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: www.cisco.com/go/trademarks. 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)
CONTENTS

Full Cisco Trademarks with Software License  iii

PREFACE

New and Changed Information  ix

CHAPTER 1

Overview of Hybrid Calling  1
  Overview of Hybrid Calling  1
  Hybrid Calling Features  2
    Cisco Webex Teams Apps as Soft Clients  2
    Hybrid Calling for Cisco Webex Devices  2
  Hybrid Call Service Architecture  3
    Hybrid Call Service Architecture  3
    Hybrid Call Service for Cisco Webex Devices Architecture  3
    Global Hybrid Calling Architecture  4

CHAPTER 2

Prepare Your Environment  5
  Requirements for Hybrid Calling  5
    Cisco Webex Teams License Requirements  5
    Unified CM Device Requirements  5
    Cisco Call Control Solution Requirements  6
    Cisco Expressway Requirements  6
    Cisco Webex Teams App Requirements  7
    Network Requirements  7
  High Availability  8
    Custom Certificates for Mutual TLS Authentication between Expressway-E and the Cloud  8
  Complete the Prerequisites for Hybrid Calling  9
Deploy Hybrid Calling for Webex Teams Users

- Hybrid Calling Deployment Task Flow 19
- Register Expressway-C Connector Hosts to the Cisco Webex Cloud 24
  - Certificate Authorities for Hybrid Services 26
- Configure an Application Account for Call Connector 27
- Configure the Connection to Cisco Unified Communications Manager 27
- Start the Call Connector 28
- Verify the Connector Status 28
- Configure Cisco Unified Communications Manager Settings for Hybrid Calling 29
- Prepare Cisco Unified Communications Manager User Accounts for Hybrid Calling 33
- Configure Cisco Spark-RD Automatically from the Call Connector 34
- Manually Create a Cisco Spark-RD and Associate it with a Unified CM User 36
- Activate Hybrid Calling for Your Organization 37
- Add SIP Destinations to Hybrid Call Expressway Clusters 39
- Restart the Call Connector from the Expressway-C 40
- Check Your User Configuration for Cisco Webex Hybrid Call Service 41
- Configure the Expressway-E for Hybrid Calling 42
  - Update the Expressway-E Trust List with Cisco Webex Cloud Certificates 43
  - Configure Call Processing Language Rules on Expressway-E 43
  - Configure Services and Mutual TLS Authentication Between a New Expressway-E and the Cisco Webex Cloud 45
  - Configure Services and Mutual TLS Authentication Between an Existing Expressway-E and the Cisco Webex Cloud 47
- Create an Automatic Webex DNS Zone (Expressway-E to the Cisco Webex Cloud) 48
- Configure a Secure Traversal Server Zone from Expressway-E to Expressway-C 48
- Create Inbound and Outbound Search Rules on Expressway-E 50
- Configure the Expressway-C for Hybrid Calling 52
  - Configure a Secure Traversal Client Zone From Expressway-C to Expressway-E 53
Restart the Call Connector from the Expressway-C 87
Mutual TLS and SIP Destination 88
Test Calls 89
Cisco Webex Control Hub and Expressway-C Connector Hosts 89
Expressway Pair Configuration 90
Unified CM Configuration 91

APPENDIX A

Tool to Migrate CTI-RD to Cisco Spark-RD 93
Migrate CTI-RD to Cisco Spark-RD 93
Cancel Cisco Spark-RD Conversion 94
Last Run Statuses for Migration Tool 95
Troubleshoot CTI-RD to Cisco Spark-RD Migration 95

APPENDIX B

Bulk Configure Unified CM Users and Cisco Spark-RD for Hybrid Calling 99
Bulk Configure Unified CM Users and Cisco Spark-RD Task Flow 99
Export Your User List 100
Edit Your User List 101
Create the Remote Device File Format 101
Edit the New File Template 103
Create a Remote Device Template 103
Upload Your Remote Device Template File 104
Insert the Remote Device Entries 104
Check the Status of Your Bulk Job 105

APPENDIX C

Important Items for Hybrid Services Deployments 107
Important Items For Hybrid Services Deployments 107
TCP Port 5062 on the Internet Firewall 107
Why the Cloud Checks Domain Ownership 110
Supported Certificate Authorities 112
New and Changed Information

This table covers new features or functionality, changes to existing content, and any major errors that were fixed in the *Deployment Guide for Cisco Webex Hybrid Call Service*.

For information about call connector software updates, see the *Call Connector Release Notes*.

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 19, 2019</td>
<td>• Added a note to <em>Create a Directory Number for Cisco Webex Devices With Hybrid Calling</em>, on page 72, regarding the recommendation to match the directory URI to the name of the Place for the device: “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.”</td>
</tr>
</tbody>
</table>
| October 21, 2019   | • Updated the following sections with routing pattern changes to cover Webex (calling domains only) and Cisco Spark (backwards compatibility) and added references to the *Migrate Cisco Spark Hybrid Call Service Organization to the Cisco Webex Domain* documentation.  
  • Configure Cisco Unified Communications Manager Settings for Hybrid Calling, on page 29 (Updates to SIP route pattern configuration.)  
  • Configure Search Rules on Expressway-C (to Unified CM), on page 58 (Updates to search pattern string configuration.)  
  • Added the Standard CTI Enabled role as a requirement for the application account configuration for the Call Connector. |
| August 23, 2019    | In *Create a Directory Number for Cisco Webex Devices With Hybrid Calling*, on page 72, added the following note:  
  “If your users want to call a Hybrid Calling-enabled Webex device by using a directory URI from their Webex Teams app or another device, we recommend that you create the directory URI to match the name of the Place in Control Hub. Then, the caller can enter the user portion of the directory URI and call the device based on directory name lookup.” |
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 22, 2019</td>
<td>Added the following note to the feature overview section:</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> When deploying a new service for your users that connects your Unified CM calling environment with the cloud, we strongly encourage you to deploy Calling in Webex Teams (Unified CM). The newer service closely follows familiar Jabber deployment models where Webex Teams registers directly to Unified CM as a soft phone. No extra Expressway connector infrastructure nor firewall traversal capacity is required beyond what is needed for remote access (MRA). Hybrid Call Service is still the recommended deployment model for providing cloud-registered Webex video devices with a Unified CM directory number or extension.</td>
</tr>
</tbody>
</table>
| July 3, 2019 | • Removed the DNS zone configuration for Expressway-E. The minimum supported traversal pair is X8.11.4 and later, so the only viable option is the automatic Webex DNS Zone (which creates a preconfigured zone for Hybrid Call Service).  
• Removed references to unsupported Expressway versions. |
| June 6, 2019 | In the “Hybrid Call Service for Cisco Webex Devices” section of the Overview chapter, added the following update:  
  • **Call from Webex Teams while connected to the device**—From Webex Teams, users can also call phone numbers while connected to a cloud-registered Webex device that is enabled for Hybrid Call Service. They can call someone's mobile phone number or the local pizza place directly from Webex Teams and have the call take place on the Webex device. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
</table>
| March 4, 2019       | To reflect the Hybrid Calling simplification activities that were announced in [this article](#), the deployment guide has been updated and restructured. The following are high-level changes that were made to the guide:  
  • Normalized the service name to Hybrid Call Service, with the exception of specific UI references (for example, Call Service Aware in the Control Hub UI).  
  • Removed overview information on Call Service Aware.  
  • Removed the Aware prerequisites and deployment chapters. Added the relevant prerequisites and deployment steps to a single Hybrid Call Service deployment chapter.  
  • In various sections and diagrams, removed all references to CTI monitoring.  
  • Added call history behavior to the [Known Issues and Limitations with Hybrid Calling for Webex Teams Users](#), on page 63 section.  
  The following supported deployment information is also changed:  
  • The minimum supported version for Unified CM with Hybrid Calling is now 11.5(1)SU3 and later. You should upgrade your Unified CM clusters that are configured for Hybrid Calling as soon as possible.  
  • The minimum supported version of the Expressway pair is now X8.11.4. You should upgrade your traversal pair for Hybrid Calling as soon as possible. See “Important Information About Versions X8.9 through X8.11.3” in the [Release Notes for Expressway X8.11.4](#) for more information.  
  • Removed CTI-RD references and related content. The Cisco Spark-RD is now a required device type for a Hybrid Call Service deployment. |
<p>| November 16, 2018   | • In Cisco Spark-RD manual creation tasks (for users and places) and the known issues, added a note that a manually created Cisco Spark-RD must be 15 characters or less. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2, 2018</td>
<td>• Added a new procedure to the Hybrid Service for Cisco Webex Devices chapter: <strong>Rename a Place Enabled for Hybrid Calling</strong>, on page 80.</td>
</tr>
<tr>
<td></td>
<td>• Added information to the end of <strong>Create a Directory Number for Cisco Webex Devices With Hybrid Calling</strong>, on page 72:</td>
</tr>
<tr>
<td></td>
<td>“After you create a Place in Control Hub and add hybrid call service to the devices in it, 2 directory URIs are associated with the directory number for those devices: The one that was created manually and added to the line on Unified CM, and the one created as a result of the onboarding process (this one has the Directory URI partition assigned).”</td>
</tr>
<tr>
<td>Sept 24, 2018</td>
<td>Added the following new sections for the Global Call Service Connect deployment feature:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Global Hybrid Calling Architecture</strong>, on page 4 (An overview and architecture recommendations.)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add SIP Destinations to Hybrid Call Expressway Clusters</strong>, on page 39 (Creates the association between the DNS SRV entry and the call connector so that call routing resources closest to the caller are chosen.)</td>
</tr>
<tr>
<td></td>
<td>Updated the following existing sections for Global Call Service Connect:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete the Prerequisites for Hybrid Calling</strong>, on page 9 (Bullet point on Expressway-E/SIP destination guidelines.)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Register Expressway-C Connector Hosts to the Cisco Webex Cloud</strong>, on page 24 (Repeat steps to add any Expressway connector clusters for which you want SIP destinations.)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activate Hybrid Calling for Your Organization</strong>, on page 37 (Configure the Default SIP Destination, which is used whenever specific Expressway clusters don't have a SIP destination.)</td>
</tr>
<tr>
<td>Date</td>
<td>Changes Made</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>September 17, 2018</td>
<td>Made the following general updates:</td>
</tr>
<tr>
<td></td>
<td>- Added more details to the hunt group limitations statement in Known Issues and Limitations with Hybrid Calling for Webex Teams Users, on page 63.</td>
</tr>
<tr>
<td></td>
<td>- In Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 13:</td>
</tr>
<tr>
<td></td>
<td>- Added a note advising not to change the MAC address of the Expressway virtual machine, because the serial number is based on the MAC address.</td>
</tr>
<tr>
<td></td>
<td>- Added a note explaining how to enable H.323 mode if you do not have the UI menu on Expressway.</td>
</tr>
<tr>
<td></td>
<td>- Added more details to the “Could not find a Place with this Email Address”, “User is missing primary Directory Number”, and “Primary Directory URI Mismatch With Directory URI of Primary Line” sections in Errors and Causes for Hybrid Call Service for Cisco Webex Devices, on page 78</td>
</tr>
<tr>
<td></td>
<td>- Added clarity to the search rule statement in Requirements for Hybrid Calling for Cisco Webex Devices, on page 69.</td>
</tr>
<tr>
<td>August 16, 2018</td>
<td>- In Restart the Call Connector from the Expressway-C, on page 40, added that a connector restart is required after you perform a Unified CM upgrade to ensure that the cached information is in sync.</td>
</tr>
<tr>
<td>July 30, 2018</td>
<td>- Added Troubleshooting Sources for Hybrid Call Service, on page 83, which describes and links to information and tools that you can use to troubleshoot your hybrid call service deployment.</td>
</tr>
<tr>
<td></td>
<td>- Added new troubleshooting sections: Unable to Add Cisco Spark SIP Address in Unified CM, on page 86 and The User is Configured on More Than One Unified CM Cluster, on page 87.</td>
</tr>
<tr>
<td>Date</td>
<td>Changes Made</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>July 3, 2018</td>
<td>Added a new section, Create an Automatic Webex DNS Zone (Expressway-E to the Cisco Webex Cloud), on page 48, which covers new functionality in Expressway X8.11:</td>
</tr>
<tr>
<td></td>
<td>• X8.11 introduces a new &quot;Webex&quot; zone type—a DNS zone that is specifically designed for connecting to Cisco Webex. This feature simplifies the configuration of Cisco Webex Hybrid Call Service. You can create or delete one Webex zone, but you cannot modify it.</td>
</tr>
<tr>
<td></td>
<td>• The SRV connectivity tester is a network utility that tests whether the Expressway can connect to particular services on a given domain. You can use this tool to proactively test your connectivity while configuring Expressway-based solutions such as Hybrid Call Service.</td>
</tr>
</tbody>
</table>
Overview of Hybrid Calling

When deploying a new service for your users that connects your Unified CM calling environment with the cloud, we strongly encourage you to deploy Calling in Webex Teams (Unified CM). The newer service closely follows familiar Jabber deployment models where Webex Teams registers directly to Unified CM as a soft phone. No extra Expressway connector infrastructure nor firewall traversal capacity is required beyond what is needed for remote access (MRA). Hybrid Call Service is still the recommended deployment model for providing cloud-registered Webex video devices with a Unified CM directory number or extension.

With Hybrid Calling, you can get the capabilities of Cisco Webex services but also continue to use Cisco Unified Communications Manager, Business Edition 6000 or 7000, or a Cisco Powered™ cloud service from a certified Cisco Hosted Collaboration Solution partner for call control. Hybrid Calling integrates your call control so tightly with Cisco Webex Teams Message and Cisco Webex Meetings that your end users will never know they are not a single service. It connects the Cisco Webex cloud calls and the unified communications system so that they work together.

With Hybrid Calling, your users can

- Make calls from their desk phones or the Cisco Webex Teams app using the same dial plan
- Receive incoming calls in both their desk phones and the Cisco Webex Teams app and answer the call on either

Read on to understand the benefits of deploying the service and enabling it for your Webex Teams users.
Hybrid Calling Features

Cisco Webex Teams Apps as Soft Clients

Cisco Webex Teams apps can be used as desktop or mobile soft clients for voice and video calling and shares an extension with a user's Cisco desk phone. Users can answer calls on their desk phone or on a Cisco Webex Teams app, and use an app to make and receive calls as if they were in the office.

Users can use Cisco Webex Teams or their desk phone to call without worrying about which option they or the other person is using.

Related Topics

Deploy Hybrid Calling for Webex Teams Users, on page 19

Hybrid Calling for Cisco Webex Devices

Note

Hybrid Calling for Cisco Webex Devices with the Cisco Webex Device Connector is only available for organizations that reside in the European Union “geo-based” data centers. For more information, see Data Resiliency in Cisco Webex Teams for more information.

You can use Hybrid Calling for Cisco Webex Devices to provide hybrid call functionality for Room, Desk, and Cisco Webex Board devices that are added to Places in Control Hub. Cisco Webex devices are registered to the cloud, and when they are enabled with, they also connect to the enterprise. Cisco Webex devices in the Place 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 place 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 Teams while connected to the device—From Webex Teams, 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 Teams and have the call take place on the Webex device.

Related Topics

Deploy Hybrid Call Service for Cisco Webex Devices, on page 69

Hybrid Call Service Architecture

This section provides architecture diagrams. For more information about Cisco Validated Design, architecture, and call flows, see the Preferred Architecture for Hybrid Services, CVD documentation.
Hybrid Calling Architecture

Refer to this diagram which shows the components of Hybrid Calling architecture and where the connectors integrate the on-premises components with the cloud. The diagram includes Cisco Directory Connector for the use case of synchronizing Active Directory users in to Cisco Webex Control Hub to create Webex Teams accounts.

*Figure 1: Connector, On-Premises, and Cloud Components for Hybrid Calling*

Hybrid Call Service for Cisco Webex Devices Architecture

*Figure 2: Connector, On-Premises, and Cloud Components of Hybrid Call Service for Cisco Webex Devices*

This diagram shows the on-premises components that comprise the Hybrid Calling architecture. This architecture provides call connectivity to Cisco Webex cloud-registered devices in a place, so that these devices can use the Unified CM dial plan.
If you have a global deployment and use a single SIP destination for Hybrid Calling, traffic from Cisco Webex to enterprise goes through a single DNS SRV and can’t be routed to an Expressway cluster based on the location of the caller or called users. This causes media to hairpin through this node even if the caller and called users are on the other side of the world, causing potential latency.

With Multiple SIP Destinations for Hybrid Calling, when a call is made from Cisco Webex to the enterprise, Cisco Webex directs the call to an Expressway (SIP Destination) near the caller.

This deployment options provides the benefit of selecting the most appropriate downstream route for each call.

For more information, see Recommendations for Global Hybrid Calling Deployments, on page 12.
CHAPTER 2

Prepare Your Environment

- Requirements for Hybrid Calling, on page 5
- High Availability, on page 8
- Custom Certificates for Mutual TLS Authentication between Expressway-E and the Cloud, on page 8
- Complete the Prerequisites for Hybrid Calling, on page 9
- Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 13
- Cisco Spark Remote Device Overview and License Requirements, on page 17

Requirements for Hybrid Calling

Cisco Webex Teams License Requirements

To deploy Hybrid Call Service and provide its features to your users:

- You must have a Cisco Webex organization with a paid subscription.
- Cisco Webex Teams hybrid call users must be assigned a paid license that provides access to core Cisco Webex messaging and meeting services.
- The paid user licenses must not provide Cisco Webex hybrid call users access to a non-Unified CM-based calling service, such as Cisco Webex Calling (Formerly Spark Call).

Unified CM Device Requirements

Hybrid Call Service is supported only with Cisco SIP phones and Cisco Jabber clients that are registered to Unified CM.

SCCP phones may encounter problems due to the 48-character limitation on the destination address. Third-party IP phones and clients registered to Unified CM are not supported, neither are IP phones and clients registered to other call control servers (such as Cisco VCS/Expressway, Cisco Meraki, Microsoft Lync/Skype for Business, BroadSoft/BroadWorks).
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 Requirements

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

Cisco Expressway Requirements

You must deploy Expressway to host the connectors. Organizations using Cisco Hosted Collaboration Solution do not need Cisco Expressway on their premises. Instead, their Hosted Collaboration Solution partner will deploy it in the cloud as part of their Cisco Webex Hybrid Services offering.

Table 2: Cisco Expressway Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
X8.11.4 or later is required for Hybrid Calling. See the “Important Information” section in the Expressway Release Notes for more information.

This release provides added security and toll fraud mitigation. Hybrid Calling calls are classified the same as Mobile Remote Access (MRA), Business-To-Business (B2B) calls, and the calls traverse existing Expressway C and E pairs.

- Calls that include *.webex.com in the route path do not count towards the traversal license cost.
- Any B2B calls for a Cisco Webex Teams app after anchoring on the Cisco Spark-RD and then routing back out through the Expressways will consume traversal licenses.

Hybrid Calling follows existing MRA and B2B preferred architecture planning recommendations.

- Determine the total number of concurrent MRA, B2B, and Call Service Connect calls
- Deploy the appropriate number of Expressway E/C pairs
- There is no dedicated Expressway C or E required for Hybrid Calling traversal.

You can download the software image from software.cisco.com at no charge.

We recommend the latest released version of Expressway for connector host purposes. See Expressway Connector Host Support for Hybrid Services for more information about which versions are supported for new and existing registrations to the cloud.

### Cisco Webex Teams App Requirements

Cisco Webex hybrid call users must download the Cisco Webex Teams app for a supported platform from https://www.webex.com/downloads.html.

Hybrid Calling is supported on Cisco Webex Teams for Windows, Mac, and mobile (Android and iOS). The web client is not supported.

### Network Requirements

- Port access for HTTPS or secure web sockets outbound from Expressway to *.rackcdn.com, *.wbx2.com, *.webex.com, *.ciscospark.com, and *.clouddrive.com: TCP port 443 (secure)
- For AXL queries from Call Connector to Unified CM, TCP port 8443.
- Open the following ports for media traversal between phones, Expressways in the traversl pair, and the Cisco Webex cloud:
Table 3: Media Traversal Port Requirements for Hybrid Calling

<table>
<thead>
<tr>
<th>Client</th>
<th>Destination</th>
<th>Ports</th>
<th>Protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway traversal pair</td>
<td>Any</td>
<td>36000–59999</td>
<td>UDP</td>
<td>SIP media between phones and Expressways. Open these ports on the Expressways themselves.</td>
</tr>
<tr>
<td>Cisco Webex Teams app</td>
<td>Any*</td>
<td>33434–33598</td>
<td>TCP/UDP</td>
<td>Cisco Webex Hybrid Services media.</td>
</tr>
</tbody>
</table>

* If you want to restrict by IP addresses, see the IP address ranges that are documented in Webex Teams IP subnets for media.

Other Network Requirements

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

- Network Requirements for Cisco Webex
- Network Requirements for Webex Teams Services

High Availability

For Hybrid Call, if each cluster contains at least two nodes, the cluster has high availability by default. The total number of onboarded users is affected by high availability. On each connector host in a cluster, a different user number is shown. Take the sum total and divide it by two to get an accurate total of your users. You can also verify this total in Cisco Webex Control Hub (https://admin.webex.com) by choosing the applicable cluster under Services > All Resources > View all.

For more information about how each Expressway-based Hybrid Service ensures continuous service to users, see User Capacity Limits for Expressway-Based Hybrid Services.

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 Cisco 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 Call > 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 Cisco 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 Call > 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 Cisco Webex cloud cannot verify whether the certificate was revoked.

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

Related Topics

Add, Verify, and Claim Domains
Supported Certificate Authorities for Cisco Webex

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 and activation of your Cisco Webex Teams users.

Procedure

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 Cisco Webex for more information.

• 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 Cisco Webex organization.

See Why the Cloud Checks Domain Ownership, on page 110 to understand why domain checks are an important security measure.

• Install or upgrade to a supported version of Cisco Unified Communications Manager, as described in Requirements for Hybrid Calling, on page 5

• Prepare your Expressway-Es (default SIP Destination and cluster-specific SIP destinations for each location) for the secure mutual TLS connection between Cisco Webex and your call control environment:

  • 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.
In a global Hybrid Calling scenario, you'll need one SRV record for each location (see Recommendations for Global Hybrid Calling Deployments, on page 12 for deployment options and accompanying diagrams). Note these guidelines for the SIP destinations.

- 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 107 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 5. Use the recommended version for all Expressways that are handling SIP calls to take full advantage of Hybrid Calling.
  - For a global Hybrid Calling deployment, you must deploy one Expressway pair per location. See Recommendations for Global Hybrid Calling Deployments, on page 12 for deployment options and accompanying diagrams.

The Call Connector can run on a standalone or shared Expressway-C connector host, not the C or E in the Expressway pair. See Expressway Connector Host Support for Hybrid Services for the minimum supported version and User Capacity Limits for Expressway-based Hybrid Services for capacity planning guidelines.

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 Cisco Unified Communications Manager requirements:

- Install or upgrade your Cisco Unified Communications Manager to the minimum version that supports Cisco Spark-RD, as described in Requirements for Hybrid Calling, on page 5.
- Prepare your licensing. (See Cisco Spark Remote Device Overview and License Requirements, on page 17)
- 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 multicluste deployments.
  - Intercluster lookup service (ILS) routing for multicluste and business-to-business deployments.
- Check your codec configuration.

Cisco 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 Cisco Webex meeting from a SIP device. We do not support G.729 when a user dials 1:1 from Cisco 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 Cisco Webex Teams users 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 Cisco Webex cloud), as covered in the Network Requirements, on page 7.

Step 4 For all existing SIP trunks between Cisco 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.

Step 7 (Optional) Download the latest Cisco Directory Connector software from Cisco Webex Control Hub (https://admin.webex.com) and use it to import user attributes from your Active Directory:
  - Enterprise work phone numbers
  - Email addresses—These values must match the user's Cisco Webex Teams user email address.

For more information about how to use Cisco Directory Connector, see the Deployment Guide for Cisco Directory Connector.

Things to Keep in Mind

To support user-friendly mobile and web dial plans, Cisco Webex performs digit manipulation for US and Canadian locales before sending the dialed digit to enterprise call control. Cisco Webex transforms a national PSTN number (for example, convert (214) 555-2121 into +12145552121), but does not transform a private extension number. A valid national number is converted to E.164 format for Cisco Webex Teams users that are based in the US or Canada. For other locales, a minimal conversion takes place that removes everything but digits and the symbols +, *, and #. See the Dial Plans chapter in the Cisco Collaboration System Solution Reference Network Designs (SRND) guide for information about the role of dial plans and digit manipulation.
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 associated with each Call Connector cluster 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.
- The local Call Connector pulls in users from local Unified CM and searches for a user for calls outbound from the cloud across all connectors.

*Figure 3: Cloud, On-Premises, and Connector Components for Multiple SIP Destinations and Distributed Unified CM Call Control for a Hybrid Calling Deployment*

**Centralized Unified CM Call Control**

See the following diagram for an example of a global deployment with SIP destinations associated with each Call Connector cluster and a centralized Unified CM call control solution. If you are designing this architecture, we recommend that you deploy dedicated Hybrid Connector Expressways with Call Connector for each geography or site.

---

**Note**

Deploy all Expressway connector hosts at the same site as the centralized Unified CM cluster to minimize AXL latency.

**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.

• Call Connector clusters are dedicated to each location.

Figure 4: Cloud, On-Premises, and Connector Components for Multiple SIP Destinations and Centralized Unified CM Call Control for a Hybrid Calling Deployment

Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services

Use this checklist to prepare an Expressway-C for Cisco Webex Hybrid Services, before you register it to the Cisco Webex cloud to host hybrid services connector software.

Before you begin

We recommend that the Expressway-C be dedicated to hosting connectors for Cisco Webex Hybrid Services. You can use the Expressway-C connector host for other purposes, but that can change the supported number of users.

See User Capacity Limits for Expressway-based Hybrid Services so that you can plan your deployment accordingly.

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

**Step 1** Obtain full organization administrator rights before you register any Expressways, and use these credentials when you access the customer view in Cisco Webex Control Hub (https://admin.webex.com).

**Step 2** Plan your connector capacity by referring to User Capacity Limits for Expressway-based Hybrid Services.

**Step 3** Deploy the Expressway-C connector host in a cluster to account for redundancy. Follow the supported Expressway scalability recommendations:

- For Hybrid Call Service on a dedicated Expressway-C:
  - Call Connector supports multiple Expressway-C clusters with no specific upper limit.
  - Each cluster supports up to 6 Expressway-C nodes for active/active redundancy.

Hybrid Calling is highly available if Unified CM and Cisco Expressways are deployed in a cluster. The same guidelines apply for the Expressway-C connector host clustering. For more information, see User Capacity Limits for Expressway-Based Hybrid Services.

**Step 4** Follow these requirements for the Expressway-C connector host.

- Install the minimum supported Expressway software version. See the version support statement for more information.
- Install the virtual Expressway OVA file according to the Cisco Expressway Virtual Machine Installation Guide, after which you can access the user interface by browsing to its IP address. You can find the document in the list of Cisco Expressway Install and Upgrade Guides on cisco.com.

  **Note** The serial number of a virtual Expressway is based on the virtual machine’s MAC address. The serial number is used to validate Expressway licenses and to identify Expressways that are registered to the Cisco Webex cloud. **Do not change the MAC address of the Expressway virtual machine when using VMware tools, or you risk losing service.**

- You do not require a release key, or an Expressway series key, to use the virtual Expressway-C for Cisco Webex Hybrid Services. You may see an alarm about the release key. You can acknowledge it to remove it from the interface.
- Use the Expressway web interface in a supported browser. (See the Cisco Expressway Administrator Guide.) The interface may or may not work in unsupported browsers. You must enable JavaScript and cookies to use the Expressway web interface.

**Step 5** If this is your first time running Expressway, you get a first-time setup wizard to help you configure it for Cisco Webex Hybrid Services.

Select **Cisco Webex Hybrid Services**. This ensures that you will not require a release key.

**Step 6** Check that the following requirements are met for the Expressway-C connector host. You would normally do this during installation. See the Cisco Expressway Basic Configuration Deployment Guide, in the list of Cisco Expressway Configuration Guides on cisco.com, for details.

- Basic IP configuration (**System > Network interfaces > IP**)
- System name (**System > Administration settings**)
- DNS settings (**System > DNS**)
- NTP settings (**System > Time**)
Prepare Your Environment

Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services

- New password for admin account (Users > Administrator accounts, click Admin user then Change password link)
- New password for root account (Log on to CLI as root and run the passwd command)

**Note**  
Expressway-C connector hosts do not support dual NIC deployments.

**Step 7**  
Configure the Expressway-C as a "cluster of one":

- We recommend that you configure the Expressway as a primary peer before you register it, even if you do not currently intend to install an extra peer.

**Caution**  
When you change clustering settings on X8.11 and later, be aware that removing all peer addresses from the System > Clustering page signals to the Expressway that you want to remove it from the cluster. **This causes the Expressway to factory reset itself on its next restart.** If you want to remove all peers but keep configuration on the remaining Expressway, leave its address on the clustering page and make it the primary in a "cluster of one".

- Here are the minimum clustering settings required, but the Cisco Expressway Cluster Creation and Maintenance Deployment Guide has more detail:
  
    H.323 mode is required for clustering, even if the Expressway does not process H.323 calls.
  
  **Note**  
  You may not see the H.323 menu item if you used the Service Select wizard to configure the Expressway for Hybrid Services. You can work around this problem by signing into the Expressway console and issuing the command `xconfig H323 Mode: "On"`.  

  - System > Clustering > Cluster name should be an FQDN.
  
    Typically this FQDN is mapped by an SRV record in DNS that resolves to A/AAAA records for the cluster peers.

  - System > Clustering > Configuration primary should be 1.

  - System > Clustering > TLS verification mode should be Permissive, at least until you add a second peer.
  
    Select Enforce if you want cluster peers to validate each others' certificates before allowing intercluster communications.

  - System > Clustering > Cluster IP version should match the type of IP address of this Expressway-C.

  - System > Clustering > Peer 1 address should be the IP address or FQDN of this Expressway
  
    Each peer FQDN must match that Expressway's certificate if you are enforcing TLS verification.

  **Caution**  
  To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Expressway-C. Capitalization is not supported at this time.

**Step 8**  
If you have not already done so, open required ports on your firewall.

- All traffic between Expressway-C and the Cisco Webex cloud is HTTPS or secure web sockets.
- TCP port 443 must be open outbound from the Expressway-C. See [https://collaborationhelp.cisco.com/article/WBX000028782](https://collaborationhelp.cisco.com/article/WBX000028782) for details of the cloud domains that are requested by the Expressway-C.
Step 9  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. The Expressway 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.

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

Note  The details of the proxy, as configured on the primary Expressway in the connector host cluster, are shared throughout the Expressway cluster. You cannot configure different proxies for different nodes in the cluster.

Step 10  Review these points about certificate trust. You can choose the type of secure connection when you begin the main setup steps.

- Cisco Webex Hybrid Services requires a secure connection between Expressway-C and Cisco Webex.

You can let Cisco Webex manage the root CA certificates for you. However, if you choose to manage them yourself, be aware of certificate authorities and trust chains; you must also be authorized to make changes to the Expressway-C trust list.

Management Connector

The Management Connector is included in the Expressway-C base. You use it to register an Expressway to the cloud and link the Expressway interface with Cisco Webex Control Hub. The Management Connector plays an important role as the coordinator of all connectors running on the Expressway server or cluster: It provides you with a single point of control for connector activities. The Management Connector enables cloud-based management of the on-premises connectors, handles initial registration with the cloud, manages the connector software lifecycle, and provides status and alarms.

For an HTTPS connection to be established between the Management Connector and the cloud, you must update the trust list on the Expressway-C connector host with certificates that were signed by certificate authorities in use by the Cisco Webex cloud. You can allow the Cisco Webex cloud to upload CA certificates to the Expressway-C trust store. Or, in the case where security policies prevent the Cisco Webex cloud from uploading trusted certificate authority certificates on Expressway-C, you may upload them manually.

Call Connector

The Call Connector is the on-premises component Hybrid Call Service. The connector runs on a dedicated or shared Expressway-C connector host that you register to the Cisco Webex cloud.

Hybrid Call Service use the Call Connector software that runs as a module within Cisco Expressway. Call Connector uses AXL APIs to discover user devices configured in Cisco call control.

Call Connector also creates or updates a virtual remote device that represents Cisco Webex within Cisco call control. Hybrid Call Service uses this remote device to extend calls to Webex Teams, and to allow calls from Webex Teams to be identified with the calling user. In addition, Hybrid Call Service requires a Cisco
Expressway firewall traversal solution to enable these calls between Webex Teams and your existing call control.

---

**Note**

SIP traffic to and from the cloud is not routed to the same Expressway-C on which Call Connector runs. The Call Connector provisions aspects of users and their devices, but does not handle the calls themselves.

The Call Connector acts like a broker between the cloud and your on-premises call control environment (Cisco Unified Communications Manager, Business Edition 6000/7000, or Hosted Collaboration Solution). The connector establishes a secure connection and, in addition to securely connecting your on-premises environment to the cloud, the connector is used to:

- Discover users’ telephony devices and associated settings.
- Provide active/active redundancy if you configure the connector on a second Expressway-C.
- Provide automatic load balancing of users across different Expressway-C connector clusters (1 cluster with 2 nodes)—no manual administration is required.
- Retrieve users’ Directory URIs from Cisco Unified Communications Manager and makes them available to Cisco Webex for reaching users.
- Automatically create Cisco Spark Remote Device (Cisco Spark-RD) with a basic configuration for each user enabled for Hybrid Calling.
- Configure a user's Cisco Spark-RD with a Webex SIP address automatically created as the remote destination (for Hybrid Calling).
- Builds a table that the user directory URIs to cluster fully qualified domain names (FQDN) in a multi-cluster scenario.
- Does a lookup to add the correct route header information to the SIP message.

---

**Cisco Spark Remote Device Overview and License Requirements**

To activate Cisco Webex Hybrid Calling for a user, you must create a virtual device for that user in Unified CM. The device ties in with the user's remote destination so that incoming calls are forked to both Webex Teams and the user's main device. Outgoing calls can be made from the app as if from the user's desk phone, too.

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 (Cisco 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

A standalone Cisco Spark-RD uses one Enhanced UCL. If a user has any other UC device that requires an Enhanced UCL, then Cisco Spark-RD does not count towards the license total.
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**

<table>
<thead>
<tr>
<th>Device</th>
<th>License Requirement for Unified CM or HCS</th>
</tr>
</thead>
</table>
| Cisco Spark-RD alone | • Enhanced UCL for Unified CM  
• HCS Foundation |
| Cisco Spark-RD plus desk phone | • Enhanced UCL for Unified CM—A Basic UCL must be upgraded to Enhanced UCL.  
• HCS Foundation |
| Cisco Spark-RD plus 2 desk phones | • Enhanced Plus UCL for Unified CM  
• HCS Standard |
| Cisco Spark-RD plus Hybrid Call for Cisco Webex (Room, Desk, and Board) Devices in a Place | Enhanced UCL—For a newly deployed system, this license must be provided.  
For a Webex device that is converted from Unified CM-registered to Cisco Webex-registered, its existing Unified CM license is sufficient. |
CHAPTER 3

Deploy Hybrid Calling for Webex Teams Users

- Hybrid Calling Deployment Task Flow, on page 19
- Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 24
- Configure an Application Account for Call Connector, on page 27
- Configure the Connection to Cisco Unified Communications Manager, on page 27
- Start the Call Connector, on page 28
- Verify the Connector Status, on page 28
- Configure Cisco Unified Communications Manager Settings for Hybrid Calling, on page 29
- Prepare Cisco Unified Communications Manager User Accounts for Hybrid Calling, on page 33
- Configure Cisco Spark-RD Automatically from the Call Connector, on page 34
- Manually Create a Cisco Spark-RD and Associate it with a Unified CM User, on page 36
- Activate Hybrid Calling for Your Organization, on page 37
- Add SIP Destinations to Hybrid Call Expressway Clusters, on page 39
- Restart the Call Connector from the Expressway-C, on page 40
- Check Your User Configuration for Cisco Webex Hybrid Call Service, on page 41
- Configure the Expressway-E for Hybrid Calling, on page 42
- Configure the Expressway-C for Hybrid Calling, on page 52
- Enable Hybrid Calling for Cisco Webex Teams Users, on page 60
- Test the Softphone Functionality for Hybrid Calling, on page 62
- Known Issues and Limitations with Hybrid Calling for Webex Teams Users, on page 63
- Deactivate Hybrid Calling For Your Organization, on page 66
- Related Documentation, on page 67

Hybrid Calling Deployment Task Flow

With Hybrid Calling deployed in your organization and enabled for your Webex Teams users, you get the following feature set:

- Cisco Webex Teams Apps as Soft Clients, on page 2
- Hybrid Calling for Cisco Webex Devices, on page 2 (Further steps are required in Deploy Hybrid Call Service for Cisco Webex Devices, on page 69)
Before you begin

Complete the Prerequisites for Hybrid Calling, on page 9

After you've verified the prerequisites are met, you must perform all of the required configuration in this chapter, including Aware and Connect activation for users. Connect is the required activation state and Aware no longer supports any user features. These features may still work between Connect and Aware users, but are not supported and may stop working without advanced notice.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** Add and Verify Domains | 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 users in sales.example.com and support.example.com, you must add both domains.

If your organization enforces email addresses, you are presented with warnings about possible user 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** Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 24 | Cisco Webex Hybrid Services use software connectors to securely connect the Cisco Webex service to your organization's environment. Use Cisco Webex Control Hub to register your Expressway-C to the cloud. After you complete the registration steps, the connector software is automatically deployed on your on-premises Expressway-C (the software connector host). |

| **Step 3** Configure an Application Account for Call Connector, on page 27 | Configure an administrator account with the required AXL access permissions. Call Connector uses this account to communicate with Cisco Unified Communications Manager, monitor any user's phone, and validate user configuration. |

| **Step 4** Configure the Connection to Cisco Unified Communications Manager, on page 27 | Before you can enable Hybrid Calling, you must link Call Connector to your Cisco Unified |


### Hybrid Calling Deployment Task Flow

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Start the Call Connector, on page 28&lt;br&gt;Manually enable the Call Connector after you register your Expressway-C for Cisco Webex Hybrid Services.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Verify the Connector Status, on page 28&lt;br&gt;Ensure that you correctly installed the Call Connector by viewing the status on the Expressway.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Configure Cisco Unified Communications Manager Settings for Hybrid Calling, on page 29&lt;br&gt;Configure Cisco 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.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Perform one of the following tasks:&lt;br&gt;• Prepare Cisco Unified Communications Manager User Accounts for Hybrid Calling, on page 33 for individual user configuration.&lt;br&gt;• Bulk Configure Unified CM Users and Cisco Spark-RD Task Flow, on page 99 for bulk user and Cisco Spark Remote Device configuration using the Bulk Administration Tool.&lt;br&gt;Configure Unified CM users so that their corresponding Cisco Webex Teams accounts in the cloud are activated with the correct call settings. Call Connector creates the remote destination on the user's Cisco Spark Remote Device after all the Unified CM settings are properly configured.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Perform one of the following tasks:&lt;br&gt;• Configure Cisco Spark-RD Automatically from the Call Connector, on page 34&lt;br&gt;• Manually Create a Cisco Spark-RD and Associate it with a Unified CM User, on page 36&lt;br&gt;Every Hybrid Calling user requires a virtual device called a Cisco Spark Remote Device (Cisco Spark-RD). This virtual device is attached to a user's work number and links the user's Cisco Webex Teams account SIP identity to the enterprise SIP identity so that calls anchor on the Unified CM side or fork to the Cisco Webex cloud side. From a technical standpoint, the Cisco Spark-RD masks outbound calls from Cisco Webex and displays the user's work number for calls from the Cisco Webex Teams app. Incoming calls also ring both the user's Cisco Webex Teams app and desk phone.</td>
</tr>
<tr>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>To automate your configuration, on the Expressway-C connector host you can create Cisco Spark-RD for all your users in one step. The connector shows the remote device field values from your Cisco Unified Communications Manager, and then you can choose the values specific to your deployment. After the connector creates Cisco Spark-RDs, they are automatically moved to the users' control lists and their Cisco Webex SIP addresses are automatically created as remote destinations.</td>
<td><strong>Step 10</strong> Activate Hybrid Calling for Your Organization, on page 37 Use this procedure to begin the initial setup for Hybrid Call Service Connect in Cisco Webex Control Hub. These settings ensure that Hybrid Call Service Connect is first enabled for your organization before you do further configuration. You specify the desired subdomain for your company, and that setting creates Cisco Webex SIP addresses to identify users in the Cisco Webex cloud. Then, you toggle on Hybrid Call Service 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.</td>
</tr>
<tr>
<td>After you add a default SIP destination for Hybrid Call Service Connect, you can add more SIP destinations to specific hybrid call resources in Cisco Webex Control Hub. A single 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 and override the default entry so that you have more control over where the hybrid call traffic is routed.</td>
<td><strong>Step 11</strong> Add SIP Destinations to Hybrid Call Expressway Clusters, on page 39</td>
</tr>
</tbody>
</table>
| 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 12** Configure the Expressway-E for Hybrid Calling, on page 42 by following these tasks:  
- Update the Expressway-E Trust List with Cisco Webex Cloud Certificates, on page 43  
- Choose one depending on your deployment:  
  - Configure Services and Mutual TLS Authentication Between a New |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway-E and the Cisco Webex Cloud, on page 45</td>
<td>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.</td>
</tr>
<tr>
<td>• Configure Services and Mutual TLS Authentication Between an Existing Expressway-E and the Cisco Webex Cloud, on page 47</td>
<td></td>
</tr>
<tr>
<td>• Create an Automatic Webex DNS Zone (Expressway-E to the Cisco Webex Cloud), on page 48</td>
<td></td>
</tr>
<tr>
<td>• Configure a Secure Traversal Server Zone from Expressway-E to Expressway-C, on page 48</td>
<td></td>
</tr>
<tr>
<td>• Create Inbound and Outbound Search Rules on Expressway-E, on page 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> Configure the Expressway-C for Hybrid Calling, on page 52 by following these tasks:</td>
<td>Enable Hybrid Call Service Connect for your users in Cisco Webex Control Hub—you can enable the service for individual users or in bulk.</td>
</tr>
<tr>
<td>• Configure a Secure Traversal Client Zone From Expressway-C to Expressway-E, on page 53</td>
<td></td>
</tr>
<tr>
<td>• Create an Expressway-C Neighbor Zone for each Unified CM Cluster, on page 55</td>
<td></td>
</tr>
<tr>
<td>• Configure Search Rules on Expressway-C (to Unified CM), on page 58</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> Enable Hybrid Calling for Cisco Webex Teams Users, on page 60</td>
<td>Disable and reenable the Call Connector, so that the connector captures Unified CM user and device configuration changes that you made while deploying Hybrid Call Service. During this restart cycle, the connector creates a remote destination with the Cisco Webex SIP address on the Cisco Spark Remote Device. This address is associated with end user accounts and the corresponding Webex Teams accounts. Toggle this setting as a troubleshooting step if you experience any issues, too.</td>
</tr>
<tr>
<td><strong>Step 15</strong> Restart the Call Connector from the Expressway-C, on page 40</td>
<td>Use this procedure to test Hybrid Calling call scenarios. These steps verify whether you correctly configured Hybrid Calling and can help isolate any potential issues.</td>
</tr>
<tr>
<td><strong>Step 16</strong> Test the Softphone Functionality for Hybrid Calling, on page 62</td>
<td></td>
</tr>
</tbody>
</table>
Register Expressway-C Connector Hosts to the Cisco Webex Cloud

Cisco Webex Hybrid Services use software connectors hosted on Expressway-C to securely connect Cisco Webex to your organization's environment. Use this procedure to register Expressway-C resources to the cloud.

After you complete the registration steps, the connector software is automatically deployed on your on-premises Expressway-C.

Before you begin

- Make sure your Expressway-C is running on a version that's supported for hybrid services. See the Supported Versions of Expressway for Cisco Webex Hybrid Services Connectors documentation (https://help.webex.com/article/ruyceab) for more information about which versions are supported for new and existing registrations to the cloud.
- Sign out of any open connections to the Expressway-C interface that are open in other browser tabs.
- If your on-premises environment proxies the outbound traffic, you must first enter the details of the proxy server on Applications > Hybrid Services > Connector Proxy before you complete this procedure. Doing so is necessary for successful registration.

If you enter proxy information for call connector, the call connector automatically detects this configuration.

Procedure

Step 1
From the customer view in https://admin.webex.com, go to Services, and then choose one:

- If this is the first connector host you're registering, click Set up on the card for the hybrid service you're deploying, and then click Next.
- If you've already registered one or more connector hosts, click View all on the card for the hybrid service you're deploying, and then click Add Resource.

The Cisco Webex cloud rejects any attempt at registration from the Expressway web interface. You must first register your Expressway through Cisco Webex Control Hub, because the Control Hub needs to hand out a token to the Expressway to establish trust between premises and cloud, and complete the secure registration.

Step 2
Choose a method to register the Expressway-C:

- **New Expressways**—choose Register a new Expressway with its Fully Qualified Domain Name (FQDN), enter your Expressway-C IP address or fully qualified domain name (FQDN) so that Cisco Webex creates a record of that Expressway-C and establishes trust, and then click Next. You can also enter a display name to identify the resource in Cisco Webex Control Hub.

  **Caution** To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Expressway-C. Capitalization is not supported at this time.
• **Existing Expressways**—choose Select an existing Expressway cluster to add resources to this service, and then choose the node or cluster from the drop-down that you previously registered. You can use it to run more than one hybrid service.

**Tip**  
If you're registering a cluster, register the primary peer. You don't need to register any other peers, because they register automatically when the primary registers. If you start with one node set up as a primary, subsequent additions do not require a system reboot.

---

**Step 3**  
Click **Next**, and for new registrations, click the link to open your Expressway-C. You can then sign in to load the **Connector Management** window.

---

**Step 4**  
Decide how you want to update the Expressway-C trust list:

A check box on the welcome page determines whether you will manually append the required CA certificates to the Expressway-C trust list, or whether you allow Cisco Webex to add those certificates for you.

Choose one of the following options:

- **Check** the box if you want Cisco Webex to add the required CA certificates to the Expressway-C trust list.

  When you register, the root certificates for the authorities that signed the Cisco Webex cloud certificates are installed automatically on the Expressway-C. This means that the Expressway-C should automatically trust the certificates and be able to set up the secure connection.

  **Note**  
  If you change your mind, you can use the **Connector Management** window to remove the Cisco Webex cloud CA root certificates and manually install root certificates.

- **Uncheck** the box if you want to manually update the Expressway-C trust list. See the Expressway-C online help for the procedure.

  **Caution**  
  When you register, you will get certificate trust errors if the trust list does not currently have the correct CA certificates. See Certificate Authorities for Hybrid Services, on page 26.

---

**Step 5**  
Click **Register**. After you're redirected to Cisco Webex Control Hub, read the on-screen text to confirm that Cisco Webex identified the correct Expressway-C.

---

**Step 6**  
After you verify the information, click **Allow** to register the Expressway-C for Cisco Webex Hybrid Services.

- Registration can take up to 5 minutes depending on the configuration of the Expressway and whether it's a first-time registration.

- After the Expressway-C registers successfully, the Cisco Webex Hybrid Services window on the Expressway-C shows the connectors downloading and installing. The management connector automatically upgrades itself if there is a newer version available, and then installs any other connectors that you selected for the Expressway-C connector host.

- Each connector installs the interface pages that you need to configure and activate that connector.

  This process can take a few minutes. When the connectors are installed, you can see new menu items on the **Applications > Hybrid Services** menu on your Expressway-C connector host.
Troubleshooting Tips

If registration fails and your on-premises environment proxies the outbound traffic, review the Before You Begin section of this procedure. If the registration process times out or fails (for example, you must fix certificate errors or enter proxy details), you can restart registration in Cisco Webex Control Hub.

What to do next

If you want to add resources for specific geographies, return to View all > Add Resource from the Hybrid Call card and repeat the above steps to register more Expressway resources to the Cisco Webex cloud.

Certificate Authorities for Hybrid Services

The table lists the Certificate Authorities that your on-premises or existing environment must trust when using Cisco Webex Hybrid Services.

If you opted to have Cisco Webex manage the required certificates, then you do not need to manually append CA certificates to the Expressway-C trust list.

Note

The issuers used to sign the Cisco Webex host certificates may change in future, and the table below may then be inaccurate. If you are manually managing the CA certificates, you must append the CA certificates of the issuing authorities that signed the currently valid certificates for the hosts listed below (and remove expired/revoked CA certificates).

<table>
<thead>
<tr>
<th>Cloud hosts signed by this CA</th>
<th>Issuing CA</th>
<th>Must be trusted by</th>
<th>For this purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDN</td>
<td>O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root</td>
<td>Expressway-C</td>
<td>To ensure Expressway downloads connectors from a trusted host</td>
</tr>
<tr>
<td>Common identity service</td>
<td>O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority</td>
<td>Windows Server 2003 or Windows Server 2008 hosting the Cisco Directory Connector Expressway-C</td>
<td>To synchronize users from your Active Directory with Cisco Webex and to authenticate Cisco Webex Hybrid Services users</td>
</tr>
<tr>
<td>Cisco Webex</td>
<td>O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority</td>
<td>Expressway-C</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Supported Certificate Authorities for Cisco Webex
Configure an Application Account for Call Connector

Configure an administrator account with the required AXL access permissions. Call Connector uses this account to communicate with Cisco Unified Communications Manager, monitor any user's phone, and validate user configuration.

Procedure

Step 1
From Cisco Unified CM Administration, go to User Management > Application User, and then choose one:

• Click Find and, from the list, choose the administrator account that the connector will use to communicate with Cisco Unified Communications Manager.
• Click Add New to create a new application user account.

Step 2
Configure the account with following access roles:

• Standard AXL API Access
• Standard CTI Enabled

Step 3
Click Save.

Configure the Connection to Cisco Unified Communications Manager

To enable Hybrid Calling, you must link Call Connector to your Cisco Unified Communications Manager environment by entering server information for a single node. This step provides secure bridge between Cisco Unified Communications Manager and the Cisco Webex cloud, with the connector acting as the broker between the two.

Before you begin

• For each cluster in your call environment, you must only enter server information in the connector for a single Cisco Unified Communications Manager node. The node doesn't have to be primary, but enter one that is enabled for AXL Web Service and Cisco CallManager Serviceability.

• The connector on Expressway maintains a resilient connection between your cluster and the cloud. The connector is aware of all the server nodes in your cluster, so you only need to add 1 node to the Expressway-C connector host. If a specific node goes down in the cluster, the connector will move to another server.

Procedure

Step 1
From Expressway-C, go to Applications > Hybrid Services > Call Service > Unified CM Servers, and then click New.
Start the Call Connector

Manually enable the Call Connector after you register your Expressway-C for Cisco Webex Hybrid Services.

**Before you begin**

Configure the Connection to Cisco Unified Communications Manager, on page 27

**Procedure**

**Step 1**
From Expressway-C, go to Applications > Hybrid Services > Connector Management, and then click Call Connector.

**Step 2**
Choose Enabled from the Active drop-down list.

**Step 3**
Click Save.

The connector starts and the status changes to Running on the Connector Management window.

Verify the Connector Status

Before you enable your users for Hybrid Calling, ensure that you correctly installed the Call Connector.

**Procedure**

From Expressway-C, go to Applications > Hybrid Services > Call Service > Call Connector Status, and then verify the configuration items in the Status column.

---

**Step 2**
Enter the hostname or IP address of a single Cisco Unified Communications Manager node on which Cisco AXL Web Service and Cisco CallManager Serviceability are enabled.

**Step 3**
Enter the credentials of the Call Connector account that you configured for Call Connector to connect to Cisco Unified Communications Manager.

Enter a single node per cluster. The connector will automatically discover the other nodes in a cluster environment and identify those that can service AXL requests.

**Step 4**
Click Verify Credentials to test the connection and authentication for the provided credentials.

After the page refreshes, a new Hybrid Call Service Connect Configuration section appears.

**Step 5**
After the connection test is successful, click Add to store the connector configuration on the Expressway-C.

---

## Start the Call Connector

Manually enable the Call Connector after you register your Expressway-C for Cisco Webex Hybrid Services.

**Before you begin**

Configure the Connection to Cisco Unified Communications Manager, on page 27

**Procedure**

**Step 1**
From Expressway-C, go to Applications > Hybrid Services > Connector Management, and then click Call Connector.

**Step 2**
Choose Enabled from the Active drop-down list.

**Step 3**
Click Save.

The connector starts and the status changes to Running on the Connector Management window.

---

## Verify the Connector Status

Before you enable your users for Hybrid Calling, ensure that you correctly installed the Call Connector.

**Procedure**

From Expressway-C, go to Applications > Hybrid Services > Call Service > Call Connector Status, and then verify the configuration items in the Status column.
Configure Cisco Unified Communications Manager Settings for Hybrid Calling

Configure Cisco 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 9.

Procedure

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:

<table>
<thead>
<tr>
<th>FQDN Guideline</th>
<th>Description and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple clusters</td>
<td>The entry must be unique for each cluster with Hybrid Calling—For example, cluster1.example.com, cluster2.example.com, and so on.</td>
</tr>
<tr>
<td>No wildcards</td>
<td>Do not use entries with wildcards, such as <em>.example.com or example</em>.com.</td>
</tr>
<tr>
<td>First FQDN entry for Hybrid Calling</td>
<td>In a list of multiple entries, the Cisco 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): cluster1.example.com <em>.example.com example</em>.com.</td>
</tr>
<tr>
<td>Different from Expressway-E</td>
<td>Must be different from the Expressway-E system, DNS, and domain name. Otherwise, Expressway-E strips the route header.</td>
</tr>
</tbody>
</table>
| 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 *.example.com *.example.org, add a unique, non-wildcard entry at the beginning of the field: "cluster1.example.com *.example.com *.example.org"
You are not required to restart Cisco 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 58.**

**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.

a) Click **Find**, choose **Standard SIP Profile For Cisco VCS**, and then click **Copy**.
b) Enter a name for the new profile—for example, **Standard SIP Profile for Cisco Webex Hybrid Calling**.
c) 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 Cisco Webex cloud (routed by external domain **webex.com**). The setting does not affect any existing SIP trunking or call routing.
d) 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 Cisco Webex Hybrid Services.

a) Enter a name for the new profile that is related to Cisco Webex or Hybrid Calling—for example, **SIP Trunk Security Profile for Cisco Webex Hybrid Calling**.
b) Leave the **Enable Digest Authentication** check box unchecked.
c) 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.
d) 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 Cisco Webex SIP profile to this trunk.

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Hybrid_Calling_SIP_Trunk (for example)</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool that contains the device-specific settings that you want the SIP trunk to inherit.</td>
</tr>
</tbody>
</table>
**Field Name** | **Value**
---|---
Calling and Connected Party Info Format | **Deliver URI and DN in connected party, if available**
| This setting enables blended identity. It allows the SIP trunk to transmit the enterprise-side party's directory URI to Cisco Webex.
| The directory URI is what allows the cloud to match the enterprise end user to Webex Teams user account. This match enables parallel ringing on the user's enterprise devices and Webex Teams.
| **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.
| Destination Address | Enter the Expressway-C node addresses in the fields.
| SIP Profile | **Standard SIP Profile for Cisco 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 Cisco Webex Domain For Hybrid Calling for Users*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Pattern</td>
<td>*.calls.webex.com</td>
</tr>
<tr>
<td>Pattern Usage</td>
<td>Domain Routing</td>
</tr>
<tr>
<td>Description</td>
<td><strong>Routing for Cisco Webex hybrid calling users</strong></td>
</tr>
<tr>
<td>Route Partition</td>
<td>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 &lt;None&gt; partition.)</td>
</tr>
<tr>
<td>SIP Trunk/Route List</td>
<td>Choose the trunk you created—<strong>Hybrid_Calling_SIP_Trunk</strong> (for example)</td>
</tr>
<tr>
<td>SIP Profile</td>
<td><strong>Standard SIP Profile for Cisco Webex Hybrid Calling</strong> (for example)</td>
</tr>
</tbody>
</table>

*Table 6: SIP Route Pattern for Cisco Webex Domain For Hybrid Calling for Devices*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Pattern</td>
<td>*.rooms.webex.com</td>
</tr>
<tr>
<td>Pattern Usage</td>
<td>Domain Routing</td>
</tr>
<tr>
<td>Description</td>
<td><strong>Routing for Cisco Webex hybrid calling devices</strong></td>
</tr>
</tbody>
</table>
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.)

Choose the trunk you created—Hybrid_Calling_SIP_Trunk (for example)

Standard SIP Profile for Cisco Webex Hybrid Calling (for example)

We include this route pattern so that your deployment remains backwards compatible. If you're not sure if your Webex Teams 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 ciscospark.com domains over to webex.com.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Pattern</td>
<td>*.ciscospark.com</td>
</tr>
<tr>
<td>Pattern Usage</td>
<td>Domain Routing</td>
</tr>
<tr>
<td>Description</td>
<td>Routing for Cisco Spark hybrid calling</td>
</tr>
<tr>
<td>Route Partition</td>
<td>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 &lt;None&gt; partition.)</td>
</tr>
<tr>
<td>SIP Trunk/Route List</td>
<td>Choose the trunk you created—Hybrid_Calling_SIP_Trunk (for example)</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Standard SIP Profile for Cisco Webex Hybrid Calling (for example)</td>
</tr>
</tbody>
</table>

Example

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

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

### Prepare Cisco Unified Communications Manager User Accounts for Hybrid Calling

Configure Unified CM users so that their corresponding Cisco Webex Teams accounts in the cloud are activated with the correct call settings. Call Connector creates the remote destination on the user's Cisco Spark Remote Device after all the Unified CM settings are properly configured.

#### Before you begin

Use this diagram to understand the required fields for Hybrid Calling:

*Figure 5: Required Unified CM User Fields for Hybrid Calling*

---

**Note**

If you use LDAP synchronization in your Unified CM deployment, some of this user configuration may already be complete.
Procedure

Step 1 From Cisco Unified CM Administration, go to User Management > End Users, choose any criteria, click Find, and then open the user account that you want to configure.

Step 2 Verify that the user has a valid Directory URI that contains the same domain as your organization.

Step 3 Verify that Mail ID contains the user's email address.

Step 4 Under the user's Service Settings, check the Home Cluster checkbox.

Configure this setting on the Cisco Unified Communications Manager where each user is homed and where their devices are registered.

The user only requires a Cisco Spark-RD at a minimum to be activated for Hybrid Call Service.

Note If Cisco Spark-RD is the user's only device, you must configure the desired Call Forward Busy (CFB) destination (for example, Unity Connection) for when a hybrid call is declined in the Cisco Webex Teams app.

When you set up Hybrid Calling, you cannot activate a user with only an Extension Mobility profile and no associated device. For a user who is associated to a device (including a Cisco Spark-RD) and has an Extension Mobility profile, Hybrid Calling activates and should work.

Step 5 (Optional) To associate a line appearance to an end user for presence and to enable the on-the-phone status information to IM and Presence clients when this line appearance is off-hook, click Line Appearance Association from Presence. The Line Appearance Association for Presence window appears from where you can choose product type, device name, directory, partition, or description. The choices available in this window depend on the lines associated with the controlled devices. Click Save.

Step 6 Return to the user account, scroll to Directory Number Associations, and then set the primary extension to the user's directory number.

Before you enable Webex Teams users for Hybrid Calling, make sure that the user's associated Directory Number Alerting Name and ACSII Alerting Name are no more than 30 characters in length. The names can only contain letters, numbers, spaces, and the following special characters: !#$'()*+,./:;=?@^_.

Step 7 Save your changes.

Step 8 If you created Cisco Spark-RD automatically from the call connector, set the primary extension to a directory number, and then save your changes.

Configure Cisco Spark-RD Automatically from the Call Connector

Every Hybrid Calling user requires a virtual device called a Cisco Spark Remote Device (Cisco Spark-RD). This virtual device is attached to a user's work number and links the user's Cisco Webex Teams account SIP identity to the enterprise SIP identity so that calls anchor on the Unified CM side or fork to the Cisco Webex cloud side. From a technical standpoint, the Cisco Spark-RD masks outbound calls from Cisco Webex and displays the user's work number for calls from the Cisco Webex Teams app. Incoming calls also ring both the user's Cisco Webex Teams app and desk phone.

To automate your configuration, on the Expressway-C connector host you can create Cisco Spark-RD for all your users in one step. The connector shows the remote device field values from your Cisco Unified Communications Manager, and then you can choose the values specific to your deployment. After the connector
creates Cisco Spark-RDs, they are automatically moved to the users' control lists and their Cisco Webex SIP addresses are automatically created as remote destinations.

**Before you begin**

- Cisco Spark-RD is required for your hybrid deployment. For manual and automatic creation on a supported release, you must use Cisco Spark-RD for new activations.

- If you choose automatic configuration, a new remote device (CTI or Cisco Spark-RD) and remote destination is created when the new user is activated in https://admin.webex.com.

- CTI-RDs created with an earlier release must be migrated over to Cisco Spark-RD. You can use a conversion tool on the Call Connector to transition existing CTI-RD to Cisco Spark-RD. See [Tool to Migrate CTI-RD to Cisco Spark-RD, on page 93](#).

**Procedure**

**Step 1**

From the Expressway-C connector host, go to **Applications > Hybrid Services > Call Service > Unified CM Servers**, and then the Cisco Unified Communications Manager node that you configured.

**Step 2**

For **Spark Remote Device Configuration Type**, choose **Automatic**.

**Caution** When using automatic remote device configuration, do not manually create a remote device and add the Cisco Webex SIP address as a remote destination.

**Step 3**

Choose values from the prepopulated lists for the **Device Pool, Location, Calling Search Space**, and **Reroute Calling Search Space**.

These settings are shared across all of the automatically created Cisco Spark-RD. Read these documents to understand the settings:

- Device pools
- Locations
- Calling search spaces

**Note**

- For Cisco Spark-RD, the CSS is used for outbound calls initiated by the Cisco Webex Teams app to enterprise phones or the PSTN.

  The Rerouting CSS determines the route to remote destinations of the Cisco Spark-RD. This CSS must include the partition that contains the SIP route pattern for the Cisco Webex cloud. It does not need any other partitions.

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

**Step 4**

Click **Add** to automatically create the Cisco Spark-RD.
Manually Create a Cisco Spark-RD and Associate it with a Unified CM User

Every Hybrid Calling user requires a virtual device called a Cisco Spark Remote Device (Cisco Spark-RD). This virtual device is attached to a user's work number and links the user's Cisco Webex Teams account SIP identity to the enterprise SIP identity so that calls anchor on the Unified CM side or fork to the Cisco Webex cloud side. From a technical standpoint, the Cisco Spark-RD masks outbound calls from Cisco Webex and displays the user's work number for calls from the Cisco Webex Teams app. Incoming calls also ring both the user's Cisco Webex Teams app and desk phone.

The Call Connector's automatic option applies the same set of device pool, location, and calling search space to all devices. This option may not be ideal for a large scale deployment. Use the manual device creation method if you need to specify different settings in some of the remote devices.

Before you begin

- Follow the remote device creation steps only if you didn't automatically create remote devices from the connector on the Expressway-C connector host.
- A user can have multiple remote devices, but only one can be in the list of controlled devices for Cisco Webex purposes.
- Whether you manually or automatically create remote devices, Call Connector will automatically create the remote destination, which contains the user's Cisco Webex SIP address.

Procedure

Step 1 From the Expressway-C connector host, go to Applications > Hybrid Services > Call Service > Unified CM Servers, and then the Cisco Unified Communications Manager node that you configured.

Step 2 For Spark Remote Device Configuration Type, choose Manual, and then click Save.

Step 3 From Cisco Unified CM Administration, go to Device > Phone, then Add New, and then choose Cisco Webex Remote Device.

Step 4 For Owner User ID, specify the user who 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.

Note A manually created Cisco Spark-RD must be 15 characters or less. If the device name is 15 characters or more, the user remains in a pending activation state.

Step 5 For line association, specify the user’s primary extension (the user’s shared line).

Step 6 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

Note

- For Cisco Spark-RD, the CSS is used for outbound calls initiated by the Cisco Webex Teams app to enterprise phones or the PSTN.

The Rerouting CSS determines the route to remote destinations of the Cisco Spark-RD. This CSS must include the partition that contains the SIP route pattern for the Cisco Webex cloud. It does not need any other partitions.

- 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 Cisco Webex Teams users to be able to reach (conference bridges, enterprise-to-enterprise trunks, and so on).

Step 7
Save your changes.

Step 8
From Cisco Unified CM Administration, go to User Management > End User, and then open the user's account.

Step 9
Under Device Information, click Device Association.

Step 10
Specify any search criteria and click Find.

Step 11
Check the remote device that you created, and then save your changes.

The remote device is associated to the user and is added to the controlled devices list. The Cisco Webex SIP address is automatically created as the remote destination.

Activate Hybrid Calling for Your Organization

Use this procedure to begin the initial setup for Hybrid Call Service Connect in Cisco Webex Control Hub. These settings ensure that Hybrid Call Service Connect is first enabled for your organization before you do further configuration. You specify the desired subdomain for your company, and that setting creates Cisco Webex SIP addresses to identify users in the Cisco Webex cloud. Then, you toggle on Hybrid Call Service 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 will be 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.

Procedure

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 Cisco Webex organization, go to Settings, and then scroll to Cisco Webex SIP Addresses.

**Step 2**
Follow the on-screen instructions to configure a custom SIP subdomain for your organization. This subdomain value creates individual Cisco Webex SIP addresses for each user and Webex-registered device. The addresses are used to receive calls from any standards-based SIP calling service. See Cisco Webex SIP Addresses for more information.

**Step 3**
Go to Services, 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:

<table>
<thead>
<tr>
<th>Address Format</th>
<th>Example Of Value to Enter (In Bold)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV domain</td>
<td>_sips._tcp.sipmtls.example.com</td>
</tr>
<tr>
<td>Hostname/FQDN:port</td>
<td>example.com:5062</td>
</tr>
<tr>
<td>IP address:port</td>
<td>203.0.113.0:5062</td>
</tr>
</tbody>
</table>

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 83 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.
Add SIP Destinations to Hybrid Call Expressway Clusters

A single 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 so that you have more control over where the hybrid call traffic is routed. After you add a default SIP destination for Hybrid Call Service Connect, you can add more SIP destinations to individual hybrid call clusters in Cisco Webex Control Hub.

Before you begin
Finish registration of any new or existing Call Connector resources by using these steps: Register Expressway-C Connector Hosts to the Cisco Webex Cloud, on page 24

Procedure

Step 1 From the customer view in https://admin.webex.com, go to Services, and then click View all from the Hybrid Call card.

Step 2 Click the resource, and then click Edit cluster settings.

Step 3 Scroll to Cluster > Default SIP Destination Override, choose Configure a SIP Destination for the cluster, 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:

<table>
<thead>
<tr>
<th>Address Format</th>
<th>Example Of Value to Enter (In Bold)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV domain</td>
<td>_sips._tcp.sipmtls.example.com</td>
</tr>
<tr>
<td>Hostname/FQDN:port</td>
<td>example.com:5062</td>
</tr>
<tr>
<td>IP address:port</td>
<td>203.0.113.0:5062</td>
</tr>
</tbody>
</table>

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 4 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 5 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 83 for more information.

**Step 6**

Save your changes.

**What to do next**

Repeat these steps to associate more SIP destinations with specific Call Connector clusters. (Any clusters that don't have a SIP destination continue to use the default one that you initially configured.)

**Restart the Call Connector from the Expressway-C**

Disable and reenable the Call Connector, so that the connector captures Unified CM user and device configuration changes that you made while deploying Cisco Webex Hybrid Call Service. During this restart cycle, the connector creates a remote destination with the Cisco Webex SIP address on the Cisco Spark Remote Device. This address is associated with end user accounts and the corresponding Cisco Webex Teams accounts. Toggle this setting as a troubleshooting step if you experience any issues, too.

When you upgrade your Unified CM an environment with Cisco Webex Hybrid Services and Webex Teams, information that is cached in the Call Connector might be stale. In this case, the affected items are the automatic synchronization of the database cache or reporting the new Unified CM version to the Cisco Webex cloud. Restart the Call Connector to select the latest information in the new database and also publish the new Unified CM version information to the Cisco Webex cloud services.

**Before you begin**

![Caution]

Restarting the Call Connector creates extra load on Unified CM publishers. Consider restarting the Call Connector during off-peak hours; during busy hours, a restart may cause service issues.

**Procedure**

**Step 1**

From Expressway-C, go to Applications > Hybrid Services > Call Service > Call Service Overview, change the call connector status to Disabled, and then click Save.

**Step 2**

Change the status back to Enabled, and then save again.

**Troubleshooting Tips**

Later, you may need to change to Unified CM end users or devices. If you do this to fix a configuration error, even if the call connector's "user validation test" passes for that user, you must restart Call Connector so that it selects the configuration change.

**Things to Keep in Mind About Unified CM Cache**
Call Connector maintains a cache of Unified CM data, so that AXL requests have limited performance impact on Unified CM nodes during user discovery and activation.

Cached data includes:

- Users
- Devices (including user associations)
- Directory numbers (including line appearances, user association, URIs)
- Remote Destinations

Call Connector uses change notifications on the publisher nodes to pull new user data. The poll interval is every 2 minutes. Because of limitations with Unified CM change notifications, the cache is rebuilt every night at 11 pm local time or upon Call Connector restart.

**Check Your User Configuration for Cisco Webex Hybrid Call Service**

With the user validation check, you can check whether Cisco Unified Communications Manager users are properly configured for Hybrid Calling. The test checks all the configuration prerequisites, such as email, directory URI, and Cisco Spark Remote Device settings. To assist with your configuration or troubleshooting, you can save any user errors or warnings as a CSV file.

To prevent activation errors, we recommend that you run this test and address any configuration issues before you activate users for Hybrid Calling in Cisco Webex Control Hub.

**Before you begin**

Configure the Connection to Cisco Unified Communications Manager, on page 27

**Procedure**

1. **Step 1**
   From the Expressway-C connector host, choose Applications > Hybrid Services > Call Service > Unified CM Servers, and choose the registered Cisco Unified Communications Manager that you want to check.

2. **Step 2**
   Perform one of the following steps:
   - Upload a CSV file of a user list if you want to check the configuration of specific user accounts, and then click Run (Specific User List).
   - Click Run (All Users) to check the configuration of all the user accounts registered to the Cisco Unified Communications Manager.

   A report appears with user accounts that contain configuration errors or warnings.

3. **Step 3**
   Save the information as a CSV file and use it as a checklist to fix user and system settings in Cisco Unified Communications Manager.

4. **Step 4**
   Address any configuration issues in the Cisco Unified Communications Manager device and user settings.
# 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Update the Expressway-E Trust List with Cisco Webex Cloud Certificates, on page 43</td>
<td>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 Cisco Webex cloud. To establish this trust, you must add these certificates to the trusted CA list on your Expressway-E.</td>
</tr>
</tbody>
</table>
| **Step 2** | Perform one of the following tasks, depending on your configuration:  
- Configure Services and Mutual TLS Authentication Between a New Expressway-E and the Cisco Webex Cloud, on page 45  
- Configure Services and Mutual TLS Authentication Between an Existing Expressway-E and the Cisco Webex Cloud, on page 47 | 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 Cisco 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 Cisco Webex Cloud), on page 48 | The DNS zone allows your Expressway-E to identify and route calls between Cisco Unified Communications Manager and the Cisco 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 48 | 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 50 | Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the |
### Command or Action

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

### Update the Expressway-E Trust List with Cisco 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 Cisco 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

#### Procedure

**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 Rules on Expressway-E

If Expressway-C and Expressway-E run both Hybrid Call Service 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 Cisco Webex 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.

**Procedure**

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source type</td>
<td>From address</td>
</tr>
<tr>
<td>Rule applies to</td>
<td>Unauthenticated callers</td>
</tr>
<tr>
<td>Source pattern</td>
<td>.<em>@example.calls.webex.com.</em>, where example is your company's subdomain.</td>
</tr>
<tr>
<td>Destination pattern</td>
<td>.*</td>
</tr>
<tr>
<td>Action</td>
<td>Reject</td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source type</td>
<td>Zone</td>
</tr>
<tr>
<td>Originating Zone</td>
<td>DefaultZone</td>
</tr>
<tr>
<td>Destination pattern</td>
<td>.*</td>
</tr>
<tr>
<td>Action</td>
<td>Reject</td>
</tr>
</tbody>
</table>

e) Click Add to save this new rule.
Configure Services and Mutual TLS Authentication Between a New Expressway-E and the Cisco 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 Cisco Webex Cloud Certificates, on page 43
- If you configured a DNS SRV as the SIP destination in Cisco Webex Control Hub (Activate Hybrid Calling for Your Organization, on page 37), ensure that that value specifies the MTLS port.

Procedure

Step 1 From Expressway-E, go to Configuration > Protocols > H.323, and then set H.323 mode to Off, and then save your changes.

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>SIP mode</td>
<td>On</td>
</tr>
<tr>
<td>UDP mode</td>
<td>Off</td>
</tr>
<tr>
<td>UDP port</td>
<td>5060</td>
</tr>
<tr>
<td>TCP mode</td>
<td>Off</td>
</tr>
<tr>
<td>TCP port</td>
<td>5060</td>
</tr>
<tr>
<td>TLS mode</td>
<td>On</td>
</tr>
<tr>
<td>TLS port</td>
<td>5061</td>
</tr>
<tr>
<td>Mutual TLS mode</td>
<td>On</td>
</tr>
<tr>
<td>Mutual TLS port</td>
<td>5062</td>
</tr>
<tr>
<td>TCP outbound port start</td>
<td>25000</td>
</tr>
<tr>
<td>TCP outbound port end</td>
<td>299999</td>
</tr>
<tr>
<td>Session refresh interval (seconds)</td>
<td>1800</td>
</tr>
<tr>
<td>Minimum session refresh interval (seconds)</td>
<td>500</td>
</tr>
<tr>
<td>TLS handshake timeout (seconds)</td>
<td>5</td>
</tr>
</tbody>
</table>
### Field Name | Value
--- | ---
**Certificate revocation checking** | 
Certificate revocation checking mode | Off

### Registration controls

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard registration refresh strategy</td>
<td>Maximum</td>
</tr>
<tr>
<td>Standard registration refresh minimum (seconds)</td>
<td>45</td>
</tr>
<tr>
<td>Standard registration refresh maximum (seconds)</td>
<td>60</td>
</tr>
<tr>
<td>Outbound registration refresh strategy</td>
<td>Variable</td>
</tr>
<tr>
<td>Outbound registration refresh minimum (seconds)</td>
<td>300</td>
</tr>
<tr>
<td>Outbound registration refresh maximum (seconds)</td>
<td>3600</td>
</tr>
</tbody>
</table>

### SIP registration proxy mode

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP registration proxy mode</td>
<td>Off</td>
</tr>
</tbody>
</table>

### Authentication

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delegated credential checking</td>
<td>Off</td>
</tr>
</tbody>
</table>

### Advanced

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP max size</td>
<td>32768</td>
</tr>
<tr>
<td>SIP TCP connect timeout</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**Step 3**  
Click Save.

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

**Step 5**  
Configure the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td></td>
</tr>
</tbody>
</table>
Authentication mode | Do not check credentials |

| SIP | 
Media encryption mode | Auto |
| ICE support | Off |
Configure Services and Mutual TLS Authentication Between an Existing Expressway-E and the Cisco Webex Cloud

Expressway-E can be shared between mobile and remote access (MRA), business-to-business (B2B), and Cisco 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 Cisco Webex Cloud Certificates, on page 43
- If using a dedicated MTLS port, ensure that the DNS SRV in Cisco Webex Control Hub specifies this MTLS port. (See Activate Hybrid Calling for Your Organization, on page 37.)
- 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.

Procedure

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.

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP mode</td>
<td>On</td>
</tr>
<tr>
<td>UDP mode</td>
<td>Off</td>
</tr>
<tr>
<td>TCP mode</td>
<td>Off, if possible. If this breaks services such as B2B, set it back to On.</td>
</tr>
<tr>
<td>TLS mode</td>
<td>On</td>
</tr>
<tr>
<td>Mutual TLS mode</td>
<td>On</td>
</tr>
</tbody>
</table>
### Create an Automatic Webex DNS Zone (Expressway-E to the Cisco Webex Cloud)

The DNS zone allows your Expressway-E to identify and route calls between Cisco Unified Communications Manager and the Cisco 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.

**Before you begin**

This option is only available in Expressway X8.11.4 and later. Ensure that you're on a supported Expressway traversal pair for Hybrid Calling, as documented in Cisco Expressway Requirements, on page 6.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Expressway-E, navigate to Configuration &gt; Zones &gt; Zones and click New.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>For Type, choose Webex, and then save your changes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) Next to the hybrid domain, click Check Connectivity.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual TLS port</td>
<td>5062</td>
</tr>
</tbody>
</table>
• 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-E and Expressway-E if they are used for B2B and Hybrid Calling.

Procedure

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

Step 2
Configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Webex hybrid traversal server</td>
</tr>
<tr>
<td>Type</td>
<td>Traversal server</td>
</tr>
<tr>
<td>Hop count</td>
<td>15 (Default)</td>
</tr>
<tr>
<td>Connection credentials</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Enter traversal, for example.</td>
</tr>
<tr>
<td>Password</td>
<td>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.</td>
</tr>
<tr>
<td>H.323</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Off</td>
</tr>
<tr>
<td>Protocol</td>
<td>Assent (Default)</td>
</tr>
<tr>
<td>Port</td>
<td>6006 (Default)</td>
</tr>
<tr>
<td>H.460.19 demultiplexing mode</td>
<td>Off (Default)</td>
</tr>
<tr>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>On</td>
</tr>
<tr>
<td>Port</td>
<td>7004 or any value in 7XXX range. (This value must match the port number that is configured on Expressway-C.)</td>
</tr>
<tr>
<td>Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>TLS verify mode</td>
<td>On</td>
</tr>
<tr>
<td>TLS verify subject name</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 Cisco Webex cloud and route down the traversal zone to Expressway-C.
- Identify calls from Cisco Unified Communications Manager and route through the DNS zone to Cisco Webex.

Before you begin

Configure a Secure Traversal Server Zone from Expressway-E to Expressway-C, on page 48

Procedure

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 Cisco Webex (through the DNS zone) and route them inwards (through the traversal zone) to Expressway-C.

Step 3
Configure the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Enter <strong>Webex Hybrid inbound calls</strong>, for example.</td>
</tr>
</tbody>
</table>
Click Create search rule.

Step 5
Click New.

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

Step 6
Configure the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter Webex Hybrid outbound calls, for example.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter Route traffic from Expressway-E to Webex Hybrid Cloud, for example.</td>
</tr>
<tr>
<td>Priority</td>
<td>100 (Default)</td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Source</td>
<td>Named</td>
</tr>
<tr>
<td>Source name</td>
<td>Webex hybrid traversal server, for example. Choose the traversal server zone (or Unified Communications traversal zone) that you modified in the previous section.</td>
</tr>
<tr>
<td>Request must be authenticated</td>
<td>No (Default)</td>
</tr>
<tr>
<td>Mode</td>
<td>Alias pattern match</td>
</tr>
<tr>
<td>Pattern Type</td>
<td>Regex</td>
</tr>
</tbody>
</table>
Configure the Expressway-C for Hybrid Calling

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern string</td>
<td><em>@.</em>.webex.com</td>
</tr>
<tr>
<td>Pattern behavior</td>
<td>Leave</td>
</tr>
<tr>
<td>On successful match</td>
<td>Stop (Default)</td>
</tr>
<tr>
<td>Target</td>
<td>Webex hybrid DNS zone, for example. Choose the Cisco Webex DNS zone from the drop-down list.</td>
</tr>
<tr>
<td>State</td>
<td>Enabled (Default)</td>
</tr>
</tbody>
</table>

**Step 7**  
Click Create search rule.

**What to do next**  
Configure a Secure Traversal Client Zone From Expressway-C to Expressway-E, on page 53

**Configure the Expressway-C for Hybrid Calling**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure a Secure Traversal Client Zone From Expressway-C to Expressway-E, on page 53</td>
<td>Create a dedicated traversal client zone on Expressway-C. Though Cisco 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 Cisco Webex traffic, and the other direction won't be affected either.</td>
</tr>
</tbody>
</table>
| Step 2 | Create an Expressway-C Neighbor Zone for each Unified CM Cluster, on page 55      | Configure neighbor zones for each Cisco Unified Communications Manager cluster to which you want to route:  
• Each zone can accommodate 6 peer addresses, which supports a Cisco Unified Communications Manager cluster with 6 nodes.  
If you need to connect to a Cisco Unified Communications Manager cluster with more nodes, you can configure an SRV record for that cluster and use |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway-C to discover neighbor nodes by SRV lookup.</td>
<td></td>
</tr>
</tbody>
</table>

- This neighbor zone must route to a Cisco 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 Cisco 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 Cisco Unified Communications Manager for MRA.

**Step 3**

Configure Search Rules on Expressway-C (to Unified CM), on page 58

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 Cisco 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 Cisco Webex traffic, and the other direction won't be affected either.

**Procedure**

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

**Step 2**
Configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Webex Hybrid traversal client (for example)</td>
</tr>
</tbody>
</table>
### Configure a Secure Traversal Client Zone From Expressway-C to Expressway-E

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td><strong>Traversal client</strong></td>
</tr>
<tr>
<td><strong>Hop Count</strong></td>
<td><strong>15</strong></td>
</tr>
<tr>
<td><strong>Connection credentials</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td><strong>traversal</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password that you created on the Expressway-E for the traversal account.</td>
</tr>
<tr>
<td><strong>H.323</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td><strong>Off</strong></td>
</tr>
<tr>
<td><strong>SIP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td><strong>On</strong></td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td><strong>7004</strong> or any value in 7XXX range. (This value must match the port number that is configured on Expressway-E.)</td>
</tr>
<tr>
<td><strong>Transport</strong></td>
<td><strong>TLS</strong></td>
</tr>
<tr>
<td><strong>TLS verify mode</strong></td>
<td><strong>On</strong></td>
</tr>
<tr>
<td><strong>Accept proxied registrations</strong></td>
<td><strong>Deny</strong></td>
</tr>
<tr>
<td><strong>Media encryption mode</strong></td>
<td><strong>Force encrypted</strong></td>
</tr>
<tr>
<td><strong>ICE support</strong></td>
<td><strong>Off</strong></td>
</tr>
<tr>
<td><strong>Multistream mode</strong></td>
<td><strong>On</strong></td>
</tr>
<tr>
<td><strong>SIP poison mode</strong></td>
<td><strong>Off</strong></td>
</tr>
<tr>
<td><strong>Preloaded SIP routes support</strong></td>
<td><strong>On</strong></td>
</tr>
<tr>
<td><strong>SIP parameter preservation</strong></td>
<td><strong>On</strong> (Enables this zone to process SIP INVITE requests that contain the route header.)</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This parameter needs to be set to <strong>On</strong> for all zones on all Expressways that are involved in call routing to and from the enterprise.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication policy</strong></td>
<td><strong>Check credentials</strong></td>
</tr>
<tr>
<td><strong>Accept delegated credential checks</strong></td>
<td><strong>Off</strong></td>
</tr>
<tr>
<td><strong>Client settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Retry Interval</strong></td>
<td><strong>120</strong></td>
</tr>
</tbody>
</table>
Create an Expressway-C Neighbor Zone for each Unified CM Cluster

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

- Each zone can accommodate 6 peer addresses, which supports a Cisco Unified Communications Manager cluster with 6 nodes.

If you need to connect to a Cisco 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 Cisco 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 Cisco 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 Cisco Unified Communications Manager for MRA.

Procedure

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>UCM Neighbor for Cisco Webex (for example)</td>
</tr>
<tr>
<td>Type</td>
<td>Neighbor</td>
</tr>
<tr>
<td>Hop Count</td>
<td>15</td>
</tr>
</tbody>
</table>

Step 3 Click Create Zone.
### Field | Value
--- | ---
H.323 | Off
Mode | On
SIP | On

**Port**
Enter the Cisco 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**

**Look up peers by**

**Address** or **Service record**

Choose **Address** if you want to enter up to 6 IP addresses, hostnames, or FQDNs of individual Unified CM nodes in the neighbor cluster.

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.
Value Field

If you choose to Lookup peers by Address, enter IP addresses or hostnames for each server in the 6 peer address fields.

For TLS negotiation, the peer address must match the CN name that is used in the Unified CM certificates; otherwise, TLS negotiation fails.

Service Domain

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.

For example, if SIP mode is On and TLS verify mode is on, then when you enter example.com, Expressway queries DNS for _sips._tcp.example.com.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Configure these fields for the zone profile:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td></td>
<td>Advanced</td>
</tr>
<tr>
<td>Zone profile</td>
<td>Custom, the zone profile to use for the supported version of Unified CM for Hybrid Call Service.</td>
</tr>
<tr>
<td>Monitor peer status</td>
<td>Yes</td>
</tr>
<tr>
<td>Call signaling routed mode</td>
<td>Always</td>
</tr>
<tr>
<td>Automatically respond to H.323 searches</td>
<td>Off</td>
</tr>
<tr>
<td>Automatically respond to SIP searches</td>
<td>Off</td>
</tr>
<tr>
<td>Send empty INVITE for interworked calls</td>
<td>On</td>
</tr>
<tr>
<td>SIP Parameter Preservation</td>
<td>On</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>SIP poison mode</td>
<td>Off</td>
</tr>
<tr>
<td>SIP encryption mode</td>
<td>Auto</td>
</tr>
<tr>
<td>SIP REFER mode</td>
<td>Forward</td>
</tr>
<tr>
<td>SIP multipart MIME strip mode</td>
<td>Off</td>
</tr>
<tr>
<td>SIP UPDATE strip mode</td>
<td>Off</td>
</tr>
</tbody>
</table>
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 Cisco Unified Communications Manager Settings for Hybrid Calling, on page 29.

Procedure

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 Cisco 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>From Webex Hybrid Cloud to Unified CM via Expressway-E, for example.</td>
</tr>
<tr>
<td>Description</td>
<td>Route traffic from Expressway-C to Unified CM, for example.</td>
</tr>
<tr>
<td>Priority</td>
<td>60</td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Source</td>
<td>Named</td>
</tr>
</tbody>
</table>

Table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetworking SIP search strategy</td>
<td>Options</td>
</tr>
<tr>
<td>SIP UDP/BFCP filter mode</td>
<td>Off</td>
</tr>
<tr>
<td>SIP UDP/IX filter mode</td>
<td>Off</td>
</tr>
<tr>
<td>SIP record route address type</td>
<td>IP</td>
</tr>
<tr>
<td>SIP Proxy-Require header strip list</td>
<td>Leave this field blank.</td>
</tr>
</tbody>
</table>

Step 4  Click Create Zone.
We're going to create one rule to identify any calls (by Hybrid Calling users or Cisco Webex devices in a Place) arriving at Expressway-C that are destined for Cisco Webex, and route them outwards (through the traversal client zone) to the Expressway-E.

**Step 4**
Click Create search rule.

**Step 5**
Click New.

**Step 6**
Configure the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>From Unified CM to Webex Hybrid Cloud via Expressway-E, for example.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter Route traffic from Unified CM to Expressway-E, for example.</td>
</tr>
<tr>
<td>Priority</td>
<td>70</td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Source</td>
<td>Named</td>
</tr>
<tr>
<td>Source name</td>
<td>UCM Neighbor for Cisco Webex, for example.</td>
</tr>
<tr>
<td>Request must be authenticated</td>
<td>No</td>
</tr>
<tr>
<td>Mode</td>
<td>Alias pattern match</td>
</tr>
</tbody>
</table>
Enable Hybrid Calling for Cisco Webex Teams Users

Use this procedure to enable a small number of Cisco Webex Teams users for Hybrid Calling. See Ways to Add and Manage Users in Your Organization for other methods, such as using a bulk CSV template or Active Directory synchronization through Cisco Directory Connector.

**Note**

When you use bulk import or directory synchronization to import users, users must have email addresses in the source system. Those must be the addresses they use for Cisco Webex Teams because you map them to the Cisco Webex user ID.

If a user does not have an email address in Unified CM, the Call Connector cannot discover the user. Hybrid Call Service does not work for that user.

Using Cisco Directory Connector you can map either the mail attribute or the userPrincipalName attribute to the Cisco Webex UID, but the value must be the user's email address.

**Before you begin**

- Cisco Webex Teams users must already be assigned a paid license that provides them with core Cisco Webex messaging and meeting capabilities.

- You cannot enable the same user for both Hybrid Call Service and Cisco Webex Calling (Formerly Spark Call).

---

**Step 7**

Click **Create search rule**.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern type</td>
<td>Regex (The string is treated as a regular expression.)</td>
</tr>
<tr>
<td>Pattern string</td>
<td>.+@.<em>.((ciscospark)|((rooms|calls).webex).com).</em></td>
</tr>
<tr>
<td>Note</td>
<td>We include this pattern string so that your deployment remains backwards compatible. If you're not sure if your Webex Teams 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 ciscospark.com domains over to webex.com.</td>
</tr>
<tr>
<td>Pattern behavior</td>
<td>Leave (The alias is not modified.)</td>
</tr>
<tr>
<td>On successful match</td>
<td>Stop</td>
</tr>
<tr>
<td>Target</td>
<td>Webex Hybrid traversal client</td>
</tr>
<tr>
<td>State</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Procedure

Step 1  
From the customer view in https://admin.webex.com, go to Users, choose a specific user from the list, or use the search to narrow the list, and then click the row to open an overview of the user.

Step 2  
Click Edit, and then ensure that the user is assigned at least one paid service under Licensed Collaboration Services. Make necessary changes, and then click Save.

Step 3  
In the user's overview under Hybrid Services, click Call Service, and then click the the Aware toggle to turn it on.  
Aware does not provide any features to the user, but it is still a required step when you enable users for Hybrid Call Service.

Step 4  
Save your changes. Return to the user's overview and under Hybrid Services, click Call Service, and then click the the Connect toggle to turn it on.

Step 5  
Click Save.

After you enable users for the service, these steps occur:

- The connector service in the cloud waits for 2 minutes to collect users in batches.
- Call Connectors are notified about user discovery; one designated connector for each cluster is notified.
- The connectors request a batch of users to be discovered and then consult the local cache to verify the user configuration.
- The Cisco Webex Teams user status changes from Pending Activation to Activated. The length of time for this change depends on the number of users that you're enabling for the service.

This diagram shows how fields from Unified CM (on the left) are mapped in the Cisco Webex Teams user account view (on the right).

Figure 6: Field Mapping Between The Unified CM End User Account and Webex Teams User Account Cisco Webex Control Hub
What to do next

On the user's overview, you can find this information:

- User status and history
- Further details on status (Activation, errors, and so on)
- Cluster and node the user is hosted on
- Directory URI
- Primary DN
- Phone Number
- Unified CM FQDNs

Test the Softphone Functionality for Hybrid Calling

Use this procedure to test Hybrid Calling softphone call scenarios in the Cisco Webex Teams app. These steps verify whether you correctly configured Hybrid Call Service Connect and can help isolate any potential issues.

Calls are anchored through the caller's Unified Communications Manager. Any transformations and routing rules are applied exactly as if the call had been placed from a desk phone.

When dialing from Cisco Webex Teams, use the same dial strings or prefixes as you do on your desk phone; Cisco Webex Teams functions like any other desk phone registered to your Unified Communications Manager.

Before you begin

- Unless otherwise stated, these steps assume that the person who initiates the test calls (you or another test user) is enabled for Hybrid Calling.
- Open your Cisco Webex Teams apps.

Procedure

Step 1
Place a call from your primary desk phone to another hybrid user's desk phone.

If you configured the service correctly:
- For the called party, both the Cisco Webex Teams app and desk phone ring.
- A space appears at the top of both of your lists in Cisco Webex Teams.
- If the call is answered on the app, the call duration appears.
- After the call ends, a record of the call appears under \( \) in your apps.

Step 2
Place a call from your Cisco Webex Teams app to another hybrid user in one of the following ways.

- Search for the user in Cisco Webex, and from the space with that user, go to the activity menu \( \) and then choose Call \( \).
• From 
  enter the user’s primary directory number or directory URI.
In all of these cases, the called party is notified on both the app and desk phone.

What to do next

• If any of the above calls fail, double-check the configuration steps in the deployment chapter and see Troubleshoot Hybrid Calling, on page 83 for further guidance.
• If your configuration seems correct but you encounter unexpected behavior, see the Known Issues and Limitations with Hybrid Calling for Webex Teams Users, on page 63.

Known Issues and Limitations with Hybrid Calling for Webex Teams Users

This section covers the known issues and limitations for Hybrid Calling for users. Each entry is presented in a logical flow with the expected behavior, from registering the Expressway-C to enabling users for Hybrid Calling to call behavior (including call history).

If you also have Mobile and Remote Access deployed, see Unsupported Expressway Features and Limitations.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Expected Behavior</th>
<th>Limitations and Exceptions</th>
<th>Issues and Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Register the Expressway-C to host Call Connector</td>
<td>Download and install Call Connector on Expressway-C</td>
<td>Each Expressway-C cluster must have a unique IP address for the master peer</td>
<td>N/A</td>
</tr>
<tr>
<td>Configure Call Connector</td>
<td>Establish AXL connection between Call Connector and Unified CM</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Configure SIP connection between Unified CM and Cisco Webex through Expressway-C/E</td>
<td>Calls to and from domain callservice.webex.com securely routed through the Expressway-C/E over public Internet</td>
<td>Multiple secure SIP trunks between Unified CM and Expressway-C are not supported by Unified CM</td>
<td>N/A</td>
</tr>
</tbody>
</table>
# Known Issues and Limitations with Hybrid Calling for Webex Teams Users

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Expected Behavior</th>
<th>Limitations and Exceptions</th>
<th>Issues and Workarounds</th>
</tr>
</thead>
</table>
| Enable User for Hybrid Calling       | • Find user’s home cluster, assign user to Call Connector                         | The name for an automatically created Cisco Spark-RD is based on the Unified CM user ID and are limited to a maximum of the first 15 characters. A manually created Cisco Spark-RD must also be 15 characters or less. | The user remains in a pending activation state because the remote destination URI (Webex SIP address) is too long:  
  • Replace CTI-RD with Cisco Spark-RD (may require Unified CM upgrade) |
|                                      | • Use call connector to create Cisco Spark-RD on Unified CM 11.5(1) SU3 or later. Or manually provision Cisco Spark-RD in Unified CM. | A remote destination for hybrid call users (such as `user@example.calls.webex.com`) cannot be associated to both a Cisco Spark-RD and Remote Destination Profile at the same time. Otherwise, the remote device fails to activate. | |
|                                      | • Call Connector automatically adds the remote destination URI (Cisco Webex SIP Address) in both cases. |                                                                                              | |

## Call Behavior

| Call from Hybrid Calling user’s Cisco Webex Teams app to company extension or PSTN number | Address is interpreted and call is routed by Connect user’s Unified CM | N/A | No video or share:  
  • Replace CTI-RD with Cisco Spark-RD (may require Unified CM upgrade)  
  Unified CM licensing out of compliance:  
  • Replace CTI-RD with Cisco Spark-RD (may require Unified CM upgrade) |
<table>
<thead>
<tr>
<th>Use Case</th>
<th>Expected Behavior</th>
<th>Limitations and Exceptions</th>
<th>Issues and Workarounds</th>
</tr>
</thead>
</table>
| Call to Hybrid Calling user’s UC device also offered to Connect user’s Cisco Webex Teams app | Notification and option to “Answer” on Connect user’s Cisco Webex Teams app | Call may be offered to Hybrid Calling user’s Jabber client or SNR Remote Destination on same platform as Cisco Webex Teams app, with resulting conflicts. Calls from a user’s Cisco Webex Teams app to a hunt group are not offered to the Cisco Webex Teams app of a hunt group member who is also a Connect user. Depending on the Unified CM release, users' UC devices may continue to alert after the call is declined on the Hybrid Calling user’s Cisco Webex Teams app. | Call does not alert on user’s Cisco Webex Teams app:  
- Replace CTI-RD by Cisco Spark-RD (may require Unified CM upgrade)  

Call answered on UC device may be reported as missed on user’s Cisco Webex Teams app  
Persistent Call busy  
- Replace CTI-RD with Cisco Spark-RD (may require Unified CM upgrade)  

Users' UC devices continue to alert  
- Upgrade to Unified CM 11.5(1) SU5 or 12.5(1), which contains a fix that immediately diverts a call to the user's UC voicemail when declined in the Webex Teams app. |
| Call history entry for when an incoming call ends that was placed to a Hybrid Calling user | Calls answered on Webex Teams are logged in call history. | Calls answered on UC endpoints are logged as a “missed call” in call history. | N/A |
| Call history entry for when a Hybrid Calling makes an outgoing call | • Calls that originate from Webex Teams are logged in call history.  
• Calls that originate from UC endpoint depend on the remote party:  
  • Calls to a Webex Teams or Meetings URI are logged in call history.  
  • Calls to a fellow Hybrid Calling user who answers on Webex Teams are logged in call history. | • Calls from a UC endpoint to a PSTN or UC only user do not appear in Webex Teams call history.  
• Calls from a UC endpoint to a fellow Hybrid Calling user that are answered on the user's UC endpoint appear as a "missed call" in call history. | N/A |
<table>
<thead>
<tr>
<th>Use Case</th>
<th>Expected Behavior</th>
<th>Limitations and Exceptions</th>
<th>Issues and Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call to a Hybrid Calling user from a Cisco Webex Calling (formerly Spark Call) user.</td>
<td>If the call originates in the calling user's Webex Teams app, the call is offered to the Hybrid Call Service user's Webex Teams app and enterprise desk phone.</td>
<td>If the call originates from a connected desk phone in the calling user's Webex Teams app, the call is offered to the Hybrid Call user's Webex Teams app but is not offered to the Hybrid Call Service user's enterprise desk phone.</td>
<td>—</td>
</tr>
<tr>
<td>Call to a Hybrid Calling user who is configured for Single Number Reach (SNR).</td>
<td>The call is offered to the user's mobile Cisco Webex Teams app and mobile number at about the same time.</td>
<td>The call that arrives first takes priority in the native dialer (whether or not the device is on the lock screen). So if the Cisco Webex Teams app call arrives first, there is no opportunity to answer the SNR call on mobile voice. If the SNR call arrives first, the user can still answer the Cisco Webex Teams call, but only by first opening the app.</td>
<td>On mobile, users can prevent Cisco Webex Teams calls from using the native dialer by using this procedure. If the option is set to disallow answering on the lock screen, the user must always open the Cisco Webex Teams app to answer an in-app call.</td>
</tr>
<tr>
<td>Calls to a hunt group may or may not alert the Webex Teams app of a Hybrid Calling user. This behavior depends on the specific configuration of the hunt group. Alerting the Webex Teams apps of a Hybrid Calling user does not depend on whether the user is logged into or out of the hunt group.</td>
<td>Hunt groups are not supported.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Call from Hybrid Calling user’s Cisco Webex Teams app to IP address</td>
<td>IP address dialing is not supported.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Deactivate Hybrid Calling For Your Organization**

You can temporarily deactivate Hybrid Calling for your organization if you need to perform maintenance (such as changing Webex SIP addresses). You can permanently deactivate Hybrid Calling if you no longer need to run the service.
Procedure

Step 1

From the customer view in https://admin.webex.com, deactivate Hybrid Calling for your organization by going to Services, choosing Edit settings on the Hybrid Call card, scrolling to Call Service Connect, and then clicking Deactivate.

As soon as the service is deactivated, Hybrid Calling calls will not route. This step temporarily converts you to a cloud calling organization; during this state, you can perform related maintenance as needed (for example, modify the SIP addresses for calling).

Note: Deactivating Hybrid Calling does not remove the service from Webex Teams users or clean up any automatically created Cisco Spark-RD on Unified CM.

Step 2

Choose a step, depending on your goal:

• If you deactivated the service temporarily, ensure that any needed configuration is completed, go back to the customer view in https://admin.webex.com, and reactivate Hybrid Calling for your organization by going to Services, choosing Edit settings on the Hybrid Call card, scrolling to Call Service Connect, and then clicking Activate.

• If you deactivated the service permanently, you may need to perform additional cleanup on Webex Teams user accounts and Unified CM.
  • Remove the Hybrid Calling toggles from Webex Teams user accounts. (You can do this individually or in bulk.)
  • Remove any remaining Cisco Spark-RD on Unified CM.

Related Documentation

See the following documents for further information about Cisco Webex Hybrid Services, including how to manage and troubleshoot your deployment:

Table 8: Related Documentation for Cisco Webex Hybrid Services

<table>
<thead>
<tr>
<th>Category</th>
<th>Links to Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>• Cisco Collaboration Preferred Architectures</td>
</tr>
<tr>
<td></td>
<td>• Add, Verify, and Claim Domains</td>
</tr>
<tr>
<td></td>
<td>• Requirements for Business-to-Business (B2B) Calls To and From Cisco Webex</td>
</tr>
<tr>
<td></td>
<td>• Network Requirements for Cisco Webex Services</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex SIP Addresses</td>
</tr>
<tr>
<td>Category</td>
<td>Links to Documentation</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>• Manage Hybrid Services Resources</td>
</tr>
<tr>
<td></td>
<td>• Call Connector Release Notes</td>
</tr>
<tr>
<td></td>
<td>• Resource Groups for Hybrid Services</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>• Send Expressway Connector Logs to the Cloud</td>
</tr>
<tr>
<td></td>
<td>• Troubleshooting Guide for Hybrid Call Service Connect</td>
</tr>
<tr>
<td></td>
<td>• Hybrid Services and Connector Troubleshooting</td>
</tr>
</tbody>
</table>

If you're looking for something else, you can search [https://collaborationhelp.cisco.com](https://collaborationhelp.cisco.com). You can also bookmark [https://www.cisco.com/go/hybrid-services](https://www.cisco.com/go/hybrid-services).
CHAPTER 4

Deploy Hybrid Call Service for Cisco Webex Devices

• Requirements for Hybrid Calling for Cisco Webex Devices, on page 69
• Hybrid Calling for Cisco Webex Devices Task Flow, on page 70
• Create a Directory Number for Cisco Webex Devices With Hybrid Calling, on page 72
• Create a Unified CM Account for Cisco Webex Devices with Hybrid Calling, on page 73
• Create an Automatic Cisco Spark-RD for Cisco Webex Devices with Hybrid Call Service, on page 75
• Create a Cisco Spark-RD for Cisco Webex Devices With Hybrid Call Service, on page 76
• Enable Hybrid Calling for a New or Existing Place With Webex Devices, on page 77
• Check Status of Cisco Webex Devices With Hybrid Call Service, on page 78
• Errors and Causes for Hybrid Call Service for Cisco Webex Devices, on page 78
• Rename a Place Enabled for Hybrid Calling, on page 80
• Known Issues and Limitations with Hybrid Call Service for Cisco Webex Devices, on page 81
• Remove Hybrid Calling from A Cisco Webex Device, on page 81

Requirements for Hybrid Calling for Cisco 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 Cisco 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 Cisco Webex Devices. (See Hybrid Calling for Cisco Webex Devices, on page 2)

• Before you can set up Hybrid Calling for Cisco Webex Devices, you require a Cisco Webex organization with Hybrid Calling already deployed. A typical deployment also has these services enabled for Webex Teams users. See these chapters for more information on the requirements and deployment steps to get up and running:
  • Prepare Your Environment, on page 5
  • Deploy Hybrid Calling for Webex Teams Users, on page 19

• A Expressway-C search rule with a
  .+\.*\.(ciscospark)\((rooms|calls)\.webex\.com\).* search pattern string. This is the search rule that you're required to configure when you set up Hybrid Calling for your organization,
so it should already be configured if Hybrid Calling is working for your organization. The rule identifies
any calls (by Cisco Webex devices in a Place) arriving at Expressway-C that are destined for the Cisco
Webex cloud, and routes them outwards (through the traversal client zone) to the Expressway-E. (See
the second search rule in Configure Search Rules on Expressway-C (to Unified CM), on page 58 for
more information.)

- Supported Cisco Webex Room, Board, and Desk Devices (not including phones)
- The Unified CM user account that'll represent the Place account must have a minimum Enhanced UCL
license. (See Cisco Spark Remote Device Overview and License Requirements, on page 17 for more
information.)
- Hybrid Calling for Cisco 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 5 for more information.) These devices are associated with Unified CM accounts that represent
Cisco Webex Places.
- A supported Expressway traversal pair release. (See Requirements for Hybrid Calling, on page 5 for
more information.)
- The latest version of Call Connector (See Call Connector Release Notes and Manage Installations and
Automatic Upgrades for Cisco Webex Hybrid Services Resources for more information.)

Hybrid Calling for Cisco Webex Devices Task Flow

This task flow walks you through how to configure Unified CM settings for Cisco Webex devices and how
to add Hybrid Calling to either a newly created Place with Cisco Webex devices or an existing Place with
Cisco Webex devices. A Place is configured in Cisco Webex Control Hub.

Figure 7: Field Mapping Between Cisco Webex Control Hub and Unified CM

As you configure Hybrid Call Service Cisco Webex Devices, refer to this screenshot which shows the mapping
of fields between Cisco Webex Control Hub (on the left) and Unified CM (on the right).
The following points provide a functional overview of the feature:

- This feature creates and uses a Cisco Spark Remote Device (Cisco Spark-RD) in on-premises Unified CM to route calls to enterprise extensions, users, and PSTN.

- Features that are initiated from on-premises phones (such as hold, transfer, and conference) can include Cisco Webex devices with Hybrid Call Service.

- Any calls from Cisco 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 Cisco Webex Devices, on page 2
- Complete the requirements: Requirements for Hybrid Calling for Cisco Webex Devices, on page 69

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Create a Directory Number for Cisco Webex Devices With Hybrid Calling, on page 72</td>
<td>Use Cisco Unified CM Administration to configure directory numbers that you want to assign to room devices in a place and assign directory URIs to the directory numbers.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Create a Unified CM Account for Cisco Webex Devices with Hybrid Calling, on page 73</td>
<td>Cisco Webex devices in a place are registered to the cloud, but you can associate a number to them from an on-premises Cisco Unified Communications Manager (Unified CM). You...</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>can use a Unified CM end user account to represent a place. (The place contains Cisco Webex-registered devices in a physical location.) 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 place.</td>
</tr>
</tbody>
</table>

**Step 3** Choose a method to create Cisco Webex Remote Devices:  
- Create an Automatic Cisco Spark-RD for Cisco Webex Devices with Hybrid Call Service, on page 75  
- Create a Cisco Spark-RD for Cisco Webex Devices With Hybrid Call Service, on page 76   

Call Connector can automatically associate a Cisco Spark-RD and Cisco Webex SIP address to the user account that represents Cisco Webex devices in a place. Or you may choose to create them manually and assign them to this account, if you need to make granular changes to the settings for each Cisco Spark-RD. Behind the scenes, the Cisco Spark-RD ties together call activity in the cloud and the premises.

**Step 4** Enable Hybrid Calling for a New or Existing Place With Webex Devices, on page 77.   

You can register shared Cisco Webex devices to the Cisco Webex cloud. Whatever device you choose to add to a place, the device is assigned to the place, not a user. That's the key advantage of the Place feature: shared usage.  

You can add Hybrid Calling to Cisco Webex devices in a new Place that you create or an existing Place that you've already created.

**Step 5** Check Status of Cisco Webex Devices With Hybrid Call Service, on page 78  

---

**Create a Directory Number for Cisco Webex Devices With Hybrid Calling**

Use Cisco Unified CM Administration to configure directory numbers that you want to later assign to Cisco Webex devices in a Place. You'll also assign directory URIs to the directory numbers.

**Before you begin**

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

**Procedure**

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

**Step 2**
For the place, 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 place.

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: !#$'()*+,./:;=?@^_

*Note* The Alerting Name field is used to populate the display name (part of the line presentation) when autocreating the Cisco Spark-RD for the place. If you'll create Cisco Spark-RD automatically from the call connector, make sure that the Alerting Name and Alerting Name ASCII values don't exceed 30 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.

**Things to Keep in Mind**

After you create a Place in Control Hub and add Hybrid Calling to the devices in it, 2 directory URIs are associated with the directory number for those devices: The one that was created manually and added to the line on Unified CM, and the one created as a result of the onboarding process (this one has the Directory URI partition assigned).

---

**Create a Unified CM Account for Cisco Webex Devices with Hybrid Calling**

Even though the Cisco 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 Cisco Webex devices in a place. The place contains Cisco Webex-registered devices in a physical location.

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 place.
The call connector for your hybrid call environment associates the place with the account for the device. The connector identifies the Unified CM cluster that can service that particular place, assigns a directory number and URI, and assigns a Cisco Webex SIP address. Behind the scenes, the Cisco Spark-RD ties together activity in the cloud and the premises.

**Before you begin**

- The email address domain must be one of your verified domain entries in Cisco Webex Control Hub (https://admin.webex.com). See Add, Verify, and Claim Domains.
- Hybrid Calling must be enabled for your organization, but you don't have to enable the corresponding Cisco Webex Teams user account for Hybrid Calling in Cisco Webex Control Hub.
- Create an Automatic Cisco Spark-RD for Cisco Webex Devices with Hybrid Call Service, on page 75 on the Call Connector.

**Procedure**

**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 place.
- Click Add New to create a new account to represent a place.

**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 place, 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 Place. 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 Place on the devices, enter the Telephone Number as the full E.164 number.

This number will show up on your hybrid-enabled Place. You could also use an internal number or extension. If you have multiple Webex devices in the Place, 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 Cisco Webex SIP address, which Cisco Webex forks to all the Webex devices in the Place.

**Step 5**
Verify that Mail ID contains a unique email address that you'll use for the Place.

The email address must be an exact match between both Cisco Webex and on-premises. Use unique email accounts for each Place.

**Caution**
Do not use the same account for:

- Multiple Cisco Webex Places
- A Cisco Webex Teams user and a Cisco Webex Place

**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 place, and then save your changes.

**Note** If you are going to manually create each Cisco Spark-RD, do this step after you create the devices.

---

**Create an Automatic Cisco Spark-RD for Cisco Webex Devices with Hybrid Call Service**

Call Connector can automatically create and associate a Cisco Spark-RD and Cisco Webex SIP address to user accounts that represent Cisco Webex devices in a Place. Behind the scenes, the Cisco Spark-RD ties together call activity in the cloud and the premises.

**Procedure**

**Step 1**
From the Expressway-C connector host, go to **Applications > Hybrid Services > Call Service > Unified CM Servers**, and then the Cisco Unified Communications Manager node that you configured.

**Step 2**
For **Cisco Spark Remote Device Configuration Type**, choose **Automatic**.

**Caution** A name for an automatically created Cisco Spark-RD is generated based on the Unified CM user account that is associated with a place. The resulting device names are limited to a maximum of the first 15 characters of the Unified CM user account name. If you observe any activation failures because of duplicate names for the devices, use Cisco Unified CM Administration to manually create a Cisco Spark-RD.

**Step 3**
Choose values from the prepopulated lists for the **Device Pool**, **Location**, **Calling Search Space**, and **Reroute Calling Search Space**.

For automatic creation, these settings are applied to each Cisco Spark-RD. Read these documents to understand the settings:

- **Device pools**
- **Locations**
- **Calling search spaces**

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

**Step 4**
Click **Save** to automatically create each Cisco Spark-RD.
Create a Cisco Spark-RD for Cisco Webex Devices With Hybrid Call Service

The Cisco Spark-RD is a virtual device that is attached to a user's work number and links the user's Cisco Webex account SIP identity to the enterprise SIP identity so that calls anchor on the Unified CM side or fork to the Cisco Webex cloud side.

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

Procedure

Step 1 From the Expressway-C connector host, go to Applications > Hybrid Services > Call Service > Unified CM Servers, and then the Cisco Unified Communications Manager node that you configured.
Step 2 For Cisco Spark Remote Device Configuration Type, choose Manual, and then click Save.
Step 3 From Cisco Unified CM Administration, go to Device > Phone, click Add New, and then choose Cisco Spark Remote Device.
Step 4 For Owner UserID, specify the user account for the place 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 5 For line association, specify the primary extension (the shared line).
Step 6 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 Place to be able to reach (conference bridges, enterprise-to-enterprise trunks, and so on).
Step 7 Save your changes.
Step 8 From Cisco Unified CM Administration, go to User Management > End User, and then reopen the user account for the Place.
Step 9 Under Device Information, click Device Association.
Step 10 Specify any search criteria and click Find.
Step 11 Check the remote device that you created, and then save your changes.
The remote device is associated with the Place end user account and is added to the controlled devices list. The Cisco Webex SIP address is automatically created as the remote destination under Associated Remote Destinations.

**Note**  
The Cisco Spark-RD is the only device in the controlled device list; you must configure the desired Call Forward Busy (CFB) destination (for example, Unity Connection) for when a hybrid call is declined in the Cisco Webex Teams app.

User accounts in Unified CM that represent Cisco Webex devices will not usually have voicemail box. If calls are forwarded to Unity Connection, they will reach the top-level menu. An alternative treatment (for example, playing a busy tone or an announcement) may be preferable.

**Step 12**  
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 Place, and then save your changes.

---

**Enable Hybrid Calling for a New or Existing Place With Webex Devices**

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

**Procedure**

- To create a new Place, add a device, and enable Hybrid Calling:
  a) From the customer view in https://admin.webex.com, go to Places, and then click Add Place.
  b) Enter a name for the Place (such as the name of the physical room), and then click Next.
  c) Choose Other Cisco device (for Webex cloud-registered devices), and then click Next.

  You can only have one type of device in a single Place. For example, you can a single Cisco Webex Room Device or a Webex Board, but not a combination of the two.

  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 Place.

  The service discovers where the email address is located on a Unified CM cluster. Once discovered, the service creates the Cisco Spark-RD and identifies the directory number and SIP URI associated with the account.

  e) Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration.
  f) Click Next, and then activate the device with the code provided.

- To enable Hybrid Calling for devices in an existing Place:
  a) From the customer view in https://admin.webex.com, go to Places, and then choose the Place that you want to update.
  b) Click Edit, 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 Cisco Webex devices in the Place.
The service discovers where the email address is located on a Unified CM cluster. Once discovered, the service creates the Cisco Spark-RD and identifies the directory number and SIP URI associated with the account.

c) Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration and then click Done.

Check Status of Cisco Webex Devices With Hybrid Call Service

Before you begin

You must wait over night after creating the new user on Unified CM for Cisco Webex devices added to a new place. The call connector does a nightly synchronization to pick up these changes.

Procedure

Step 1
From the customer view in https://admin.webex.com, go to Devices, and then search for any room devices to which you added Hybrid Calling.

Step 2
Click the room device name to view the Hybrid Calling activation status.

Step 3
(Optional) If the status is Pending Activation for some time, click Launch Advanced Settings to open the device's web interface, and then go to Maintenance > Restart to restart the device remotely.

Step 4
Click the status indicator to change the mail ID, if needed. Click further to see the history.

What to do next

- Later, you may need to make a change to Unified CM end users or devices. If you do this to fix a configuration error, even if the call connector's “user validation test” passes for that user, you must go to the Expressway-C and restart call connecter so that it picks up the configuration change.

- If there are issues with the device itself, you can report an issue, which creates a ticket and automatically attaches the device logs.

Errors and Causes for Hybrid Call Service for Cisco Webex Devices

Table 9: Errors and Causes for Hybrid Call Service for Cisco Webex Devices

<table>
<thead>
<tr>
<th>Error</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place Update Error: Cisco Spark-RD not supported</td>
<td>Unsupported Unified CM version</td>
<td>Upgrade Unified CM to a version that supports Cisco Spark-RD.</td>
</tr>
<tr>
<td>The Cisco Spark-RD has no configured Directory Numbers</td>
<td>Cisco Spark-RD associated with user does not have a line</td>
<td>Add the line specified in the end user to the Cisco Spark-RD.</td>
</tr>
<tr>
<td>Error</td>
<td>Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Could not find a Place with this Email Address</td>
<td>No end user with the specified email was found in Unified CM</td>
<td>Make sure that an end user with the email address is configured in Unified CM. Also make sure the home cluster is enabled on that user account. Make sure you are using the email as the directory URI for the user on Unified CM and when adding the Place in Webex Control Hub.</td>
</tr>
<tr>
<td>User is missing primary Directory Number</td>
<td>The end user for a Place has device(s) but no primary DN is configured. This is likely to happen when another device already exists in the end user account.</td>
<td>Manually add the primary directory number. Make sure the directory URI is set for the directory number on Unified CM. The value should also match the email address/directory URI for the user and the directory URI you're using when adding the Place in Webex Control Hub.</td>
</tr>
<tr>
<td>Primary Directory URI Mismatch With Directory URI of Primary Line</td>
<td>Directory URI configured for user is not found in the line</td>
<td>This is generally possible when there are multiple lines associated with a Cisco Spark-RD but the primary directory number does not match the Directory URI configured in the end user account. Make sure the directory URI is set for the directory number on Unified CM. The value should also match the email address/directory URI for the user and the directory URI you're using when adding the Place in Webex Control Hub.</td>
</tr>
<tr>
<td>Unable to Add the User's Cisco Webex SIP Address</td>
<td>Associating Cisco Webex SIP Address to Cisco Spark-RD failed.</td>
<td>Missing Cisco Spark-RD or appropriate routing to Cisco Webex is not configured.</td>
</tr>
<tr>
<td>Primary Directory Number is not Configured on User's Controlled Devices</td>
<td>The primary directory number specified for the user is not provisioned in any of the user's controlled devices</td>
<td>Verify in Unified CM that the primary directory number configured for the end user is at least found in the user's controlled devices. This is likely when a device (like a Conference Room phone) is associated with the user.</td>
</tr>
</tbody>
</table>
Rename a Place Enabled for Hybrid Calling

You can change the name of a Place 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.

Procedure

**Step 1** From the customer view in https://admin.webex.com, go to Places, and then choose a place from the list to open the overview panel.

**Step 2** Click edit, enter the new name for the place, and then click the check box to save the changes.

**Step 3** Under Services, click Calling, then verify that the Webex SIP address is updated and marked as primary.

Next, the call connector needs to pick up on these changes and replicate them to the premises side in Unified CM as the remote destination for each Cisco Spark-RD.

**Step 4** Choose an option:

- Wait for the daily rediscovery, which occurs between 7 am and 11 am Universal Time Coordinated (UTC). The changes are picked up after this discovery period.
- Restart each call connector by following the steps in Restart the Call Connector from the Expressway-C, on page 40. In a multicluster deployment, restarting the connector on the primary node automatically restarts the other connectors in the cluster. The changes are picked up after the connector comes back online.

  **Caution** Restarting the Call Connector creates extra load on Unified CM publishers. Consider restarting the Call Connector during off-peak hours; during busy hours, a restart may cause service issues.

**Step 5** 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 Place has a remote destination that starts with the new Place name that you saved in Cisco Webex Control Hub.
Known Issues and Limitations with Hybrid Call Service for Cisco Webex Devices

- The name for an automatically created Cisco Spark-RD is generated based on the Unified CM user account that is associated with a Place. The resulting device names are limited to a maximum of the first 15 characters of the Unified CM user account name. If you observe any activation failures because of duplicate names for the devices, use Cisco Unified CM Administration to manually create a Cisco Spark-RD and specify a device name.

  A manually created Cisco Spark-RD must also be 15 characters or less.

- Call Connector immediately picks up new end user in Unified CM for activation. But any changes to that user afterwards (because of a failed activation) requires deactivation and reactivation of the Place.

- When you configure Cisco Webex devices with Hybrid Call Service, you first configure a URI while creating your directory number. Then, when the place 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 Cisco Webex SIP address for Cisco Webex devices is generated from the Place name. If this name is changed after you activate the devices with Hybrid Call Service, the remote destination (the Cisco Webex SIP address) on Unified CM is not updated. As a workaround, if the name is changed, deactivate and reactivate the Place.

Remove Hybrid Calling from A Cisco Webex Device

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

Procedure

**Step 1**
From the customer view in https://admin.webex.com, go to Places, search for the Place enabled for Hybrid Calling, and then open it.

**Step 2**
Next to Services, click Edit, choose Free Calling (default), and then click Save.

This step does not delete the Place. It removes Hybrid Calling functionality from the Cisco Webex devices in the Place and the Cisco Spark-RD from Unified CM. Any devices in the remaining place can still support the features that come with free calling, specifically SIP dialing and pairing to the Cisco Webex Teams app.
CHAPTER 5

Troubleshoot Hybrid Calling

- Troubleshooting Sources for Hybrid Call Service, on page 83
- Cisco Webex Status Page, on page 87
- Restart the Call Connector from the Expressway-C, on page 87
- Mutual TLS and SIP Destination, on page 88
- Test Calls, on page 89
- Cisco Webex Control Hub and Expressway-C Connector Hosts, on page 89
- Expressway Pair Configuration, on page 90
- Unified CM Configuration, on page 91

Troubleshooting Sources for Hybrid Call Service

This section covers the various troubleshooting information sources and tools that are at your disposal. You can access these troubleshooting sources from Cisco Webex Control Hub or on the Expressway connector host.

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 below.

Related Topics
- Known Issues and Limitations with Hybrid Calling for Webex Teams Users, on page 63
- Known Issues and Limitations with Hybrid Call Service for Cisco Webex Devices, on page 81

Hybrid Connectivity Test Tool (Control Hub)

You can access the Hybrid Connectivity Test Tool from Cisco Webex Control Hub: from the customer view in https://admin.webex.com, go to Services, click Edit settings in the Hybrid Call card, scroll to Call Service Connect, 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>
<thead>
<tr>
<th>Error</th>
<th>Keyword</th>
<th>More Information and Troubleshooting Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>No DNS addresses found</td>
<td>DNS SRV</td>
<td>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 <a href="#">Unable to resolve the Expressway-E DNS SRV/hostname</a> in the troubleshooting guide for more information.</td>
</tr>
</tbody>
</table>
| 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:  
  - 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](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:  
  - Socket Failure: Port 5062 is Blocked Inbound to Expressway  
  - Socket Failure: Expressway-E is not Listening on Port 5062 |
| TCP read/write failure         | Socket failure           | TCP read/write failure: Please try again. If the error persists, check network connectivity, firewall configuration, and Mutual TLS configuration. See these sections of the troubleshooting guide for more information:  
  - Socket Failure: Port 5062 is Blocked Inbound to Expressway  
  - Socket Failure: Expressway-E is not Listening on Port 5062 |
**Status History (Control Hub)**

You can access the user status history in Cisco Webex Control Hub: from the customer view in https://admin.webex.com, go to Users, click the user to open the overview pane, click Call Service, then Aware, and next to Status, click See history.

The status history in Cisco Webex Control Hub does the following:

- Displays alarm and other status messages that pertaining to a user
- Indicates the cluster and node that generated the status event for the user
- Provides the last 20 historical events for the user

**User Status Report (Control Hub)**

You can access the user status report from Cisco Webex Control Hub: from the customer view in https://admin.webex.com, go to Services, choose Edit settings from the Hybrid Call card, and then click User Status Report.

The user status report shows which users are in error for service and why. You can export the report as a CSV file.

---

<table>
<thead>
<tr>
<th>Error</th>
<th>Keyword</th>
<th>More Information and Troubleshooting Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Failure</td>
<td>Socket failure</td>
<td>TCP failure: TCP read/write failure: Please try again. If the error persists, check network connectivity, firewall configuration, and Mutual TLS configuration. See these sections of the troubleshooting guide for more information:</td>
</tr>
</tbody>
</table>
|               |               | - Socket Failure: Port 5062 is Blocked Inbound to Expressway  
|               |               | - Socket Failure: Expressway-E is not Listening on Port 5062 |
Alarms for Hybrid Call Service (Expressway Connector)

During or after Cisco Webex Hybrid Call Service deployment, you may receive an error message in Cisco Webex Control Hub (and email, if you have alerts configured). The Expressway connector host can provide troubleshooting information in the form of alarms. The Expressway connector alarms are triggered for various reasons:

- Connector crashes
- Connectivity issues with the Webex cloud or Unified CM.
- User errors

Use this information to understand the issue, possible causes, and actions that you can take to correct the issue.

Failed to Create Cisco Spark-RD

**Cause**

When a user is enabled for Hybrid Calling, the Call Connector attempts to create a Cisco Spark-RD for the user.

- The remote device creation may fail because you already have a device or a remote destination profile with the same name. Duplicate names are not supported.
- Cisco Spark-RD devices are created with the naming convention SparkRD<username>. If that name goes beyond 15 characters, the system uses just the username. You may already have a phone or remote destination profile that is named after that same username.

**Solution**—Identify the duplicated naming issue on Unified CM, resolve the name, and then wait for a day to allow the Call Connector's cache to synchronize with the Unified CM change or restart the Call Connector through the Expressway UI (disable and reenable the connector by using the steps in Restart the Call Connector from the Expressway-C, on page 40). Then reenable Hybrid Calling for the user in Control Hub.

Failed to Create the User's Remote Device

**Possible Cause**—Call Connector did not create a remote device for the user. Some required configuration is missing.

**Solutions**

- Check the required user configuration on Unified CM as detailed in the Prepare and Deploy chapters in www.cisco.com/go/hybrid-services-call.
- Before you enable Webex Teams users for Hybrid Calling, make sure that the user's associated Directory Number Alerting Name and ACSII Alerting Name are no more than 30 characters in length. The names can only contain letters, numbers, spaces, and the following special characters: !#$'()*+,./:;=?@^_

Unable to Add Cisco Spark SIP Address in Unified CM

**Possible Cause**—This error typically appears if you created remote destinations manually. Even though you can create a Cisco Spark Remote Device automatically or manually, remote destinations are created automatically in all cases.

**Solution**—Remove the manually created remote destination, restart the call connector to flush the Unified CM cache, and then reattempt the user activation.
The User is Configured on More Than One Unified CM Cluster

Possible Causes

• The user is configured on multiple Unified CM clusters and has the home cluster value checked on them.

• If the user is configure on just one cluster with the home cluster value checked, the Unified CM and subscribers were added to the call connector inadvertently. You only need one Unified CM node per cluster.

Solutions

• Ensure that the Unified CM end user account is on a single home cluster.

• In the Call Connector, add only a single node per cluster running AXL and serviceability service.

User Validation Check (Expressway Connector)

You can access the user validation check from the Expressway connector host: go to Applications > Hybrid Services > Call Service > Unified CM Servers, and choose the registered Cisco Unified Communications Manager that you want to check.

With the user validation check, you can check whether Cisco Unified Communications Manager users are properly configured for Hybrid Calling. The test checks configuration prerequisites, such as email, directory URI, Cisco Spark Remote Device settings, whether home cluster is enabled, and whether the primary directory number has a directory URI. The check is based on which users were attempted to be discovered on the specific Call Connector node.

For more information, see Check Your User Configuration for Cisco Webex Hybrid Call Service, on page 41.

Cisco Webex Status Page

If calls from Cisco 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.

Related Topics

Sign Up for Issue Notifications

Restart the Call Connector from the Expressway-C

Disable and reenable the Call Connector, so that the connector captures Unified CM user and device configuration changes that you made while deploying Cisco Webex Hybrid Call Service. During this restart cycle, the connector creates a remote destination with the Cisco Webex SIP address on the Cisco Spark Remote Device. This address is associated with end user accounts and the corresponding Cisco Webex Teams accounts. Toggle this setting as a troubleshooting step if you experience any issues, too.
When you upgrade your Unified CM environment with Cisco Webex Hybrid Services and Webex Teams, information that is cached in the Call Connector might be stale. In this case, the affected items are the automatic synchronization of the database cache or reporting the new Unified CM version to the Cisco Webex cloud. Restart the Call Connector to select the latest information in the new database and also publish the new Unified CM version information to the Cisco Webex cloud services.

**Before you begin**

⚠️ Caution
Restarting the Call Connector creates extra load on Unified CM publishers. Consider restarting the Call Connector during off-peak hours; during busy hours, a restart may cause service issues.

**Procedure**

Step 1
From Expressway-C, go to Applications > Hybrid Services > Call Service > Call Service Overview, change the call connector status to Disabled, and then click Save.

Step 2
Change the status back to Enabled, and then save again.

**Troubleshooting Tips**
Later, you may need to change to Unified CM end users or devices. If you do this to fix a configuration error, even if the call connector's "user validation test" passes for that user, you must restart Call Connector so that it selects the configuration change.

**Things to Keep in Mind About Unified CM Cache**
Call Connector maintains a cache of Unified CM data, so that AXL requests have limited performance impact on Unified CM nodes during user discovery and activation.

Cached data includes:
- Users
- Devices (including user associations)
- Directory numbers (including line appearances, user association, URIs)
- Remote Destinations

Call Connector uses change notifications on the publisher nodes to pull new user data. The poll interval is every 2 minutes. Because of limitations with Unified CM change notifications, the cache is rebuilt every night at 11 pm local time or upon Call Connector restart.

**Mutual TLS and SIP Destination**

Check these troubleshooting points related to the mutual TLS connection and certificates:
- Install the Cisco 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 Cisco 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 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.

Test Calls

• Try a test call between two Cisco Webex Teams users in the same organization; for this test, we recommend that both callers be enabled for Cisco Webex Hybrid Call Service.
• If either of the users is configured for Cisco Webex Calling (formerly Spark Call), the call does not route to your environment.
• Try to route a call from the enterprise side to the cloud first. This test allows you to verify that mutual TLS is set up correctly without having Cisco Webex routing decisions in the equation.

Cisco Webex Control Hub and Expressway-C Connector Hosts

⚠️ Note
You must upgrade to the latest stable connector release as a prerequisite for technical support. See Configure Automatic Software Upgrades for Hybrid Services for guidance.

• From the customer view in https://admin.webex.com:
  • Check for warnings that are related to Hybrid Call Service configuration:
    • Go to Services on the settings page from the Hybrid Call card.
• Go to Users on the individual user's Call Service settings page.

• If you see user activation errors, run a user status report from Services > Hybrid Call > Edit settings > User Status Report.

• From the Expressway-C connector host, run the user validation check to identify any on-premises user configuration issues.

• From the Expressway-C connector host, check the following items:
  • Cisco Unified Communications Manager connectivity under Applications > Hybrid Services > Call Service > Unified CM Servers.
  • Connectivity to the cloud and user status under Applications > Hybrid Services > Call Service > Call Connector Status.

• Check for alarms on the Call Connector that are related to hybrid call service users or user activation under Applications > Hybrid Services > Connector Management > Call Connector.

Note: User activation status is not real time; toggling on the hybrid call services for users can take up to six minutes to process.

Related Topics
Check Your User Configuration for Cisco Webex Hybrid Call Service, on page 41

Expressway Pair Configuration

• For calls that route from Cisco 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.

• For calls between hybrid users in Cisco Webex Teams that result in two call notifications on the called party’s app: ensure that SIP Parameter Preservation is enabled on the Expressways. This setting is required to carry a parameter that Cisco Webex adds to the contact header and fixes the double-call issue.

• 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 Cisco 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 Cisco 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**.
  
  • The call connector takes that value from the cluster FQDN setting on that same Cisco Unified Communications Manager, caches the value in the cloud, and uses it for every call that must go to that cluster.

• If a hybrid user calls a phone number from the Cisco Webex Teams app, the cloud sends it to the Expressway in the **user=phone** format as `phonenumber@CFQDN;user=phone`. The CFQDN in the route header determines the path that the call takes from Expressway to Cisco Unified Communications Manager. Cisco Unified Communications Manager accepts the **user=phone** format and CFQDN as the domain.

## Unified CM Configuration

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

• Directory URLs must match any domains that you verified in your organization.

• Check your codec configuration. See this document for more information about 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 Cisco Webex Teams meeting from a SIP device. We do not support G.729 for dialing 1:1 from Cisco Webex Teams to a SIP device or bridge.

• On the home Cisco 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:

<table>
<thead>
<tr>
<th>FQDN Guideline</th>
<th>Description and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple clusters</td>
<td>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.</td>
</tr>
<tr>
<td>No wildcards</td>
<td>Do not use entries with wildcards, such as <code>*.example.com</code> or <code>example*.com</code>.</td>
</tr>
</tbody>
</table>
### FQDN Guideline

<table>
<thead>
<tr>
<th>Description and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First FQDN entry for Hybrid Calling</strong></td>
</tr>
<tr>
<td><strong>Different from Expressway-E</strong></td>
</tr>
<tr>
<td><strong>New entry for Hybrid Calling</strong></td>
</tr>
</tbody>
</table>

- If you call another Hybrid Calling user from Cisco Webex Teams, the called user's app may ring once then stop, or the call immediately drops after it's answered. To fix these symptoms, configure your Unified CM SIP trunk for blended identity (Set **Calling and Connected Party Info Format** to **Deliver URI and DN in connected party, if available**). 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 Call Service. If this step was missed, the SIP trunk cannot transmit the enterprise-side party’s directory URI to Cisco Webex. Use the procedure in Configure Cisco Unified Communications Manager Settings for Hybrid Calling, on page 29.
Tool to Migrate CTI-RD to Cisco Spark-RD

You may have created CTI Remote Devices (CTI-RDs) when you initially deployed Hybrid Calling in your organization and enabled the service for your users. This device type is no longer supported for Hybrid Calling deployments.

Cisco Spark-RD is the required virtual device type for Hybrid Calling, as documented in the Cisco Spark-RD overview section. If you already set up CTI-RDs that contain Cisco Webex SIP addresses as remote destinations for your users, you must automatically migrate each CTI-RD to a Cisco Spark-RD using the migration tool on the Expressway-C that hosts the call connector. Whether you created the CTI-RDs manually or automatically, the tool takes care of the conversion.

We recommend that you schedule this migration activity outside of business hours. The migration won't cause a service outage, but will briefly affect individual users while their remote device migration is taking place.

- Migrate CTI-RD to Cisco Spark-RD, on page 93
- Cancel Cisco Spark-RD Conversion, on page 94
- Last Run Statuses for Migration Tool, on page 95
- Troubleshoot CTI-RD to Cisco Spark-RD Migration, on page 95

Migrate CTI-RD to Cisco Spark-RD

Convert each CTI-RD to a Cisco Spark-RD in one click. You can schedule the conversion during a maintenance window. As a guideline, converting devices for 5000 users can take up to 2 hours.

Before you begin

- Make sure you're running a supported version of Unified CM, or the conversion tool won't appear in Expressway. See Requirements for Hybrid Calling, on page 5.

- The migration tool only converts CTI-RDs if they have a remote destination and are associated with users enabled for Hybrid Calling. Each CTI-RD should only be associated with one "Webex Teams Client" remote destination.

- The tool assumes that the user's primary directory number is the only line associated with the CTI-RD. This line is the only directory number that will be associated with the Cisco Spark-RD.
Procedure

Step 1  From Expressway-C, go to Applications > Hybrid Services > Call Service > Unified CM Servers, scroll to Call Service Connect CTI Remote Device to Spark Remote Device Conversion, and then click Schedule Time for Conversion.

Step 2  From the drop-downs, choose a date and time during which to schedule the device conversion, and then click Schedule Spark Remote Device Conversion.

During this operation, do not restart the call connector.

Caution

• Avoid scheduling overlaps with call connector software upgrades, planned Unified CM upgrades, and any other maintenance activity.

• Do not schedule multiple Unified CM clusters for CTI-RD to Cisco Spark-RD migration at the same time. For example, if cluster 1 is scheduled at 6 pm in your time zone, you should schedule cluster 2 for 7 pm, cluster 3 for 8 pm, and so on.

Step 3  When the scheduled conversion completes and you see a message that says the conversion is finished, click View Conversion Results to view a report.

The report shows the results of the conversion: whether it's finished, how long it took, how many devices converted successfully, and how many failed (with an explanation) if any.

After the conversion is completed, you do not need to restart the call connector.

• Each migrated Cisco Spark-RD is populated with the description “Automatically converted through Spark Remote Device Conversion Tool for user ID”. This overrides the existing description for the CTI-RD.

• Each migrated Cisco Spark-RD shows Active Remote Destination as not set. This is normal and does not affect the operation of Hybrid Calling.

Cancel Cisco Spark-RD Conversion

You can cancel the CTI-RD migration if the tool's conversion process is taking too long or you decide you don't want to do it at this time.

Before you begin

While you can cancel the conversion, you must convert CTI-RD to Cisco Spark-RD if you want your Hybrid Calling to remain operational and officially supported.

Procedure

During the conversion process, click Cancel Spark Remote Device Conversion.
The tool completes conversion of any CTI-RDs in progress and then stops. The results page shows a Last Run Status of Cancelled, with the number of users processed so far.

---

**Last Run Statuses for Migration Tool**

These are the possible states for Last Run Status and what each one means:

- **Finished**
  - The migration completed normally. Some or all CTI-RDs were migrated; any that failed are listed in the Conversion Errors section.

- **Cancelled**
  - The migration was cancelled during the run. The Conversion Info lists the number of CTI-RDs processed.

- **Unsupported**
  - The migration was attempted against a Unified CM that does not support Cisco Spark-RD.

- **Aborted**
  - The migration stopped because the number of CTI-RDs that failed to migrate exceeded 50 during the run. Review the conversion errors, address the actions, and reschedule the conversion.

---

**Troubleshoot CTI-RD to Cisco Spark-RD Migration**

**Logs**

Use the [Diagnostic tools on the Expressway-C connector host](#) to investigate a problem and submit the applicable level of logs as required.

**Reports**

After you run a conversion to Cisco Spark-RD, a report is created and remains on the Expressway hosting the call connector. Access these reports any time: from Expressway-C, go to Applications > Hybrid Services > Call Service > Unified CM Servers, scroll to Call Service Connect CTI Remote Device to Spark Remote Device Conversion, and then click View Conversion Results.

**Error Messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user could not be recovered from a previously failed conversion. The conversion tool was unable to extract the previously deleted CTI Remote Device name from the temporary Spark Remote Device created in the previous conversion. The conversion tool could not create a device with an automatically generated name.</td>
<td>Manually reconfigure the Spark Remote Device for this user.</td>
<td>—</td>
</tr>
<tr>
<td>Error</td>
<td>Action</td>
<td>Note</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>The user's CTI Remote Device was successfully converted to a Spark Remote Device with an automatically generated name. The conversion tool was unable to extract the previously deleted CTI Remote Device name from the temporary Spark Remote Device created in the previous conversion.</td>
<td>Rename the User's Spark Remote Device if desired.</td>
<td>During the previous run, the tool did not complete migration of the CTI-RD. During the current run, the CTI-RD was migrated to a Cisco Spark-RD but the tool was unable to use the correct device name from the old CTI-RD.</td>
</tr>
<tr>
<td>Could not create Spark Remote Device</td>
<td>Reschedule conversion and try again</td>
<td>Check if the user has a Cisco Spark-RD with a name starting with “TMP_CONV” and rename it before attempting the conversion again.</td>
</tr>
<tr>
<td>Reschedule conversion and try again</td>
<td>Enable mobility for enduser</td>
<td>Reschedule migration after resolving the issue.</td>
</tr>
<tr>
<td>Could not create Spark Remote Device</td>
<td>Set 'Auto Answer Off' for enduser's primary directory number</td>
<td>Reschedule migration after resolving the issue.</td>
</tr>
<tr>
<td>Could not create Spark Remote Device</td>
<td>Resolve licence compliance issues and try again</td>
<td>—</td>
</tr>
<tr>
<td>Could not create Spark Remote Device</td>
<td>Reschedule conversion and try again</td>
<td>If the problem recurs, go to <a href="https://admin.webex.com">https://admin.webex.com</a>, click your admin username, and choose Feedback to open a case for further investigation.</td>
</tr>
<tr>
<td>Could not rename newly created Spark Remote Device</td>
<td>Reschedule conversion and try again</td>
<td>—</td>
</tr>
<tr>
<td>Could not provision Remote Destination for Spark Remote Device</td>
<td>Reschedule conversion and try again</td>
<td>—</td>
</tr>
<tr>
<td>Could not recover Spark Remote Device with missing Remote Destination</td>
<td>remove and then reenable hybrid services for this end user</td>
<td>—</td>
</tr>
<tr>
<td>Could not connect to AXL Service</td>
<td>Check network connectivity and try again</td>
<td>—</td>
</tr>
</tbody>
</table>

**Known Issues**

**CTI-RD with no Remote Destination**

**Possible Cause** Users have a CTI-RD with no remote destination.
**Solution** To fix the configuration for these users, go to https://admin.webex.com, click **Users**, open the affected users, and then toggle Hybrid Calling off and on again.
Bulk Configure Unified CM Users and Cisco Spark-RD for Hybrid Calling

- Bulk Configure Unified CM Users and Cisco Spark-RD Task Flow, on page 99
- Export Your User List, on page 100
- Edit Your User List, on page 101
- Create the Remote Device File Format, on page 101
- Edit the New File Template, on page 103
- Create a Remote Device Template, on page 103
- Upload Your Remote Device Template File, on page 104
- Insert the Remote Device Entries, on page 104
- Check the Status of Your Bulk Job, on page 105

Bulk Configure Unified CM Users and Cisco Spark-RD Task Flow

Follow this task flow if you want to use the Bulk Administration Tool to configure your users and Cisco Spark-RD.

Hybrid Calling requires that you configure each on-premises users with a Cisco Spark-RD, which is a virtual device. After you create these virtual devices, the Cisco Webex cloud automatically creates a Cisco Webex SIP address as the remote destination for that user. These components allow for the same outgoing calls from a desk phone and Cisco Webex Teams app, and incoming calls to ring both the device and the app of the Hybrid Calling user.

Before you begin

Cisco Spark-RD is required for your hybrid deployment. For manual and automatic creation on a supported release, you must use Cisco Spark-RD for new activations.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Export Your User List, on page 100</td>
<td>Extract your user data as a text file.</td>
</tr>
<tr>
<td>Step 2 Edit Your User List, on page 101</td>
<td>Modify the user information in your file so that the attributes are correct before you upload the</td>
</tr>
</tbody>
</table>
### Export Your User List

Extract your user data as a text file.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified CM Administration, go to <strong>Bulk Administration &gt; Users &gt; Export Users</strong>, choose <strong>Find All</strong>, and then click <strong>Next</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter a filename and then choose <strong>All User Format</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Run the export job.</td>
</tr>
<tr>
<td>Step 4</td>
<td>After the job is complete, choose <strong>Bulk Administration &gt; Upload/Download Files</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Find the file that your system created and then download it to your desktop.</td>
</tr>
</tbody>
</table>

**What to do next**

**Edit Your User List, on page 101**
Edit Your User List

Modify the user information in your file so that the attributes are correct before you upload the file to your publisher node. These steps walk through prompts that you would see in Microsoft Excel; other spreadsheet programs may vary.

Before you begin

Export Your User List, on page 100

Procedure

Step 1
In your spreadsheet application, open your user list text file. At the prompt, choose Delimited and then specify your delimiter as Comma. Select Finish.

Step 2
Highlight the primary extension column, go to the data tab, and select Sort. If prompted, expand the selection.

Step 3
With the file sorted by primary extension, highlight all the rows without a primary extension and delete those rows.

Step 4
Delete all columns except FirstName, LastName, UserID, and Primary Extension.

Step 5
The primary extensions are in the format xxxxxxxx in <Partition>. Copy this value into a new column but omit the in <partition> characters. This new column must contain only the primary extension.

Step 6
Save your file and give it a meaningful name, such as UserList.

What to do next

Create the Remote Device File Format, on page 101

Create the Remote Device File Format

Prepare a new template file. This file contains the common configuration for the remote devices for your users.

Before you begin

Edit Your User List, on page 101

Procedure

Step 1
Configure a single Cisco Spark-RD for one user, if this device doesn't yet exist. This entry serves as a template for the other remote devices that you'll use the Bulk Administration Tool to create.

You can use any device name you want. For this configuration, we recommend that you use SparkRD<userid>.
Bulk Configure Unified CM Users and Cisco Spark-RD for Hybrid Calling

Step 2  From Cisco Unified CM Administration, navigate to Bulk Administration > Phones > Phone File Format > Create File Format.

Step 3  Create a new file format named SparkRD and add the following fields:

- Device fields
  - CSS
  - CSS Reroute
  - Description
  - Device Name
  - Device Pool
  - Location
  - Mobility User ID
  - Owner User ID
  - Rerouting Calling Search Space
  - User ID

- Line fields
  - Alerting Name
  - ASCII Alerting Name
  - ASCII Display
  - Display
  - Directory Number
  - External Phone Number Mask
  - Line CSS
  - Line Description
  - Line Text Label
  - Maximum Number of Calls
  - Route Partition
  - Voice Mail Profile

Step 4  Enter 1 for the Maximum Number of Lines.

Step 5  Click Save.

Step 6  Navigate to Bulk Administration > Phones > Export Phones > Specific Details.

Step 7  Search for phones with the device type Cisco Spark Remote Device to find the entry that you created, for example, SparkRD<userid>.

Step 8  Click Next, and then using the file format SparkRD, run the job.
Step 9  After the job finishes, choose Bulk Administration > Upload/Download Files and then find the text file that you just created. Download it to your desktop and give it a meaningful name such as SparkRD-fileformat.

What to do next
Edit the New File Template, on page 103

Edit the New File Template

Combine your user IDs from the users file with primary extensions in the template file and create a comma separated value (csv) file.

Procedure

Step 1  In Microsoft Excel, open the Cisco Spark-RD file format file. At the prompt, choose Delimited and then specify your delimiter as Comma.
Step 2  Select Finish.
Step 3  Open your modified user list file.
Step 4  Copy your list of user IDs from the users file into the User ID column of the file format spreadsheet. Then copy the new list of Primary Extensions into the Directory Number 1 column.
Step 5  Using the User ID column, populate the Device Name column with SparkRD<userid>. Populate the remaining columns with data that is specific to your cluster; use the data in the original Cisco Spark-RD as a guide.
Step 6  Populate the Maximum Number of Calls column with the value 4.
Step 7  Save the resulting file in the comma separated value (.csv) format.

Create a Remote Device Template

Create a template for all remote devices that you associate with users. Like the user bulk settings, this template helps you specify universal settings for the remote devices.

Before you begin
Edit the New File Template, on page 103

Procedure

Step 1  From Cisco Unified CM Administration, choose Bulk Administration > Phones > Phone Template.
Step 2  Select Add New.
Step 3  Select the Cisco Spark Remote Device phone type.
Step 4  Leave the owner user ID as Not Selected in the template.
Step 5  Name the new template SparkRD Call, enter a description, and then click Save.
Step 6 Choose a Device Pool and Location, leave the other settings with their default values, and then click Save.

Step 7 Choose Line 1. Name the Line Template SparkRD Call.

Step 8 Place the template in the appropriate Route Partition. Leave the other fields with their default values, and then click Save.

What to do next
Upload Your Remote Device Template File, on page 104

Upload Your Remote Device Template File

Upload your csv file so it is ready to be applied to your system.

Before you begin
Create a Remote Device Template, on page 103

Procedure

Step 1 From Cisco Unified CM Administration, choose Bulk Administration > Upload/Download Files, and select Add New.

Step 2 Browse to the WebexWebexRD template file that you created earlier. Set the target to Phones and set the Transaction Type to Insert Phones - Specific Details.

Step 3 Select Save.

What to do next
Insert the Remote Device Entries, on page 104

Insert the Remote Device Entries

Update the phone specific details so that the remote device information is added to your system in bulk.

Before you begin
Upload Your Remote Device Template File, on page 104

Procedure

Step 1 From Cisco Unified CM Administration, choose Bulk Administration > Phones > Insert Phones.

Step 2 Select Insert Phone Specific Details.

Step 3 For File Name, select the csv file that you uploaded.
Step 4  For **Phone Template Name**, select the Cisco Spark-RD template that you created.

Step 5  Select **Run Immediately** to run this job now or **Run Later** to schedule the job to run at a more convenient time.

Step 6  (Optional) Enter a job description to identify the job.

Step 7  Select **Submit**.

---

**What to do next**

*Check the Status of Your Bulk Job, on page 105*

---

**Check the Status of Your Bulk Job**

If needed, check the status of your bulk configuration. When your system refreshes, you can see whether the job succeeded or failed.

**Before you begin**

*Insert the Remote Device Entries, on page 104*

**Procedure**

---

**Step 1**  From Cisco Unified CM Administration, choose **Bulk Administration > Job Scheduler**.

**Step 2**  Select **Find** to show the status of the bulk job that you scheduled.

---

**What to do next**

Return to the deployment steps in the “Deploy Hybrid Calling” chapter and configure the Expressway pair.
Check the Status of Your Bulk Job
Important Items for Hybrid Services Deployments

This section provides added context about key configuration items that relate to Cisco Webex Hybrid Services. These points are crucial if you want to successfully deploy Expressway-hosted Cisco Webex Hybrid Services, such as Hybrid Calling and Hybrid Calendar Service. 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 Cisco Webex 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 Cisco 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:
Forexample, for inbound business-to-business (B2B) calls using SIP protocol, TCP ports 5060 and 5061 (5061 is used for SIP TLS) must be opened on the external firewall, together with UDP media ports used for services such as voice, video, content sharing, dual video, and so on. Which media ports to open depends on the number of concurrent calls and the number of services.

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

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

**Example**

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

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

```
_sips._tcp.example.com SRV service location:
priority = 10
weight = 10
port = 5062
svr hostname = us-expe1.example.com

_sips._tcp.example.com SRV service location:
priority = 10
weight = 10
port = 5062
svr hostname = us-expe2.example.com
```

These records mean that calls are directed to `us-expe1.example.com` and `us-expe2.example.com` with equal load sharing (priority and weight) using TLS as the transport type and 5062 as the listening port number.
A device that is external to the network (on the Internet) and that makes a SIP call to a user of the corporate domain (user1@example.com) must query the DNS to understand which transport type to use, the port number, how to load-share the traffic, and which SIP servers to send the call to.

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

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

TLS handshake is shown in the following diagram:

- 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 Cisco Webex cloud. This concept is called TLS with mutual authentication and is required when integrating with Cisco Webex.

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

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

Business-to-business and Mobile and Remote Access calls use port 5061 for SIP TLS, and Cisco 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 Cisco 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.

**A Story to Show the Importance of the Domain Ownership Check**

The Cisco 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 Cisco 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 Cisco Webex Teams 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 Cisco Webex Teams 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 Cisco Webex cloud is to make sure that the identity of anyone calling from Cisco Webex is correct and not falsified.

To check the identity, Cisco Webex requires that the company proves that it owns the domains used in hybrid calling. If it doesn't, 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 Cisco 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 Cisco Webex cloud, the domain is verified.
   - As an example, the administrator must prove that she owns the domain "example.com", if she wants Cisco 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 Cisco Webex cloud generated:

     ![Verify Domain](image)

     - The DNS administrator then creates a TXT record for this domain with the value set to 123456789abcdef123456789abcdef123456789abcdef, 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: 168.254.73.184

Non-authoritative answer:
example.com text = "123456789abcdef123456789abcdef123456789abcdef0"
```

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 Expressway-C connector host must be registered to Cisco Webex in order for hybrid services Cisco Webex Calling for Branch Offices to work.

Expressway-C is deployed in the internal network, and the way it registers to the cloud is through an outbound HTTPS connection—the same type that is used for any browser that connects to a web server.

Registration and communication to the Cisco Webex cloud uses TLS. Expressway-C is the TLS client, and the Cisco Webex cloud is the TLS server. As such, Expressway-C 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 Expressway-C 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 Expressway's trust store. Doing so, the Expressway can verify that the call is truly coming from the Cisco Webex cloud.

With manual upload, you can upload all relevant certificate authority certificates to the trust store of Expressway-C.

With automatic upload, the cloud itself uploads those certificates in the trust store of Expressway-C. We recommend that you use automatic upload. The certificate list might change, and automatic upload guarantees that you get the most updated list.

If you allow automatic installation of certificate authority certificates, you are redirected to https://admin.webex.com (the management portal). The redirection is done by the Expressway-C itself without any user intervention. You, as the Cisco Webex administrator, must authenticate through an HTTPS connection. Soon after, the cloud pushes the CA certificates to the Expressway-C.

Until the certificates are uploaded to the Expressway-C trust store, the HTTPS connection cannot be established.

To avoid this problem, the Expressway-C is preinstalled with Cisco Webex-trusted CA certificates. Those certificates are only used to set up and validate the initial HTTPS connection, and they don't appear in Expressway-C trust list. Once the certificates of the trusted certificate authorities are pulled from the cloud through this initial HTTPS connection, those certificates are available for platform-wide usage; then, they appear in the Expressway-C trust list.

This process is secure for these reasons:

- Requires admin access to Expressway-C and to https://admin.webex.com. Those connections use HTTPS and are encrypted.
- Certificates are pushed from the cloud to Expressway using the same encrypted connection.

This list shows the certificate authority certificates that the Cisco Webex cloud currently uses. This list might change in the future:

- C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root
- C=US, O=The Go Daddy Group, Inc., OU=GoDaddy Class 2 Certificate Authority
- C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2
- C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certificate Authority

A list of certificate authority certificates is also required for the Expressway-E in the traversal pair. Expressway-E communicates with the Cisco 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 Cisco Webex.

**Related Topics**

- Supported Certificate Authorities for Cisco Webex