Cisco WebEx Meeting Center with Collaboration Meeting Rooms

Enterprise Deployment Guide

November, 2014

Contents

Introduction

This guide helps you set up your video devices and telepresence infrastructure to use Cisco WebEx Meeting Center with Collaboration Meeting Rooms, also known as CMR Cloud.

Deployment Scenarios

Participants can join a CMR Cloud 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 H323 (SIP is recommended). Cisco TelePresence infrastructure may be used for call control and firewall traversal, but is not required.

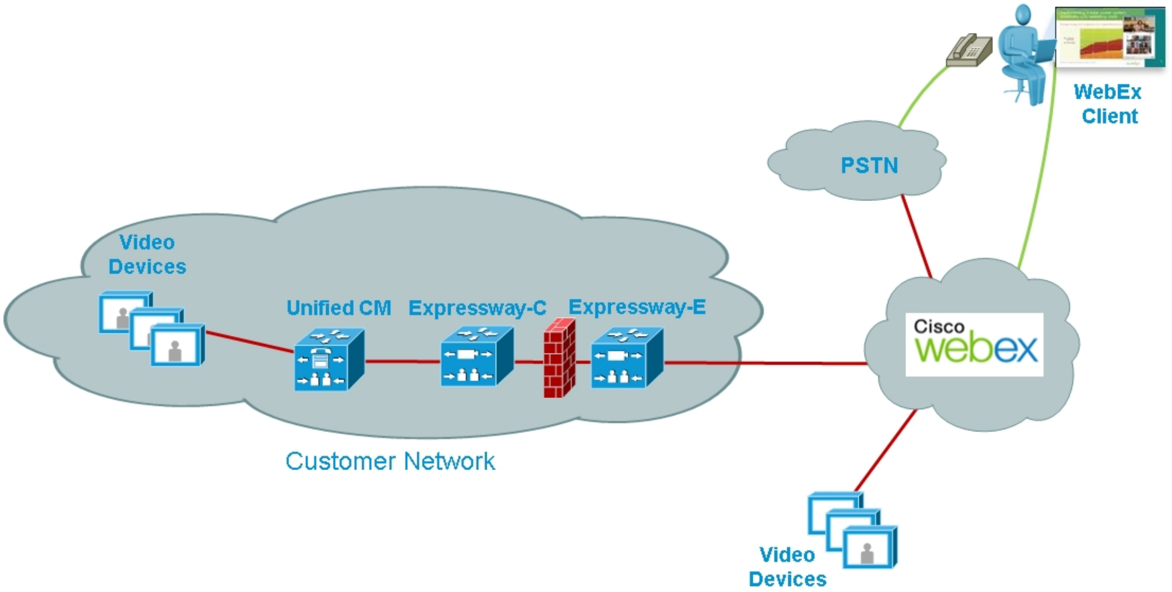
WebEx offers multiple audio solution options for WebEx application users and phone participants. For CMR Cloud, available options are WebEx Audio (including Cloud Connected Audio) and Teleconferencing Service Provider (TSP) audio that has been verified compatible with WebEx Enabled TelePresence/CMR Cloud.

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

In Figure 1: SIP Site Using Cisco Unified Communications Manager [p.4], the enterprise video devices are registered to Cisco Unified Communications Manager, with Cisco Expressway-C and Cisco Expressway-E being used for secure calling and firewall traversal.

Figure 1: SIP Site Using Cisco 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 and/or Cisco VCS Expressway only.
- Cisco VCS Control and Cisco VCS Expressway with Unified CM
  Video are registered to Cisco VCS Control and/or Cisco VCS Expressway and Unified CM (a combination of the above two models).

Prerequisites

Requirements

Table 1: Requirements for CMR Cloud Deployments

Requirement	Description
Cisco WebEx Meeting Center	The Cisco WebEx Meeting Center site must be running release WBS29.
Audio	WebEx offers multiple audio solution options for WebEx application users and phone participants. For CMR Cloud, available options are WebEx Audio (including Cloud Connected Audio) and Teleconferencing Service Provider (TSP) audio that has been verified compatible with WebEx Enabled TelePresence/CMR Cloud. Contact your Cisco Account Manager for more information about WebEx Audio, and to obtain the latest list of verified TSP Audio Provider partners.
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 signaling traffic from the WebEx cloud over TCP for ports 5060 and 5061 ■ outbound media traffic to the WebEx cloud over UDP for the RTP port range 36000 – 59999 ■ outbound signaling traffic to the WebEx cloud over TCP for the ports 5060 – 5070 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 CMR Cloud Deployments

Component	Recommended Options from Cisco
Call control, device registration	■ Cisco Unified Communications Manager (tested releases: 9.1(1), 9.1(2) and 10.5) ■ Cisco VCS Control and Cisco VCS Expressway (tested release X8.1)
Firewall traversal, mobile and remote access	■ Cisco Expressway-C and Cisco Expressway-E (tested release: X8.1) ■ Cisco VCS Control and Cisco VCS Expressway (tested release: X8.1)

Note: In version X8.1/X8.1.1, calls to the WebEx cloud will fail if you configure the Cisco Expressway-E or Cisco VCS Expressway for static NAT and enable media encryption (caveat CSCum90139). To secure calls when using static NAT, we recommend upgrading to X8.2.

Video Devices

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

Table 3: Video Device Requirements for CMR Cloud 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**: CMR Cloud does not support SIP endpoints that are configured in standalone mode.
H.323	■ H.323 devices must use URI dialing (Annex 0) to call in to the WebEx cloud. See your vendor-provided documentation for instructions on setting up URI dialing. ■ To use the IVR to start a meeting as host or join a meeting before the host, H.323 devices must support either H.245 User Input or RFC 2833 methods of DTMF signaling. To start a meeting without this capability, the user must sign in to the WebEx application as host before joining from the H.323 device. ■ 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. ■ H.323 devices with three or more screens are not supported. In order for a device with three or more screens to display video on more than one screen, the device must be configured to negotiate the TelePresence Interoperability Protocol (TIP) with the WebEx cloud servers (and since TIP runs over SIP, this implicitly means it must be reconfigured to use TIP/SIP instead of H.323).

Deployment Tasks

This section takes you through specific tasks in each of the following high-level workflows:

1. Preparation—understanding the service offering and prerequisites, getting ready to order.
2. Set-up—connecting the infrastructure to the WebEx cloud, configuring service settings.
3. Security configuration—configuring call security (requires Cisco Expressway Series or Cisco VCS).
4. Verification and completion—verifying the operation of the service and making it available to users.

Preparation

Task 1: Understanding the Offering

As you begin, review the prerequisites in Prerequisites [p.6].

To understand how users connect to and use the service, see Hosting, Joining and Participating in CMR Cloud Meetings [p.18].

If your site will use telephony service provider (TSP) integrated audio, see About TSP Audio [p.22]

Task 2: Preparing to Order

Prior to ordering CMR Cloud, the Cisco partner or Cisco Account Manager must submit and have an approved Assessment to Quality (A2Q). The A2Q allows Cisco to review the customer environment to ensure a successful deployment.

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

Setup

Task 3: Opening the Port Range for the WebEx Cloud

For instructions, see the "Configuring firewall rules" section of the applicable administration guide:

- Cisco Expressway Administrator Guide
- Cisco VCS Administrator Guide

Task 4: Creating a DNS Zone and Search Rule for the WebEx cloud on the Cisco Expressway-E

You can use the default DNS zone configuration on the Cisco Expressway-E (or Cisco VCS Expressway) to route calls to the WebEx cloud. However, we recommend the following zone settings, especially if you want to enforce encryption. (If you don't want to modify your existing DNS zone settings, you can create a separate DNS zone just for WebEx and set it according to these recommendations.)

	Non Secure	Secure (3rd-Party CA Signed Certificate)	Secure (Self Signed Certificate)
H.323 Mode	*On* (default) or *OFF* (recommended)	*On* (default) or *OFF* (recommended)	*On* (default) or *OFF* (recommended)
SIP Media encryption mode	*Auto* (default) or *Best Effort*	*Forced Encrypted* or *Best Effort* (required if **H.323 Mode** is set to *On*)	*Forced Encrypted* or *Best Effort* (required if **H.323 Mode** is set to *On*)
TLS Verify mode	*Off*	*On*	*Off*
TLS verify subject name field	Not Applicable	`sip.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*)	*Default* or *Custom* (required if **H.323 Mode** is set to *Off*)
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*)	*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*)	*Off* (required if **Advanced zone profile** is set to *Custom*)

Create a search rule for the WebEx domain with the following properties:

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

Task 5: Enabling BFCP in the Neighbor Zone to the Unified CM on Cisco Expressway-C (or Cisco VCS Control)

Note: BFCP requires Cisco Unified Communications Manager version 8.6(1) or later. We strongly recommend that you use a version no earlier than 8.6(2a)SU3 for BFCP interoperability.

To enable presentation sharing, verify that BFCP is enabled on the Unified CM neighbor zone in Cisco Expressway-C or Cisco VCS Control.

In X8.1 and later, BFCP is automatically enabled when you choose the appropriate advanced zone profile for Unified CM versions 8.6(1) or later on the Unified CM neighbor zone.

In Cisco VCS Control X7.2 and X7.1, you explicitly set custom advanced zone profile parameters on the Unified CM neighbor zone. For instructions, see the "Enabling BFCP" appendix of the applicable deployment guide:

- Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide (X7.2)
- Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide (X7.1)

Task 6: Configuring the Unified CM with a SIP trunk to Cisco Expressway

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

To enable presentation sharing, be sure to 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.)

For detailed instructions, see the applicable guide.

- Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide
- Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide

Task 7: Adding a Route Pattern in Unified CM

On the Unified CM, add a SIP route pattern for *.webex.com (or *.*) and point it at the SIP trunk to Cisco Expressway-C (or Cisco VCS Control) .

For route pattern configuration instructions, see the Cisco Unified Communications Manager Administration Guide for your release.

Task 8: Configuring Bandwidth Controls

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.

- In Cisco Expressway or Cisco VCS, set zones and pipes appropriately (according to your network's requirements) to allow the minimum desired bandwidth.
  For instructions, see the "Bandwidth control" chapter of the applicable administration guide:
  - Cisco Expressway Administrator Guide
  - Cisco VCS Administrator Guide
- In Unified CM, set the region to permit the minimum desired bandwidth, to ensure optimum SIP audio and video connectivity between endpoints on Unified CM and the WebEx cloud.
  For region configuration instructions, see the Cisco Unified Communications Manager Administration Guide for your release.

Task 9: Simplifying the Video Dial String

To join a scheduled CMR Cloud 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@example.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 CM 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 means of a Unified CM route pattern and a Cisco Expressway transform.

To set up simplified dialing, do the following:

1. Select a prefix beginning with a digit that is not frequently used in your dial plan. This can include * or #.
2. On Unified CM, 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`**
3. Configure the route pattern to direct the call to the Cisco Expressway.
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})`**
5. Configure the transform to strip the prefix digit (7 in this example) and append the domain (@example.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@example.webex.com`**.

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

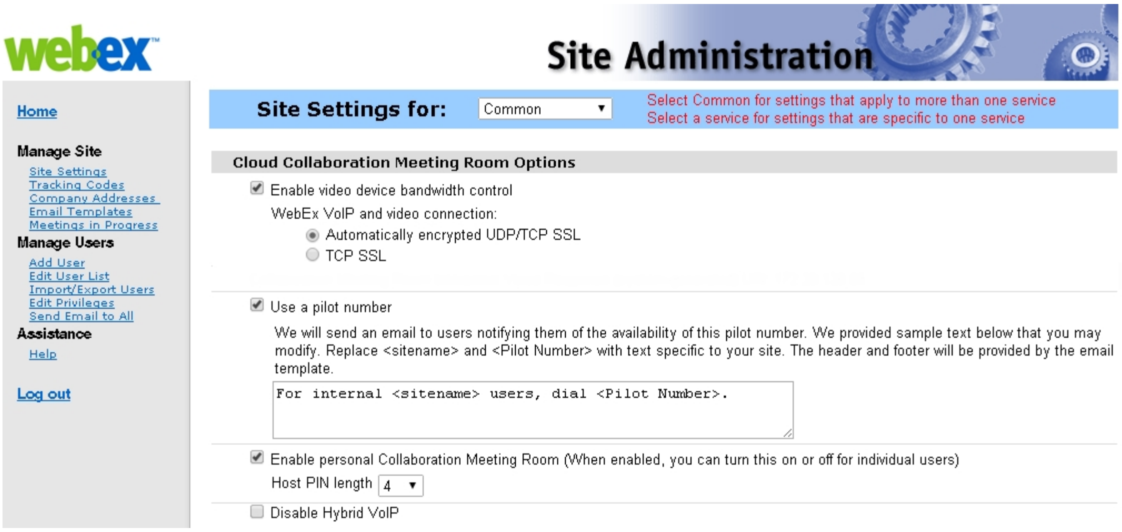
Note that this simplification only applies to devices within your enterprise, joining meetings that are hosted by your own enterprise. Users who need to dial meetings hosted by other enterprises and external video participants will need to dial the full video dial string, including the domain.

Task 10: Configuring Site Administration Settings for CMR Cloud

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.

To configure site-wide settings for CMR Cloud, in the Site Administration left navigation bar under **Manage Site**, choose **Site Settings**, and scroll down to **Cloud Collaboration Meeting Room Options**.

Figure 2: Site settings for CMR Cloud



Site Settings for: Common ▾

Select Common for settings that apply to more than one service
Select a service for settings that are specific to one service

Cloud Collaboration Meeting Room Options

☑ Enable video device bandwidth control

WebEx VoIP and video connection:

● Automatically encrypted UDP/TCP SSL
○ TCP SSL

☑ Use a pilot number

We will send an email to users notifying them of the availability of this pilot number. We provided sample text below that you may modify. Replace <sitename> and <Pilot Number> with text specific to your site. The header and footer will be provided by the email template.

```
For internal <sitename> users, dial <Pilot Number>.
```

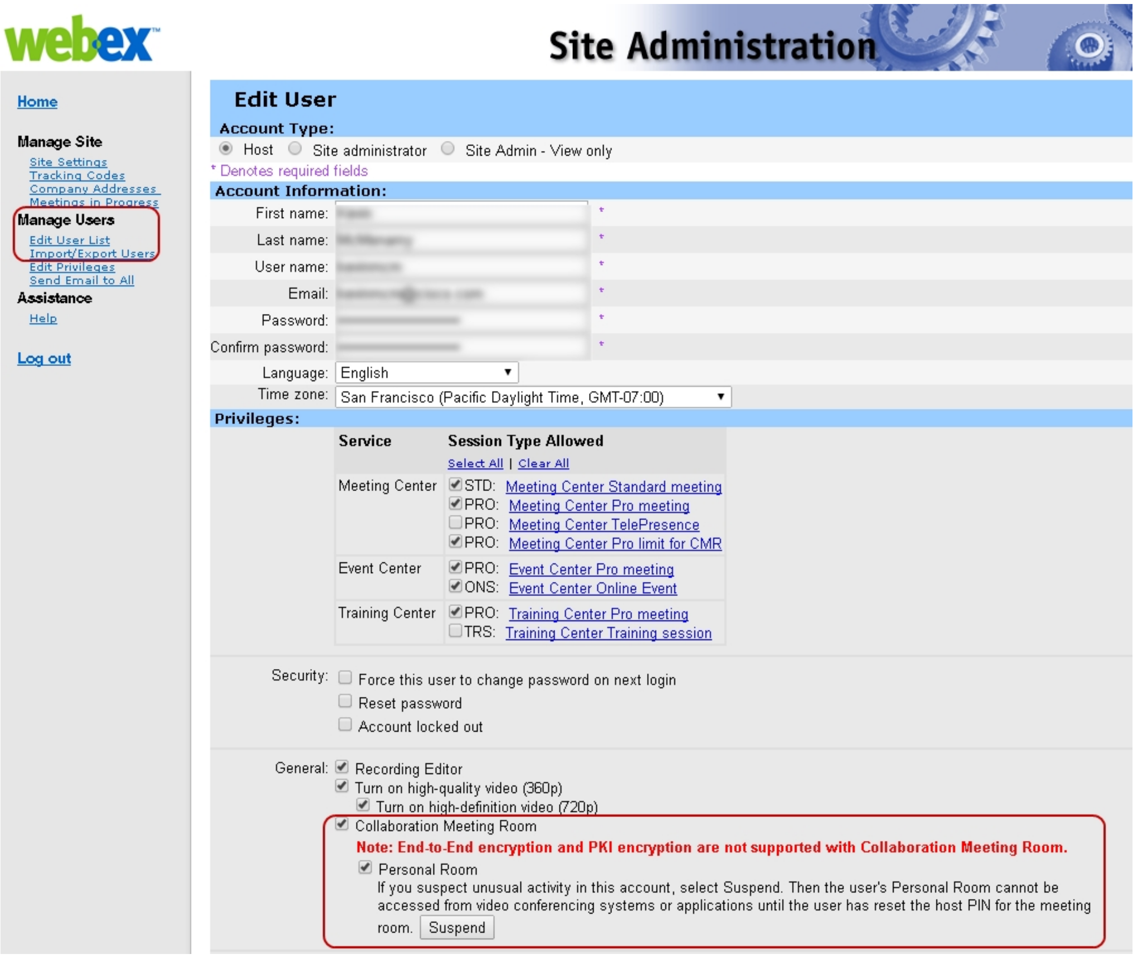
☑ Enable personal Collaboration Meeting Room (When enabled, you can turn this on or off for individual users)

Host PIN length 4 ▾

☐ Disable Hybrid VoIP

When adding or editing a user, you can enable or disable the Cloud Collaboration Meeting Room option for the user. If you enable personal Collaboration Meeting Rooms (also referred to as Personal Rooms) at the site level, you can enable or disable them for each individual user. On the Edit User page, you can also suspend a personal CMR, which blocks host and guest access until the owner changes his or her host PIN.

Figure 3: User settings for Cloud Collaboration Meeting Room



Site Administration

Home

Manage Site

Site Settings
Tracking Codes
Company Addresses
Meetings in Progress

Manage Users

Edit User List
Import/Export Users
Edit Privileges
Send Email to All

Assistance

Help

Log out

Edit User

Account Type:

● Host ○ Site administrator ○ Site Admin - View only

* Denotes required fields

Account Information:

First name: [redacted] *
Last name: [redacted] *
User name: [redacted] *
Email: [redacted] *
Password: [redacted] *
Confirm password: [redacted] *
Language: English
Time zone: San Francisco (Pacific Daylight Time, GMT-07:00)

Privileges:

Service	Session Type Allowed Select All | Clear All
Meeting Center	☑ STD: Meeting Center Standard meeting ☑ PRO: Meeting Center Pro meeting □ PRO: Meeting Center TelePresence ☑ PRO: Meeting Center Pro limit for CMR
Event Center	☑ PRO: Event Center Pro meeting ☑ ONS: Event Center Online Event
Training Center	☑ PRO: Training Center Pro meeting □ TRS: Training Center Training session

Security:
□ Force this user to change password on next login
□ Reset password
□ Account locked out

General:
☑ Recording Editor
☑ Turn on high-quality video (360p)
☑ Turn on high-definition video (720p)
☑ Collaboration Meeting Room
Note: End-to-End encryption and PKI encryption are not supported with Collaboration Meeting Room.
☑ Personal Room
If you suspect unusual activity in this account, select Suspend. Then the user's Personal Room cannot be accessed from video conferencing systems or applications until the user has reset the host PIN for the meeting room. Suspend

Note: The **Meeting Center TelePresence** check box enables WebEx Enabled TelePresence. It does not need to be checked to enable the Cloud Collaboration Meeting Room options. For information on using the two offerings together, see Using Both WebEx Enabled TelePresence and Cloud Collaboration Meeting Room Offerings Together [p.21]

For detailed instructions, see the Cisco WebEx Site Administration User Guide available from the **Support > User Guides** page of your WebEx site.

Security Configuration

For SIP based calls, the Cisco WebEx Cloud CMR service supports four levels of security (in order of preference):

1. encrypted TLS signaling with CA-signed certificates and sRTP media encryption

2. encrypted TLS signaling with self-signed certificates and sRTP media encryption

3. non-secure TCP signaling with sRTP media encryption

4. non-secure TCP signaling with non-secure RTP media.

For H.323 based calls, the Cisco WebE Cloud CMR service supports H.235 encryption method.

These are automatically negotiated in signaling for each call. By default, the Cisco Expressway and VCS Expressway series use a self-signed certificate, so they would negotiate security level 2 with the WebEx cloud when using SIP. The following section outlines the configuration steps you can take on your equipment to enable CA-signed certificates for the highest level of security.

Do the tasks in this section if you want 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.

Task 11: Selecting a Supported Root Certificate Authority

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[1]
- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- globalsign_root_ca
- 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.

[1] 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).

Task 12: Generating a Certificate Signing Request using the Cisco Expressway-E

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

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

For detailed instructions on the certificate signing request process, 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

Task 13: Installing the Signed SSL Server Certificate and Configuring the Trusted CA list on the Cisco Expressway-E

Do the following to finish the secure calling set-up:

1. Once you receive the SSL server certificate from your public CA, load it on the Cisco Expressway-E (or Cisco VCS Expressway).
2. If necessary, add the CA certificate and the root certificate used by the WebEx cloud (DST Root CA X3) to the trusted CA certificate list on the Cisco Expressway-E (or Cisco VCS Expressway).
   - Cisco VCS Expressway X7.2 is preloaded with a default trusted CA certificate list that contains 140 certificates, including the DST Root CA X3 certificate. If your server certificate was issued by a public root CA, it is likely already part of the default trusted CA certificate list. If the certificate was issued by an intermediate CA, or if the root CA is not part of the default list, you must "stack" or add the CA Certificate to the trusted CA certificate list.
   - New installations of Cisco Expressway-E (or Cisco VCS Expressway) X8.1 or later do not contain any certificates in the default trusted CA list. With a new installation, you must add your CA certificate and the DST Root CA X3 certificate to the list.
   - If you upgraded to X8.1, the Cisco VCS Expressway retains the trusted CA certificate list from X7.2.

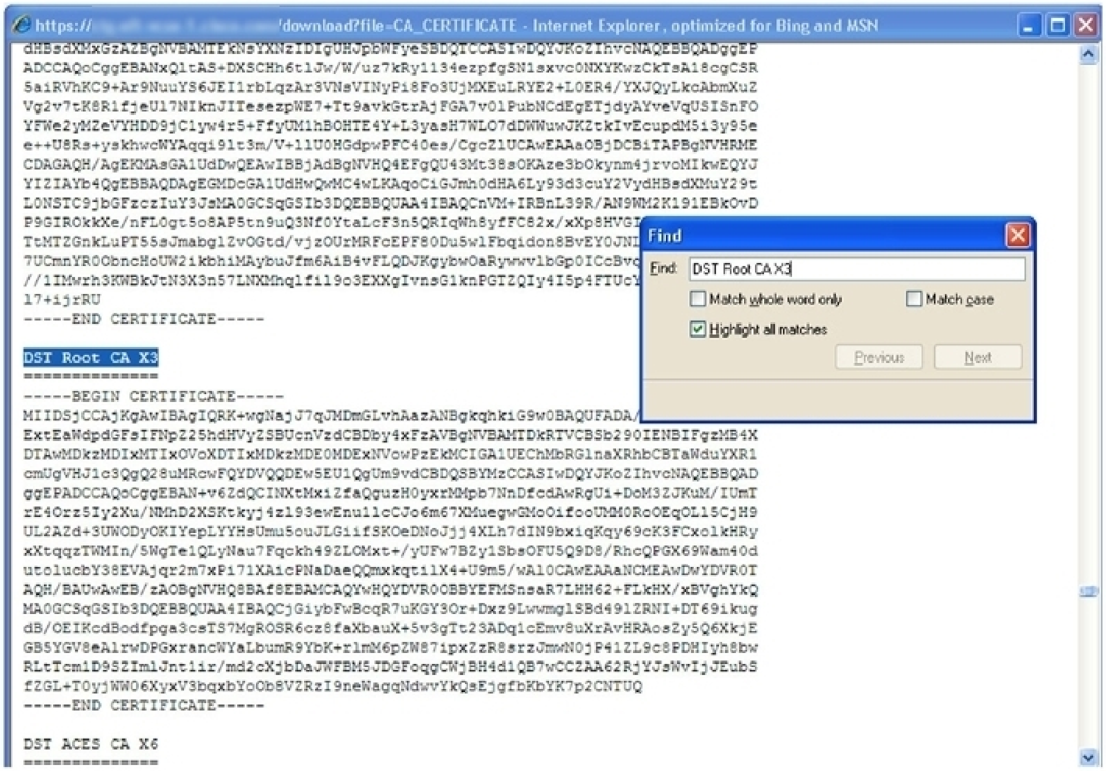
For detailed instructions on loading certificates and configuring the trusted CA list, see the section whose title begins with "Loading certificates and keys" in the applicable guide:

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

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

1. In Cisco Expressway-E or Cisco VCS Expressway:
   - X8.1, go to **Maintenance > Security certificates > Trusted CA certificate**.
   - X7.2.3, go to **Maintenance > Certificate management > Trusted CA certificate**.
2. Click **Show CA certificate.**

   A new window displays the current Trusted CA list.
3. Search for the name of the CA that issued the certificate, for example, **`DST Root CA X3`**.


https://[redacted]/download?file=CA_CERTIFICATE - Internet Explorer, optimized for Bing and MSN
Find
Find: DST Root CA X3
☐ Match whole word only
☐ Match case
☑ Highlight all matches
Previous
Next

```
dHBsdXMxGzAZBgNVBAMTEkNsYXNzIDIgUHJpbWFyeSBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANxQltAS+DXSCHh6tlJw/W/uz7kRy1134ezpfgSN1sxvc0NXYKwzCkTsA18cgCSR
5aiRVhKC9+Ar9NuuYS6JEI1rbLqzAr3VNsVINyPi8Fo3UjMXEuLRYE2+L0ER4/YXJQyLkcAbmXuZ
Vg2v7tK8R1fjeUl7NIknJITesezpWE7+Tt9avkGtrAjFGA7v0lPubNCdEgETjdyAYveVqUSISnFO
YFWe2yMZeVYHDD9jC1yw4r5+FfyUM1hBOHTE4Y+L3yasH7WLO7dDWWuwJKZtkIvEcupdM5i3y95e
e++U8Rs+yskhwcWYAqqi9lt3m/V+llU0HGdpwPFC40es/CgcZlUCAwEAAaOBjDCBiTAPBgNVHRME
CDAGAQH/AgEKMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQU43Mt38sOKAze3bOkynm4jrvoMIkwEQYJ
YIZIAYb4QgEBBAQDAgEGMDcGA1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly93d3cuY2VydHBsdXMuY29t
L0NSTC9jbGFzczIuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQCnVM+IRBnL39R/AN9WM2K191EBkOvD
P9GIROkkXe/nFL0gt5o8AP5tn9uQ3Nf0YtaLcF3n5QRIqWh8yfFC82x/xXp8HVGI
TtMTZGnkLuPT55sJmabgl2vOGtd/vjzOUrMRFcEPF80Du5wlFbqidon8BvEY0JNI
7UCmnYR0ObncHoUW2ikbhiMAybuJfm6AiB4vFLQDJKgybwOaRywwvlbGp0ICcBvq
//1IMwrh3KWBkJtN3X3n57LNXMhqlfil9o3EXXgIvnsG1knPGTZQIy4I5p4FTUcY
l7+ijrRU
-----END CERTIFICATE-----

DST Root CA X3
==============
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
ExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMTDkRTVCBSb290IENBIFgzMB4X
DTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVowPzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1
cmUgVHJ1c3QgQ28uMRcwFQYDVQQDEw5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmT
rE4Orz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEqOLl5CjH9
UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9bxiqKqy69cK3FCxolkHRy
xXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40d
utolucbY38EVAjqr2m7xPi71XAicPNaDaeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0T
AQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQ
MA0GCSqGSIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69ikug
dB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXrAvHRAosZy5Q6XkjE
GB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZzR8srzJmwN0jP41ZL9c8PDHIyh8bw
RLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubS
fZGL+T0yjWW06XyxV3bqxbYoOb8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----

DST ACES CA X6
==============
```

Verification and Completion

Task 14: Verifying the CMR Cloud Service

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

2. Sign in to your WebEx site as the test host, download Productivity Tools for Windows, and go through the personal CMR set-up (if applicable).
3. Schedule a WebEx meeting by using Productivity Tools for Windows.
   - Verify that the meeting appears on the calendar.
   - Verify that the test host receives the meeting confirmation email from WebEx.
4. Call in to the personal CMR (if applicable) or to a scheduled meeting.
   - Verify two-way video between the WebEx Meeting application and telepresence, Jabber, or other video devices.
   - Verify that devices that support presentation sharing can do so.

Hosting, Joining and Participating in CMR Cloud Meetings

Creating Scheduled CMR Cloud Meetings

The meeting organizer can schedule the meeting using the Cisco WebEx and TelePresence Integration to Outlook or the WebEx web site.

The meeting starts the following way:

- At any time, the host can join to start the meeting.
- At the scheduled start time of the meeting participants can call into the meeting. If the host is required but has not joined the meeting, participants receive a message that the meeting has not yet started, and must wait to join.
- If the "Join Before Host" feature is enabled on the site, and the host has set Attendees Can Join Meeting Before Starting Time when scheduling the meeting using the WebEx and TelePresence Integration to Outlook, participants may join the meeting 5, 10, or 15 minutes before the scheduled time (as configured by the host). Otherwise, participants must wait for the meeting to be started by the host before they can join.

Using a Personal Collaboration Meeting Room

Personal Collaboration Meeting Rooms (personal CMRs or personal meeting rooms) provide hosts with rendezvous-type permanent meeting rooms. When a personal CMR is enabled, the host can invite other participants and start the meeting at any time by using the host PIN. If the host needs privacy or has back-to-back meetings, he or she can lock the CMR so that additional callers cannot join it until it is unlocked.

In the My WebEx profile, hosts can configure their host PINs and choose whether to use their personal CMR for instant meetings. Each personal CMR has a static meeting number and a web URL with the format https://<sitename>.webex.com/meet/<hostID>. Users can also reach a host's personal CMR from video devices or applications by dialing the URI <userid>@<sitename>.webex.com.

Joining Cloud Collaboration Meeting Room Meetings

WebEx participants can join a CMR by using the link in the meeting invitation, or, for a personal CMR, by going to https://<sitename>.webex.com/meet/<hostID>.

Participants on SIP-standard and H.323 video devices can join the meeting by dialing one of the following:

- the pilot URI of the interactive voice response (IVR) server, and entering the nine-digit meeting number, plus host PIN if applicable. (H.323 devices must support either H.245 User Input or RFC 2833 methods of DTMF signaling to use the IVR.)
- a video dial string consisting of the nine-digit meeting number followed by the @ symbol and the WebEx site domain -- for example, `123456789@example.webex.com`.

- a simplified dial string (for devices within your enterprise only) as described in Task 9: Simplifying the Video Dial String [p.11].

Telepresence Meeting Experience

During the meeting, telepresence participants see live video of all other telepresence participants, and the video of the most recently active WebEx participant. WebEx participants see the video of all other WebEx participants, and the video of the most recently active telepresence participant. (If a WebEx participant's camera is not on, the participant displays as a black silhoutte.)

For presentation sharing, the telepresence user connects the video display cable to their computer and (if required) presses a button to start sharing their presentation to telepresence and WebEx participants. Video of the active telepresence speaker is streamed to the Cisco WebEx Web client. Video and presentation from WebEx is visible to telepresence participants.

Cisco WebEx Meeting Experience

Participants join the Cisco WebEx meeting by logging in to the Cisco WebEx Meeting Center Web and/or mobile applications. Content shared by a telepresence participant is displayed automatically in the Meeting Center application, and WebEx participants can share their desktop or application with telepresence participants. By default, WebEx participants see the live video of the actively speaking telepresence or WebEx participant.

WebEx participants also see an integrated list of all meeting participants. The WebEx annotation feature is supported. WebEx participants can annotate using the standard Meeting Center application annotations tools and both WebEx and telepresence participants can see the annotations. The annotation tools are not available, however, for telepresence participants.

For WebEx participants to share their presentation with telepresence participants, they must do the following:

1. Log into the Cisco WebEx Meeting Center application on their computers.
2. Grab the ball or be designated as presenter by the WebEx host.
3. Start application or desktop sharing.

Passing the Ball

WebEx users share a presentation by taking the ball and then selecting the content to present. There is no need for the host to manually pass the ball. For more information about using Cisco WebEx meeting functions, log into your Cisco WebEx Meeting Center account and click **Support** in the left navigation pane.

Video Quality

The video quality sent from telepresence participants to WebEx participants is set by the WebEx client with the lowest bandwidth. The bandwidth can go up as soon as the WebEx client with the poorest bandwidth leaves the meeting. For example, if a WebEx client that joins the meeting is only capable of 360p, the maximum bandwidth from telepresence to all WebEx participants will be 360p. When that participant leaves the meeting, if all other clients are capable of a higher bandwidth, like 720p, the bandwidth will go up for all WebEx participants.

Presentation Display Details for Multiple Presenters

For telepresence participants to present, the presenter connects the video display cable to the video device and (if necessary) presses a presentation button on the device. When multiple telepresence participants are presenting at the same time, the device that started presenting last is the one that is displayed. As cables are unplugged, the next presenter must start presenting again.

For WebEx participants to present, they grab the ball and then select the content to present. If a WebEx user cannot grab the ball, the host must pass it to them. Alternatively, they can use the host key to become the new host.

Note: The WebEx site can be provisioned so that any WebEx attendee can grab the ball to present without the host passing them the ball or using the host key.

Meeting Participants List

The meeting participant list in WebEx includes both WebEx and telepresence participants. Functions for muting or unmuting a single participant or all participants apply to both WebEx and telepresence participants. If a user ends the meeting from the WebEx interface, all participants are disconnected.

The display name for a telepresence participant using a SIP-based video device is determined from any of a number of different fields in re-INVITE or UPDATE messages from the endpoint. The display name for an H.323 endpoint is determined from either the Q.931 display name or H323-ID. In either case, if more than one candidate for display name is available, the system chooses a display name according to the following order of preference:

Table 4: Order of Preference for Endpoint Display Name Selection

Device Type	Order
SIP	■ RPID display name ■ PAI display name ■ Contact display name ■ From/To display name ■ RPID user name ■ PAI user name ■ From/To user name ■ Contact user name ■ Contact host name

Table 4: Order of Preference for Endpoint Display Name Selection (continued)

Device Type	Order
H.323	■ H323-ID ■ Q.931 display name

Network-Based Recording of CMR Cloud Meetings

Meeting organizers can record CMR Cloud meetings.

- Playback of a recorded meeting displays both WebEx and telepresence video with content share, chat and polling (if enabled).
- User can navigate through recording via playback controls or clicking thumbnails of the video.
- User can see a visual representation in the recording of when participants are talking.

Note: Network-based recording is enabled by WebEx Cloud Services.

Using Both WebEx Enabled TelePresence and Cloud Collaboration Meeting Room Offerings Together

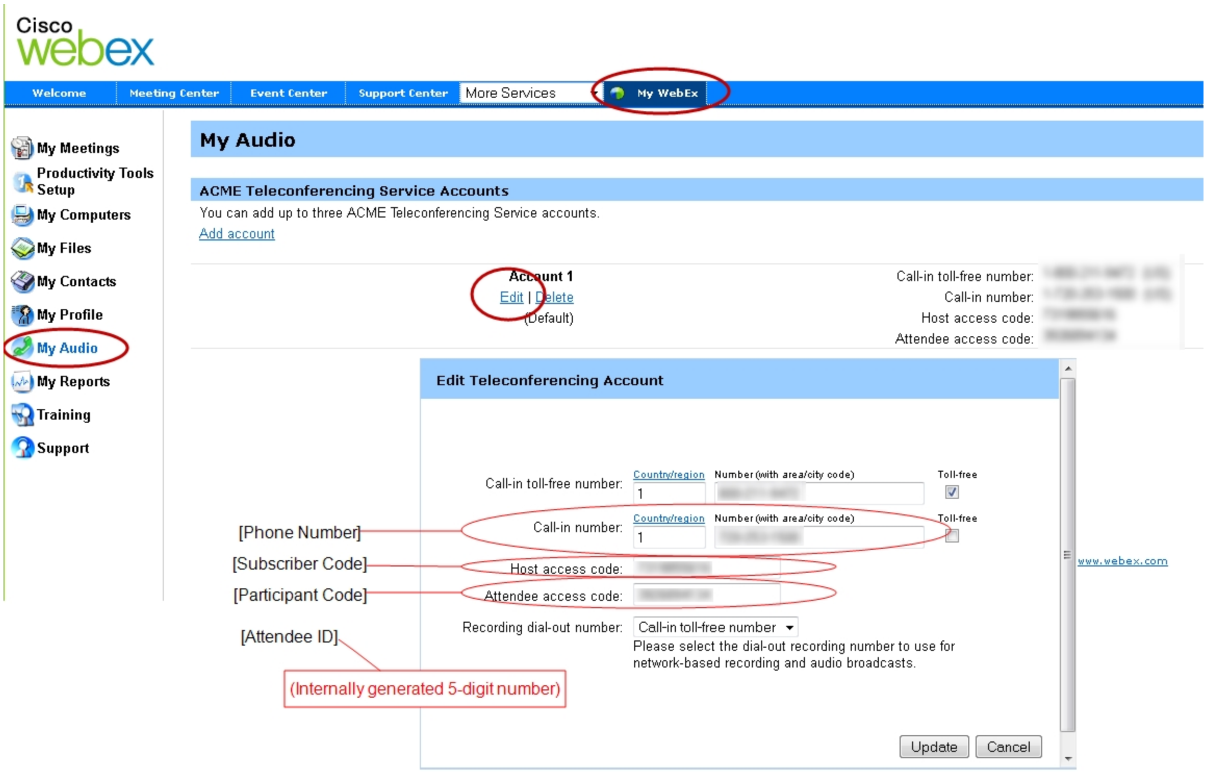
Hosts who have been enabled with both WebEx Enabled TelePresence and Cloud Collaboration Meeting Room options can use Productivity Tools for Windows to manage meetings with cloud resources.

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 CMR Cloud 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, as shown in Figure 4: WebEx Host Account / TSP Audio Account [p.22].

Figure 4: WebEx Host Account / TSP Audio Account



My Audio

ACME Teleconferencing Service Accounts

You can add up to three ACME Teleconferencing Service accounts.

Add account

Account 1
Edit | Delete
(Default)

Call-in toll-free number: [redacted]
Call-in number: [redacted]
Host access code: [redacted]
Attendee access code: [redacted]

Edit Teleconferencing Account

Call-in toll-free number: Country/region 1 Number (with area/city code) [redacted] Toll-free ☑

Call-in number: Country/region 1 Number (with area/city code) [redacted] Toll-free ☐

Host access code: [redacted]

Attendee access code: [redacted]

Recording dial-out number: Call-in toll-free number
Please select the dial-out recording number to use for network-based recording and audio broadcasts.

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

To troubleshoot issues with TSP audio, see Troubleshooting Problems with TSP Audio [p.23]

Troubleshooting

Cisco WebEx Site Administration Online Help

For complete information about using Cisco WebEx Site Administration, go to the Cisco WebEx Site Administration Help:

1. Log in to Site Administration for your WebEx site.
   This is the URL for your WebEx site, followed by a forward slash (/) and the word "admin".
   Example—*https://example.webex.com/admin*
2. In the left-hand side of page under Assistance, click the **Help** link.

Troubleshooting Problems with TSP Audio

Table 5: 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 CMR Cloud 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.

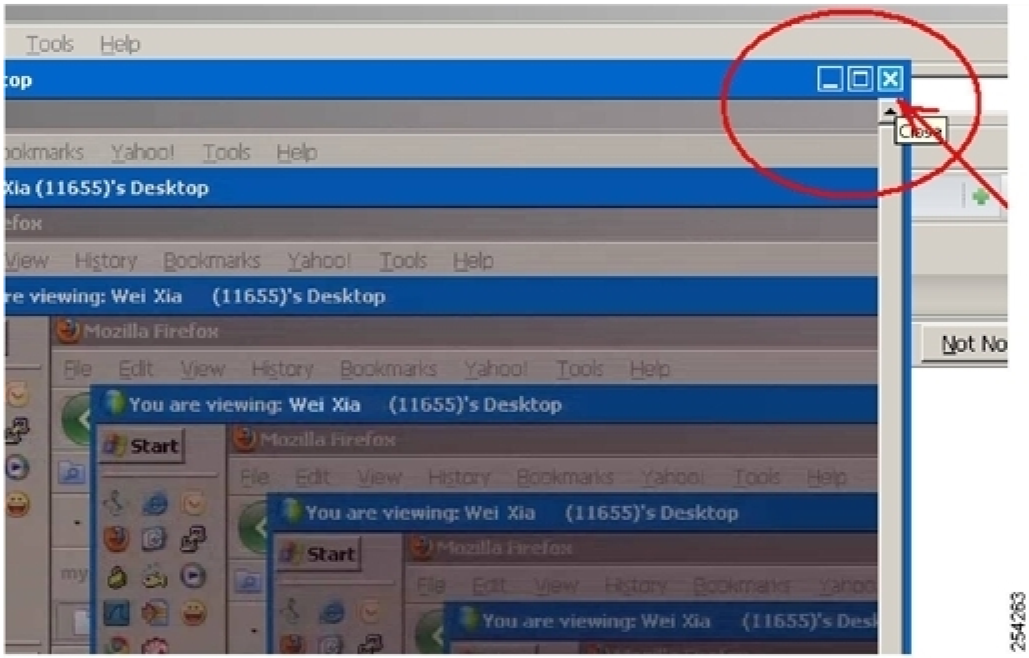
Managing System Behavior

Managing the Cisco WebEx Video View Window

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.

If you do receive a cascading screen, simply close the video view window, as shown in Figure 5: Cascading Cisco WebEx Video View Window [p.24].

Figure 5: Cascading Cisco WebEx Video View Window


Tools Help
Close
You are viewing: Wei Xia (11655)'s Desktop
Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
Start
Not No
254263

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.

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.