# CONTENTS

## PREFACE

- New and Changed Information vii
- Full Cisco Trademarks with Software License xiii

## CHAPTER 1

### Overview of Calling in Webex Teams (Unified CM) 1

- Calling in Webex Teams (Unified CM) Overview 1
- Calling Experience with Calling in Webex Teams (Unified CM) for Users 8
  - Call Comparison 8
  - User Experience Changes for Hybrid Call Service Users 8
- Call Flows for Calling in Webex Teams (Unified CM) 9
  - Calling in Webex Teams (Unified CM) Call Answered on Webex Teams 9
  - Calling in Webex Teams (Unified CM) Incoming Call Answered on Desk Phone 10
  - Webex Teams Call to a User with no Directory Number 10
  - Unified CM Call in Webex Teams to PSTN Number 11
  - Unified CM Call in Desk Phone Control Mode 11
  - Meeting Join in Desk Phone Control Mode 12

## CHAPTER 2

### Prepare Your Environment for Calling in Webex Teams (Unified CM) 13

- Requirements for Calling in Webex Teams (Unified CM) 13
  - Call Control Environment Requirements for Calling in Webex Teams (Unified CM) 13
  - Network Requirements for Calling in Webex Teams (Unified CM) 14
    - IPv6 Requirements 14
    - Ports and Protocols 15
    - Supported Codecs 17
- Certificate Requirements for Calling in Webex Teams (Unified CM) 17
  - Unified CM Certificates (No MRA) 17
New and Changed Information

This table covers content updates related to new features or functionality, changes to existing content, and any major errors that were fixed in the Deployment Guide for Calling in Webex Teams (Unified CM).

For more information about Webex Teams app updates, see the What's New in Cisco Webex Teams for major updates and a preview of what's coming soon, and see the Cisco Webex Teams Release Notes for minor updates and bug fixes.

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 10, 2019</td>
<td>• Added network requirements information to the Prepare Your Environment chapter.</td>
</tr>
<tr>
<td></td>
<td>• In the Configure SIP Address Routing for your Organization, section, added the following clarification: “*.example.com only matches subdomains, not top-level domains.”</td>
</tr>
<tr>
<td>November 27, 2019</td>
<td>• Added call history to the feature overview table for desktop platforms.</td>
</tr>
<tr>
<td></td>
<td>• In the “Set DSCP Values on the Network”, changed the signaling packets marking from AF31 to CS3.</td>
</tr>
<tr>
<td>Date</td>
<td>Changes Made</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>November 15, 2019</td>
<td>• In the Deploy chapter, added relevant deployment steps and Webex Teams authentication steps for mobile softphone mode.</td>
</tr>
<tr>
<td></td>
<td>• Added the following mobile features to the feature overview table:</td>
</tr>
<tr>
<td></td>
<td>• Make call</td>
</tr>
<tr>
<td></td>
<td>• Answer call</td>
</tr>
<tr>
<td></td>
<td>• Mute/Unmute</td>
</tr>
<tr>
<td></td>
<td>• End call</td>
</tr>
<tr>
<td></td>
<td>• On a Call presence—In Webex Teams, users in the same organization can see this presence indicator during an active call.</td>
</tr>
<tr>
<td></td>
<td>• Basic Shared Line Appearance</td>
</tr>
<tr>
<td></td>
<td>• DTMF input during the call</td>
</tr>
<tr>
<td>November 7, 2019</td>
<td>• Added the following features to the feature overview table:</td>
</tr>
<tr>
<td></td>
<td>• Webex Teams call (Windows or Mac)—Users can choose whether to call people using their phone number or using a Webex Teams call. A Webex Teams call is a quick way to call someone else who's using Webex Teams. Users can share their screen and whiteboard while in the call, but they can't put the call on hold, transfer the call, or use other features only available in phone calls.</td>
</tr>
<tr>
<td></td>
<td>• SIP (URI) address routing—Configurable in Control Hub, this setting allows you to decide which SIP addresses are routed through the Webex cloud. The default is for all SIP URIs to be routed through Unified CM except for Webex services. (Also added new section Configure SIP Address Routing for Your Organization, on page 41.)</td>
</tr>
<tr>
<td>October 9, 2019</td>
<td>• In Unified CM Certificates (With MRA), on page 18, removed reference to Cisco CallManager certificate and added the following note: “The Tomcat certificate is also used for secure SIP when Webex Teams is enabled for encrypted calls (SIP Outh operates on the default port 5091 for MRA). See “Configure the Phone Security Profile for Encrypted Calls” in this guide for more details.”</td>
</tr>
<tr>
<td></td>
<td>• In Unified CM Certificates (No MRA), on page 17, added the following note: “The Tomcat certificate is also used for secure SIP when Webex Teams is enabled for encrypted calls (SIP Oauth operates on the default port 5090). See “Configure the Phone Security Profile for Encrypted Calls” in this guide for more details.”</td>
</tr>
<tr>
<td>Date</td>
<td>Changes Made</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>September 26, 2019</td>
<td>• Added the following features to the feature table in Calling in Webex Teams (Unified CM) Overview, on page 1:</td>
</tr>
<tr>
<td></td>
<td>• Suppress call notifications when presenting or when DND is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Support for tel, sip and clicktocall protocols.</td>
</tr>
<tr>
<td></td>
<td>• Support for Click to Call from Outlook.</td>
</tr>
<tr>
<td></td>
<td>• Support for Cisco 500 series headsets</td>
</tr>
<tr>
<td></td>
<td>• Added new section Headset Requirements for Calling in Webex Teams (Unified CM), on page 20</td>
</tr>
<tr>
<td></td>
<td>• Removed this incorrect known issue: “Webex Teams does not register to Unified CM in secure softphone mode. You must use non-secure mode as a</td>
</tr>
<tr>
<td></td>
<td>workaround.” Removed other incorrect information that stated secure mode wasn’t supported.</td>
</tr>
<tr>
<td></td>
<td>• Fixed steps for SIP Oath configuration in Configure the Phone Security Profile for Encrypted Calls, on page 38. Called out that Unified CM</td>
</tr>
<tr>
<td></td>
<td>12.5(1) or later is required for encrypted calls.</td>
</tr>
<tr>
<td></td>
<td>• Added note to Authenticate with Phone Services in Webex Teams, on page 41: “If both Server address and UC domain are configured, Server Address</td>
</tr>
<tr>
<td></td>
<td>is used to connect to Unified CM while on-premises only. Autodiscovery through DNS SRV is ignored. For MRA, Server Address is ignored.”</td>
</tr>
<tr>
<td>August 29, 2019</td>
<td>• Added new section Configure the Phone Security Profile for Encrypted Calls, on page 38.</td>
</tr>
<tr>
<td></td>
<td>• For both softphone and desk phone control modes, added new midcall features to feature table in Calling in Webex Teams (Unified CM)</td>
</tr>
<tr>
<td></td>
<td>Overview, on page 1:</td>
</tr>
<tr>
<td></td>
<td>• Conference</td>
</tr>
<tr>
<td></td>
<td>• Merge</td>
</tr>
<tr>
<td></td>
<td>• Transefer</td>
</tr>
<tr>
<td>July 25, 2019</td>
<td>• Rewrote the “Authenticate with Webex Teams” content to show the user configuration path to take if you have autodiscovery or if you don’t.</td>
</tr>
<tr>
<td>July 9, 2019</td>
<td>• Removed the limited availability disclaimer for Merge and Transfer features for Webex Teams in softphone mode. (These features are now G</td>
</tr>
<tr>
<td></td>
<td>enerally Available.)</td>
</tr>
<tr>
<td>Date</td>
<td>Changes Made</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>June 27, 2019</td>
<td>• Removed the Preview Release Disclaimer. (Calling in Webex Teams (Unified CM) is officially Generally Available.)</td>
</tr>
<tr>
<td></td>
<td>• Added Merge and Transfer as limited availability features for Webex Teams in softphone mode.</td>
</tr>
<tr>
<td></td>
<td>• Added new section Allow Untrusted Certificates on Unified CM, on page 54 to the Appendix.</td>
</tr>
<tr>
<td></td>
<td>• Added the following information to the certificate requirements and known issues: “Certificates issued with a deprecated signature algorithm (such as SHA-1) do not work; you must use a supported secure signature algorithm such as SHA-256 or later, as documented in the Certificates chapter in the Administration Guide for Cisco Unified Communications Manager.”</td>
</tr>
<tr>
<td>June 14, 2019</td>
<td>• In Calling Experience with Calling in Webex Teams (Unified CM) for Users, on page 8, added the following information under the &quot;User Experience Changes for Hybrid Call Service Users&quot; section:</td>
</tr>
<tr>
<td></td>
<td>“If the Webex device is configured in Control Hub as a Place that is enabled for Hybrid Call Service, the user can dial from Webex Teams and the call then starts on the Webex device using that device's directory number as the caller ID on the receiving end.”</td>
</tr>
<tr>
<td></td>
<td>• In Certificate Requirements for Calling in Webex Teams (Unified CM), on page 17, added MRA certificate requirements and restructured as 3 subsections: Unified CM Certificates (No MRA), Unified CM Certificates (MRA), and Expressway Certificates (MRA).</td>
</tr>
<tr>
<td></td>
<td>• In Set DSCP Values on the Network, on page 53, corrected QoS port range information. Previously, it read &quot;16384 to 24574&quot; for audio streams and &quot;24575 to 32766&quot; for video streams; now, it reads &quot;16384 to 24575&quot; and &quot;24576 to 32676&quot;, respectively.</td>
</tr>
<tr>
<td>April 24, 2019</td>
<td>• Restructured the Requirements section—Each Calling in Webex Teams (Unified CM) requirement now has its own subsection to make it easier to find.</td>
</tr>
<tr>
<td></td>
<td>• Added new section (Configure Unified CM End Users for Calling in Webex Teams (Unified CM), on page 34) to the Deploy chapter.</td>
</tr>
</tbody>
</table>
Changes Made

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes Made</th>
</tr>
</thead>
</table>
| April 10, 2019 | - Added **Meeting Join in Desk Phone Control Mode**, on page 12 to the Call Flows.  
- In **Requirements for Calling in Webex Teams (Unified CM)**, on page 13, added the following points:  
  - In **Cisco Unified CM Administration > System > Server**, the Unified CM server names must be defined as FQDN.  
  - We do not support the deployment model of MRA without SSO and Unified CM with SSO.  
  - At this time, we support internal only automatic discovery. Service discovery enables clients to automatically detect and locate services on your enterprise network. Clients query domain name servers to retrieve service (SRV) records that provide the location of servers.  
  - If you're using Server Information for configuration and not SRV records, your users' Webex Teams email addresses must match their Unified CM email addresses—at a minimum, the user ID portion before the domain must match.  
  - Added **Retain Configuration for Hybrid Call Service for Webex Devices**, on page 23 to the Prepare Your Environment chapter.                                                                                           |
| March 28, 2019 | - Initial version of the document.                                                                                                                                                                                                                                                                                                                                     |

Thank you for agreeing to provide feedback on the deployment documentation (intended for partner and customer administrators) for Calling in Webex Teams (Unified CM). We value your feedback and will endeavor to iterate our documentation, based on feedback we hear from you. With your help, we can ensure that the documentation is high quality and relevant to top-of-mind questions and concerns from our partners and customers.

Please note that the documentation set is considered Early Field Trial (EFT) friendly. This means the documentation may have gaps or errors that need to be addressed. Similar to EFT agreements you may've been involved with outside of this effort, the documentation is under Non-Disclosure Agreement (NDA) and thus should not be shared publically.

Calling in Webex Teams (Unified CM) documentation is produced in a continuous development environment, so please always use https://cisco.box.com/v/teams-ucm-EFT to refer to the latest guide as you deploy Calling in Webex Teams (Unified CM) and other related workflows.

As mentioned in EFT slide decks you may've seen and discussions with the trials team, mid-call features for this solution are to be delivered in phases ("drops").* The documentation captures the features and functionality that is available to you at the time of reading/testing, and future drops or roadmap items are outside the scope of this documentation. Please work with the trials team and product management if you have questions about roadmap items.

* Many of the new features and support covered as part of this trial are in varying stages of development and will be offered on a when-and-if-available basis. The features and support covered in the trial and any future product release are subject to change at the sole discretion...
of Cisco. Accordingly, Cisco will have no liability for delay in the delivery or failure to deliver any future products or features described during trial and any such delay or failure would not in any way imply the right to return any previously purchased Cisco products.
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)
CHAPTER 1

Overview of Calling in Webex Teams (Unified CM)

• Calling in Webex Teams (Unified CM) Overview, on page 1
• Calling Experience with Calling in Webex Teams (Unified CM) for Users, on page 8
• Call Flows for Calling in Webex Teams (Unified CM), on page 9

Calling in Webex Teams (Unified CM) Overview

The Calling in Webex Teams (Unified CM) solution lets you register Webex Teams directly to your Cisco Unified Communications Manager call control environment (on-premises enterprise, Business Edition 6000/7000, or as delivered through an HCS partner solution).

In softphone mode, Webex Teams registers as a SIP device with the product type "Cisco Unified Client Services Framework" or CSF for desktop, TCT or BOT for mobile, and TAB for tablets. Alternatively, Webex Teams can connect to Unified CM using CTI to control the user’s endpoints.

This solution enhances the calling experience for end users, allowing them to directly make calls in Webex Teams through your Unified CM environment, use midcall features, and control their Unified CM registered desk phone from Webex Teams.

When dialing from Cisco Webex Teams, users can use the same dial strings or prefixes as they do on their desk phones; Cisco Webex Teams functions like any other desk phone registered to your Unified CM. Unified CM calls that are established in Webex Teams use the configuration that's in place for your Unified CM deployment (such as location, bandwidth settings, point to point media, and so on).
Calling Features

This integration provides the following feature set in Webex Teams for desktop (Windows and Mac) and for mobile (Android, iPad, and iPhone).

**Table 1: Calling Features for Calling in Webex Teams (Unified CM)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Desktop (Softphone)</th>
<th>Desktop (Desk Phone Control)</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Features</td>
<td>• Make call</td>
<td>• Make call</td>
<td>• Make call</td>
</tr>
<tr>
<td></td>
<td>• Answer call</td>
<td>• Answer call</td>
<td>• Answer call</td>
</tr>
<tr>
<td></td>
<td>• Mute</td>
<td>• Mute</td>
<td>• Mute/Unmute</td>
</tr>
<tr>
<td></td>
<td>• End call</td>
<td>• End call</td>
<td>• End call</td>
</tr>
<tr>
<td></td>
<td>• DTMF input during the call</td>
<td>• On a Call presence—In Webex Teams, users in the same organization can see this presence indicator during an active call.</td>
<td>• On a Call presence—In Webex Teams, users in the same organization can see this presence indicator during an active call.</td>
</tr>
<tr>
<td></td>
<td>• On a Call presence—In Webex Teams, users in the same organization can see this presence indicator during an active call.</td>
<td>• DTMF input during the call</td>
<td>• Basic Shared Line Appearance</td>
</tr>
<tr>
<td></td>
<td>• Call forwarding—If users need to take your work calls from another number, they can set up call forwarding right from Webex Teams. They just enter the call forwarding number, and their calls all ring at that number.</td>
<td></td>
<td>• DTMF input during the call</td>
</tr>
<tr>
<td></td>
<td>• Single Number Reach—Users can access the Self Care Portal from Webex Teams and add more numbers for devices they want to ring simultaneously with their enterprise directory number.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Desktop (Softphone)</td>
<td>Desktop (Desk Phone Control)</td>
<td>Mobile</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Midcall Features</td>
<td>• Conference calls—When users are on a call with someone else, they might want to add other people into the call to start a conference call right away. They can add up to 8 other people into conference calls started in this way.</td>
<td>• Conference calls—When a user is on a call with someone else, they might want to add other people into the call to start a conference call right away. Users can add up to 8 other people into conference calls started in this way.</td>
<td>• Conference calls—When a user is on a call with someone else, they might want to add other people into the call to start a conference call right away. Users can add up to 8 other people into conference calls started in this way.</td>
</tr>
<tr>
<td></td>
<td>• Hold/Resume—Users place a call on hold and resume in Webex Teams.</td>
<td>• Hold/Resume—A user can place a call on hold and resume in Webex Teams with desk phone selected.</td>
<td>• Hold/Resume—A user can place a call on hold and resume in Webex Teams with desk phone selected.</td>
</tr>
<tr>
<td></td>
<td>• Merge—Users take 2 active calls and merge them into a single conference call in Webex Teams.</td>
<td>• Merge—A user can take 2 active calls and merge them into a single conference call in Webex Teams with desk phone selected.</td>
<td>• Merge—A user can take 2 active calls and merge them into a single conference call in Webex Teams with desk phone selected.</td>
</tr>
<tr>
<td></td>
<td>• Transfer—Redirects a connected call within Webex Teams. The target is the user to which another user wants to transfer the call.</td>
<td>• Transfer—Redirects a connected call within Webex Teams in desk phone control mode. The target is the user to which to transfer the call.</td>
<td>• Transfer—Redirects a connected call within Webex Teams in desk phone control mode. The target is the user to which to transfer the call.</td>
</tr>
<tr>
<td></td>
<td>• Screen sharing—Share content from a computer screen during a call in Webex Teams.</td>
<td>• Screen sharing—Share content from a computer screen during a call in Webex Teams with desk phone selected.</td>
<td>• Screen sharing—Share content from a computer screen during a call in Webex Teams with desk phone selected.</td>
</tr>
<tr>
<td>Category</td>
<td>Desktop (Softphone)</td>
<td>Desktop (Desk Phone Control)</td>
<td>Mobile</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Additional Features</td>
<td></td>
<td></td>
<td>• Phone numbers under the Video call icon—Work numbers and mobile numbers are synchronized from Active Directory and appear in Webex Teams. (Requires Cisco Directory Connector.)</td>
</tr>
</tbody>
</table>

Overview of Calling in Webex Teams (Unified CM)

Deployment Guide for Calling in Webex Teams (Unified CM)
### Overview of Calling in Webex Teams (Unified CM)

<table>
<thead>
<tr>
<th>Category</th>
<th>Desktop (Softphone)</th>
<th>Desktop (Desk Phone Control)</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Call history—When a user calls other people in the organization, they see more details about phone numbers in the call history. So, to call someone back, that user can see if they’re calling a work or mobile number. See Webex Teams</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Phone numbers in contact cards—Work numbers and mobile numbers are synchronized from Active Directory and appear as clickable items in Webex Teams. (Requires Cisco Directory Connector to synchronize user phone number attributes to the Webex cloud.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Webex Teams call (Windows and Mac)—Users can choose whether to call people using their phone number or using a Webex Teams call. A Webex Teams call is a quick way to call someone else who's</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Sherry McKenna**
sherry@source.com
Active 20 minutes ago

- Work: +1 500 234 0000
- Mobile: +1 505 236 0000

---

**Deployment Guide for Calling in Webex Teams (Unified CM)**

5
<table>
<thead>
<tr>
<th>Category</th>
<th>Desktop (Softphone)</th>
<th>Desktop (Desk Phone Control)</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>using Webex Teams. Users can share their screen and whiteboard while in the call, but they can't put the call on hold, transfer the call, or use other features only available in phone calls. • Suppress call notifications when presenting or when DND is enabled. • Support for tel, sip and clickto call protocols. • Support for Click to Call from Outlook. • Support for Cisco 500 series headsets.</td>
<td>• Secure and encrypted calls (configurable from Unified CM) • SIP (URI) address routing—Configurable in Control Hub, this setting allows you to decide which SIP addresses are routed through the Webex cloud. The default is for all SIP URIs to be routed through Unified CM except for Webex services. • Expressway Mobile Remote Access (MRA) for Webex Teams • Service Discovery • Single Sign-On (SSO)</td>
<td>• Secure and encrypted calls (configurable from Unified CM) • SIP (URI) address routing—Configurable in Control Hub, this setting allows you to decide which SIP addresses are routed through the Webex cloud. The default is for all SIP URIs to be routed through Unified CM except for Webex services. • Expressway Mobile Remote Access (MRA) for Webex Teams • Service Discovery</td>
</tr>
</tbody>
</table>
Desk Phone Control for Webex Teams for Windows and Mac

Any desk phones or Extension Mobility profiles that are associated with the user's Unified CM account are listed as an available device to connect to in Webex Teams for Windows or Mac. If the device is selected, Unified CM calls that are dialed from or answered in Webex Teams use that desk phone. Users can start or stop the call, enter DTMF input (which the phone acknowledges), and use the midcall features that are documented in the preceding feature table.

Note

This feature only supports calls and doesn't currently support joining a meeting from a desk phone that is connected to Webex Teams. When you join the meeting with a desk phone selected, the audio stream still goes through your Windows or Mac system.
Calling Experience with Calling in Webex Teams (Unified CM) for Users

Call Comparison

This table lists what types of Webex Teams calls go through Unified CM and types of Webex Teams calls or meetings that do not go through Unified CM (and instead go "over the top" as calls to cloud microservices).

<table>
<thead>
<tr>
<th>Webex Teams Calls Done on Unified CM (On-Premises)</th>
<th>Webex Teams Calls and Meetings Not Done on Unified CM (Cloud)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calls initiated directly from a 1:1 space or from a contact card in Webex Teams</td>
<td>Ad hoc meetings from a group space in Webex Teams</td>
</tr>
<tr>
<td>Search and then call a user in Webex Teams</td>
<td>Using the Join button in Webex Teams to join an ad hoc or scheduled meeting</td>
</tr>
<tr>
<td>Dialing directory numbers or PSTN numbers from Call 📞 in Webex Teams</td>
<td>Dialing premises Directory URIs from Call 📞 in Webex Teams</td>
</tr>
<tr>
<td>Desk phone control calls (outgoing: dial a directory or PSTN number in Webex Teams, take the call on the Unified CM device; incoming: answer the call in Webex Teams, take the call on the device).</td>
<td>Joining a meeting while paired through Room, Desk, or Board devices</td>
</tr>
<tr>
<td>1:1 calls that are placed directly in Webex Teams to a free user in the consumer organization, to a user in another organization, or to a user in the same organization who doesn't have a directory number. (Numbers are not shared across organizations, so don't appear in contact cards.)</td>
<td></td>
</tr>
</tbody>
</table>

User Experience Changes for Hybrid Call Service Users

For users who are paired to a cloud-registered Room, Desk, or Board device:

- Unified CM registration in the Webex Teams app stays active.
- Incoming calls to a user's directory number are presented in Webex Teams and, when accepted, calls are answered on the desktop app and do not use the paired Room, Desk, or Board device.
- If the Webex device is configured in Control Hub as a Place that is enabled for Hybrid Call Service, the user can dial from Webex Teams and the call then starts on the Webex device using that device's directory number as the caller ID on the receiving end.
- If the Webex device is not in a Place that's enabled for Hybrid Call Service, the directory number or PSTN dialing fails and an error message is presented in the user's Webex Teams app.
For users who are in deskphone control mode in Webex Teams:

- Media (audio and video) for 1:1 calls to users with contact cards and calls that are started from the search or dial view go through the on-premises desk phone.

- Media (audio and video) for group space meetings, Webex meetings (scheduled or ad-hoc), and calls to users without contact cards go through the Webex Teams desktop app.

For scenarios involving a call going to voicemail:

- Incoming calls that don't go through Unified CM do not roll over to voicemail and continue to ring until the user answers or declines.

- Incoming calls that go through Unified CM (for example, to a user's corporate directory number roll over to voicemail.

---

**Call Flows for Calling in Webex Teams (Unified CM)**

**Calling in Webex Teams (Unified CM) Call Answered on Webex Teams**

*Figure 1: Call between Two Users on Calling in Webex Teams (Unified CM), Call Answered on Webex Teams*

1. Using Webex Teams, Alice calls Bob's directory number from the contact card in their 1:1 space.
2. The call rings on Bob's Webex Teams app.
3. Bob answers the call in the Webex Teams app. Call signaling is established through Unified CM.
4. Both parties can turn on video and share content. (Video is on by default if a camera is present.)
**Calling in Webex Teams (Unified CM) Incoming Call Answered on Desk Phone**

Figure 2: Call Between Two Users on Calling in Webex Teams (Unified CM), Call Answered on Desk Phone

1. From her Webex Teams app, Alice calls Bob's directory number from their Webex Teams 1:1 space. (Bob's directory number is available on his contact card in the app.)

2. Call signaling is established through Unified CM. The call rings on both Bob’s desk phone and his Webex Teams app.


4. Both parties can turn on video and share content. (Video is on by default if a camera is present on the Webex Teams desktop device.)

**Webex Teams Call to a User with no Directory Number**

Figure 3: Call Between User on Calling in Webex Teams (Unified CM) and a User with no Directory Number, Call Answered on Webex Teams

1. Using Webex Teams, Alice calls Bob's Webex Teams app from their 1:1 space. (Bob's directory number is not available on his contact card in the app.)
2. Bob answers the call on Webex Teams.
3. The call is established between the two Webex Teams apps as a cloud call. Media flows between the two Webex Teams apps over the cloud or through a Video Mesh Node if deployed.

**Unified CM Call in Webex Teams to PSTN Number**

*Figure 4: Call From User on Calling in Webex Teams (Unified CM) To PSTN Number*

1. Alice calls a PSTN number from Webex Teams using the Call \( \text{Call} \) tab.
2. Call signaling is established through the Unified CM to PSTN gateway.
3. Media flows directly between Webex Teams and the PSTN gateway.

**Unified CM Call in Desk Phone Control Mode**

*Figure 5: Call between two Users with Calling in Webex Teams (Unified CM). Call is Answered on Webex Teams app in Deskphone Control Mode*
1. Using Webex Teams, Alice (in desk phone control mode) calls Bob's directory number from their Webex Teams 1:1 space. (Bob's directory number is available on his contact card in the app.)

2. The call goes through her desk phone. Call signaling is established through Unified CM.

3. Bob's desk phone rings and he gets a notification on Webex Teams.

4. Bob answers the call in Webex Teams in desk phone control mode. Media flows directly between the two desk phones.

Meeting Join in Desk Phone Control Mode

1. Using the Webex Teams app, Alice (while in desk phone control mode) joins a meeting (Webex Teams backed or traditional Webex).

2. Even though Alice is in desk phone control mode, the media is established between the Webex Teams app and the meeting over the cloud. Media flows between the two over the cloud or through a Video Mesh Node if deployed. The meeting is not joined through Unified CM, so the chosen desk phone is not used in this scenario.
Prepare Your Environment for Calling in Webex Teams (Unified CM)

Requirements for Calling in Webex Teams (Unified CM)

Call Control Environment Requirements for Calling in Webex Teams (Unified CM)

To enable Calling in Webex Teams (Unified CM), 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>
<thead>
<tr>
<th>Call Solution</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Release 11.5(1) SU3 and later; we recommend the latest SU release.</td>
</tr>
<tr>
<td></td>
<td>Release 12.5(1) and later for SIP Oath encrypted calls support.</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 at a minimum.</td>
</tr>
<tr>
<td></td>
<td>12.5 and later for for SIP Oath encrypted calls support.</td>
</tr>
</tbody>
</table>

While not required, if you want Mobile and Remote Access (MRA) support (so Webex Teams can be used in softphone mode outside the corporate network), you must use a Cisco Expressway traversal pair, and ensure that you're on the minimum supported version or later.
### Network Requirements for Calling in Webex Teams (Unified CM)

When using Calling in Webex Teams (Unified CM) over your corporate Wi-Fi network, we recommend that you do the following:

- Design your Wi-Fi network to eliminate gaps in coverage as much as possible, including in areas such as elevators, stairways, and outside corridors.
- Ensure that all access points assign the same IP address to the mobile device. Calls are dropped if the IP address changes during the call.
- Ensure that all access points have the same service set identifier (SSID). Hand-off may be much slower if the SSIDs do not match.
- Ensure that all access points broadcast their SSID. If the access points do not broadcast their SSID, the mobile device may prompt the user to join another Wi-Fi network, which interrupts the call.
- Ensure that the Enterprise firewall is configured to allow the passage of Session Traversal Utilities for NAT (STUN) packets.

Conduct a thorough site survey to minimize network problems that could affect voice quality. We recommend that you do the following:

- Verify nonoverlapping channel configurations, access point coverage, and required data and traffic rates.
- Eliminate rogue access points.
- Identify and mitigate the impact of potential interference sources.

For more information, see the following documentation:

- The “VoWLAN Design Recommendations” section in the Enterprise Mobility Design Guide.
- The Cisco Unified Wireless IP Phone 7925G Deployment Guide.
- The Capacity Coverage & Deployment Considerations for IEEE 802.11g white paper.
- The Solutions Reference Network Design (SRND) for your Cisco Unified Communications Manager release.

### IPv6 Requirements

Calling in Webex Teams (Unified CM) is fully IPv6 ready. It works in pure IPv6 and hybrid networks with the limitations listed in this section. Cisco Collaboration solutions do not currently fully support IPv6. For

---

### Table 3:

<table>
<thead>
<tr>
<th>Call Solution</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway E and C traversal pair for Mobile and Remote Access (MRA)</td>
<td>X8.11.4 or later is required for Calling in Webex Teams (Unified CM). See the &quot;Important Information&quot; section in the Expressway Release Notes for more information. This release and later provide added security. See the Mobile and Remote Access via Expressway Deployment Guide for more information.</td>
</tr>
</tbody>
</table>
example, Cisco Expressway for Mobile and Remote Access (MRA) has limitations in pure IPv6 networks that require NAT64/DNS64 to be deployed in mobile carrier networks. Cisco Unified Communications Manager doesn't support HTTPS in pure IPv6 networks.

The network IP protocol used by Calling in Webex Teams (Unified CM) when connecting to services is determined by the following factors:

- The client operating system IP capabilities.
- The server operating system IP capabilities.
- The availability of a DNS record for IPv4 and IPv6.
- Cisco Unified Communications Manager SIP setting for softphone devices configuration for IPv4, IPv6, or both.
- Underlying network IP capabilities.

On Cisco Unified Communications Manager, the IP capability is determined by generic server settings and device-specific settings.

When the Client OS and Server OS are set to Two Stacks, Calling in Webex Teams (Unified CM) uses either IPv4 or IPv6 address for connections with the server in accordance with RFC6555.

When you use Jabber in IPv6-Only mode, NAT64/DNS64 is required to connect to an IPv4 infrastructure, such as Cisco Expressway for Mobile and Remote Access.

For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0.

### Ports and Protocols

Calling in Webex Teams (Unified CM) uses the ports and protocols listed in the following table. If you plan to deploy a firewall between the client and a server, configure the firewall to allow these ports and protocols.

<table>
<thead>
<tr>
<th>Port</th>
<th>Application Layer Protocol</th>
<th>Transport Layer Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6970</td>
<td>HTTP</td>
<td>TCP</td>
<td>Connect to the TFTP server to download client configuration files.</td>
</tr>
<tr>
<td>6972</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Connects to the TFTP server to download client configuration files securely for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
<td>UDP</td>
<td>Hostname resolution.</td>
</tr>
<tr>
<td>3804</td>
<td>CAPF</td>
<td>TCP</td>
<td>Issues Locally Significant Certificates (LSC) to IP phones. This port is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.</td>
</tr>
<tr>
<td>8443</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Traffic to Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>8191</td>
<td>SOAP</td>
<td>TCP</td>
<td>Connects to local port to provide Simple Object Access Protocol (SOAP) web services.</td>
</tr>
<tr>
<td>Port</td>
<td>Application Layer Protocol</td>
<td>Transport Layer Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2748</td>
<td>CTI</td>
<td>TCP</td>
<td>Computer Telephony Interface (CTI) used for desk phone control.</td>
</tr>
<tr>
<td>5060</td>
<td>SIP</td>
<td>TCP</td>
<td>Provides Session Initiation Protocol (SIP) call signaling.</td>
</tr>
<tr>
<td>5061</td>
<td>SIP over TLS</td>
<td>TCP</td>
<td>SIP over TCP provides secure SIP call signaling. (Used if Secure SIP is enabled for device.)</td>
</tr>
<tr>
<td>30000 to 39999</td>
<td>FECC</td>
<td>UDP</td>
<td>Far end camera control (FECC).</td>
</tr>
<tr>
<td>5070 to 6070</td>
<td>BFCP</td>
<td>UDP</td>
<td>Binary Floor Control Protocol (BFCP) for video screen sharing capabilities.</td>
</tr>
</tbody>
</table>

**Voice or Video Media Exchange**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Transport Layer Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16384 to 32766</td>
<td>RTP/SRTP</td>
<td>UDP</td>
<td>Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share.</td>
</tr>
<tr>
<td>33434 to 33598</td>
<td>RTP/SRTP</td>
<td>UDP</td>
<td>Cisco Webex Hybrid Services media port range used for audio and video.</td>
</tr>
<tr>
<td>49152 to 65535</td>
<td>RDP</td>
<td>TCP</td>
<td>IM-only desktop share. Applies to Cisco Jabber for Windows only.</td>
</tr>
<tr>
<td>8000</td>
<td>RTP/SRTP</td>
<td>TCP</td>
<td>Allows users to receive video transmitted to their desk phone devices on their computers through the client.</td>
</tr>
</tbody>
</table>
Supported Codecs

<table>
<thead>
<tr>
<th>Type</th>
<th>Codec</th>
<th>Codec Type</th>
<th>Webex Teams for Android</th>
<th>Webex Teams for iPhone and iPad</th>
<th>Webex Teams for Mac</th>
<th>Webex Teams for Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>G.711</td>
<td>A-law</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>µ-law/Mu-law</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>G.722</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>G.722.1</td>
<td>24 kb/s and 32 kb/s</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>G.729</td>
<td></td>
<td>No</td>
<td>Does not support Visual Voicemail with G.729; however, you can access voice messages using G.729 and the Call Voicemail feature.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>G.729a</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Opus</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video</td>
<td>H.264/AVC</td>
<td>Baseline profile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High profile</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Certificate Requirements for Calling in Webex Teams (Unified CM)

Unified CM Certificates (No MRA)

To establish a secure connection with Unified CM, Webex Teams validates the certificate that is presented by the server during the connection process. Unlike Jabber, Webex Teams does not prompt users with the option to accept an untrusted certificate.

Unified CM must be configured with certificates that Webex Teams can validate, preferably a CA root that signed the tomcat certificate (which is known to the operating system that Webex Teams is on, Windows or MacOS by default), or a self-signed trusted certificate (which must be deployed to the OS in advance by the enterprise administrator).

Note

The Tomcat certificate is also used for secure SIP when Webex Teams is enabled for encrypted calls (SIP OAuth operates on the default port 5090). See “Configure the Phone Security Profile for Encrypted Calls” in this guide for more details.
Certificates issued with a deprecated signature algorithm (such as SHA-1) do not work; you must use a supported secure signature algorithm such as SHA-256 or later, as documented in the Certificates chapter in the Administration Guide for Cisco Unified Communications Manager.

**Note**
The certificates that are deployed on Unified CM servers must include the fully qualified domain name (FQDN) as the server identity rather than a simple hostname or IP address (for example, cucm-server-1.example.com rather than cucm-server-1 or 203.0.113.1).

In Cisco Unified CM Administration > System > Server, the Unified CM server names must be defined as FQDN.

See High Level View of Certificates and Authorities in CUCM and CUCM Certificate Management and Change Notification for information about certificate management in Unified CM.

**Unified CM Certificates (With MRA)**
The Unified CM Tomcat certificate is significant for Mobile and Remote Access. This certificate is automatically installed on the Cisco Unified Communications Manager. By default, it is self-signed and has the same common name (CN).

**Note**
The Tomcat certificate is also used for secure SIP when Webex Teams is enabled for encrypted calls (SIP Outh operates on the default port 5091 for MRA). See “Configure the Phone Security Profile for Encrypted Calls” in this guide for more details.

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. So if the CallManager and tomcat self-signed certificates have the same CN in the Expressway's trusted CA list, the Expressway can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

**Expressway Certificates (With MRA)**
The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant Subject Alternative Name (SAN) entries as appropriate for the Unified Communications features that are supported on that Expressway.

The following table shows which CSR alternative name elements apply to which Unified Communications features.
Table 4: CSR Alternative Name Element and Mobile Remote Access

<table>
<thead>
<tr>
<th>Add These Items as Subject Alternative Names</th>
<th>When Generating a CSR For Mobile Remote Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)</td>
<td>Required on Expressway-E only</td>
</tr>
<tr>
<td>Unified CM phone security profile names</td>
<td>Required on Expressway-C only</td>
</tr>
<tr>
<td>(Clustered systems only) Expressway cluster name</td>
<td>Required on Expressway-C only</td>
</tr>
</tbody>
</table>

- You may need to produce a new server certificate for the Expressway-C if chat node aliases are added or renamed. Or when new TLS phone security profiles are added.
- You must restart the Expressway for any new uploaded server certificate to take effect.

Expressway-C Server Certificate Requirements

The Expressway-C server certificate needs to include the following element in its list of subject alternate names:

- **Unified CM phone security profile names**: the names of the Phone Security Profiles in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.

  Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.

Expressway-E Server Certificate Requirements

The Expressway-E server certificate needs to include the following element in its list of subject alternative names (SAN):

- **Unified CM registrations domains**: all of the domains which are configured on the Expressway-C for Unified CM registrations. Required for secure communications between endpoint devices and Expressway-E.

  The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate, are used by Mobile and Remote Access clients to lookup the _collab-edge DNS SRV record during service discovery. They enable MRA registrations on Unified CM, and are primarily for service discovery.

  These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a .local or similar private domain with Unified CM on the internal network, and public domain names for the Expressway-E
FQDN and service discovery. In this case, you need to include the public domain names in the Expressway-E certificate as SANs. There is no need to include the private domain names used on Unified CM. You only need to list the edge domain as a SAN.

Select the DNS format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. You may select CollabEdgeDNS format instead, which simply adds the prefix collab-edge to the domain that you enter. This format is recommended if you do not want to include your top level domain as a SAN (see example in following screenshot).

### Headset Requirements for Calling in Webex Teams (Unified CM)

Calling in Webex Teams (Unified CM) supports the following Cisco 500 series headsets. Click the links for more information on each model:

- 520 Series
- 530 Series
- 560 Series

### License Requirements for Calling in Webex Teams (Unified CM)

You require a Cisco Webex organization (managed in Cisco Webex Control Hub) with a paid subscription. Additionally, for softphone functionality, each Webex Teams app registers to Unified CM as a softphone client. Like Cisco Jabber, this registration uses the Cisco Unified Client Services Framework (CSF) client for desktop and a BOT, TCT, or TAB device for mobile, and counts as a device toward Unified CM licensing. Users with three or more apps and/or devices require CUWL perpetual licensing or for the organization to be on a Flex Calling subscription. (Flex Calling is the recommended subscription channel.)

### Webex Teams App Requirements for Calling in Webex Teams (Unified CM)

- Version 3.0.11421.0 and later for Windows and Mac
- Version 4.0.62 and later for Android
- Version 4.0.17 and later for iPhone and iPad

**Note**

We recommend that users be on the latest release of the Webex Teams app for desktop or mobile.

- For installation and upgrade instructions, see [Cisco Webex Teams Installation and Automatic Upgrade](#).
- For release information, see the [Release Notes](#) and [What's New](#) documentation.
Recommended Configuration for Calling in Webex Teams (Unified CM)

- For Calling in Webex Teams (Unified CM), SSO is supported with Unified CM and Expressway. You must either enable or disable SSO on both. For a consistent user experience with SSO, we recommend that you extend your Identity Provider (IdP) integration to Webex Teams so that users can sign in with the same credentials. With Single Sign-On (SSO) integration between your IdP, your premises environment, and the Webex cloud, users can sign in across applications with one set of credentials.
  - For premises Unified CM configuration, see the SAML SSO Deployment Guide for Cisco Unified Communications Applications for your release.
  - For Expressway configuration, see the Mobile and Remote Access via Cisco Expressway Deployment Guide for your release.
  - For cloud (Webex Teams) configuration, see Single Sign-On Integration with Webex Control Hub.

- User phone numbers can appear in contact cards in the Webex Teams app for Windows and Mac:
  
  For the numbers to appear, you must deploy Cisco Directory Connector to synchronize the numbers from an existing Active Directory attribute into the cloud. See the attribute mapping information in the Deployment Guide for Cisco Directory Connector at https://www.cisco.com/go/hybrid-services-directory.

- We recommend the following additional configuration to provide further benefits for your Calling in Webex Teams (Unified CM) deployment:
  - Quality of Service (QoS), covered in the Appendix, on page 51 in this guide. QoS helps manage packet loss, delay and jitter on your network infrastructure.
  - Call Admission Control (CAC) on Unified CM, covered in the System Configuration Guide for Cisco Unified Communications Manager. CAC enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time.

Hybrid Call Service Removal Requirements for Calling in Webex Teams (Unified CM)

You must disable Hybrid Call Service for any users in your organization, because Hybrid Call Service for users cannot coexist with Calling in Webex Teams (Unified CM) for users. See the migration guidance that follows.
Considerations for Migrating from Hybrid Call Service to Calling in Webex Teams (Unified CM)

This table summarizes the key points you must consider as you transition your organization from the old Hybrid Call Service (server-side integration) solution to the new Calling in Webex Teams (Unified CM) (client-side integration) solution. This table takes into account what is required to transition users over to the new solution and what needs to be preserved if you want to continue to use Webex cloud-registered video devices with Hybrid Call Service. Specific configuration steps for Hybrid Call Service (user) removal and end-to-end deployment of Calling in Webex Teams (Unified CM) follow in this guide.

<table>
<thead>
<tr>
<th>Before Migration</th>
<th>After Migration</th>
<th>Impact</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Spark Remote Devices (Cisco Spark-RD) for both users and Webex cloud-registered video devices</td>
<td>Cisco Spark-RD for only Webex cloud-registered video devices</td>
<td>None</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Spark-RD for users</td>
<td>Jabber-type devices (desktop on Client Service Framework (CSF), mobile on TCT, BOT, or TAB) for users</td>
<td>Unified CM Configuration</td>
<td>Remove any Cisco Spark-RD for users; add Jabber devices of desired types (CSF, TCT, BOT, TAB) for users</td>
</tr>
<tr>
<td>One Spark RD per user for apps (desktop, mobile, and so on.)</td>
<td>One Jabber-type device per app (desktop, mobile)</td>
<td>Licensing</td>
<td>Convert perpetual licensing to Flex (recommended); or upgrade perpetual UCL Enh/Enh+ to CUWL</td>
</tr>
<tr>
<td>—</td>
<td>—</td>
<td>Capacity</td>
<td>Review Unified CM device capacity utilization; deploy additional capacity (larger OVAs or more servers) as necessary</td>
</tr>
</tbody>
</table>
Recommendation Impact After Migration

<table>
<thead>
<tr>
<th>Before Migration</th>
<th>After Migration</th>
<th>Impact</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Connector required for Hybrid Call Service users and video devices</td>
<td>Call Connector required only for video devices</td>
<td>Less Call Connector capacity required</td>
<td>Reduce or remove Expressway capacity for Call Connectors; reallocate capacity to other connectors (Calendar, Messaging, Serviceability)</td>
</tr>
<tr>
<td>Webex Teams apps connect to cloud for calling</td>
<td>Webex Teams apps register directly to Unified CM for calling</td>
<td>Off-premises Webex Teams apps require Mobile Remote Access (MRA) for registration</td>
<td>Evaluate MRA registration capacity needed; reallocate Expressway capacity from Hybrid Call Service to MRA</td>
</tr>
<tr>
<td>All call attempts between Hybrid Call Service users traverse the firewall</td>
<td>Call attempts traverse the firewall only for off-premises Webex Teams apps that use MRA</td>
<td>Off-premises Teams apps require MRA for calling; on-premises Webex Teams apps do not require any firewall traversal</td>
<td>Evaluate MRA calling capacity needed; reallocate capacity from Hybrid Call Service to MRA</td>
</tr>
<tr>
<td>Jabber and Webex Teams apps installed separately</td>
<td>Webex Teams apps install with embedded Jabber-type device</td>
<td>Webex Teams app install does not replace existing Jabber client</td>
<td>Remove existing Jabber client manually</td>
</tr>
</tbody>
</table>

Retain Configuration for Hybrid Call Service for Webex Devices

Before removing Hybrid Call Service for users, you must ensure that the following configuration remains in place for Webex devices in a Place that are enabled for Hybrid Call Service.

**Procedures**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Do not remove configuration from the Expressway-C and Expressway-E traversal pair.</td>
<td>Enterprise calls to and from Webex devices in a Place are securely routed over the Expressway pair for Hybrid Call Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Do not remove SIP Destinations.</td>
<td>The SIP destination address in Control Hub resolves to your Expressway-E in the call traversal pair for Hybrid Call Service. All the hybrid call traffic goes through this address. This entry is typically a DNS-SRV record which can resolve to multiple Expressway-Es.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Do not deactivate Hybrid Call Service Connect for your organization.</td>
<td>This setting resides in Control Hub and is organization-wide. When enabled, Hybrid Call Service is active and available and can then be assigned to Webex-registered devices.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Do not remove Cisco Spark-RD or end user accounts that are tied to Webex devices in a Place.</td>
<td>The Cisco Spark-RD is a virtual device that is attached to a user's work number and links the 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</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> Do not remove Cisco Unified Communications Manager Settings for Hybrid Call Service.</td>
<td>Behind the scenes, the Cisco Spark-RD ties together call activity in the cloud and the premises and the end user account is associated with devices in a Place.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> Do not unregister Expressway-Cs that host Call Connectors supporting hybrid Webex devices.</td>
<td>Cisco Unified Communications Manager receives calls from Expressway-C. The configuration in place enables URI routing between the cloud and the on-premises enterprise. The cluster FQDN specified in the enterprise parameter is used in SIP routing decisions, and that helps identify multiple clusters so that calls can occur between them.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> Do not remove verified domains used for hybrid Webex devices or those who administer them.</td>
<td>Domain verification is essential to the security and integrity of your organization. The established verification proves to us that you own a particular domain and is required for this service to work. For Hybrid Call Service, the verified domains are the ones in on-premises directory URIs tied to Webex devices and anyone who administers the devices.</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Carefully follow the steps in Remove Hybrid Call Service Configuration From Users, on page 24.

**Remove Hybrid Call Service Configuration From Users**

If you already have Hybrid Call Service deployed in your organization, you must remove it for your users before you can deploy Calling in Webex Teams (Unified CM). Use these steps to disable Hybrid Call Service for your users, and remove any of the related configuration from Unified CM.

⚠️ **Caution**

If any Hybrid Call Service users have personal mode devices configured, these devices also lose Hybrid Call Service because the service is disabled for the user. The workaround is to convert the personal mode device to shared mode, add it to a Place, and activate it for Hybrid Call Service. See Deploy Hybrid Call Service for Cisco Webex Devices for more information.

**Before you begin**

Hybrid Call Service is still required if you added the service to Room, Desk, or Board devices that are in a Place in Control Hub. You must not remove anything necessary for Room, Desk, and Board devices enabled with Hybrid Call Service. Review the following sections before you proceed:

- Considerations for Migrating from Hybrid Call Service to Calling in Webex Teams (Unified CM), on page 22
Step 1  
To remove Call Service Aware and Call Service Connect from user accounts in Cisco Webex Control Hub, sign in to the customer view in https://admin.webex.com. You can then use any of the following methods:

**Table 5: Options to Remove the Service from Webex Teams User Accounts in Control Hub**

<table>
<thead>
<tr>
<th>User Configuration Method</th>
<th>Steps to Disable Hybrid Call Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Users</td>
<td>Go to Users, click a username in the list to open the overview pane, click Call Service, then Connect, and then toggle off the setting. Then return and toggle off the Aware setting.</td>
</tr>
<tr>
<td>Bulk users accounts using the CSV template</td>
<td>Go to Users, click Manage Users &gt; Export Users List, enter FALSE in the Call Service Aware and Call Service Connect columns, save the file, and then go back to <a href="https://admin.webex.com">https://admin.webex.com</a> to click Import and then choose the file that you updated. Click Add and remove services and then click Submit.</td>
</tr>
<tr>
<td>Directory-synchronized user accounts (through the Cisco Directory Connector)</td>
<td>Go to Users, click Manage Users, choose Modify all synchronized users, and then click Next. Click through the prompts to get to the Sync Status screen. Click the refresh arrow, click Next, and then remove Call Service Aware and Call Service Connect from users.</td>
</tr>
</tbody>
</table>

This step completely disables Hybrid Call Service for your users only, but it remains configured at the organization level (Hybrid Call Service is still necessary for Room, Desk, and Board devices in a Place that are registered to the cloud). Next, you must remove the Cisco Spark Remote Device (Cisco Spark-RD) for any users who used Hybrid Call Service. Whether you chose the automatic creation option in the Call Connector or manually created them in Unified CM, you must manually remove them in the next step.

Step 2  
To remove any Cisco Spark-RD that was associated with a user, go to Cisco Unified CM Administration and follow these steps:

a) Click Device > Phone.

b) In the Find phone where drop-down, choose Device Type, and in the Select item or enter search text drop-down, choose Cisco Spark Remote Device. Click Find.

c) Check any of the devices that you want to remove, and then click Delete selected. Read the prompt and when you're sure, click OK.

This step removes all selected Cisco Spark-RD and corresponding remote destinations for users.

**Caution**  
If you have Hybrid Call Service configured for Room, Board, and Desk devices in a place, only remove Cisco Spark-RD that are associated with Webex Teams users on Hybrid Call Service in your organization. Do not proceed to the next steps.

d) Return to Device > Phone and search for CTI-RDs that may've been used for Hybrid Call Service: in the Find phone where drop-down, choose Device Type, and in the Select item or enter search text drop-down, choose CTI Remote Device. Click Find.

**Tip**  
CTI-RDs that were used for Hybrid Call Service contain a remote destination with *.call.ciscospark.com as the address.

e) Check any of the devices that you want to remove, and then click Delete selected. Read the prompt and when you're sure, click OK.
This step removes all selected CTI-RDs and corresponding remote destinations for users.

**Step 3**  
(Optional) Do this optional cleanup configuration if you want to remove Hybrid Call Service entirely and you don’t have Room, Desk, or Board devices in a Place set up for Hybrid Call Service.

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

b) Scroll to **Call Service Connect**, click **Deactivate**, read the prompt, and then when you understand the changes, click **Deactivate** again.

   This step disables Hybrid Call Service functionality for your organization.

c) Scroll to **Deactivate**, and then click **Deactivate**. Read the prompt, and then when you understand the changes, click **Deactivate** again.

   This step removes Call Connector and related configuration from the Expressway clusters registered to the cloud.

d) Remove nodes from any Expressway cluster hosting by following the steps in this document.

e) When you are done removing nodes from the clusters, deregister the clusters by following the steps in this document.
Deploy Calling in Webex Teams (Unified CM)

• Calling in Webex Teams (Unified CM) Deployment Task Flow, on page 27
• Overview of Service Profile, on page 29
• Configure CTI Service Workflow, on page 30
• Service Discovery Options, on page 32
• Authentication Options, on page 33
• Set Parameters on Phone Configuration for Desktop Clients, on page 34
• Configure Unified CM End Users for Calling in Webex Teams (Unified CM), on page 34
• Create Softphones Workflow, on page 35
• Set Calling Behavior in Control Hub, on page 40
• Configure SIP Address Routing for Your Organization, on page 41
• Authenticate with Phone Services in Webex Teams, on page 41
• Known Issues and Limitations With Calling in Webex Teams (Unified CM), on page 43

Calling in Webex Teams (Unified CM) Deployment Task Flow

These steps walk you through a typical phone only deployment that's used for Calling in Webex Teams (Unified CM). For this deployment, Webex Teams is going to register to Unified CM as a softphone client, just like Cisco Jabber does.

Before you begin

Prepare Your Environment for Calling in Webex Teams (Unified CM), on page 13

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Create Default Service Profile, on page 30</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure CTI Service Workflow, on page 30</td>
</tr>
<tr>
<td></td>
<td>• Add a CTI Service, on page 30</td>
</tr>
<tr>
<td></td>
<td>• Apply a CTI Service, on page 31</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Choose from the Service Discovery Options, on page 32:</td>
</tr>
<tr>
<td></td>
<td>• Configure DNS SRV Records, on page 32</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| • Manual Connection Settings, on page 41 | configure service discovery using one of the following options.  
  • DNS SRV Records—The client (Webex Teams) automatically locates and connects to services. This is the recommended option.  
  • Manual Connection Settings—Manual connection settings provide a fallback mechanism when service discovery is not used. With administrator guidance, users must manually enter a server address or UC domain followed by their SSO or non-SSO credentials, as documented at the end of the task flow. |

**Step 4** Choose from the Authentication Options, on page 33:  
• SAML SSO in the Client, on page 33  
• Authenticate with the LDAP Server, on page 33  
These options determine the authentication mechanism that is used when a user signs into phone services in Webex Teams:  
• SAML Single Sign-On (SSO)—End user passwords are authenticated against the password that resides in the identity provider used for SSO.  
• LDAP Server—End user passwords are authenticated against the password that is assigned in the company LDAP directory.  

**Step 5** Set Parameters on Phone Configuration for Desktop Clients, on page 34  
The client can retrieve configuration settings in the phone configuration from specific locations on Cisco Unified Communications Manager.  

**Step 6** Configure Unified CM End Users for Calling in Webex Teams (Unified CM), on page 34  
For Calling in Webex Teams (Unified CM) to work, you must create new users or configure existing users on Unified CM with the following settings.  

**Step 7** Follow these steps in the Create Softphones Workflow, on page 35:  
• Create and Configure Webex Teams Softphone Devices, on page 36  
• Add a Directory Number to the Device, on page 37  
• Associate Users with Devices, on page 38  
• Configure the Phone Security Profile for Encrypted Calls, on page 38  
Follow these steps to create and configure softphone devices on Unified CM (these correspond to each Webex Teams app for softphone use), add a directory number to the softphone device, associate the device with an end user account, and optionally configure devices and Webex Teams apps for secure and encrypted calls.  

**Step 8** Set Calling Behavior in Control Hub, on page 40  
You can use Control Hub set the calling behavior for some of your users (recommended) or for your entire organization (when you're ready to roll out the service). For Calling in Webex Teams (Unified CM), you configure this setting so that users can use the calling feature set.
### Overview of Service Profile

*Figure 6: Service Profiles Workflow*

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> Configure SIP Address Routing for Your Organization, on page 41</td>
<td>If you configure this setting in Control Hub, SIP calls in Webex Teams for Windows or Mac can route through your enterprise for domains that you enter.</td>
</tr>
<tr>
<td><strong>Step 10</strong> Authenticate with Phone Services in Webex Teams, on page 41</td>
<td>If you have DNS SRV implemented, users will be autodiscovered for phone services in the Webex Teams app. If you don't, they'll have to enter a server address for the UDS server or the UC domain (FQDN or IP address of Unified CM).</td>
</tr>
</tbody>
</table>

1. Create UC services.
2. Associate the UC Service with the Service Profile.
3. Associate the User with the Service Profile.
Create Default Service Profile

Create a service profile to add the UC services.

Step 1
Open the Cisco Unified CM Administration interface.

Step 2
Select User Management > User Settings > Service Profile.
The Find and List Service Profiles window opens.

Step 3
Select Add New.
The Service Profile Configuration window opens.

Step 4
Enter a name for the service profile in the Name field.

Step 5
Select Make this the default service profile for the system if you want the service profile to be the default for the cluster.

Step 6
Select Save.

What to do next
Create the UC services for your deployment.

Configure CTI Service Workflow

The CTI Service provides Webex Teams with the devices that are associated with the user.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Add a CTI Service, on page 30</td>
<td>Create a CTI UC service to provide Webex Teams with the location of the CTI service.</td>
</tr>
<tr>
<td>Step 2 Apply a CTI Service, on page 31</td>
<td>Apply the CTI UC service to the service profile.</td>
</tr>
</tbody>
</table>

Add a CTI Service

Create a CTI UC service to provide Webex Teams with the location of the CTI service.

Step 1
Open the Cisco Unified CM Administration interface.

Step 2
Select User Management > User Settings > UC Service.
The Find and List UC Services window opens.

Step 3
Select Add New.
The UC Service Configuration window opens.

Step 4
In the Add a UC Service section, select CTI from the UC Service Type drop-down list.
Step 5  Select Next.

Step 6  Provide details for the CTI service as follows:
   a) Specify a name for the service in the Name field.
      The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

   b) Specify the CTI service address in the Host Name/IP Address field.
      Enter the address in the form of a hostname, IP address, or fully qualified domain name (FQDN). This value corresponds to the Unified CM publisher that's running the CTI Manager service. You'll create a second service for the subscriber.

   c) Specify the port number for the CTI service in the Port field.

Step 7  Select Save.

What to do next
Create a second CTI service for the Unified CM subscriber.
Add the CTI service to your service profile.

Apply a CTI Service

After you add a CTI service on Cisco Unified Communications Manager, you must apply it to a service profile so that the client can retrieve the settings.

Before you begin
   • Create a service profile if none already exists or if you require a separate service profile for CTI.
   • Add CTI services for the Unified CM publisher and subscriber.

Step 1  Open the Cisco Unified CM Administration interface.

Step 2  Select User Management > User Settings > Service Profile.
        Find and List Service Profiles window opens.

Step 3  Find and select your service profile.
        Service Profile Configuration window opens.

Step 4  Navigate to CTI Profile section, and select up to three services from the following drop-down lists:
   • Primary
   • Secondary
   • Tertiary

Step 5  Select Save.
## Service Discovery Options

Service discovery enables clients to automatically detect and locate services on your enterprise network. You can configure service discovery using one of the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure DNS SRV Records, on page 32</strong></td>
<td>The client automatically locates and connects to services.</td>
</tr>
<tr>
<td></td>
<td>This is the recommended option.</td>
</tr>
<tr>
<td><strong>Manual Connection Settings, on page 41</strong></td>
<td>Manual connection settings provide a fallback mechanism when service discovery is not used.</td>
</tr>
</tbody>
</table>

### Note

At this time, we support internal only automatic discovery. Service discovery enables clients to automatically detect and locate services on your enterprise network. Clients query domain name servers to retrieve service (SRV) records that provide the location of servers.

## Configure DNS SRV Records

**Before you begin**

Review your SRV record requirements in the *Service Discovery* chapter of the *Planning Guide for Cisco Jabber*.

Create the SRV records for your deployment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_cisco-uds</td>
<td>Provides the location of Cisco Unified Communications Manager. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.</td>
</tr>
<tr>
<td>_collab-edge</td>
<td>Provides the location of Cisco VCS Expressway or Cisco Expressway-E. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.</td>
</tr>
</tbody>
</table>

### Example of an SRV record

```
_cisco-uds._tcp.DOMAIN service location:
priority = 0
weight = 0
port = 8443
svr hostname=_cisco-uds._tcp.example.com
```
What to do next
Test SRV Records, on page 33

Test SRV Records

After creating your SRV records test to see if they are accessible.

Tip
You can also use the SRV check tool on the Collaboration Solutions Analyzer site if you prefer a web-based option.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open a command prompt.</td>
</tr>
<tr>
<td>2</td>
<td>Enter <code>nslookup</code>. The default DNS server and address is displayed. Confirm that this is the expected DNS server.</td>
</tr>
<tr>
<td>3</td>
<td>Enter <code>set type=SRV</code>. Enter the name for each of your SRV records. For example, <code>_cisco-uds._tcp.exampledomain</code></td>
</tr>
<tr>
<td>4</td>
<td>Displays server and address—SRV record is accessible. Displays <code>_cisco-uds_tcp.exampledomain</code>: Non-existent domain—There is an issue with your SRV record.</td>
</tr>
</tbody>
</table>

Authentication Options

SAML SSO in the Client

For more information about integrating SSO with Unified CM so that Webex Teams users can sign in using a single set of credentials, see the SAML SSO Deployment Guide for Cisco Unified Communications Applications. For cloud (Webex Control Hub) configuration, see Single Sign-On Integration With Webex Control Hub.

Authenticate with the LDAP Server

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. When users sign in to the client, Webex Teams routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then sends that authentication to the directory server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open the Cisco Unified CM Administration interface.</td>
</tr>
</tbody>
</table>
Set Parameters on Phone Configuration for Desktop Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

**Enterprise Phone Configuration**
Applies to the entire cluster.

**Common Phone Profile Configuration**
Applies to groups of devices and takes priority over the cluster configuration.

**Cisco Unified Client Services Framework (CSF) Phone Configuration**
Applies to individual CSF desktop devices and takes priority over the group configuration.

Configure Unified CM End Users for Calling in Webex Teams (Unified CM)

For Calling in Webex Teams (Unified CM) to work, you must create new users or configure existing users on Unified CM with the following settings.

If you use LDAP synchronization, these settings may already be in place. If setting up a new LDAP synchronization, see “LDAP Synchronization Overview” in the On-Premises Deployment for Cisco Jabber documentation at https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.

**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 **Mail ID** contains the user's email address.

**Note**
If you're using Server Information for configuration and not SRV records, your users' Webex Teams email addresses must match their Unified CM email addresses—at a minimum, the user ID portion before the domain must match.

**Step 3**
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.

**Step 4** Ensure that the Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile) option is not checked.

**Step 5** (Optional) Choose your service profile from the UC Service Profile drop-down list if you need to make user-level overrides.

**Step 6** Save your changes, and then you'll assign applicable roles to the user.

**Step 7** Click Add to Access Control Group.

**Step 8** Click the corresponding check box for each access control group that you want to assign to the end users.

At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**—This option is used for desk phone control.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf.**
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode.**

---

**What to do next**

Associate devices to the user.

---

**Create Softphones Workflow**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Create and Configure Webex Teams Softphone Devices, on page 36</td>
<td>Create at least one device for every user that wants to use Webex Teams in softphone mode. You can add one softphone device for any supported Webex Teams platforms that the users are on—for example, appropriate device types for desktop, mobile and tablet.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Add a Directory Number to the Device, on page 37</td>
<td>For each device you create, add a directory number.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Associate Users with Devices, on page 38</td>
<td>Associate users with devices.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Configure the Phone Security Profile for Encrypted Calls, on page 38</td>
<td>Complete this task to set up secure phone capabilities for all devices and Webex Teams.</td>
</tr>
</tbody>
</table>
Create and Configure Webex Teams Softphone Devices

To make the Webex Teams app a softphone client, create at least one device for every user that you're configuring for Calling in Webex Teams (Unified CM). Webex Teams registers to Unified CM using the same device type as Cisco Jabber.

**Step 1** Log into the Cisco Unified CM Administration interface.

**Step 2** Select Device > Phone. Find and List Phones window opens.

**Step 3** Select Add New.

**Step 4** From the Phone Type drop-down list, select the option that is applicable to the device type you are configuring and then select Next.

For Webex Teams users, you can only create one type of device per user although you can create multiple devices for each user. For example, you can create one dual mode mobile device and one CSF device but not two CSF devices.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Webex Teams for Mac or Webex Teams for Windows.
  - Cisco Dual Mode for iPhone—Select this option to create a TCT device for Webex Teams for iPhone users.
  - Cisco Jabber for Tablet—Select this option to create a TAB device for Webex Teams on an iPad, Android tablet, or for Chromebooks.
  - Cisco Dual Mode for Android—Select this option to create a BOT device for Webex Teams for Android phone users.

**Step 5** From the Owner User ID drop-down list, select the user for whom you want to create the device.

**Step 6** In the Device Name field, use the applicable format to specify a name for the device:

<table>
<thead>
<tr>
<th>If You Select</th>
<th>Required Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Client Services Framework</td>
<td>• Valid characters: a–z, A–Z, 0–9.</td>
</tr>
<tr>
<td></td>
<td>• 15-character limit.</td>
</tr>
<tr>
<td>Cisco Dual Mode for iPhone</td>
<td>• The device name must begin with TCT.</td>
</tr>
<tr>
<td></td>
<td>For example, if you create a TCT device for user, Tanya Adams, whose username is tadams, enter TCTTADAMS.</td>
</tr>
<tr>
<td></td>
<td>• Must be uppercase.</td>
</tr>
<tr>
<td></td>
<td>• Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-).</td>
</tr>
<tr>
<td></td>
<td>• 15-character limit.</td>
</tr>
</tbody>
</table>
If You Select | Required Format
---|---
Cisco Jabber for Tablet | • The device name must begin with *TAB*.  
For example, if you create a TAB device for user,  
Tanya Adams, whose username is tadams, enter  
**TABTADAMS**.  
• Must be uppercase.  
• Valid characters: A–Z, 0–9, period (.), underscore (_),  
hyphen (-).  
• 15-character limit.

Cisco Dual Mode for Android | • The device name must begin with *BOT*.  
For example, if you create a BOT device for user,  
Tanya Adams, whose username is tadams, enter  
**BOTTADAMS**.  
• Must be uppercase.  
• Valid characters: A–Z, 0–9, period (.), underscore (_),  
hyphen (-).  
• 15-character limit.

**Note** You need to deploy Mobile and Remote Access (MRA) on Expressway if your Webex Teams users need to connect outside of the corporate network.

**Step 7** Select Save.
**Step 8** Click Apply Config.

**What to do next**
Add a Directory Number to the device.

**Add a Directory Number to the Device**
After you create and configure each device, you must add a directory number to the device. This topic provides instructions on adding directory numbers using the **Device > Phone** menu option.

**Before you begin**
Create a device.

**Step 1** Locate the **Association Information** section on the **Phone Configuration** window.
**Step 2** Click **Add a new DN**.
**Step 3** In the **Directory Number** field, specify a directory number.
Step 4 In the Users Associated with Line section, click Associate End Users.
Step 5 In the Find User where field, specify the appropriate filters and then click Find.
Step 6 From the list that appears, select the applicable users and click Add Selected.
Step 7 Specify all other required configuration settings as appropriate.
Step 8 Select Apply Config.
Step 9 Select Save.

Associate Users with Devices

Before you begin

Note A softphone device for Webex Teams should not be associated to multiple users if you intend to use different service profiles for these users.

Step 1 Associate users with devices.
   a) Open the Unified CM Administration interface.
   b) Select User Management > End User.
   c) Find and select the appropriate user.
      The End User Configuration window opens.
   d) Select Device Association in the Device Information section.
   e) Associate the user with devices as appropriate.
   f) Return to the End User Configuration window and then select Save.

Step 2 Set the User Owner ID field in the device configuration.
   a) Select Device > Phone.
   b) Find and select the appropriate device.
      The Phone Configuration window opens.
   c) Locate the Device Information section.
   d) Select User as the value for the Owner field.
   e) Select the appropriate user ID from the Owner User ID field.
   f) Select Save.

Configure the Phone Security Profile for Encrypted Calls

You can optionally set up secure phone capabilities for all devices and Webex Teams apps. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection. Secure call support requires Unified CM 12.5 and later.
Before you begin

- You must use Unified CM Release 12.5 or later and we support only SIP OAuth with Webex Teams. CAPF is not supported. For more details, see the chapter on SIP OAuth in the Feature Configuration Guide for Cisco Unified Communications Manager at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

- Configure the Cisco Unified Communications Manager security mode. At minimum, select mixed mode security.

For instructions on how to configure mixed mode, see the Cisco Unified Communications Manager Security Guide.

- For conference calls, ensure that the conferencing bridge supports secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

**Step 1**

In *Cisco Unified Communications Manager*, select **System > Security > Phone Security Profile**.

**Step 2**

Select **Add New**.

**Step 3**

From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Webex Teams for Mac or Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TFT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.
- **CTI Remote Device**—Select this option to create a CTI remote device.

CTI remote devices are virtual devices that monitor and have call control over a user’s remote destination.

**Step 4**

In the **Name** field of the **Phone Security Profile Configuration** window, specify a name for the phone security profile.

**Step 5**

For **Device Security Mode**, choose **Encrypted**.

The SIP connection is over TLS using AES 128/SHA encryption. The client uses Secure Real-time Transport Protocol (SRTP) to offer encrypted media streams.

**Step 6**

For **Transport Type**, leave the default value of **TLS**.

**Step 7**

Check **Enable Oath Authentication**

**Step 8**

For **Authentication Mode**, select **By Authentication String** or **By Null String**.

**Note**  
Using the CAPF Authentication mode **By Null String** with Webex Teams for Windows CSF devices is not supported. It causes Webex Teams registration with Cisco Unified Communications Manager to fail.

**Step 9**

For **Key Size (Bits)**, select the appropriate key size for the certificate. Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

Webex Teams was tested using authentication strings with 1024-bit length keys. Webex Teams requires more time to generate 2048-bit length keys than 1024-bit length keys. As a result, if you select 2048, expect it to take longer to complete the CAPF enrollment process.
Step 10  For SIP Phone Port, leave the default value.
The port that you specify in this field takes effect only if you select Non Secure as the value for Device Security Mode.

Step 11  Click Save.

Set Calling Behavior in Control Hub

You can use Control Hub to set the calling behavior for specific users in your organization or for your entire organization. For Calling in Webex Teams (Unified CM), you configure this setting for users so that they can use the calling feature set.

For more information about the calling behavior options in Control Hub, see Set Up Cisco Webex Teams Calling Behavior.

Before you begin

The option is not available if Hybrid Call Service is still enabled for users in your organization. (The calling behavior option for Hybrid Call Service is Calling in Webex Teams.) You must remove Hybrid Call Service from users before you can assign Calling in Webex Teams (Unified CM). See the “Prepare Your Environment” chapter for more information.

Note  We recommend that you configure this setting based on your organization's needs—for example, you may want to enable specific users in your organization, have them test out the service, and then configure the service for your entire organization when you're ready.

Procedure

• To change this setting at the user level from the customer view in https://admin.webex.com, go to Users, locate and open a user account, scroll to Settings, select Calling Behavior (you'll see the user set up with an organization-wide default), and then choose Calling in Webex Teams (Unified CM).

  A message appears that indicates that the calling behavior is updated. The user account is set up with Calling in Webex Teams (Unified CM) as an override to the organization-wide setting. The specific users you enabled are now able to make Unified CM calls in Webex Teams. See Explore Calling in Cisco Webex Teams (Unified CM) for more information.

• To change this setting at the organization level from the customer view in https://admin.webex.com, go to Settings, scroll to Calling Behavior, and then choose Calling in Webex Teams (Unified CM).

Caution  Only choose the organization-wide option if you're ready to migrate your entire organization.

  A message appears that indicates that the calling behavior is updated. All users in your organization are now able to make Unified CM calls in Webex Teams. See Explore Calling in Cisco Webex Teams (Unified CM) for more information.
Manual Connection Settings

Manual connection settings provide a fallback mechanism when Service Discovery is not used.

When you start Webex Teams, you can specify the authenticator and server address in the Phone Services window. The app caches the server address to the local application configuration that loads on subsequent starts. Webex Teams prompts users to enter advanced settings on the initial start if the app cannot get the authenticator and server addresses from the service profile.

Settings that are entered in Webex Teams take priority over any other sources including SRV records and bootstrap settings.

Configure SIP Address Routing for Your Organization

If you configure this setting in Control Hub and change the default option, SIP calls in Webex Teams for Windows or Mac can route through your Unified CM on-premises environment for the domains that you enter.

Before you begin

This setting is only available if you've deployed Calling in Webex Teams (Unified CM) as a calling service in your Control Hub organization.

**Step 1**
From the customer view in https://admin.webex.com, go to Services, and then choose Client Settings on the Call card.

**Step 2**
Scroll to Unified CM SIP Address Routing, and then change the SIP Address Call Path setting depending on how you want calls to route:

- **All SIP address calls, except addresses that match cloud Webex services**—The default option routes all SIP calls to your enterprise except for any domains that match cloud Webex services.

- **Only calls that match the specified (comma separated) domains**—This option overrides the default and only routes SIP calls through the domains that you enter in the field.

Enter a comma-separated list of up to 200 domains. You can also enter an asterisk as a wildcard. For example: *.example.com, example1.com, example2.com. The routing behavior is the same for any subdomains that fall under a wildcard entry. Alternatively, you can list IP addresses.

**Note**

*.example.com only matches subdomains, not top-level domains.

Authenticate with Phone Services in Webex Teams

If you have DNS SRV implemented, users will be autodiscovered for phone services in the Webex Teams app and they can use their SSO or manual credentials to sign in. If you don't, they'll have to enter a server address for the UDS server or the UC domain (FQDN or IP address of Unified CM) that you provide to them.
**Procedure**

- **If you have autodiscovery through DNS SRV**, users simply open Webex Teams and are prompted for SSO or manual credentials. No further steps are needed.

  The option to enter the server address or UC domain is not presented if you use service discovery with matching login and UC domains.

- **If you don't have autodiscovery through DNS SRV**, help your users follow these steps:
  
  a) Access the Phone Services settings using the applicable Webex Teams platform:
     
     - For Windows, click your profile picture, choose **Settings**, and then click **Phone Services**.
     - For Mac, click your profile picture, choose **Preferences**, and then click **Phone Services**.
     - For Android, tap your profile picture, choose **Settings**, and then choose **Phone Services**.
     - For iPhone and iPad, tap your profile picture, and then choose **Phone Services**

  b) Enter an option, depending on the authentication type and platform:

     For Windows or Mac, enter one of the following:

     - **Server address**—Enter the User Data Service (UDS) server if you don't have SRV records configured. Typically, this is the Unified CM publisher.
     - **UC Domain**—Enter the domain name of the Unified CM that is used for service discovery.

     For Android, iPhone, or iPad, enter the UDS server or domain name in the **Server Address or UC Domain** field, and then tap **Apply** or **Apply Changes**.

  c) Tell users to enter their username and password when they're prompted in the app, and then they can sign in.

---

**Note**

If both Server address and UC domain are configured, Server Address is used to connect to Unified CM while on-premises only. Autodiscovery through DNS SRV is ignored. For MRA, Server Address is ignored.

---

**Note**

The sign in screen varies, depending on the existing SSO setup.

---

Users are authenticated with phone services and can use Calling in Webex Teams (Unified CM) features.

**What to do next**

- **Train Your Users**—You can direct users to the Explore Calling in Cisco Webex Teams (Unified CM) article or use it in your training materials to assist your users with learning how to use the feature set (such as putting a call on hold in Webex Teams or using desk phone control) in Calling in Webex Teams (Unified CM).

- **Troubleshoot Issues**—If there are errors with registration, see the troubleshooting material in this guide for more information.
• **Reset Server Information**—If you need any desktop users to reenter the server information for the Unified CM (for example, moving from a lab to production server), they must reset the database by following the procedure in How Do I Reset the Database for Cisco Webex Teams?.

## Known Issues and Limitations With Calling in Webex Teams (Unified CM)

### Mobile

- Calling in Webex Teams (Unified CM) for mobile and proximity pairing do not work together.
- When running two instances of the app on a mobile platform, a message about another active connection appears.
- For numbers in a contact card on the mobile apps, users must tap the green video icon to see other users’ numbers.

### General

- Calling in Webex Teams (Unified CM) does not support the jabber-config.xml file.
- The Webex Teams login flow uses the embedded Internet Explorer browser, whereas phone services and MRA use the Chromium Embedded Framework (CEF). This means that the web sessions are separated. For example, a user can be prompted two times for authentication even through the same IdP (SSO) is configured for on-premises components and the Webex cloud.
- Calling in Webex Teams (Unified CM) does not work alongside Hybrid Call Service or Cisco Webex Calling (formerly Spark Call). You must disable Hybrid Call Service or Cisco Webex Calling (formerly Spark Call) before you can enable Calling in Webex Teams (Unified CM) for your users. See the Prepare Your Environment chapter for more information on how to disable Hybrid Call Service for users.
- Certificates issued with a deprecated signature algorithm (such as SHA-1) do not work; you must use a supported secure signature algorithm such as SHA-256 or later, as documented in the Certificates chapter in the Administration Guide for Cisco Unified Communications Manager.
- Cross-launch calling app functionality and Calling in Webex Teams (Unified CM) cannot be configured for a single user. You can use Control Hub to do overrides and set calling behavior for individual users—for example, you may want some on Calling in Webex Teams (Unified CM) and some on a Cisco Jabber app cross-launch.
- Coexistence with Jabber:
  - Jabber and Webex Teams each try to register as the same softphone device in Unified CM. A registration popup lets you choose which client you want to use for calling.
  - The registration pop-up does not show when Jabber and Webex Teams run on same machine. If a user is running both clients on the same machine, that user experiences call drops.
- Calls through Calling in Webex Teams (Unified CM) do not leverage Webex Video Mesh nodes.
Known Issues and Limitations With Calling in Webex Teams (Unified CM)
Manage and Troubleshot Calling in Webex Teams (Unified CM)

- Access Call Statistics for Calling in Webex Teams (Unified CM), on page 45
- Troubleshoot Issues with Calling in Webex Teams (Unified CM), on page 46
- Webex Teams Desktop Error Codes For Calling in Webex Teams (Unified CM), on page 48

Access Call Statistics for Calling in Webex Teams (Unified CM)

During a call, users on Webex Teams for Windows or Mac can access call statistics that indicate whether the call is going through Unified CM.

During the active call, access the statistics using one of these steps:

- For Webex Teams for Windows, click on the profile picture, and then choose Help > Show Call Statistics.
- For Webex Teams for Mac, choose Help > Show Call Statistics.

A call statistic window appears with details about the call, such as video framerate, audio codec used, packet loss, jitter, bandwidth usage, and so on. An indicator appears if the call is going through the Unified CM call control environment.
Troubleshoot Issues with Calling in Webex Teams (Unified CM)

If you see registration issues when trying to use Calling in Webex Teams (Unified CM), go through these checklist items before you submit a ticket.

A warning icons appear in the app if Webex Teams failed to register to Unified CM because of a sign in failure or other reason.
Before you begin

Tip
You can hover over the icon to show an error message that may give you clues about what to troubleshoot.

Note
If https://status.webex.com shows a Webex cloud full or partial outage, Calling in Webex Teams (Unified CM) still works, so long as the call type is a Unified CM call. If Unified CM is not reachable from Webex Teams, users can use the Self Care Portal to set up Single Number Reach (SNR) so that calls get routed to mobile through the PSTN. For administrative steps, see the Cisco Unified Mobility Features chapter in the Feature Configuration Guide for Cisco Unified Communications Manager. For user self-care configuration, see the Self Care Portal User Guide.

Step 1
Disable Hybrid Call Service for users in Control Hub. (See the Prepare Your Environment chapter for further details.)

Step 2
Verify that any CTI-RD or Cisco Spark-RD was removed from Unified CM for the user; if not, delete any stray remote devices. (See the Prepare Your Environment chapter for further details.)

Step 3
If your organization is enabled for a different call behavior (such as a calling app cross launch) in Control Hub, disable this feature and reselect Calling in Webex Teams (Unified CM) because Unified CM registration and cross-launch cannot be enabled together.

Step 4
Exit Jabber if it's installed on the same machine, because Jabber and Webex Teams cannot both be registered to Unified CM in softphone mode at the same time.

Step 5
Check other configuration on Unified CM. Some common culprits include the following:

- No Controlled Devices in the Unified CM end user account. Ensure that the soft phone device is added to the Controlled Devices.
- Missing SUBSCRIBE Calling Search Space for Extension Mobility users. Ensure that a value is selected for this setting.
- A missing Access Control Group permission on the end user account: Standard CTI Allow Control of Phones supporting Connected Xfer and conf. Ensure this box is checked.

What to do next
If you addressed all of these steps and issues still persist, restart Webex Teams and then choose Help > Send Feedback to submit logs and open a case for the support team to investigate.
Webex Teams Desktop Error Codes For Calling in Webex Teams (Unified CM)

When the Webex Teams app signs in, you may see an icon on the left side that lets you know if there's an error.

When you hover over the icon, you'll see an error code and message. Below is a list of the error codes related to Unified CM sign in, explanations of the issue, and possible fixes:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Name</th>
<th>Explanation and Possible Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000:1</td>
<td>Unknown</td>
<td>Unexpected internal error. This requires a restart and logs to analyze. (Users can submit logs and create a ticket using Webex Teams under Help &gt; Send Feedback.)</td>
</tr>
<tr>
<td>1000:7</td>
<td>InvalidStartupHandlerState</td>
<td>Unexpected internal error. The user must restart their Webex Teams app.</td>
</tr>
<tr>
<td>1000:8</td>
<td>InvalidLifeCycleState</td>
<td>Unexpected internal error. The user must restart their Webex Teams app.</td>
</tr>
<tr>
<td>1000:400</td>
<td>SSOPageLoadError</td>
<td>Users can click Renew in phone services. They may need to try again later if it's a network or server side issue.</td>
</tr>
<tr>
<td>1000:500</td>
<td>SSOSTartSessionError</td>
<td>Users can click Renew in phone services. They may need to try again later if it's a network or server side issue.</td>
</tr>
<tr>
<td>1000:600</td>
<td>SSOUnknownError</td>
<td>Unexpected internal error. Users can click Renew in phone services. They may need to try again later if it's a network or server side issue. We may need logs to analyze. (Users can submit logs and create a ticket using Webex Teams under Help &gt; Send Feedback.)</td>
</tr>
<tr>
<td>1000:601</td>
<td>SSOCancelled</td>
<td>User error caused by closing the SSO window. Users can click Renew in phone services.</td>
</tr>
<tr>
<td>1000:603</td>
<td>SSOCertificateError</td>
<td>The SSO server provided an invalid cert. (Users can submit logs and create a ticket using Webex Teams under Help &gt; Send Feedback.)</td>
</tr>
<tr>
<td>1000:604</td>
<td>SSOInvalidUserSwitch</td>
<td>Caused if the user types a user ID in to the SSO web page that is different from their Webex Teams user ID. Users can click Renew in phone services and then enter the correct ID.</td>
</tr>
</tbody>
</table>
### Error Code | Name | Explanation and Possible Fix
---|---|---
1000:605 | SSOWhoAmIFailure | Cannot identify the user that signed in using the browser. This requires logs to analyze. (Users can submit logs and create a ticket using Webex Teams under Help > Send Feedback.)
1000:606 | SSOSessionExpired | Users can click Renew in phone services.
1000:608 | InvalidBrowserResponse | Users can click Renew in phone services. They may need to try again later if it's a network or server side issue.
1000:1001 | ServiceDiscoveryFailure | Unexpected internal error. This requires logs for further analysis. (Users can submit logs and create a ticket using Webex Teams under Help > Send Feedback.)
1000:1002 | ServiceDiscoveryAuthenticationFailure | Failed to sign in to Unified CM. Double-check the user credentials.
1000:1003 | ServiceDiscoveryCUCMCannotConnect | Failed to connect to Unified CM. This may be a network issue or users may need your help to input the UC domain or the server. This needs logs for further analysis. (Users can submit logs and create a ticket using Webex Teams under Help > Send Feedback.)
1000:1004 | ServiceDiscoveryNoCUCMConfiguration | Unable to detect the on-premises calling server addresses. This can be solved by the user entering the UC domain or the server or by you setting the proper SRV records. This needs logs for further analysis.
1000:1005 | ServiceDiscoveryNoSRVRecords | Unable to find the on-premises calling server addresses on the DNS. This can be solved the user entering the UC domain or the server or by you setting the proper SRV records. This needs logs for further analysis. (Users can submit logs and create a ticket using Webex Teams under Help > Send Feedback.)
1000:1006 | ServiceDiscoveryCUCMFailed | Unable to connect or to authenticate for Mobile Remote Access (MRA). Verify user credentials, the MRA SRV record, and the MRA server status.
1000:1007 | ServiceDiscoveryNoNetworkConnectivity | We couldn't find cached information about the on-premises calling server and the user has no network. Check the network connectivity.
1000:1008 | ServiceDiscoveryUntrustedCertificate | Either the MRA server or one of the on-premises services provided an invalid certificate. Verify that the certificates installed on the servers are valid.
1000:1010 | ServiceDiscoveryNoUserLookup | Unexpected condition. Requires logs to for further analysis. (Users can submit logs and create a ticket using Webex Teams under Help > Send Feedback.)
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Name</th>
<th>Explanation and Possible Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000:1100</td>
<td>ConnectionFailedByMRAPolicy</td>
<td>The MRA server refused to provide an access token and returned a 403 error. Check the configuration on the MRA Expressways and the Unified CM.</td>
</tr>
</tbody>
</table>
Appendix

- Quality of Service, on page 51
- Allow Untrusted Certificates on Unified CM, on page 54

Quality of Service

Quality of Service Options

Use the following options to configure the quality of service for Webex Teams:

- Supported Codecs, on page 51
- Define a Port Range on the SIP Profile, on page 52
- Set DSCP Values, on page 52

Supported Codecs

<table>
<thead>
<tr>
<th>Type</th>
<th>Codec</th>
<th>Codec Type</th>
<th>Webex Teams for Mac</th>
<th>Webex Teams for Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>G.711</td>
<td>A-law</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>µ-law/Mu-law</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>G.722</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>G.722.1</td>
<td></td>
<td>24 kb/s and 32 kb/s</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>G.729</td>
<td></td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>G.729a</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Opus</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Define a Port Range on the SIP Profile

The client uses the port range to send RTP traffic across the network. The client divides the port range equally and uses the lower half for audio calls and the upper half for video calls. As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

### Step 1
Open the Cisco Unified CM Administration interface.

### Step 2
Select Device > Device Settings > SIP Profile.

### Step 3
Find the appropriate SIP profile or create a new SIP profile. The SIP Profile Configuration window opens.

### Step 4
Specify whether you want common or separate port ranges for audio and video. If you are separating your audio and video port ranges, provide audio and video ports. Specify the port range in the following fields:

- **Start Media Port** — Defines the start port for media streams. This field sets the lowest port in the range.
- **Stop Media Port** — Defines the stop port for media streams. This field sets the highest port in the range.

### Step 5
Select Apply Config and then OK.

### Set DSCP Values

Set Differentiated Services Code Point (DSCP) values in RTP media packet headers to prioritize Webex Teams traffic as it traverses the network.

### Set DSCP Values on Cisco Unified Communications Manager

You can set DSCP values for audio media and video media on Cisco Unified Communications Manager. Webex Teams can then retrieve the DSCP values from the device configuration and apply them directly to the IP headers of RTP media packets.

### Restriction

Operating systems such as Microsoft Windows 7 or 10 have a security feature that prevents applications from setting DSCP values on IP packet headers. For this reason, you should use an alternate method for marking DSCP values, such as Microsoft Group Policy.

### Step 1
Open the Cisco Unified CM Administration interface.
Set DSCP Values With Group Policy

If you deploy Webex Teams for Windows on an operating system such as Microsoft Windows 7 or later, you can use Microsoft Group Policy to apply DSCP values.

Complete the steps in the following Microsoft support article to create a group policy:

You should create separate policies for audio media and video media with the following attributes:

These directions apply to Unified CM calls that go through Webex Teams. For Webex Teams only calls, use the guidelines in Network Requirements for Webex Teams.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Audio Policy</th>
<th>Video Policy</th>
<th>Signaling Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>CiscoCollabHost.exe</td>
<td>CiscoCollabHost.exe</td>
<td>CiscoCollabHost.exe</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
<td>UDP</td>
<td>TCP</td>
</tr>
<tr>
<td>Port number or range</td>
<td>Corresponding port</td>
<td>Corresponding port</td>
<td>5060 for SIP</td>
</tr>
<tr>
<td></td>
<td>number or range from the SIP</td>
<td>number or range from the SIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>profile on Cisco</td>
<td>profile on Cisco</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unified Communications</td>
<td>Unified Communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manager.</td>
<td>Manager.</td>
<td></td>
</tr>
<tr>
<td>DSCP value</td>
<td>46</td>
<td>34</td>
<td>24</td>
</tr>
</tbody>
</table>

Set DSCP Values on the Network

You can configure switches and routers to mark DSCP values in the IP headers of RTP media.

To set DSCP values on the network, you must identify the different streams from the client application.

- Media Streams — Because the client uses different port ranges for audio streams and video streams, you can differentiate audio media and video media based on those port range. Using the default port ranges in the SIP profile, you should mark media packets as follows:
  - Audio media streams in ports from 16384 to 24575 as EF
  - Video media streams in ports from 24576 to 32767 as AF41

- Signaling Streams — You can identify signaling between the client and servers based on the various ports required for SIP, CTI QBE, and XMPP. For example, SIP signaling between Webex Teams and Cisco Unified Communications Manager occurs through port 5060.
You should mark signaling packets as CS3.

- For port ranges for Webex Teams only calls, use the guidelines in Network Requirements for Webex Teams.

Allow Untrusted Certificates on Unified CM

If needed, you can use Control Hub to allow untrusted certificates from your Unified CM. They may be untrusted because they're self-signed or if the certificate doesn't match the address that is being used for the connection.

⚠️ Caution

This setting downgrades your deployment's security. We strongly advise that you use a more secure method for certificate trust. Use this method as a last resort for limited deployments, such as those in a lab testing environment.

Before you begin

Before you use this option, understand certificate requirements and best practices Certificate Requirements for Calling in Webex Teams (Unified CM), on page 17.

Step 1

From the customer view in https://admin.webex.com, go to Services, and then choose Client Settings from the calling card.

Step 2

In Unified CM Settings, toggle on Allow Unified CM registration without trusted certificate.

After this toggle is enabled, Webex Teams apps register to the premises, regardless of what type of certificate is being used.