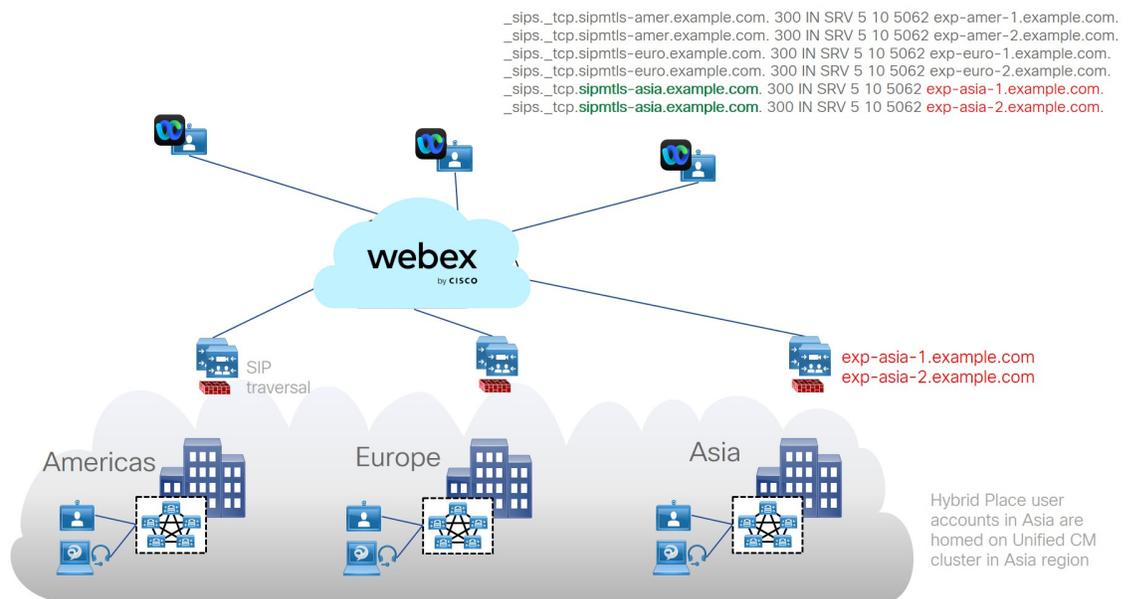
Distributed Unified CM call control

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

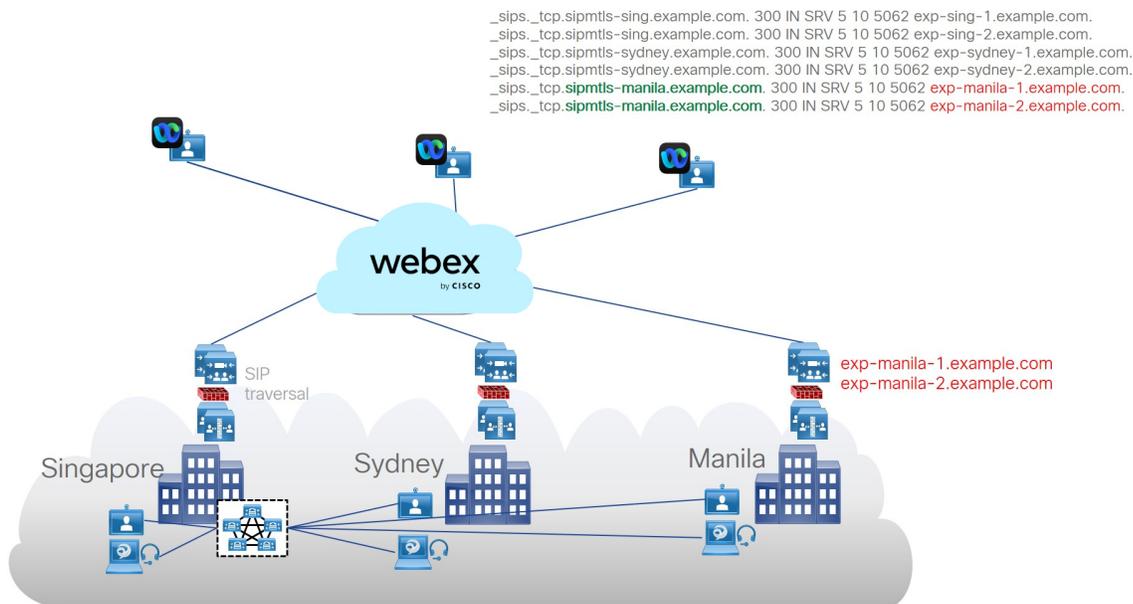


Centralized Unified CM call control

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 3: 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 12](#) 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 7](#)
- 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-expel.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 9](#) 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 7](#). 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 7](#).
- Prepare your licensing. (See [Cisco Spark Remote Device overview and license requirements, on page 16](#))
- 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 9](#).

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.



CHAPTER 3

Deploy Hybrid Calling for Webex Devices

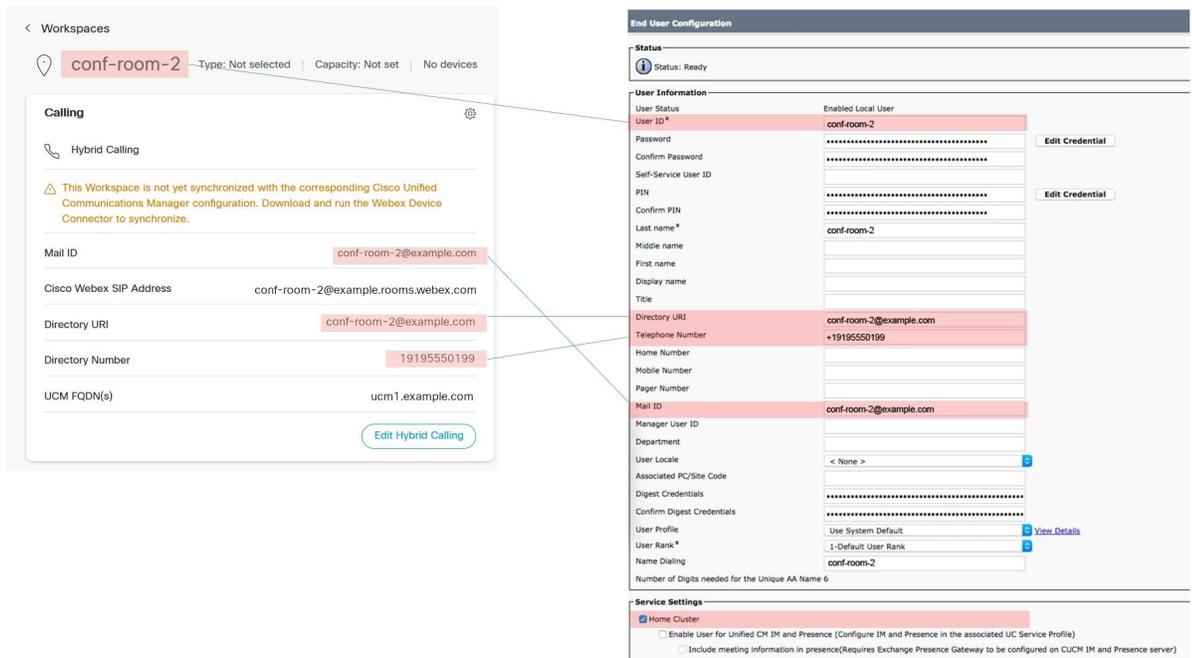
- [Hybrid Calling for Webex Devices deployment task flow, on page 21](#)
- [Configure Unified Communications Manager settings for Hybrid Calling, on page 24](#)
- [Configure the Expressway-E for Hybrid Calling, on page 28](#)
- [Configure the Expressway-C for Hybrid Calling, on page 38](#)
- [Activate Hybrid Calling for your organization, on page 45](#)
- [Configure Workspace settings, on page 47](#)
- [Enable Hybrid Calling for Webex devices, on page 50](#)
- [Install Webex Device Connector, on page 53](#)
- [Synchronize device configuration changes with Webex Device Connector, on page 54](#)
- [Known issues and limitations with Hybrid Calling for Webex devices, on page 55](#)

Hybrid Calling for Webex Devices deployment task flow

This task flow walks you through how to first configure Unified CM settings for Webex devices, configure Expressway settings, activate Hybrid Calling for your organization, and then add Hybrid Calling to either a newly created Workspace or an existing Workspace with Webex cloud-registered video devices. A Workspace is configured in Control Hub. After you complete all the required configuration on-premises and in the cloud, you can install and run the Webex Device Connector to synchronize the configuration between both.

Figure 4: Field mapping between Control Hub and Unified CM

As you configure Hybrid Calling for Webex Devices, refer to this screenshot which shows the mapping of fields between Control Hub (on the left) and Unified CM (on the right).



The following points provide a functional overview of the feature:

- This feature uses a Cisco Spark Remote Device (Cisco Spark-RD) in on-premises Unified CM to route calls on the device to enterprise extensions, users, and PSTN.
- Features that are initiated from on-premises phones (such as hold, transfer, and conference) can include Webex devices with Hybrid Calling.
- Any calls from Webex devices to PSTN or on-premises extensions are anchored to the Cisco Spark-RD in Unified CM.

Before you begin

- Read the overview: [Hybrid Calling for Webex Devices, on page 1](#)
- Complete the requirements: [Requirements for Hybrid Calling for Webex Devices , on page 5](#)

Procedure

	Command or Action	Purpose
Step 1	Manage domains (external article)	Domain verification is essential to the security and integrity of your organization. Verification proves to us that you own a particular domain and is required for this service to work. If your company has multiple domains, add each domain one at a time. For example, if you have Webex devices and administrators of the devices in sales.example.com and in support.example.com, you must add both domains.

	Command or Action	Purpose
		If your organization enforces email addresses, you are presented with warnings about possible lockout. You are forced to verify and remove domains in a particular order to prevent administrator lockout. When adding domains, for example, you must add the administrator domain first, followed by all other domains.
Step 2	Configure Unified Communications Manager settings for Hybrid Calling, on page 24	Configure Unified Communications Manager to receive calls directly from Expressway-E. This configuration enables URI routing between the cloud and the on-premises enterprise. You'll create a cluster FQDN, which is the enterprise parameter that is used in SIP routing decisions and that helps identify multiple clusters so calls can occur between them.
Step 3	<p>Configure the Expressway-E for Hybrid Calling, on page 28 by following these tasks:</p> <ul style="list-style-type: none"> • Update the Expressway-E trust list with Webex cloud certificates, on page 29 • Choose one depending on your deployment: <ul style="list-style-type: none"> • Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud, on page 30 • Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud, on page 33 • Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud), on page 34 • Configure a secure traversal server zone from Expressway-E to Expressway-C, on page 34 • Create inbound and outbound search rules on Expressway-E, on page 36 	Enterprise calls are securely routed over the Expressway pair. If you want to reuse an existing pair, some of the required traversal configuration for Hybrid Calling may already be in place. However, read the procedures that follow to ensure that Expressway-E and Expressway-C are correctly configured.
Step 4	<p>Configure the Expressway-C for Hybrid Calling, on page 38 by following these tasks:</p> <ul style="list-style-type: none"> • Configure a secure traversal client zone from Expressway-C to Expressway-E, on page 39 • Create an Expressway-C neighbor zone for each Unified CM cluster, on page 40 • Configure search rules on Expressway-C (to Unified CM), on page 43 	Enterprise calls are securely routed over the Expressway pair. If you want to reuse an existing pair, some of the required traversal configuration for Hybrid Calling may already be in place. However, read the procedures that follow to ensure that Expressway-E and Expressway-C are correctly configured.
Step 5	Activate Hybrid Calling for your organization, on page 45	Use this procedure to begin the initial setup for Hybrid Calling in Control Hub. These settings ensure that Hybrid Calling is first enabled for your organization before you do further configuration. You specify the desired subdomain for your company, and that setting creates Webex App SIP

	Command or Action	Purpose
		addresses as unique identifiers. Then, you toggle on hybrid call connect for your organization. Last, you enter the SIP destination address which resolves to your Expressway-E in the call traversal pair. This entry is typically a DNS-SRV record which can resolve to multiple Expressway-Es.
Step 6	<p>Configure Workspace settings, on page 47 by following these tasks:</p> <ul style="list-style-type: none"> • Create a directory number and directory URI for Webex devices with Hybrid Calling, on page 47 • Create a Unified CM account for Webex devices with Hybrid Calling, on page 48 • Create a Cisco Spark-RD for Webex devices with Hybrid Calling, on page 49 • Enable Hybrid Calling for Webex devices, on page 50 	Follow these tasks to configure the necessary Unified CM settings that are required for enabling Workspaces or Personal Mode devices for Hybrid Calling.
Step 7	Install Webex Device Connector, on page 53	You can get the Webex Device Connector software from Control Hub. After you install the software, you can use it to synchronize Unified CM configuration (dial plan, directory number, extension, and so on) to Webex devices that are in Workspaces enabled for Hybrid Calling. The tool also synchronizes cloud configuration such as the Webex SIP address down to Unified CM.
Step 8	Synchronize device configuration changes with Webex Device Connector, on page 54	Webex Device Connector keeps your on-premises and cloud configuration for Webex devices in sync. The software also identifies any mismatch issues that you can resolve before you resync the changes.

Configure Unified Communications Manager settings for Hybrid Calling

Configure Unified Communications Manager to receive calls directly from Expressway-E. This configuration enables URI routing between the cloud and the on-premises enterprise. You'll create a cluster FQDN, which is the enterprise parameter that is used in SIP routing decisions and that helps identify multiple clusters so calls can occur between them.

Before you begin

Follow the Unified CM prerequisites that are covered in [Complete the prerequisites for Hybrid Calling, on page 18](#).

-
- Step 1** From Cisco Unified CM Administration on your publisher node, go to **System > Enterprise Parameters**, scroll to **Clusterwide Domain Configuration**, and then check the value for the **Cluster Fully Qualified Domain Name** field.

Step 2 If the field is empty or the field contains domain entries with wildcards, enter a new value for Hybrid Calling and follow these guidelines:

FQDN Guideline	Description and Example
Multiple clusters	The entry must be unique for each cluster with Hybrid Calling—For example, <code>cluster1.example.com</code> , <code>cluster2.example.com</code> , and so on.
No wildcards	Do not use entries with wildcards, such as <code>*.example.com</code> or <code>example*.com</code> .
First FQDN entry for Hybrid Calling	In a list of multiple entries, the Webex cloud uses the first entry on the left for Hybrid Calling, and that first entry must not contain a wildcard. See this example of three FQDN entries from left to right (the first one being for Hybrid Calling): <code>cluster1.example.com *.example.com example*.com</code>
Different from Expressway-E	Must be different from the Expressway-E system, DNS, and domain name. Otherwise, Expressway-E strips the route header.
New entry for Hybrid Calling	If your current FQDN entry in Unified CM doesn't meet the requirements listed above, you can add a new element to the beginning of the cluster FQDN setting for Hybrid Calling. For example, if your existing FQDN setting in Cisco Unified Communications Manager is <code>*.example.com *.example.org</code> , add a unique, non-wildcard entry at the beginning of the field: <code>"cluster1.example.com *.example.com *.example.org"</code>

You are not required to restart Unified Communications Manager or services for a cluster FQDN change to take effect.

Step 3 Record or write down the name of the FQDN value that you want to use for Hybrid Calling. You need it for this procedure: [Configure search rules on Expressway-C \(to Unified CM\), on page 43](#).

Step 4 Go to **Device > Device Settings > SIP Profile** to create a new SIP profile that is based on the **Standard SIP Profile For Cisco VCS** template.

- Click **Find**, choose **Standard SIP Profile For Cisco VCS**, and then click **Copy**.
- Enter a name for the new profile—for example, **Standard SIP Profile for Webex Hybrid Calling**.
- Scroll to **Trunk Specific Configuration**, and then set **Early Offer support for voice and video calls** to **Best Effort (no MTP inserted)**.

You can apply this setting to a new SIP trunk to the Webex cloud (routed by external domain **webex.com**). The setting does not affect any existing SIP trunking or call routing.

- Leave all other fields with their default values and save your changes.

Step 5 (Optional) If your Expressway pair runs MRA or B2B, go to **System > Security > SIP Trunk Security Profile** and create a new SIP trunk security profile for Hybrid Services.

- Enter a name for the new profile that is related to Webex or Hybrid Calling—for example, **SIP Trunk Security Profile for Webex Hybrid Calling**.
- Set **Device Security Mode** to **Encrypted**.

This is required because Expressway supports only encrypted TLS. This setting avoids an encryption mismatch between Expressway-C and Unified CM.

- Leave the **Enable Digest Authentication** check box unchecked.
- Do not set the incoming port value to 5061. Instead, change to an appropriate alternative—We recommend 5561.

We recommend that you use TLS. This setting doesn't require Unified CM to be in mixed mode. In this case, you must specify the following:

- **Transport type**—TLS instead of TCP/UDP
- **X.509 Subject Name**—Must match one of the Subject Alternative Names (SANs) of the Expressway-C.

e) Leave all other fields with their default values and save your changes.

Step 6

Go to **Device > Trunk** to create a new SIP trunk to the Expressway-C, and then link the Webex SIP profile to this trunk.

- Choose **SIP Trunk** as the trunk type; leave the other settings, and click **Next**.
- Configure these settings and leave the defaults for any settings not mentioned:

Field name	Value
Name	Hybrid_Calling_SIP_Trunk (for example)
Device Pool	Choose a device pool that contains the device-specific settings that you want the SIP trunk to inherit.
Calling and Connected Party Info Format	<p>Deliver URI and DN in connected party, if available</p> <p>This setting enables blended identity. It allows the SIP trunk to transmit the enterprise-side party's directory URI to Webex.</p> <p>The directory URI is what allows the cloud to match the enterprise end user account to the Webex-registered device in a Workspace or Personal Mode. This match enables the Webex device to be provided with a Unified CM directory number.</p> <p>Note You must also apply this setting on any intercluster trunks within your organization and SIP trunks to any organizations that you want to work with Hybrid Calling.</p>
Destination Address	Enter the Expressway-C node addresses in the fields.
Destination Port	Enter 5060/5061 .
SIP Profile	Standard SIP Profile for Webex Hybrid Calling (for example)

c) Save your changes.

Step 7

Go to **Call Routing > SIP Route Pattern** to create the following new route patterns that match the required subdomains for Hybrid Calling.

Table 5: SIP route pattern for Webex domain For Hybrid Calling for devices

Field Name	Value
IPv4 Pattern	*.rooms.webex.com
Pattern Usage	Domain Routing
Description	Routing for Webex hybrid calling devices

Field Name	Value
Route Partition	Choose a route partition to contain this SIP route pattern. You must also include the same partition in the rerouting calling search space (CSS) of the Cisco Spark-RD. (We do not recommend using the <None> partition.)
SIP Trunk/Route List	Choose the trunk you created— Hybrid_Calling_SIP_Trunk (for example)
SIP Profile	Standard SIP Profile for Webex Hybrid Calling (for example)

Note We include this route pattern so that your deployment remains backwards compatible. If you're not sure if your Webex Devices have a webex.com SIP address, we recommend that you follow the directions in the [Migrate Cisco Spark Hybrid Call Service organization to the Cisco Webex domain](#) documentation to convert ciscospark.com domains over to webex.com.

Table 6: SIP route pattern for Cisco Spark domain (backwards compatibility)

Field name	Value
IPv4 Pattern	*.ciscospark.com
Pattern Usage	Domain Routing
Description	Routing for Cisco Spark hybrid calling
Route Partition	Choose a route partition to contain this SIP route pattern. You must also include the same partition in the rerouting calling search space (CSS) of the Cisco Spark-RD. (We do not recommend using the <None> partition.)
SIP Trunk/Route List	Choose the trunk you created— Hybrid_Calling_SIP_Trunk (for example)
SIP Profile	Standard SIP Profile for Webex Hybrid Calling (for example)

Example

Combine Hybrid Calling with other solutions, such as B2B and MRA

- You can run Webex hybrid calls, B2B calls, and MRA calls across the same Expressway.
- If MRA is set up on your Expressway: For the trunk that you create for Webex, use a port other than 5060/5061 on Unified Communications Manager. This setup avoid conflicts with MRA calls and device registrations. On Unified Communications Manager, set up the Device Security Profile for your Webex trunk to use a port other than 5060 or 5061.
- If B2B is set up on your Expressway: You can reuse your existing B2B trunks between Unified Communications Manager and Expressway for Webex hybrid calls. If you want to run B2B calls and Webex hybrid calls on separate trunks between the Expressway-C and Unified

Communications Manager, you cannot run TLS on both trunks at the same time. See [this bug overview](#) for more information.

- If any of your Webex Hybrid Calling traffic goes over B2B, you must preserve the SIP parameters on all zones for all Expressways that are involved in call routing to and from the enterprise.

Configure the Expressway-E for Hybrid Calling

Enterprise calls are securely routed over the Expressway pair. If you want to reuse an existing pair, some of the required traversal configuration for Hybrid Calling may already be in place. However, read the procedures that follow to ensure that Expressway-E and Expressway-C are correctly configured.

Procedure

	Command or Action	Purpose
Step 1	Update the Expressway-E trust list with Webex cloud certificates, on page 29	Your Expressway-E must trust the certificate issuer of the server certificates that are passed by the server during the client/server SSL handshake with the Webex cloud. To establish this trust, you must add these certificates to the trusted CA list on your Expressway-E.
Step 2	Perform one of the following tasks, depending on your configuration: <ul style="list-style-type: none"> • Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud, on page 30 • Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud, on page 33 	Set up a mutual TLS port as part of establishing a trusted connection between your on-premises and the cloud. From a technical standpoint, Hybrid Calling SIP uses mutual TLS between the Expressway-E and Webex, so each side authenticates the other. This behavior requires valid and verifiable certificate and trust configuration on both sides.
Step 3	Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud), on page 34	The DNS zone allows your Expressway-E to identify and route calls between Unified Communications Manager and the Webex cloud. The DNS zone is used because a secure mutual TLS connection between the cloud and Expressway-E is required to map the appropriate domains. The Webex Zone pre-configures the zone with the correct settings for Hybrid Calling.
Step 4	Configure a secure traversal server zone from Expressway-E to Expressway-C, on page 34	If you already have a traversal zone pair (typically for business-to-business (B2B) calling) or Unified Communications traversal zone pair (typically for Mobile and Remote Access (MRA)), or both, then we recommend that you create a separate traversal zone pair for Hybrid Calling.
Step 5	Create inbound and outbound search rules on Expressway-E, on page 36	Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified

	Command or Action	Purpose
		<p>according to the conditions defined in the search rule. Create search rules on Expressway-E to:</p> <ul style="list-style-type: none"> • Identify calls from the Webex cloud and route down the traversal zone to Expressway-C. • Identify calls from Unified Communications Manager and route through the DNS zone to Webex.

Update the Expressway-E trust list with Webex cloud certificates

Your Expressway-E must trust the certificate issuer of the server certificates that are passed by the server during the client/server SSL handshake with the Webex cloud. To establish this trust, you must add these certificates to the trusted CA list on your Expressway-E.

Before you begin

If you don't have an existing Expressway pair deployed, read the following documents 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](#)

Step 1 From Expressway-E, go to **Applications > Cloud Certificate management**.

Step 2 Click **Get certificates** for the cloud to automatically add and manage the certificates.

Step 3 To verify the added certificates, go to **Maintenance > Security certs > Trusted CA certificate** to view the entries that were added.

Configure call processing language (CPL) rules on Expressway-E

If Expressway-C and Expressway-E run both hybrid call and mobile and remote access (MRA) traffic, but no business-to-business traffic, the system must reject any SIP message not generated by MRA endpoints or Hybrid Services.

You can create call processing language (CPL) rules to mitigate fraudulent call attempts. We recommend doing this for toll fraud mitigation.

If business-to-business traffic is not included in the same Expressway, and because this traffic enters from the default zone, the following CPL rule will prevent any fraudulent access to Expressway-E.

Step 1 From Expressway-E, go to **Configuration > Call Policy > Configuration**, set **Call Policy mode** to **Local CPL**, and then click **Save**.

Step 2 Go to **Configuration > Call Policy > Rules**, click **New**.

This opens the **Add Call Policy rule** page.

Step 3 Configure the following settings:

Field	Setting
Source type	From address
Rule applies to	Unauthenticated callers
Source pattern	.*@example.calls.webex.com.* , where example is your company's subdomain.
Destination pattern	.*
Action	Reject

Step 4 Click **Add** to save this new rule.

Step 5 (Optional) In case TLS must be set to **On**, or B2BUA must be engaged on Expressway-E for some unknown reason, create the following CPL rule to block any TLS call from the Default Zone.

This step is not needed if TLS is switched off.

- From Expressway-E, go to **Configuration > Call Policy > Configuration**, set **Call Policy mode** to **Local CPL**, and then click **Save**.
- From related tasks, go to **Edit Call Policy rules**.
- Click **New**.
- Configure the following settings:

Field	Setting
Source type	Zone
Originating Zone	DefaultZone
Destination pattern	.*
Action	Reject

- Click **Add** to save this new rule.

Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud

If Expressway-C and Expressway-E are dedicated to Hybrid Calling, or more generally to Cloud services using Mutual TLS only (such as Hybrid Services and CMR Hybrid), you don't require H.323, SIP UDP, SIP TCP and SIP TLS on Expressway-E.

Before you begin

- [Update the Expressway-E trust list with Webex cloud certificates, on page 29](#)
- If you configured a DNS SRV as the SIP destination in Control Hub ([Activate Hybrid Calling for your organization, on page 45](#)), ensure that that value specifies the MTLS port.

Step 1 From Expressway-E, go to **Configuration > Protocols > H.323**, and then set **H.323 mode** to **Off**, unless this setting is critical for your organization, and then save your changes.

Note If your Expressway-E is clustered, you can't disable H.323 box-wide because clustering relies on H.323. For this reason, we recommend setting up firewall rules on Expressway or the Internet firewall to block H.323 inbound.

Step 2 Go to **Configuration > Protocols > SIP**, and then configure these settings:

Field Name	Value
Configuration	
SIP mode	On
UDP mode	Off
UDP port	5060
TCP mode	Off
TCP port	5060
TLS mode	On
TLS port	5061
Mutual TLS mode	On
Mutual TLS port	5062
TCP outbound port start	25000
TCP outbound port end	29999
Session refresh interval (seconds)	1800
Minimum session refresh interval (seconds)	500
TLS handshake timeout (seconds)	5
Certificate revocation checking	
Certificate revocation checking mode	Off
Registration controls	

Field Name	Value
Standard registration refresh strategy	Maximum
Standard registration refresh minimum (seconds)	45
Standard registration refresh maximum (seconds)	60
Outbound registration refresh strategy	Variable
Outbound registration refresh minimum (seconds)	300
Outbound registration refresh maximum (seconds)	3600
SIP registration proxy mode	Off
Authentication	
Delegated credential checking	Off
Advanced	
SDP max size	32768
SIP TCP connect timeout	10

Step 3 Click **Save**.

Step 4 Go to **Configuration > Zones > Zones**, and then click **DefaultZone**.

Step 5 Configure the following fields:

Field Name	Value
Policy	
Authentication mode	Do not check credentials
SIP	
Media encryption mode	Auto
ICE support	Off
Multistream mode	On
Enable Mutual TLS on Default Zone	On This setting enables mutual TLS (Mutual Transport Layer Security) on the dedicated mutual TLS port 5062 on incoming connections through the Default Zone.

Step 6 Click **Save**.

Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud

Expressway-E can be shared between mobile and remote access (MRA), business-to-business (B2B), and Webex Hybrid Calling media traffic. If Expressway is used for B2B traffic, turn off those services that are not needed. H.323 is a signaling protocol that doesn't allow for encryption and should be switched off if it's not critical for the company. SIP UDP must be switched off for security reasons. This change won't affect the calling scenarios, because only SIP endpoints with IP dialing use SIP UDP. Endpoints that are involved with IP dialing are typically H.323-based. SIP TCP should be switched off if it's not critical for the company.

Before you begin

- [Update the Expressway-E trust list with Webex cloud certificates, on page 29](#)
- If using a dedicated MTLS port, ensure that the DNS SRV in Control Hub specifies this MTLS port. (See [Activate Hybrid Calling for your organization, on page 45.](#))
- You cannot use Hybrid Calling on an Expressway firewall traversal pair that is used for Jabber Guest. In this case, set up a dedicated Expressway pair for Hybrid Calling.

Step 1 From Expressway-E, go to **Configuration > Protocols > H.323**, and then set **H.323 mode** to **Off**, unless this setting is critical for your organization, and then save your changes.

Note If you Expressway-E is clustered, you can't disable H.323 box-wide because clustering relies on H.323. For this reason, we recommend setting up firewall rules on Expressway or the Internet firewall to block H.323 inbound.

Step 2 Go to **Configuration > Protocols > SIP**, and then configure these settings:

Field Name	Value
SIP mode	On
UDP mode	Off
TCP mode	Off , if possible. If this breaks services such as B2B, set it back to On .
TLS mode	On
Mutual TLS mode	On
Mutual TLS port	5062

Step 3 Click **Save**.

Step 4 Go to **Configuration > Zones**, and then click **Default zone**.

Step 5 Set **Enable Mutual TLS on Default Zone** to **Off**.

Step 6 Click **Save**.

Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud)

The DNS zone allows your Expressway-E to identify and route calls between Unified Communications Manager and the Webex cloud. The DNS zone is used because a secure mutual TLS connection between the cloud and Expressway-E is required to map the appropriate domains.

On Expressway, you can choose the Webex DNS zone which automatically creates a pre-configured zone for Hybrid Services. The system applies the correct settings and you cannot modify the zone. You can only have one zone of this type.

Step 1 From Expressway-E, navigate to **Configuration > Zones > Zones** and click **New**.

Step 2 For **Type**, choose **Webex**, and then save your changes.

This step creates the Hybrid DNS zone, identified by the automatically populated name **Webex Zone**.

Step 3 (Optional) Next to the hybrid domain, click **Check Connectivity**.

The connectivity test tool queries DNS for the supplied SRV domain and displays the results of the query if the lookup was successful. It then attempts a TCP connection followed by a TLS connection if applicable according to the DNS SRV protocol.

Configure a secure traversal server zone from Expressway-E to Expressway-C

If you already have a traversal zone pair (typically for business-to-business (B2B) calling) or Unified Communications traversal zone pair (typically for Mobile and Remote Access (MRA)), or both, then we recommend that you create a separate traversal zone pair for Hybrid Calling.

However, if you need to share the zones between the different services:

- You can share the Unified Communications traversal pair between MRA and Hybrid Calling (you can only have one Unified Communications traversal zone pair between Expressway-C and Expressway-E).
- Do not share a B2B traversal pair with Hybrid Calling. Create a separate traversal pair between Expressway-C and Expressway-E if they are used for B2B and Hybrid Calling.

Step 1 From Expressway-E, go to **Configuration > Zones > Zones**, and then click **New**.

Step 2 Configure these settings:

Field	Value
Configuration	
Name	Webex hybrid traversal server
Type	Traversal server

Field	Value
Hop count	15 (Default)
Connection credentials	
Username	Enter traversal , for example.
Password	Go to Add/Edit Local authentication database , click New , enter traversal as the username, and then set a password. Click Create Credentials , and then close the window.
H.323	
Mode	Off
Protocol	Assent (Default)
Port	6006 (Default)
H.460.19 demultiplexing mode	Off (Default)
SIP	
Mode	On
Port	7004 or any value in 7XXX range. (This value must match the port number that is configured on Expressway-C.)
Transport	TLS
TLS verify mode	On
TLS verify subject name	Enter one of the Subject Alternative Names (SANs) of an Expressway-C certificate. For a cluster, enter at least a common SAN that is shared between all Expressway-C cluster peers.
Media encryption mode	Force encrypted
ICE support	Off (Default)
Multistream mode	On (Default)
SIP poison mode	Off (Default)
Preloaded SIP routes support	On
SIP parameter preservation	On Note This parameter must be set to On for all zones on all Expressways that are involved in call routing to and from the enterprise.

Step 3 Do not change settings under **Authentication** or **UDP/TCP Probes**.

Step 4 Click **Create zone**.

Create inbound and outbound search rules on Expressway-E

Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule. Create search rules on Expressway-E to:

- Identify calls from the Webex cloud and route down the traversal zone to Expressway-C.
- Identify calls from Unified Communications Manager and route through the DNS zone to Webex.

Before you begin

[Configure a secure traversal server zone from Expressway-E to Expressway-C, on page 34](#)

Step 1 From Expressway-E, go to **Configuration > Dial Plan > Search rules**, and then click **New**.

Step 2 Click **New**.

We're creating a rule to identify calls coming from Webex (through the DNS zone) and route them inwards (through the traversal zone) to Expressway-C.

Step 3 Configure the following settings:

Field	Value
Rule Name	Enter Webex Hybrid inbound calls , for example.
Description	Enter Route traffic from Webex Hybrid Cloud to UCM via Expressway-C , for example.
Priority	100 (Default)
Protocol	SIP
Source	Named
Source name	Webex hybrid DNS zone , for example. Choose the Webex DNS zone from the drop-down list.
Request must be authenticated	No (Default)
On successful match	Stop
Target	Webex hybrid traversal server , for example. Choose the traversal server zone (or Unified Communications traversal zone) that you modified in the previous section.
State	Enabled (Default)

Step 4 Click **Create search rule**.

Step 5 Click **New**.

We're creating a rule to identify calls coming from Unified Communications Manager (through the traversal zone) and route them outwards (through the DNS zone) to Webex.

Step 6 Configure the following settings:

Field	Value
Name	Enter Webex Hybrid outbound calls , for example.
Description	Enter Route traffic from Expressway-E to Webex Hybrid Cloud , for example.
Priority	100 (Default)
Protocol	SIP
Source	Named
Source name	Webex hybrid traversal server , for example. Choose the traversal server zone (or Unified Communications traversal zone) that you modified in the previous section.
Request must be authenticated	No (Default)
Mode	Alias pattern match
Pattern Type	Regex
Pattern string	. *@ . * \ . webex \ . com
Pattern behavior	Leave
On successful match	Stop (Default)
Target	Webex hybrid DNS zone , for example. Choose the Webex DNS zone from the drop-down list.
State	Enabled (Default)

Step 7 Click **Create search rule**.**What to do next**

[Configure a secure traversal client zone from Expressway-C to Expressway-E, on page 39](#)

Configure the Expressway-C for Hybrid Calling

Procedure

	Command or Action	Purpose
Step 1	Configure a secure traversal client zone from Expressway-C to Expressway-E, on page 39	Create a dedicated traversal client zone on Expressway-C. Though Webex traffic can coexist on the same traversal zone with MRA or B2B, we recommend that you create a dedicated traversal client zone on Expressway-C, specifically for handling Hybrid Calling signaling and media. That way, any settings for B2B or MRA won't affect Webex traffic, and the other direction won't be affected either.
Step 2	Create an Expressway-C neighbor zone for each Unified CM cluster, on page 40	<p>Configure neighbor zones for each Unified Communications Manager cluster to which you want to route:</p> <ul style="list-style-type: none"> • Each zone can accommodate 6 peer addresses, which supports a Unified Communications Manager cluster with 6 nodes. <p>If you need to connect to a Unified Communications Manager cluster with more nodes, you can configure an SRV record for that cluster and use Expressway-C to discover neighbor nodes by SRV lookup.</p> <ul style="list-style-type: none"> • This neighbor zone must route to a Unified Communications Manager home cluster—the zone can route to an SME if the SME is Unified CM 12.0(1). • The exact port to use for each zone depends on the SIP trunk security profile that you configured on Unified Communications Manager. If you have B2B or MRA configured, we recommend that you use 5561 for SIP TLS and 5560 for SIP TCP so that the new configuration doesn't interfere with your existing setup. • Do not reuse any existing neighbor zones to Unified Communications Manager for MRA.
Step 3	Configure search rules on Expressway-C (to Unified CM), on page 43	Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule. Configure search rules on Expressway-C to route calls to the correct Unified Communications Manager cluster based on the route header.

Configure a secure traversal client zone from Expressway-C to Expressway-E

Create a dedicated traversal client zone on Expressway-C. Though Webex traffic can coexist on the same traversal zone with MRA or B2B, we recommend that you create a dedicated traversal client zone on Expressway-C, specifically for handling Hybrid Calling signaling and media. That way, any settings for B2B or MRA won't affect Webex traffic, and the other direction won't be affected either.

Step 1 From Expressway-C, go to **Configuration > Zones > Zones**, and then click **New**.

Step 2 Configure these settings:

Field	Value
Configuration	
Name	Webex Hybrid traversal client (for example)
Type	Traversal client
Hop Count	15
Connection credentials	
Username	traversal
Password	Enter the password that you created on the Expressway-E for the traversal account.
H.323	
Mode	Off
SIP	
Mode	On
Port	7004 or any value in 7XXX range. (This value must match the port number that is configured on Expressway-E.)
Transport	TLS
TLS verify mode	On
Accept proxied registrations	Deny
Media encryption mode	Force encrypted
ICE support	Off
Multistream mode	On
SIP poison mode	Off
Preloaded SIP routes support	On (Enables this zone to process SIP INVITE requests that contain the route header.)

Field	Value
SIP parameter preservation	On Note This parameter needs to be set to On for all zones on all Expressways that are involved in call routing to and from the enterprise.
Authentication	
Authentication policy	Check credentials
Accept delegated credential checks	Off
Client settings	
Retry Interval	120
Location	
Peer 1-6 address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal server's certificate. IP addresses or hostnames are not recommended. If the traversal server is a cluster of VCS Expressways, enter the FQDN of each of the peers in that cluster.

Step 3 Click **Create Zone**.

Create an Expressway-C neighbor zone for each Unified CM cluster

Configure neighbor zones for each Unified Communications Manager cluster to which you want to route:

- Each zone can accommodate 6 peer addresses, which supports a Unified Communications Manager cluster with 6 nodes.
If you need to connect to a Unified Communications Manager cluster with more nodes, you can configure an SRV record for that cluster and use Expressway-C to discover neighbor nodes by SRV lookup.
- This neighbor zone must route to a Unified Communications Manager home cluster—the zone can route to an SME if the SME is Unified CM 12.0(1).
- The exact port to use for each zone depends on the SIP trunk security profile that you configured on Unified Communications Manager. If you have B2B or MRA configured, we recommend that you use 5561 for SIP TLS and 5560 for SIP TCP so that the new configuration doesn't interfere with your existing setup.
- Do not reuse any existing neighbor zones to Unified Communications Manager for MRA.

Step 1 From Expressway-C, go to **Configuration > Zones > Zones**, and then click **New**. Create a zone for each cluster.

Step 2 Configure these settings:

Field	Value
Configuration	
Name	UCM Neighbor for Webex (for example)
Type	Neighbor
Hop Count	15
H.323	
Mode	Off
SIP	
Mode	On
Port	Enter the Unified Communications Manager listening port number, such as 5561 . If MRA is deployed, standard 5060 and 5061 ports are used as line-side registration. The configured port (5561) must match the listening port configured in the Communications Manager SIP Trunk Security Profile. Ports 5060 and 5061 can be used if MRA is not enabled.
Transport	TCP is the default, but we recommend TLS for connecting Expressway-C to Unified CM. For a trunk that is enabled for SIP TLS, Unified CM does not need to be in mixed mode. If you want to use TLS, see “Connecting Expressway to Unified CM Using TLS” in the Cisco Expressway and CUCM via SIP Trunk Deployment Guide for your Expressway and Unified CM version.
TLS Verify Mode	On to verify the CallManager certificate for subsequent SIP communications.
Accept proxied registrations	Allow
Media encryption mode	Auto
ICE support	Off
Multistream mode	On
Preloaded SIP routes support	On
AES GCM support	On
Authentication	
Authentication policy	Do not check credentials
SIP authentication trust mode	Off
Location	

Create an Expressway-C neighbor zone for each Unified CM cluster

Field	Value
Look up peers by	<p>Address or Service record</p> <p>Choose Address if you want to enter up to 6 IP addresses, hostnames, or FQDNs of individual Unified CM nodes in the neighbor cluster.</p> <p>Choose Service record if you want Expressway to query DNS for an SRV record that resolves to the addresses of the nodes in the neighbor cluster.</p>
Peer 1-6 addresses	<p>If you chose to Lookup peers by Address, enter IP addresses or hostnames for each server in the 6 peer address fields.</p> <p>For TLS negotiation, the peer address must match the CN name that is used in the Unified CM certificates; otherwise, TLS negotiation fails.</p>
Service Domain	<p>If you chose to Lookup peers by Service Record, enter the domain to search for. Expressway will prepend the protocol and transport, then do the DNS query based on the other parameters in your neighbor zone configuration.</p> <p>For example, if SIP mode is On and TLS verify mode is on, then when you enter <code>example.com</code>, Expressway queries DNS for <code>_sips._tcp.example.com.</code></p>

Step 3 Configure these fields for the zone profile:

Field	Value
Advanced	
Zone profile	Custom , the zone profile to use for the supported version of Unified CM for Hybrid Call Service.
Monitor peer status	Yes
Call signaling routed mode	Always
Automatically respond to H.323 searches	Off
Automatically respond to SIP searches	Off
Send empty INVITE for interworked calls	On
SIP Parameter Preservation	<p>On</p> <p>Note This parameter needs to be set to On for all zones on all Expressways that are involved in call routing to and from the enterprise.</p>
SIP poison mode	Off
SIP encryption mode	Auto
SIP REFER mode	Forward

Field	Value
SIP multipart MIME strip mode	Off
SIP UPDATE strip mode	Off
Internetworking SIP search strategy	Options
SIP UDP/BFCP filter mode	Off
SIP UDP/IX filter mode	Off
SIP record route address type	IP
SIP Proxy-Require header strip list	Leave this field blank.

Step 4 Click **Create Zone**.

Configure search rules on Expressway-C (to Unified CM)

Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule. Configure search rules on Expressway-C to route calls to the correct Unified Communications Manager cluster based on the route header.

Before you begin

For the Expressway-E to Unified CM search rule, you need the cluster fully qualified domain name (FQDN) value that you configured in this procedure: [Configure Unified Communications Manager settings for Hybrid Calling, on page 24](#).

Step 1 Go to **Configuration > Dial plan > Search rules**.

Step 2 Click **New**.

We're going to create a rule to identify calls coming from the Expressway-E (through the traversal zone) and route them inwards (through the neighbor zone) to Unified Communications Manager.

You'll need a rule for each Unified CM cluster that is trunked to the Expressway-C.

Step 3 Configure the following settings:

Field	Value
Rule Name	From Webex Hybrid Cloud to Unified CM via Expressway-E , for example.
Description	Route traffic from Expressway-C to Unified CM , for example.
Priority	60
Protocol	SIP

Field	Value
Source	Named
Source name	Choose Webex Hybrid Traversal client .
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Prefix
Pattern string	cluster1.example.com , for example. This is the Cluster Fully Qualified Domain Name enterprise parameter value for the Unified Communications Manager cluster. Add the other cluster FQDNs (cluster2.example.com , cluster3.example.com , and so on) for the corresponding Unified Communications Manager neighbor zones that you need to create on the Expressway-C.
Pattern behavior	Leave (The alias is not modified.)
On successful match	Stop
Target	Choose the Unified Communications Manager neighbor zone—for example, UCM Neighbor for Webex . This setting will be different for each cluster; each cluster should have its own neighbor zone.

Step 4 Click **Create search rule**.

Step 5 Click **New**.

We're going to create one rule to identify any calls (by Webex devices) arriving at Expressway-C that are destined for Webex, and route them outwards (through the traversal client zone) to the Expressway-E.

Step 6 Configure the following settings:

Field	Value
Rule Name	From Unified CM to Webex Hybrid Cloud via Expressway-E , for example.
Description	Enter Route traffic from Unified CM to Expressway-E , for example.
Priority	70
Protocol	SIP
Source	Named
Source name	UCM Neighbor for Webex , for example.
Request must be authenticated	No
Mode	Alias pattern match

Field	Value
Pattern type	Regex (The string is treated as a regular expression.)
Pattern string	.+@.*\.(ciscopark) (rooms calls)\.webex)\.com).* Note We include this pattern string so that your deployment remains backwards compatible. If you're not sure if your Webex App users and Webex Devices have a webex.com SIP address, we recommend that you follow the directions in the Migrate Cisco Spark Hybrid Call Service Organization to the Cisco Webex Domain documentation to convert ciscopark.com domains over to webex.com.
Pattern behavior	Leave (The alias is not modified.)
On successful match	Stop
Target	Webex Hybrid traversal client
State	Enabled

Step 7 Click **Create search rule**.

Activate Hybrid Calling for your organization

Use this procedure to begin the initial setup for hybrid call connect in Control Hub. These settings ensure that hybrid call connect is first enabled for your organization before you do further configuration. You specify the desired subdomain for your company, and that setting creates Webex App SIP addresses to identify users in the Webex cloud. Then, you toggle on hybrid call connect for your organization. Last, you enter the SIP destination address which resolves to your Expressway-E in the call traversal pair. This entry is typically a DNS-SRV record which can resolve to multiple Expressway-Es.

Before you begin

- You must complete all prerequisites in the “Prepare your environment” chapter and all the required deployment steps in this chapter before you can activate Hybrid Calling. Otherwise, the **Call Service Connect** activation button is greyed out.
- If you have multiple Expressway-Es for redundancy, we recommend that you create a dedicated DNS-SRV record with a subdomain specifically for the mutual TLS port on Expressway-E. For Hybrid Calling, the secure mutual TLS connection is a requirement for the Expressway-E and cloud to trust each other.

Step 1 From the customer view in <https://admin.webex.com>, perform one of the follow steps:

- From the first-time setup wizard for a new organization, choose **Enterprise Settings**
- For an existing Webex organization, go to **Management > Organization Settings**, and then scroll to Webex SIP Address.

Step 2 Follow the on-screen instructions to configure a custom SIP subdomain for your organization.

This subdomain value creates individual Webex SIP addresses for each Webex device in the form *workspacename@example.rooms.webex.com*. The addresses are used to receive calls from any standards-based SIP calling service. See [Webex SIP addresses](#) for more information.

Step 3 Go to **Services > Hybrid**, and then click **Settings** on the Hybrid Call card.

Step 4 Scroll to **Call Service Connect**, and then click **Activate** to enable the service for your organization.

Tip At this point, you can view the prerequisites in Control Hub before activation to make sure your environment is ready.

Caution If the Connect activation button is not available, you missed necessary configuration. Make sure you start over and follow all the prerequisites in the Prepare Your Environment chapter and every deployment step in this chapter.

Step 5 Scroll to the **Default SIP Destination** field on the same page, and then enter a network value that resolves to your Expressway-E and the SIP mutual TLS port.

Enter a network value using one of these formats:

Address Format	Example Of Value to Enter (In Bold)
SRV domain	_sips._tcp.sipmtls.example.com
Hostname/FQDN:port	example.com:5062
IP address:port	203.0.113.0:5062

For multiple IP address entries, you must use the DNS SRV record method.

Tip The SRV record can take time to request. If you want to start a trial or pilot, you can use *hostname:port* for a single Expressway-E so that you can proceed with the setup steps. You can modify this setting later and use the SRV record when that becomes available.

Step 6 Click **Test** to run a tool that checks that it can connect to the Expressway-E SIP destination you entered.

The tool initiates a TLS connection to that address. The results indicate whether the Expressway-E is reachable and secure.

Note If you're a partner sales administrator, you can run this test on behalf of your customer.

Step 7 After the test shows the results, click **View test results** to get more details on what the test ran and the outcomes.

The results show the type of lookup (such as DNS SRV), FQDN, IP address, and the specific connection tests such as a socket connection, SSL handshake with the Expressway-E, and a SIP OPTIONS ping. If any tests fail, the tool shows suggested steps to troubleshoot the issue. See [Hybrid connectivity test tool \(Control Hub\)](#), on page 61 for more information.

Step 8 Save your changes.

Step 9 (Optional) If you have your own certificates, check **Upload your own certificate**, and then browse to and upload self-signed custom certificates that you want to use instead of the Webex default trust list.

For more information about manual certificate management, see [Custom certificates for mutual TLS authentication between Expressway-E and the cloud](#), on page 15.

Configure Workspace settings

Follow these tasks to configure the necessary Unified CM settings that are required for enabling Workspaces for Hybrid Calling.

Procedure

	Command or Action	Purpose
Step 1	Create a directory number and directory URI for Webex devices with Hybrid Calling, on page 47	Use Cisco Unified CM Administration to configure directory numbers that you want to later associate (through an end user account) with Webex devices. You'll also assign directory URIs to the directory numbers.
Step 2	Create a Unified CM account for Webex devices with Hybrid Calling, on page 48	Even though the Webex devices are registered to the cloud, you can associate a number to them from an on-premises Cisco Unified Communications Manager (Unified CM). You can use a Unified CM end user account to represent the Webex devices. The Workspace contains Webex-registered devices in a physical location.
Step 3	Create a Cisco Spark-RD for Webex devices with Hybrid Calling, on page 49	The Cisco Spark-RD is a virtual device that is attached to a Unified CM end user work number. The device links the Webex device to the enterprise SIP identity so that calls anchor on the Unified CM side.
Step 4	<p>Enable Hybrid Calling for Webex devices, on page 50 by following either or both these steps:</p> <ul style="list-style-type: none"> • Enable Hybrid Calling for a New or Existing Workspace With Webex Devices, on page 51 • Enable Hybrid Calling for Personal Mode Devices, on page 52 	You can use Control Hub to enable Hybrid Calling for Webex cloud-registered devices—both shared devices in workspaces and personal devices assigned to users.

Create a directory number and directory URI for Webex devices with Hybrid Calling

Use Cisco Unified CM Administration to configure directory numbers and directory URIs that you want to later associate (through an end user account) with Webex devices in a Workspace or in Personal Mode.

Before you begin

Workaround for directory URI dialing—If your users want to call a Hybrid Calling-enabled Webex device by using a directory URI from their Webex App or another device, we recommend that you create the directory URI to match the name of the Workspace in Control Hub. Then, the caller can enter the user portion of the directory URI and call the device based on directory name lookup.



Note This configuration works with devices that are in the same organization as the caller. The directory name lookup only matches devices and callers that are in the same organization.

Step 1 From Cisco Unified CM Administration, go to **Call Routing > Directory Number**, and then click **Add New**.

Step 2 For the Workspace, enter a dialable **Directory Number** and choose the **Route Partition** the number belongs to.

Step 3 In **Description**, **Alerting Name**, and **ASCII Alerting Name**, enter the name of the Workspace.

The Directory Number Alerting Name and ACSII Alerting Name can be no more than 30 characters in length. The names can only contain letters, numbers, spaces, and the following special characters: !#\$'()*+,-./:;=?@^_

Step 4 Choose a **Calling Search Space**.

A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.

Step 5 Click **Save**, enter an address in **Directory URI**, and click **Save** again.

Note Make sure the Directory URI matches the Directory URI on your end user. See the Before You Begin section for a recommendation.

Create a Unified CM account for Webex devices with Hybrid Calling

Even though the Webex devices are registered to the cloud, you can associate a number to them that comes from your Cisco Unified Communications Manager (Unified CM) environment. To tie the number to the device, you can use a Unified CM end user account to represent the Webex devices in a Workspace or in Personal Mode.

This account is not tied to a real user. Instead, the account stands in for the devices and provides a PSTN number or extension from the Unified CM dial pool to the devices in the Workspace or in Personal Mode.

When you manually run the Webex Device Connector, the configuration within the end user account is associated with the Webex device in a Workspace or in Personal Mode. The device obtains a directory number, directory URI, and Webex SIP address (the remote destination of the Cisco Spark-RD). Behind the scenes, the Cisco Spark-RD creates the link between the Webex device and the premises configuration.



Note You only need to run Webex Device Connector as and when you need to take an action, such as completing all required config on Unified CM and in the cloud, then needing to synchronize the two together.

Before you begin

- The email address domain must be one of your verified domain entries in Control Hub (<https://admin.webex.com>). See [Manage Domains](#).

-
- Step 1** From Cisco Unified CM Administration, go to **User Management > End Users**, and then choose one:
- Specify any search criteria, click **Find**, and then open the existing account that you want to represent a Workspace.
 - Click **Add New** to create a new account to represent a Workspace.
- Step 2** If creating a new account, enter a **User ID** and **Last name**.
- Because the account doesn't correspond to an actual user, you can enter values that identify the Workspace, such as a conference room location.
- Step 3** Verify that the account has a valid **Directory URI** that contains the same domain as your organization.
- The Directory URI for the user must match the Directory URI for the directory number that you created for the Workspace. The Directory URI is a linkage into more details from the Unified CM.
- Step 4** (Optional) If you want your users to see the external number of the Workspace on the devices, enter the **Telephone Number** as the full E.164 number.
- This number will show up on your hybrid-enabled Workspace. You could also use an internal number or extension. If you have multiple Webex devices in the Workspace, the same directory number is assigned to all of them, like shared lines. From a technical standpoint, a call to this number is sent to the assigned Webex SIP address, which Webex forks to all the Webex devices in the Workspace.
- Step 5** Verify that **Mail ID** contains a unique email address that you'll use for the Workspace.
- The email address must be an exact match between both Webex and on-premises. Use unique email accounts for each Workspace.
- Step 6** Under the service settings, check the **Home Cluster** checkbox.
- Configure this setting on the Cisco Unified Communications Manager where the account is homed.
- Step 7** (Optional) If the user account has a device in the controlled list, set the primary extension to a directory number. Choose one that you want to provide to the devices in the Workspace, and then save your changes.
- Note** For Cisco Spark-RD, do this step after you create the devices.
-

Create a Cisco Spark-RD for Webex devices with Hybrid Calling

The Cisco Spark-RD is a virtual device that is attached to a Unified CM end user work number. The device links the Webex device to the enterprise SIP identity so that calls anchor on the Unified CM side.



Note A Cisco Spark-RD must be 15 characters or less.

-
- Step 1** From Cisco Unified CM Administration, go to **Device > Phone**, click **Add New**, and then choose **Cisco Spark Remote Device**.
- Step 2** For **Owner User ID**, specify the user account for the Workspace that you are configuring.

The **Device Name** is automatically created after you choose the user account. If you see an error, you may have to manually shorten the device name.

- Step 3** For line association, specify the primary extension (the shared line).
- Step 4** Ensure that the partition used by the SIP route pattern is listed in the remote device's rerouting calling search space (CSS). The route from the remote device to the SIP trunk happens through the rerouting CSS.

Use these documents to understand the settings that the remote device uses:

- [Device pools](#)
- [Locations](#)
- [Calling search spaces](#)

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

- Step 5** Save your changes.
- Step 6** From Cisco Unified CM Administration, go to **User Management > End User**, and then reopen the user account for the Workspace.
- Step 7** Under Device Information, click **Device Association**.
- Step 8** Specify any search criteria and click **Find**.
- Step 9** Check the remote device that you created, and then save your changes.

The remote device is associated with the Workspace end user account and is added to the controlled devices list. The remote destination is added later when you run a sync from the Webex Device Connector tool. The tool synchronizes the Webex SIP address from the cloud and links it to the Cisco Spark-RD as the remote destination under **Associated Remote Destinations**.

- Step 10** If the user account has a device in the control list, set the primary extension to a directory number. Choose one that you want to provide to the devices in the Workspace, and then save your changes.

Enable Hybrid Calling for Webex devices

You can use Control Hub to enable Hybrid Calling for Webex cloud-registered devices—both shared devices in workspaces and personal devices assigned to users.

Procedure

	Command or Action	Purpose
Step 1	Enable Hybrid Calling for a New or Existing Workspace With Webex Devices, on page 51	You can set up shared Webex devices and add them to a Workspace, add services, and then watch the collaboration happen. Whatever device you choose to add to that Workspace, the device is assigned to the Workspace, not a user. The key advantage is shared usage.
Step 2	Enable Hybrid Calling for Personal Mode Devices, on page 52	Personal mode devices are Webex Room, Desk, or Board devices that are registered to the cloud but also assigned to

	Command or Action	Purpose
		a user in Control Hub. You can add Unified CM calling functionality by enabling Hybrid Calling for these devices.

Enable Hybrid Calling for a New or Existing Workspace With Webex Devices

When people are at work, they get together in lots of Workspaces like lunch rooms, lobbies, and conference rooms. You can set up shared Webex devices and add them to a Workspace, add services, and then watch the collaboration happen. Whatever device you choose to add to that Workspace, the device is assigned to the Workspace, not a user. The key advantage is shared usage.

Procedure

- To create a new Workspace, add a device, and enable Hybrid Calling:
 - a) From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, and then click **Add Workspace**.
 - b) Enter a name for the Workspace (such as the name of the physical room), specify other attributes (**Type**, **Capacity**, and **Avatar**), and then click **Next**.
 - c) Choose **Other Cisco device** (this option supports Webex cloud-registered devices and Hybrid Calling), and then click **Next**.

You can have a combination of devices in a single Workspace (for example, a single Webex Room Device or a Webex Board). You cannot have multiple instances of the same type of device in a Workspace (for example, 2 Webex Boards).

- d) Choose **Hybrid Calling** to use call service (PSTN access or internal extension access) through your on-premises Unified CM call control environment. Unified CM provides the phone number or extension for the devices in the Workspace. Then click **Next**.
 - e) Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration. The service discovers where the email address is located on a Unified CM cluster.
 - f) Click **Download** to get the Webex Device Connector software and choose the platform your system is running (Windows or Mac).
 - g) After you download and install the software, return to Control Hub and click **Done**.
 - h) Click **Next**, and then activate the device with the code provided.
- To enable Hybrid Calling for devices in an existing Workspace:
 - a) From the customer view in <https://admin.webex.com>, go to **Workspaces**, and then choose the Workspace that you want to update.
 - b) Next to **Calling**, click , and then choose **Hybrid Calling** to use call service (PSTN access or internal extension access) through your on-premises Unified CM call control environment. Unified CM provides the phone number or extension for the Webex devices in the Workspace. Then click **Next**.
 - c) Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration. The service discovers where the email address is located on a Unified CM cluster.
 - d) Click **Download** to get the Webex Device Connector software and choose the platform your system is running (Windows or Mac).
 - e) After you download and install the software, return to Control Hub and click **Done**.

Enable Hybrid Calling for Personal Mode Devices

Personal mode devices are Webex Room, Desk, or Board devices that are registered to the cloud but also assigned to a user in Control Hub. These devices share the same line that is assigned to the end user account in Unified CM. Once the required Unified CM configuration is in place, you can add Unified CM calling functionality by enabling Hybrid Calling for these devices.



Note Users can answer incoming calls on the device or desktop. If they answer on their desktop, there's no option to escalate to the device.

Before you begin

- Hybrid Calling must be enabled for your organization. Review the steps in “Retain Configuration for Hybrid Calling for Webex Devices” in the Prepare Your Environment chapter of this guide..
- The followed Unified CM configuration must be in place:
 - For each user that requires PSTN for their Personal Mode device, you must create an end user account (this can be a local Unified CM account) that is specific to the device and contains a mailID (this does not need to be an active email address) and directoryID that matches. If the device owner also uses Unified CM Calling in Webex App, that ID must be unique and separate from the end user account that is tied to the Webex App user.

Note the following example to understand the difference between the two accounts:

- *username@example.com* for the end user account associated with Webex App.
- *username.pstn@example.com* for the end user account associated with the personal mode device.
- A Cisco Spark-RD device that is associated with the end user's account for the personal mode device the directory number that the user uses in Webex App. Both accounts in Unified CM must be associated with the same directory number.

- [Assign a Personal Room or Desk Device to a User](#)



Note Users can also [Set Up a Webex Board, Room or Desk Device as a Personal Device](#).

Step 1 From the customer view in <https://admin.webex.com>, go to **Management > Devices**, and then choose a Webex device that you want to enable for Hybrid Calling.

Note The Webex device must have a **Type of Rooms & Desks** and have a user assigned to it in the **Belongs to** column.

Step 2 Scroll to **Calling**, and then click  **Calling** to open the Hybrid Calling configuration screen.

Step 3 Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration.

The service discovers where the email address is located on a Unified CM cluster.

- Step 4** Click **Download** to get the Webex Device Connector software and choose the platform your system is running (Windows or Mac).
- Step 5** After you download and install the software, return to Control Hub and click **Done**.
- Step 6** From Webex Device Connector, connect to the Unified CM using the AXL account.
- Step 7** Sync the new personal mode device.

Note You do not have to wait for all the devices to populate. You can synchronize the personal mode device as soon as you see it.

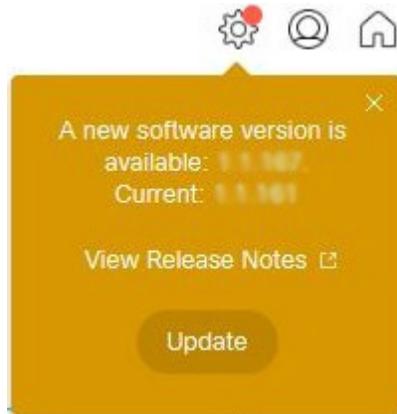
Install Webex Device Connector

You can get the Webex Device Connector software from Control Hub. After you install the software, you can use it to onboard devices in bulk or synchronize Unified CM configuration (dial plan, directory number, extension, and so on) to Webex devices that are in Workspaces enabled for Hybrid Calling.

- Step 1** From the customer view in <https://admin.webex.com>, go to **Management > Devices**, and then click **Resources**.
- Step 2** Scroll to **Tools**, click **Download**, and then choose **Download for Mac** or **Download for Windows**, depending on your platform.
- Step 3** Open the installer file and then choose one, depending on your platform:
- For Windows:
 - a. Click **Next**, check the box to accept the terms in the License Agreement, and then click **Next**.
 - b. Optionally, change the destination folder or leave the default, and then click **Next**.
 - c. Click **Install**, and then the setup wizard installs the software.
 - For Mac:
 - a. Read the introduction and then click **Continue**.
 - b. Click **Continue** and then click **Agree** to accept the software license.
 - c. Choose the disk where you want the software to be installed, and then click **Continue**.
 - d. Optionally, click **Change Install Location** if you want to install the software somewhere else; otherwise, click **Install**.
 - e. After the screen appears that says the software installed successfully, click **Close**.
-

What to do next

- You're ready to sign into the connector with your full or device admin credentials. You can then run the software manually to synchronize your devices. This step is only required once to sync the configuration changes.
- You're notified in the software whenever an upgrade is available. We recommend that you click **Update** to remain on the latest version of the software for bug fixes and security enhancements:



Synchronize device configuration changes with Webex Device Connector

Whenever you make changes to configuration on Unified CM (premises) or to Workspaces and Personal Mode devices in Control Hub (the cloud), you can run the Webex Device Connector to make sure the changes on both sides are synchronized and Webex devices continue to function properly with Hybrid Calling. The software synchronizes the SIP address, Workspace name, and device information into the cloud.



Note You only need to run Webex Device Connector as and when you need to take an action, such as completing all required config on Unified CM and in the cloud, then needing to synchronize the two together.

Before you begin

Make sure you download the software from Control Hub and install it on a supported Mac or Windows system.

-
- Step 1** Open the Webex Device Connector.
- Step 2** (Optional) Check **Remember Me** if you want the software to save your credentials so that you don't have to reenter them. After you check this box, we securely store the refresh token for the account locally on the machine. You can remove this token any time by signing out of the application or uninstalling the application.
- Step 3** Sign in with your full admin credentials (the same ones that you use for Control Hub).
- Step 4** Click **Hybrid Calling**, and then enter the following information to connect to the Unified CM:

- **Host**—Enter the IP address or FQDN of the Unified CM.
- **Username** and **Password**—Enter credentials for a Unified CM application account that is enabled for AXL.

Step 5 Click **Connect**.

The connector loads all of the Workspaces that are enabled for Hybrid Calling. For each Workspace, the connector finds a matching end user account (mail ID), directory number, and Cisco Spark-RD on Unified CM.

Step 6 Enter terms in the **Search for devices** field or use a filter (for example, **Ready to sync**) to limit the number of devices that appear in the results.

If you chose one filter but want to change to a different one, click X next to the filter name and then choose the new filter that you want to use.

Step 7 If the tool flags any mismatches in the premises and cloud configuration, resolve the configuration issue (typically in Cisco Unified CM Administration), return to the tool and click **Refresh List**. When you verify that the configuration issue is resolved, run a synchronization (click **Sync** next to one device or click **Sync All** for multiple devices) to match configuration on both sides.

- From cloud to Unified CM, the remote destination of the Cisco Spark-RD in Unified CM is automatically updated with any cloud Webex SIP address change.
- From Unified CM to cloud, relevant configuration (directory number, extension, home cluster, and so on) is associated with Webex devices in a Workspace.

Note For any configuration issues (for example, a matched user account but missing directory number), use the error messages in the tool to help you resolve configuration on Unified CM and then rerun a sync afterwards.

What to do next

If you need to synchronize changes on other Unified CM clusters, you can click **Connect to different Unified CM** and enter the host, username, and password for that Unified CM.

Known issues and limitations with Hybrid Calling for Webex devices

Workspaces

- When you configure Webex devices with Hybrid Call Service, you first configure a URI while creating your directory number. Then, when the Workspace is activated, a second URI is created and assigned to the directory number. The new URI is the same as the original, but in a different partition. The end result is that the directory number has two (almost identical) URIs configured in Unified CM.
- The Webex SIP address for Webex devices is generated from the Workspace name. If this name is changed after you enable the devices with Hybrid Call Service, the remote destination (the Webex SIP address) in the Cisco Spark-RD on Unified CM is not updated. You must rerun the Webex Device Connector to synchronize this cloud configuration change down to the Unified CM.
- Calling another Webex App device (with Hybrid Calling) by extension is not supported.

- Calling another Webex App device (with Hybrid Calling) by directory URI is not supported. Use the suggestion in [Create a directory number and directory URI for Webex devices with Hybrid Calling, on page 47](#) as a workaround.

For more information, see the [Loop Detection and Avoidance](#) section in the *Preferred Architecture for Cisco Webex Hybrid Services*.

- Whether the device has Hybrid Calling or not, calling a Webex App device by name or directory lookup is only supported within the same organization.

Personal Mode devices

- Enterprise directory URIs cannot be dialed from a Personal Mode device.

Mobile and Remote Access (MRA)

If you also have MRA deployed, see “Unsupported Expressway Features and Limitations” in the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* for your release at <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>.



CHAPTER 4

Manage and troubleshoot Hybrid Calling for Webex Devices

- [Rename a Workspace enabled for Hybrid Calling, on page 57](#)
- [Override the default SIP destination for a Workspace, on page 58](#)
- [Remove Hybrid Calling from Webex device, on page 59](#)
- [Deactivate Hybrid Calling for Webex Devices, on page 60](#)
- [Troubleshooting sources for Hybrid Calling, on page 60](#)
- [Webex status page, on page 62](#)
- [Mutual TLS and SIP destination, on page 62](#)
- [Expressway pair configuration, on page 63](#)
- [Unified CM configuration, on page 63](#)

Rename a Workspace enabled for Hybrid Calling

You can change the name of a Workspace that you configured with Hybrid Calling. This action updates the Webex SIP address, and further steps are required to synchronize the change on the premises. Use this procedure to change the name and verify the changes.

-
- Step 1** From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, and then choose a Workspace from the list to open the overview panel.
- Step 2** To the right of the Workspace name, click  **Edit**, enter the new name for the Workspace, and then click **Save**.
- Step 3** Under **Calling**, verify that the Webex SIP address is updated.

Override the default SIP destination for a Workspace

Workspaces

conf-room-2 Type: Not selected | Capacity: Not set | No devices

Calling

Hybrid Calling

⚠ This Workspace is not yet synchronized with the corresponding Cisco Unified Communications Manager configuration. Download and run the Webex Device Connector to synchronize.

Mail ID conf-room-2@example.com

Cisco Webex SIP Address conf-room-2@example.rooms.webex.com

Directory URI conf-room-2@example.com

Directory Number 19195550199

UCM FQDN(s) ucm1.example.com

Edit Hybrid Calling

Next, you must run the Webex Device Connector manually, so that these changes are replicated to Unified CM as the updated remote destination for each Cisco Spark-RD.

- Step 4** Open the Webex Device Connector, choose **Hybrid Calling**, and then sign into the Unified CM with an administration account with AXL permissions.
- Step 5** From the list, click **Sync** next to the devices to run the synchronization step and match the premises configuration to the cloud configuration.
- Step 6** Verify that the remote destinations were synchronized correctly from the cloud to the premises: From Cisco Unified CM Administration, go to **Device > Remote Destination**, choose **CTI Remote Device/Cisco Spark Remote Device** from the **Find destination where** drop down, and then click **Find**.

The results show each Cisco Spark-RD in your deployment and the remote destination (under **Destination Number**. If the name was updated correctly, the Cisco Spark-RD for the Workspace has a remote destination that starts with the new Workspace name that you saved in Control Hub.

Remote Destination (1 - 18 of 18)						
Name	Destination Number	Remote Destination Profile	Dual-Mode Phone	DNS-Integrated Mobile	CTI Remote Device/Cisco Spark Remote Device	
<input type="checkbox"/> Cisco_Spark_Client	place1@example.room.ciscospark.com					SparkRDplace1

Override the default SIP destination for a Workspace

After you add a default SIP destination for Hybrid Calling, you can add more SIP destinations to Workspaces in Control Hub. A single default SIP destination means that all of the hybrid call traffic goes through a single Expressway-E or DNS SRV entry. You may want to add more SIP destinations to override the default entry that you configure in Hybrid Call settings, so that you have more control over where the hybrid call traffic for Workspaces is routed.

Before you begin

[Recommendations for global Hybrid Calling deployments, on page 17](#)

Step 1 From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, and then search for and open the Workspace that you want to configure.

Step 2 Click **Edit Hybrid Calling**, choose **Configure a SIP Destination for the workspace**, and then enter a network value that resolves to your Expressway-E and the SIP mutual TLS port.

Enter a network value using one of these formats:

Address Format	Example Of Value to Enter (In Bold)
SRV domain	_sips._tcp.sipmtls.example.com
Hostname/FQDN:port	example.com:5062
IP address:port	203.0.113.0:5062

For multiple IP address entries, you must use the DNS SRV record method.

Tip The SRV record can take time to request. If you want to start a trial or pilot, you can use *hostname:port* for a single Expressway-E so that you can proceed with the setup steps. You can modify this setting later and use the SRV record when that becomes available.

Step 3 Click **Test** to run a tool in Control Hub that checks the connection to the Expressway-E SIP destination you entered.

The tool initiates a TLS connection to the SIP destination address. The results indicate whether the Expressway-E is reachable and secure.

Note If you're a partner sales administrator, you can run this test on behalf of your customer.

Step 4 After the test shows the results, click **View test results** to get more details on what the test ran and the outcomes.

The results show the type of lookup (such as DNS SRV), FQDN, IP address, and the specific connection tests such as a socket connection, SSL handshake with the Expressway-E, and a SIP OPTIONS ping. If any tests fail, the tool shows suggested steps to troubleshoot the issue. See [Hybrid connectivity test tool \(Control Hub\)](#), on page 61 for more information.

Step 5 Save your changes.

Remove Hybrid Calling from Webex device

Use this procedure to remove Hybrid Calling from a single workspace that contains a Webex device. This step converts a device in a Workspace to free calling (SIP calling) and disables Unified CM-based calling functionality.

Before you begin



Note This step affects individual Workspaces. If you want to remove Hybrid Calling from all enabled Workspaces in your organization, use the steps in [Deactivate Hybrid Calling for Webex Devices](#), on page 60

Step 1 From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, search for the Workspace enabled for Hybrid Calling, and then open it.

Step 2 Next to **Calling**, click , choose **Call on Webex (1:1 Call, Non-PSTN)** (default), and then click **Save**.

This step does not delete the Workspace in Control Hub or the Cisco Spark-RD in Unified CM. This step removes Hybrid Calling functionality from the Webex devices in the Workspace. Any devices in the remaining Workspace can still support the features that come with free calling, specifically SIP dialing and pairing to the Webex App. The Cisco Spark-RD remains on Unified CM; you must manually remove that device if you want to clean up that configuration.

Deactivate Hybrid Calling for Webex Devices

Use these steps to remove Hybrid Calling from all Webex devices in Workspaces in your Control Hub-managed organization. Deactivating the service does not remove the cloud-registered devices, but the step downgrades all devices to free calling (SIP calling) and disables Unified CM-based calling functionality.

Before you begin



Note This step affects all devices in a Workspace. If you only want to remove Hybrid Calling from individual devices, use the steps in [Remove Hybrid Calling from Webex device, on page 59](#).

Step 1 From the customer view in <https://admin.webex.com>, go to **Services > Hybrid**, and then click **Edit settings** from the Hybrid Call card.

Step 2 Scroll to **Deactivate Hybrid Call Service**, and then click **Deactivate**.

Step 3 Read the prompt that appears, and click **Deactivate** when you understand that the service is removed after this step.

Step 4 Go to **Workspaces**, open a few Workspace entries, and confirm that Hybrid Calling was removed.

Troubleshooting sources for Hybrid Calling

This section covers the various information sources and tools that you can use to troubleshoot your Hybrid Calling for Webex devices deployment.

If you go through the troubleshooting information in this chapter and are still having trouble, you can access more advanced troubleshooting steps in the [Troubleshooting Guide for Cisco Webex Hybrid Call Service](#). You can also access the known issues and limitation lists in this guide.

Hybrid connectivity test tool (Control Hub)

You can access the Hybrid connectivity test tool from Control Hub: from the customer view in <https://admin.webex.com>, go to **Services > Hybrid**, click **Edit settings** in the Hybrid Call card, scroll to **Default SIP Destination**, and then click **Test** next to the SIP destination that you entered.

This table lists common errors that may appear after you test a SIP destination address for Hybrid Calling. The table also provides some next steps for troubleshooting, including links to relevant details in the [Troubleshooting Guide for Hybrid Call Service](#).

Table 7: Common errors and troubleshooting steps for testing a SIP destination address for Hybrid Calling

Error	Keyword	More Information and Troubleshooting Steps
No DNS addresses found	DNS SRV	DNS Lookup failed. Check that a DNS or SRV record exists for your SIP Destination and that it resolves to one or more valid IP addresses. See Unable to resolve the Expressway-E DNS SRV/hostname in the troubleshooting guide for more information.
Connection timed out	Socket failure	Network and/or Mutual TLS connection timed out. Check network connectivity, connection speed, firewall configuration, and Mutual TLS configuration. See these sections of the troubleshooting guide for more information: <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062
TLS failure	Mutual TLS handshake failures	Mutual TLS Error: Check Mutual TLS configuration in both Expressway and https://admin.webex.com , and that Mutual TLS certificates are present and valid in both locations. See Mutual TLS Handshake Failures in the troubleshooting guide for more information.
Connect failure	Socket failure	TCP Connection failure: Check network connectivity, connection speed, and/or firewall configuration. See these sections of the troubleshooting guide for more information: <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062

Error	Keyword	More Information and Troubleshooting Steps
TCP read/write failure	Socket failure	<p>TCP read/write failure: Please try again. If the error persists, check network connectivity, firewall configuration, and Mutual TLS configuration.</p> <p>See these sections of the troubleshooting guide for more information:</p> <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062
TCP Failure	Socket failure	<p>TCP failure: TCP read/write failure: Please try again. If the error persists, check network connectivity, firewall configuration, and Mutual TLS configuration.</p> <p>See these sections of the troubleshooting guide for more information:</p> <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062

Webex status page

If calls from Webex to your enterprise are not ringing on the enterprise side, walk through the points in this checklist to double-check your configuration.

Before you walk through these troubleshooting suggestions, see <https://status.webex.com> for the latest information on any cloud outages. From that status page, you can also subscribe to notifications.

Mutual TLS and SIP destination

Check these troubleshooting points related to the mutual TLS connection and certificates:

- Install the Webex cloud root certificate bundle on the Expressway-E.
- Configure a dedicated mutual TLS port on the Expressway-E.
- Configure a DNS zone for the cloud on the Expressway-E.
- Open the mutual TLS port number in your firewall—5062, which may not be open by default.
- Determine which root certificate option you are using in the Webex cloud—The option is used to verify your Expressway-E's SIP TLS certificate.
 - Default store—Is your Expressway-E certificate signed by one of the public authorities? If you are unsure, use the custom store option.

- Custom store—Is your Expressway-E certificate or its signer installed in the cloud? Does the certificate contain verified Expressway-E hostnames?

From the customer view in <https://admin.webex.com>, go to **Services > Hybrid > Hybrid Call > Settings**. Check these points that are related to your SIP destination that you set during the deployment process:

- The value points at your Expressway-E dedicated mutual TLS port.
- Try to connect to the *IP address:port*. (Multiple addresses if you configured an SRV.)
- If you configured an IP address or hostname, specify the mutual TLS port.
- If you used an SRV, ensure it is in the format *_sips._tcp.<domain you put in as SIP Destination>*.
- If you do not want to set up an SRV, you can enter *IP address:port* or *hostname:port* as your organization's SIP destination.

Expressway pair configuration

- If calls from Expressway-E to the cloud are failing and you're using the manual certificate management method, make sure you follow the steps in [Webex Root CA Certificate Update](#) and upload the IdenTrust certificate to your Expressway devices as soon as possible.
- For calls that route from Webex toward the enterprise, check the search history and network logs on the Expressway-E. This step helps you isolate the problem to either the cloud or the enterprise.
- If you reuse an existing B2B zone and search rules, consider creating dedicated zones and search rules instead. This setup avoids interference with existing zone settings for B2B/MRA, avoids routing loops, and makes troubleshooting easier.
- Check the search history and network logs on the Expressway-E. Verify that the SIP INVITE from the cloud arrives at the Expressway-E and matches the DNS zone that you configured for the cloud.
 - If the SIP INVITE does not arrive or match the configured DNS zone, then follow the route of the call toward the Unified Communications Manager. This step helps you find where the call is failing or lost.
 - See the mutual TLS troubleshooting checklist.
- Check the route header. Verify that it contains the cluster fully qualified domain name (FQDN) value that is configured under Unified Communications Manager enterprise settings and in the Expressway search rules. See this example route header and highlighted cluster FQDN:
 - Route: <sip:[Obfuscated];transport=tls;lr>, <sip:myucmcluster.example.com;lr>
 - In this example, the home cluster FQDN is **myucmcluster.example.com**.

Unified CM configuration

- Emails in Unified Communications Manager must exactly match the email (synchronized from Active Directory or from any other source) in the Webex cloud.

- Directory URIs must match any domains that you verified in your organization.
- [Check your codec configuration.](#)

Webex services support the following codecs:

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



Note We support G.729 for joining a Webex meeting, Personal Room meeting, or Webex App meeting from a SIP device. We do not support G.729 for dialing 1:1 from Webex App to a SIP device or bridge.

- On the home Unified Communications Manager cluster of the affected users, choose **System > Enterprise Parameters**; under **Clusterwide Domain Configuration**, check the cluster fully qualified domain name (FQDN) setting. The FQDN value that you used must follow these guidelines:

FQDN Guideline	Description and Example
Multiple clusters	The entry must be unique for each cluster with Hybrid Calling—For example, <code>cluster1.example.com</code> , <code>cluster2.example.com</code> , and so on.
No wildcards	Do not use entries with wildcards, such as <code>*.example.com</code> or <code>example*.com</code> .
First FQDN entry for Hybrid Calling	In a list of multiple entries, the Webex cloud uses the first entry on the left for Hybrid Calling, and that first entry must not contain a wildcard. See this example of three FQDN entries from left to right (the first one being for Hybrid Calling): <code>cluster1.example.com</code> <code>*.example.com</code> <code>example*.com</code>
Different from Expressway-E	Must be different from the Expressway-E system, DNS, and domain name. Otherwise, Expressway-E strips the route header.
New entry for Hybrid Calling	If your current FQDN entry in Unified CM doesn't meet the requirements listed above, you can add a new element to the beginning of the cluster FQDN setting for Hybrid Calling. For example, if your existing FQDN setting in Cisco Unified Communications Manager is <code>*.example.com *.example.org</code> , add a unique, non-wildcard entry at the beginning of the field: <code>"cluster1.example.com *.example.com *.example.org"</code>