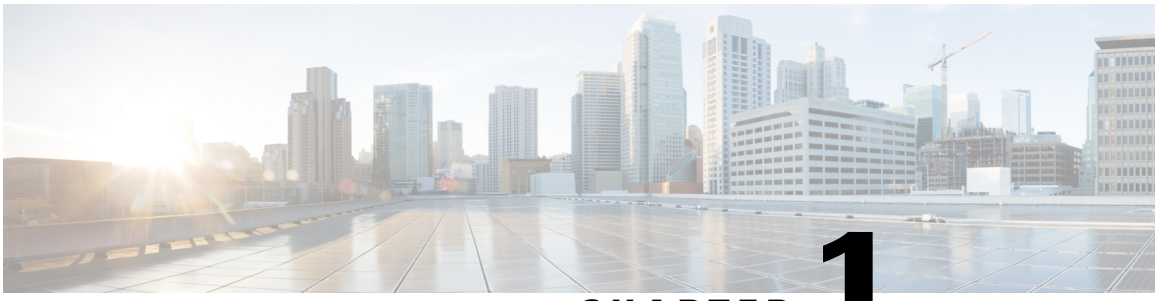
Cisco WebEx Meeting Center Video Conferencing Enterprise Deployment Guide (WBS30)

First Published: 2015-09-23

Last Modified: 2016-10-25

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

CONTENTS



CHAPTER 1

Deployment Options

About Cisco WebEx Meeting Center Video Conferencing

Participants can join a video meeting from the WebEx web application, from a phone, or from a video device. Video devices negotiate all media (main video, content, and audio) to and from the WebEx cloud. This media flows over IP negotiated by using SIP or H.323 (SIP is recommended). Cisco TelePresence infrastructure may be used for call control and firewall traversal, but is not required.

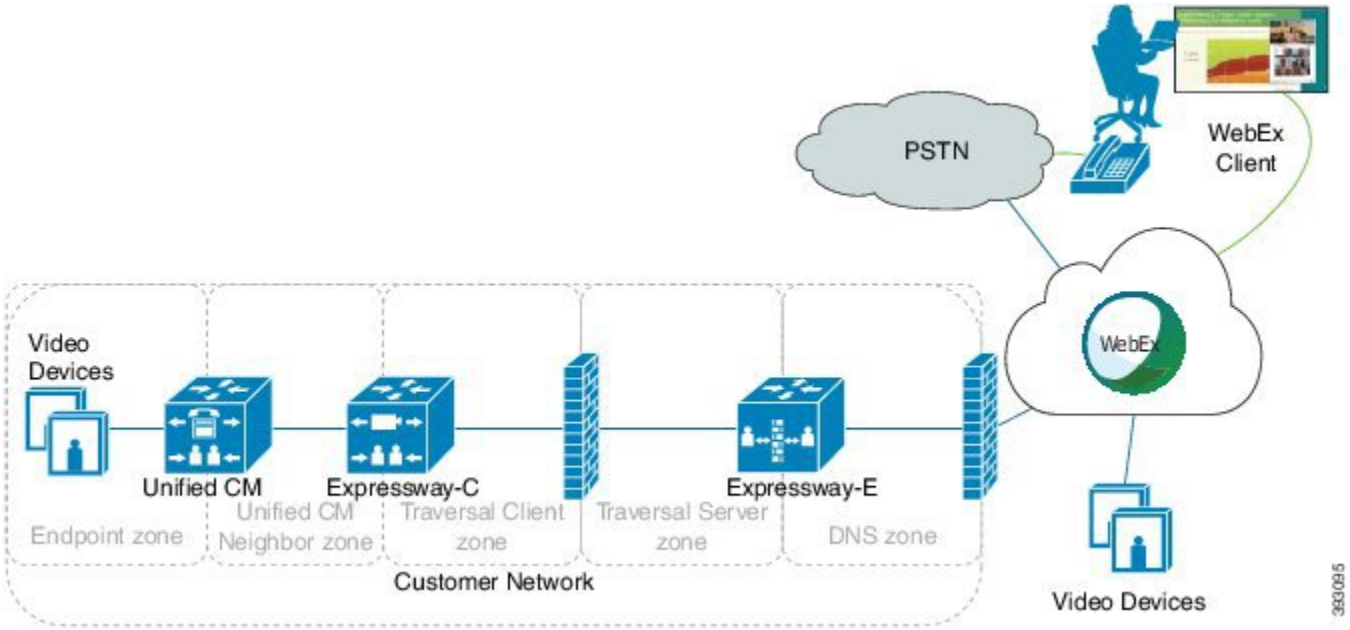
WebEx offers multiple audio solution options for WebEx application users and phone participants. For Meeting Center with video, available options are WebEx Audio (including Cloud Connected Audio) and Teleconferencing Service Provider (TSP) audio that has been verified compatible with CMR Hybrid/video conferencing.

Contact your Cisco Account Manager for more information about WebEx Audio, and to obtain the latest list of verified TSP Audio Provider partners.

Example: SIP Site with Cisco Infrastructure

In this example, the enterprise video devices are registered to Unified Communications Manager, with Cisco Expressway-C and Cisco Expressway-E being used for secure calling and firewall traversal.

Figure 1: SIP Site Using Unified Communications Manager



Other deployments are also possible with Cisco TelePresence infrastructure, including:

- Cisco VCS Control and Cisco VCS Expressway

  Video devices are registered to Cisco VCS Control rather than to Unified Communications Manager.

- Cisco VCS Control and Cisco VCS Expressway with Unified Communications Manager

  Video are registered to Cisco VCS Control and Unified Communications Manager (a combination of the above two models).

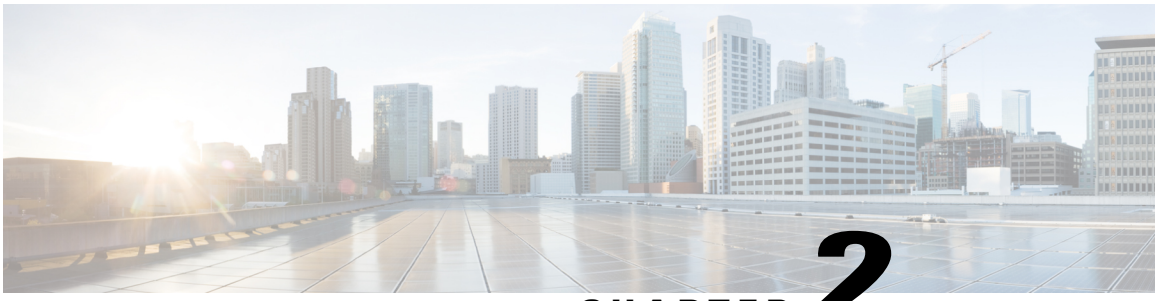
Security Options

For SIP calls, Cisco WebEx Meeting Center Video Conferencing supports any combination of certificate type, signaling, and media in the following table:

Certificates	Signaling	Media
• CA-signed certificates • Self-signed certificates	• TLS • TCP	• sRTP • RTP

By default, the Cisco Expressway (or Cisco VCS) uses self-signed certificates. For each SIP call, it attempts TLS signaling with fallback to TCP, and sRTP with fallback to RTP.

For H.323 calls, video conferencing supports non-secure H.225/H.245 signaling and H.235 media encryption methods.



CHAPTER 2

Requirements and Recommendations

System Requirements

Table 1: Requirements for Cisco WebEx Meeting Center Video Conferencing Deployments

Requirement	Description
Cisco WebEx Meeting Center	The Cisco WebEx Meeting Center site must be running release WBS29 or higher.
Audio	WebEx offers multiple audio solution options for WebEx application users and phone participants. For video conferencing, available options are WebEx Audio (including Cloud Connected Audio) and Teleconferencing Service Provider (TSP) audio that has been verified compatible with CMR Hybrid/video conferencing. Contact your Cisco Account Manager for more information about WebEx Audio, and to obtain the latest list of verified TSP Audio Provider partners.

Requirement	Description
Network access	Make sure that the port range for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls allows the following: • inbound media traffic from the WebEx cloud over UDP for the RTP port range 36000 – 59999 • inbound SIP signaling traffic from the WebEx cloud over TCP for ports 5060, 5061 and 5065 • inbound H.323 signaling traffic from the WebEx cloud over TCP port 1720 and port range 15000-19999 • outbound media traffic to the WebEx cloud over UDP for the RTP port range 36000 – 59999 • outbound SIP signaling traffic to the WebEx cloud over TCP for the ports 5060 – 5070 • outbound H.323 signaling traffic to the WebEx cloud over TCP port 1720 and port range 15000-19999 For the IP address ranges used by the WebEx cloud, by geographic location, see https://kb.webex.com/WBX264
Network bandwidth	The amount of network bandwidth required depends on the requirements of each video device to provide the desired video quality plus presentation data. We recommend at least 1.5 Mbps per screen for an optimal experience. Some video devices can take advantage of higher rates, and the service can accommodate lower rates, depending on the device.
Quality of service	The egress gateway must support the following DSCP markings: • Video traffic marked with DSCP AF41 as per RFC 2597 • Audio traffic marked with DSCP EF as per RFC 3246

Network Infrastructure

You can use any standards-based call control system for your video devices. Your deployment may also include a firewall traversal device to provide mobile and remote access.

The following table lists recommended versions of Cisco products that can provide these functions. These components are not required.

Table 2: Recommended Network Infrastructure for Cisco WebEx Meeting Center Video Conferencing Deployments

Component	Recommended Options from Cisco
Call control, device registration	• Cisco Unified Communications Manager (tested releases: 10.5, 9.1(2), and 9.1(1) • Cisco VCS Control and Cisco VCS Expressway (tested releases: X8.6)
Firewall traversal, mobile and remote access	• Cisco Expressway-C and Cisco Expressway-E (tested releases: X8.6) • Cisco VCS Control and Cisco VCS Expressway (tested release: X8.6) **Note** The minimum required version is X8.6.0 and the minimum recommended version is X8.6.1 (for free traversal/RMS calls to WebEx with full URI dialing). We also recommend reducing the default SIP TCP timeout according to the deployment tasks for video conferencing. With versions prior to X8.6, callers can experience significant delays if the primary WebEx call destination is unavailable. This happens because Cisco Expressway/Cisco VCS attempts to connect to each primary destination in the DNS SRV record in turn before it tries any backup destination, and in these versions, it applies a ten second SIP TCP timeout to every connection attempt.

Video Devices

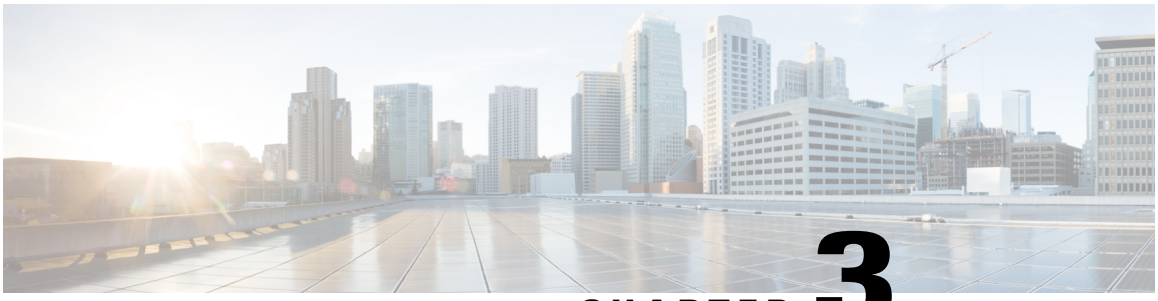
The following table lists general requirements and considerations for each type of device.

Table 3: Video Device Requirements for Cisco WebEx Meeting Center with Video Deployments

Type of Device/Client	Requirements
SIP	• In order for the participant to present or view shared content, the device must be able to negotiate Binary Floor Control Protocol (BFCP) with the cloud servers. Without BFCP, content cannot be shared and will be seen embedded in the main video channel. • In order for a device with three or more screens to display video on more than one screen, the device must be able to negotiate the TelePresence Interoperability Protocol (TIP) with the WebEx cloud servers. **Note** Cisco WebEx Meeting Center Video Conferencing does not support SIP endpoints that are configured in standalone mode.
H.323	• H.323 devices must use URI dialing (Annex O) to call in to the WebEx cloud. See your vendor-provided documentation for instructions on setting up URI dialing. • In order for the participant to present or view shared content, the device must be able to negotiate H.239 with the cloud servers. Without H.239, content cannot be shared and will be seen embedded in the video. • Multi-screen endpoints are not supported.

H.323 Mode

Cisco WebEx Meeting Center Video Conferencing supports H.323. However, SIP has a richer feature set, support for secure signaling, and greater cloud capacity. We recommend turning off H.323 mode on the Cisco Expressway (or Cisco VCS). With H.323 mode off, Cisco Expressway interworks an H.323 endpoint's traffic into SIP and then sends a SIP invite to the WebEx cloud.



CHAPTER 3

Deployment Tasks

Deployment Task Flow

Before You Begin

When your Cisco WebEx Meeting Center Video Conferencing order is complete, you will receive information regarding your Cisco WebEx site access details (URLs and Site Administration account).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Open the Port Range for the WebEx Cloud, on page 10	Set the port range for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls.
Step 2	Configure DNS Zone and Search Rule, on page 11	Configure the DNS zone and search rule if you want to ensure that TLS and sRTP are used in fallback scenarios (recommended).
Step 3	Configure a Traversal Server/Client Pair, on page 13	For secure calling, configure a Traversal Client zone and search rule on Cisco Expressway-C (or Cisco VCS Control) and a Traversal Server zone on Cisco Expressway-E (or Cisco VCS Expressway).
Step 4	Route Video Call-Back Traffic, on page 14	For video call-back, configure search rules on Cisco Expressway-C and Cisco Expressway-E (or Cisco VCS Control and Cisco VCS Expressway) to route WebEx dial-outs to users' video devices.
Step 5	Reduce the Default SIP TCP Timeout on the Cisco Expressway-E, on page 16	Configure the SIP TCP timeout value on Cisco Expressway / Cisco VCS (X8.6) to the lowest value that is appropriate for your deployment.
Step 6	Enable BFCP for Presentation Sharing, on page 16	Verify that BFCP is enabled on the Unified Communications Manager neighbor zone in Cisco Expressway-C or Cisco VCS Control, and on the SIP profile in Unified Communications Manager.
Step 7	Configure a SIP Trunk, on page 17	Configure the SIP profile and trunk to Cisco Expressway-C (or Cisco VCS Control) on Unified Communications Manager in order for endpoints

	Command or Action	Purpose
		registered to Unified Communications Manager to participate in a video meeting and to call endpoints registered to a Cisco VCS Control.
Step 8	Add a Route Pattern, on page 18	Add a SIP route pattern in Unified Communications Manager for the webex.com domain.
Step 9	Configure Bandwidth Controls, on page 18	Configure your minimum desired bandwidth in Unified Communications Manager, and in Cisco Expressway or Cisco VCS.
Step 10	Simplify the Video Dial String, on page 19	Use pattern replacement to simplify the dial string for SIP and H.323 video devices within your enterprise.
Step 11	Configure Site Administration Settings, on page 20	Configure WebEx site-wide and per-user settings for Meeting Center with Video.
Step 12	Deploy with CA-Signed Certificates, on page 20	Complete the tasks in this section if you want to use CA-signed certificates to enable secure calling to the WebEx cloud. These tasks require the Cisco Expressway Series (Cisco Expressway-C and Cisco Expressway-E) or Cisco VCS (Cisco VCS Control and Cisco VCS Expressway). To accomplish similar tasks on other vendors' equipment, refer to the vendor documentation.
Step 13	Verify the Service, on page 23	Test to ensure that your deployment of the Cisco WebEx Meeting Center Video Conferencing service works correctly.

Open the Port Range for the WebEx Cloud

This procedure specifies the port ranges that you must configure for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls. For detailed instructions, see Cisco Expressway Administrator Guide and Cisco VCS Administrator Guide.

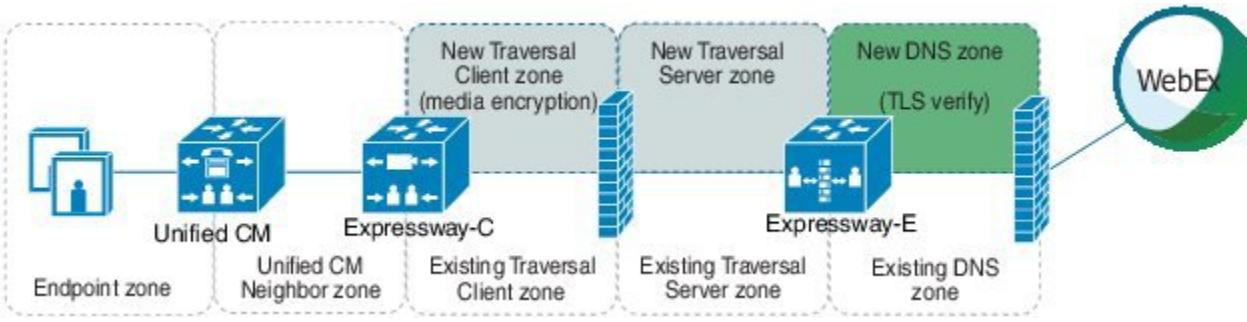
Use the management interface for your device to configure the following port ranges:

- inbound media traffic from the WebEx cloud over UDP for the RTP port range 36000 – 59999
- inbound SIP signaling traffic from the WebEx cloud over TCP for ports 5060 and 5061
- inbound H.323 signaling traffic from the WebEx cloud over TCP port 1720 and port range 15000-19999
- outbound media traffic to the WebEx cloud over UDP for the RTP port range 36000 – 59999
- outbound SIP signaling traffic to the WebEx cloud over TCP for the ports 5060 – 5070
- outbound H.323 signaling traffic to the WebEx cloud over TCP port 1720 and port range 15000-19999

Configure DNS Zone and Search Rule

You can use the default DNS zone configuration on the Cisco Expressway-E (or Cisco VCS Expressway) to route calls to the WebEx cloud. The default configuration will result in Cisco Expressway attempting best-effort TLS (with fallback to TCP) and sRTP media encryption (with fallback to RTP). However, we recommend the following zone configuration, especially if you want to ensure that TLS and sRTP are used.

Figure 2: Recommended DNS Zone Configuration for Encryption



Before You Begin

We recommend turning off H.323 mode in this procedure. This forces Cisco Expressway to interwork an H.323 endpoint's traffic into SIP and then send a SIP invite to the WebEx cloud.

Step 1 Use the following table to configure the DNS zone on Cisco Expressway-E. The configuration varies depending on the type of certificate in use, and whether you turn on H.323 mode.

Zone Configuration Setting	Value if Using 3rd-Party CA Signed Certificate	Value if Using Self-Signed Certificate
H.323 Mode	**On** (default) or **Off** (recommended)	**On** (default) or **Off** (recommended)
SIP Media encryption mode	**Auto** (default)	**Auto** (default)
TLS Verify mode	**On**	**Off**
TLS verify subject name field	sip.webex.com For secure calls to Cisco's BTS test site, such as for an EFT or for go.webex.com, create an additional DNS egress zone with TLS verify subject name sipbts.webex.com.	Not Applicable
Advanced zone profile	**Default** or **Custom** (required if **H.323 Mode** is set to **Off**)	**Default** or **Custom** (required if **H.323 Mode** is set to **Off**)

Zone Configuration Setting	Value if Using 3rd-Party CA Signed Certificate	Value if Using Self-Signed Certificate
Automatically respond to SIP searches	**Off** (default) or **On** (required if **H.323 Mode** is set to **Off**)	**Off** (default) or **On** (required if **H.323 Mode** is set to **Off)**
SIP SDP attribute line limit mode	**Off** (required if **Advanced zone profile** is set to **Custom**)	**Off** (required if **Advanced zone profile** is set to **Custom**)

Step 2 Create a search rule for the WebEx domain on the Cisco Expressway-E, with the following properties:

Search Rule Setting	Value on Expressway-E
Priority	Use a lower numeric value than the search rule for any existing DNS zones.
Protocol	**Any**
Source	<Admin Defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	(.*)@(.*)(\.webex\.com).*
Pattern Behavior	**Replace**
Replace String	\1@\2\3
On Successful Match	**Stop**
Target	<DNS zone used to route calls to the WebEx cloud>
State	**Enabled**

For detailed instructions, see the "Routing configuration" chapter of the applicable administration guide:

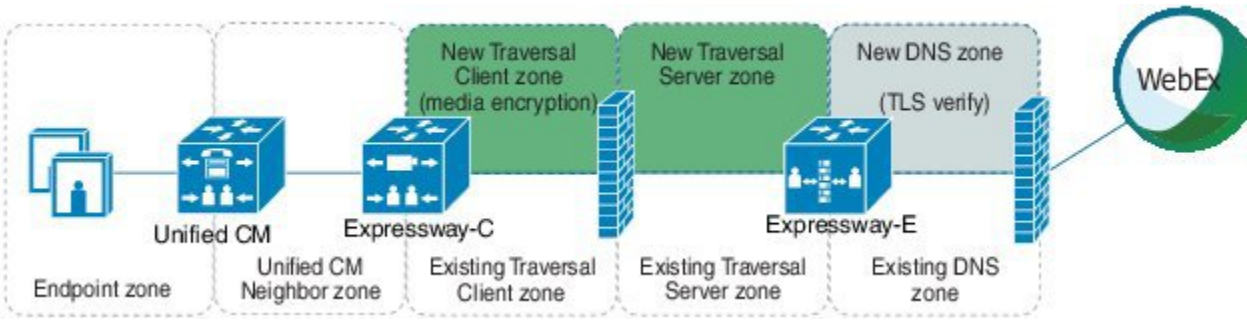
- Cisco Expressway Basic Configuration Deployment Guide
- Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide

Configure a Traversal Server/Client Pair

You can skip this task if you are happy with Cisco Expressway attempting best-effort TLS (with fallback to TCP) and sRTP media encryption (with fallback to RTP). In that case, the DNS zone configuration from the previous task is sufficient.

The recommended zone configuration for secure calling uses a Traversal Client zone on Cisco Expressway-C (or Cisco VCS Control) and a Traversal Server zone and DNS zone on Cisco Expressway-E (or Cisco VCS Expressway). If you already have one or more Traversal Client/Traversal Server zone pairs in your configuration, you can use these zones, but we recommend adding a new pair specifically for the WebEx cloud.

Figure 3: Recommended Traversal Zone Pair Configuration for Encryption



In this procedure:

- On the Cisco Expressway-C, you apply the media encryption policy on the Traversal Client zone, and create a search rule that routes outbound WebEx domain calls towards that zone.
- On the Cisco Expressway-E, you configure the TLS Verify mode on the DNS zone. (The search rule that routes outbound WebEx domain calls towards that zone was configured in the previous task.)

We recommend this configuration for two reasons:

- To avoid unnecessarily engaging the B2BUA on the Cisco Expressway-E.
- To encrypt all traffic that egresses the firewall so that someone who may have access to your DMZ cannot sniff your traffic.

Step 1 Use the following table to configure the Traversal Client and Traversal Server zones:

Zone Configuration Setting	Value On Traversal Client Zone (Cisco Expressway-C)	Value on Traversal Server Zone (Cisco Expressway-E)
H.323 Mode	**Off** (recommended) or **On** (default)	**Off** (recommended) or **On** (default)
SIP Media encryption mode	**Force Encrypted** or **Best Effort** (required if **H.323 Mode** is set to **On**)	**Auto**

Step 2 Create a search rule on Cisco Expressway-C with the following properties:

Search Rule Setting	Value on Expressway-C
Priority	Use a lower numeric value than any search rule that would match the webex.com domain (such as a default domain pattern string).
Protocol	**Any**
Source	<Admin defined>, default: **Any**
Mode	**Alias Pattern Match**
Pattern Type	**Regex**
Pattern String	(.*)@(.*)(\.webex\.com).*
Pattern Behavior	Replace
Replace String	\1@\2\3
On Successful Match	**Stop**
Target	< Traversal Client zone>
State	**Enabled**

For additional information on zones and search rules, see the "Routing configuration" chapter of the applicable administration guide:

- Cisco Expressway Basic Configuration Deployment Guide
- Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide

Route Video Call-Back Traffic

WebEx users can choose video call-back for an easier join experience, where the cloud calls the user's video directly. If you enable this for users, create search rules on the Expressway-E and Expressway-C to route these calls toward the users' home Cisco Unified Communications Manager cluster.

Step 1 Go to **Configuration** > **Dial Plan** > **Search rules** and click **New**.
Create a rule on both systems. The method is the same but the rule values are different.

Step 2 Configure the search rules as follows:

	Cisco Expressway-C	Cisco Expressway-E
Rule name	"SIP callback from WebEx toward internal call control" for example	"SIP callback from WebEx toward Expressway-C" for example
Description	"Routes calls from traversal zone toward user home cluster" for example	"Matches WebEx originated URIs, strips unnecessary parameters, and routes to traversal zone" for example
Priority	100	100
Protocol	SIP	SIP
Source	Named	Named
Source name	Traversal client zone <Admin defined name>	Default zone (This is where all calls come in from outside the organization's network)
Request must be authenticated	No	No
Mode	Alias pattern match	Alias pattern match
Pattern type	Regex	Regex
Pattern string	.*@example\.com	(.*)@(example\.com);transport=[tlscp]{3}.* **Warning!** This pattern will match any string. Create a more specific string for your usernames and DNs, and your domains to prevent fraudulent calls. For example, if your DNs are all eight digits and start with the number 8, and your domain is contoso.com: ((8\d{7})|([A-Za-z]+))@(contoso\.com);transport=[tlscp]{3}.*
Pattern behavior	Leave	Replace
Replace string	N/A	\1@\2 Only keeps the username@FQDN portion, stripping off the transport and any other attributes or trailing characters.
On successful match	Stop	Stop

	Cisco Expressway-C	Cisco Expressway-E
Target	<Admin defined>, select neighbor zone toward Cisco Unified Communications Manager	Traversal server zone, <Admin defined name>
State	Enabled	Enabled

Step 3 Click **Create search rule**.

Reduce the Default SIP TCP Timeout on the Cisco Expressway-E

From Cisco Expressway / Cisco VCS Version X8.6 the SIP TCP timeout value is configurable. The default value is 10 seconds. We strongly recommend that you set the timeout to the lowest value that is appropriate for your deployment. A value of 1 second is likely to be suitable in most cases, unless your network has extreme amounts of latency (such as video over satellite communications).

To set the SIP TCP timeout value:

Step 1 Access the command line interface (this setting cannot be configured through the web interface).

Step 2 Type the following command, replacing "n" with the required timeout value:
xConfiguration SIP Advanced SipTcpConnectTimeout: *n*

Example: xConfiguration SIP Advanced SipTcpConnectTimeout: 1

Reducing the timeout is optional, but may improve performance in the event that the Cisco Expressway-E (or Cisco VCS Expressway) times out attempting to reach the primary WebEx data center.

Enable BFCP for Presentation Sharing

This procedure specifies the BFCP settings that you must configure in the neighbor zone or SIP profile to enable presentation sharing. For detailed information about configuring zone profiles and SIP profiles, see the following documents:

- *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* for your version of Cisco Expressway, at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.
- *Cisco VCS and CUCM Deployment Guide* for your version of Cisco VCS, at http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html.

Note BFCP support was introduced in Cisco Unified Communications Manager version 8.6(1). We strongly recommend that you use a version no earlier than 8.6(2a)SU3 for BFCP interoperability.

Step 1 Verify that BFCP is enabled on the Unified Communications Manager neighbor zone in Cisco Expressway-C or Cisco VCS Control:

- If you are using X8.1 or later, BFCP is automatically enabled when you choose the Cisco Unified Communications Manager (8.6.1 or later) zone profile on the Unified Communications Manager neighbor zone.
- If you are using a release prior to X8.1, set **SIP UDP/BFCP filter mode** to **Off** on the zone profile in Cisco VCS Control.

Step 2 Verify that BFCP is enabled on the SIP profile in Unified Communications Manager:

- If you are using X8.1 or later, BFCP is automatically enabled if you choose the **Standard SIP Profile for Cisco VCS** when defining the SIP trunk to the Cisco Expressway-C or Cisco VCS Control.
- If you are using a release prior to X8.1, check the **Allow Presentation Sharing using BFCP** box on the SIP profile.

Configure a SIP Trunk

Configure the SIP profile and trunk to Cisco Expressway-C (or Cisco VCS Control) on Unified Communications Manager in order for endpoints registered to Unified Communications Manager to participate in a video meeting and to call endpoints registered to a Cisco VCS Control.

This procedure provides high-level steps. For detailed instructions, see the following documents:

- *Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide* for your version of Cisco Expressway, at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.
- *Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide* for your version of http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html.

Step 1 In Unified Communications Manager, configure a SIP trunk between Unified Communications Manager and Cisco Expressway-C (or Cisco VCS Control).

Step 2 Configure the SIP profile.

Step 3 To enable presentation sharing, check the **Allow Presentation Sharing using BFCP** check box in the **Trunk Specific Configuration** section of the **SIP Profile Configuration** window.
For third-party video devices that support BFCP, you may also need to check the **Allow Presentation Sharing using BFCP** check box in the **Protocol Specific Information** section of the **Phone Configuration** window.

Add a Route Pattern

Add a route pattern for the WebEx domain in Unified Communications Manager.

On the Unified Communications Manager, add a route pattern for *.webex.com (or *.*) and point it at the SIP trunk to Cisco Expressway-C (or Cisco VCS Control) .
For detailed instructions, see the applicable guide for your release:

- Unified Communications Manager release 11.0(1) and later: System Configuration Guide
- Earlier releases: Administration Guide

Configure Bandwidth Controls

Configure your minimum desired bandwidth in Unified Communications Manager, and in Cisco Expressway or Cisco VCS.

Step 1 In Unified Communications Manager, set the region to permit the minimum desired bandwidth, to ensure optimum SIP audio and video connectivity between and the WebEx cloud.
For detailed instructions, see "Regions" in the applicable guide for your release:

- Unified Communications Manager release 11.0(1) and later: System Configuration Guide
- Earlier releases: Administration Guide

Step 2 In Cisco Expressway or Cisco VCS, set zones and pipes appropriately (according to your network's requirements) to allow the minimum desired bandwidth.
For detailed instructions, see "Bandwidth control" in the applicable administrator guide:

- Cisco Expressway Administrator Guide
- Cisco VCS Administrator Guide

Simplify the Video Dial String

To join a scheduled video meeting, telepresence users typically must dial a string consisting of the nine-digit meeting number followed by the @ symbol and the WebEx site domain -- for example, 123456789@customer-a.webex.com.

You can simplify this string for SIP and H.323 video devices within your enterprise by using pattern replacement. In this example, you add a short prefix that replaces the need for users to include the domain when dialing. In the example deployment, where enterprise video devices are registered to Unified Communications Manager and the Cisco Expressway Series (or Cisco VCS) is used for remote devices and firewall traversal, the simplified dial string is routed and converted into the full video dial string by a Unified Communications Manager route pattern and a Cisco Expressway transform.

Note Calls dialed without the WebEx site domain consume RMS licenses on the Cisco Expressway. To take advantage of RMS license bypass in X8.6 and later, users must dial the full URI.
SIP calls made to WebEx meetings on VCS or Expressway software versions X8.9 and later can take advantage of Cloud Licensing for both full dial strings, and simplified dial strings. However, versions X8.6.1 through X8.8.3 (inclusive) consume at least one traversal or RMS license per simplified call, depending on your specific software version. For these versions, the dialed address must not have any Transforms applied, and must match the pattern (.*)@(.*)\.webex\.com to trigger Cloud Licensing for the call.

To set up simplified dialing, do the following:

Step 1 Select a prefix beginning with a digit that is not frequently used in your dial plan. This can include * or #.

Step 2 On Unified Communications Manager, create a route pattern starting with the prefix, followed by a dot (period) character, and nine X characters representing the meeting number digits.
For example, for a prefix of 7 use 7.XXXXXXXXX

Step 3 Configure the route pattern to direct the call to the Cisco Expressway.

Step 4 On the Cisco Expressway, create a transform that matches any dial string starting with 7 followed by 9 digits.
For example, for a prefix of 7 use a regex pattern string of 7(\d{9})

Step 5 Configure the transform to strip the prefix digit (7 in this example) and append the domain (@customer-a.webex.com), so that the call is routed to the appropriate WebEx site.
For example, with the regex pattern above, use a replace string of \1@customer-a.webex.com.

In this example, when a user dials 7123456789, the call is ultimately routed as 123456789@customer-a.webex.com. The substitution happens both for devices that are registered to Unified Communications Manager and for remote devices that are registered to a Cisco VCS Expressway.

This simplification only applies to devices within your enterprise, joining meetings hosted by your own enterprise. Users who dial meetings hosted by other enterprises and external video participants must dial the full video dial string, including the domain.

Configure Site Administration Settings

You have access to Cisco WebEx Site Administration through your WebEx Account Team using a unique WebEx Site Administration URL and password. As a site administrator, you must log in to integrate and provision your account during first-time setup. After you have completed the first-time setup, you can manage your account and access WebEx user and administration guides for the services and features that have been configured on your site.

For more information on configuring your site administration settings, see https://help.webex.com/community/webex-admin/content?filterID=contentstatus[published]~category[cmr-cloud].

Deploy with CA-Signed Certificates

Before You Begin

Make sure you submit your certificate signing request to a public certificate authority that issues a certificate that WebEx supports.

WebEx supports certificates that are issued by specific Root Certificate Authorities. Certificate providers may have multiple Root Certificate Authorities and not all may be supported by WebEx. Your certificate must be issued by one of the following Root Certificate Authorities (or one of their Intermediate Certificate Authorities) or the call from your Cisco Expressway-E or Cisco VCS Expressway will not be accepted by WebEx:

- entrust_ev_ca
- digicert_global_root_ca
- verisign_class_2_public_primary_ca_-_g3
- godaddy_class_2_ca_root_certificate
- Go Daddy Root Certification Authority - G2
- verisign_class_3_public_primary_ca_-_g5
- verisign_class_3_public_primary_ca_-_g3
- dst_root_ca_x3
- verisign_class_3_public_primary_ca_-_g2
- equifax_secure_ca
- entrust_2048_ca

Note To use a certificate generated by entrust_2048_ca with Cisco VCS Expressway X7.2 (or a later version upgraded from X7.2), you must replace the Entrust Root CA certificate in the trusted CA list on the Cisco VCS Expressway with the newest version available from Entrust. You can download the newer entrust_2048_ca.cer file from the Root Certificates list on the Entrust web site (https://www.entrust.net/downloads/root_index.cfm).

- verisign_class_1_public_primary_ca_-_g3

- ca_cert_signing_authority
- geotrust_global_ca
- GlobalSign Root R1

Note Contact GlobalSign to rekey the certificate to R1 if they assign you any other value.

- thawte_primary_root_ca
- geotrust_primary_ca
- addtrust_external_ca_root

This list may change over time. For the most current information, contact WebEx or review the information at the following link: https://kb.webex.com/WBX83490.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Generate Certificate Signing Request , on page 21	Use the Cisco Expressway-E (or Cisco VCS Expressway) to generate a Certificate Signing Request (CSR).
Step 2	Install the Signed SSL Server Certificate , on page 22	Load the SSL certificate on the Cisco Expressway-E (or Cisco VCS Expressway)
Step 3	Configure the Trusted CA list on the Cisco Expressway-E, on page 22	Ensure that the trusted CA list contains the correct certificates.

Generate Certificate Signing Request

For secure calling, use the Cisco Expressway-E (or Cisco VCS Expressway) to generate a Certificate Signing Request (CSR).

This procedure provides high-level steps. For detailed instructions, see the "Generating a certificate signing request" section of the applicable guide:

- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco VCS Certificate Creation and Use Deployment Guide

Step 1 Generate a Certificate Signing Request (CSR).

Step 2 Download the CSR and submit it to your chosen root certificate authority (CA).
Most certificate authorities require the CSR to be provided in a PKCS#10 request format.

Step 3 Make sure that in response, your CA provides you with an SSL server certificate that includes both Server and Client Auth keys.

Install the Signed SSL Server Certificate

This procedure provides high-level information. For detailed instructions, see the see the section whose title begins with "Loading certificates and keys" in the applicable guide:

- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco VCS Certificate Creation and Use Deployment Guide

After you receive the SSL server certificate from your public CA, load it on the Cisco Expressway-E (or Cisco VCS Expressway).

Configure the Trusted CA list on the Cisco Expressway-E

Two types of certificates must be present in the trusted CA list on your Cisco Expressway-E (or Cisco VCS Expressway) to complete the secure calling configuration:

- The root certificate (and intermediate certificate, if applicable) of the public CA that you used to sign your SSL server certificate.
- The certificates of the public CAs used by the WebEx cloud. To obtain these certificates, copy and paste the contents of each of the following links into a separate text file with a .PEM extension:
  - VeriSign Class 3 Public Primary CA
  - VeriSign Class 3 Primary CA - G5
  - VeriSign Class 3 Public Primary CA - G3
  - QuoVadis Root CA 2

  For detailed instructions on configuring the trusted CA list, see the applicable guide:

- Cisco Expressway Certificate Creation and Use Deployment Guide
- Cisco VCS Certificate Creation and Use Deployment Guide

To determine whether the trusted CA list already contains a CA certificate, do the following:

Step 1 In Cisco Expressway-E or Cisco VCS Expressway:

- X8.1 and later, go to **Maintenance** > **Security certificates** > **Trusted CA certificate**.

- X7.2.3, go to **Maintenance** > **Certificate management** > **Trusted CA certificate**.

Step 2 Click **Show CA certificate**.
A new window displays the current Trusted CA list.

Step 3 Search for the name of the CA that issued the certificate, for example, QuoVadis Root CA2.

Verify the Service

Step 1 Create a test host account and enable it for video conferencing (and personal video conferencing, if applicable). If you are using TSP audio, configure the host account with the teleconferencing access parameters for the TSP.

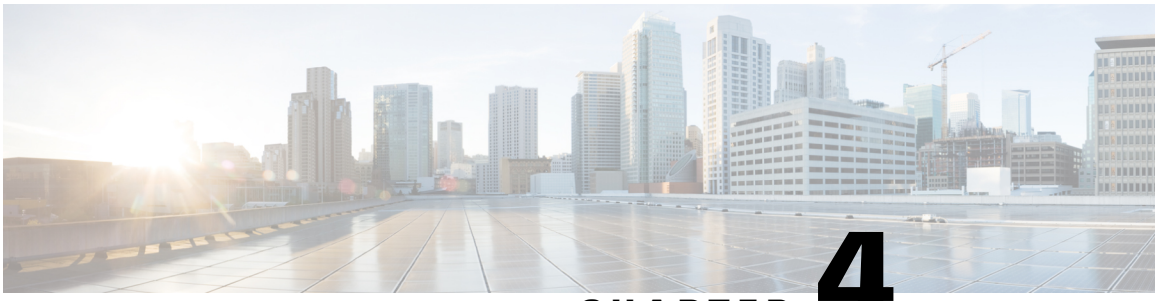
Step 2 Sign in to your WebEx site as the test host, download Productivity Tools, and go through the personal video conferencing set-up (if applicable).

Step 3 Schedule a WebEx meeting by using Productivity Tools and verify the following:

- The meeting appears on the calendar.
- The test host receives the meeting confirmation email from WebEx.

Step 4 Call in to the personal video conferencing (if applicable) or to a scheduled meeting and verify the following:

- There is two-way video between the WebEx Meeting application and telepresence, Jabber, Lync, or other video devices.
- Devices that support presentation sharing can do so.



CHAPTER 4

Video Meetings

Using Both Cisco Collaboration Meeting Rooms Hybrid and Cisco WebEx Meeting Center Video Conferencing Offerings Together

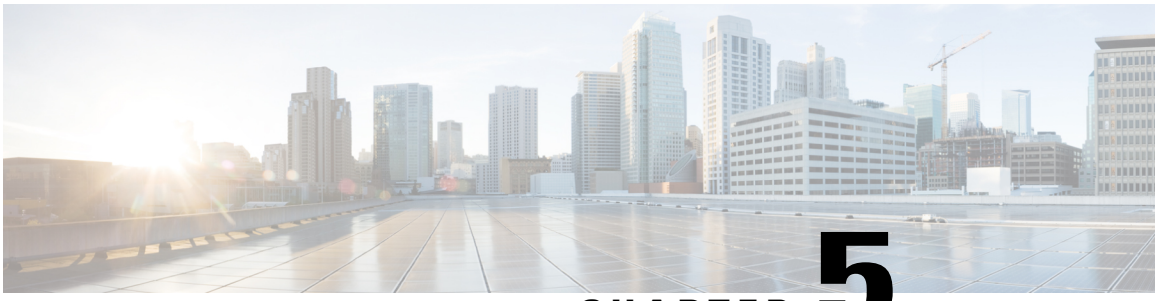
Hosts who have been enabled with both video conferencing and CMR Hybrid can only use Productivity Tools to manage video meetings.

Hosts who need to manage meetings using on-premises resources must use an alternative method, such as the Cisco Smart Scheduler or the Cisco WebEx Scheduling Mailbox.

About TSP Audio

When you use video conferencing in conjunction with teleconferencing service provider (TSP) integrated audio, WebEx establishes a PSTN call to the TSP audio service and uses a "script" of DTMF entries to join the audio conference. The phone number that is dialed, and the parameters necessary for this DTMF script, are obtained from the TSP Audio Account within the WebEx host's account. These parameters are located under **My WebEx** > **My Audio**.

WebEx works with each TSP partner to determine the dial script to use (only WebEx can view or modify the dial script).



CHAPTER 5

Troubleshooting

Troubleshooting Problems with TSP Audio

Table 4: Problems with TSP Audio

Problem or Message	Possible Causes	Recommended Action
TelePresence participants cannot hear WebEx participant audio.	The TSP Audio Account used by the WebEx host account is not valid.	Verify the validity of the Audio Account by starting a WebEx meeting (not a video meeting) using the same host account. Verify that telephony works by using the callback feature. If the callback fails, log into the WebEx site as the same host used to schedule the meeting and edit/verify the validity of the default TSP Audio Account within the host account (My WebEx > My Audio > Edit). You may need to contact your TSP service provider in order to get a valid TSP Audio Account.
	The PSTN/DTMF dial script is not successfully navigating the IVR of the TSP audio conference service.	Contact technical support. Be prepared to provide the details of the TSP Audio Account of the WebEx host account being used for the meeting.

Cascading Windows

A window cascading effect can occur if you plug in the presentation cable (VGA, DVI, HDMI) between your PC and your telepresence video device while you have your Cisco WebEx video view panel open. The WebEx application should detect that you have plugged into a telepresence video device and ask if you are sharing your screen via telepresence. Confirming that you are sharing avoids this cascading problem. To prevent this issue, close the Cisco WebEx video view application before connecting your presentation cable to your laptop to present.

If you receive a cascading screen, simply close the video view window.

Packet Loss on MPLS or Site-to-Site VPN Networks

If you experience packet loss on MPLS or site-to-site VPN networks, make sure not to set MTU and DF-bit within the VCS/Expressway.

Version Compatibility

For all the information on video compatibility and support, see http://cisco.com/go/cmr-cloud-compatibility