Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Planning Your Deployment

You can use any or all of these options when deploying the web portion of your Cisco Unified MeetingPlace system.

Contents

Cisco Unified MeetingPlace Web Traffic and QoS

If you choose to prioritize Cisco Unified MeetingPlace Web Conferencing traffic by using QoS, we recommend that you mark this traffic as DSCP/PHB 34/AF41.

Note: This recommendation only applies when you are using the Cisco Unified MeetingPlace web meeting room, not the Cisco WebEx web meeting room.

Related Topics

For details on QoS design recommendations for Cisco Unified Communications applications, see the Unified Communications and Enterprise QoS SRNDs at http://www.cisco.com/go/designzone.

About Cisco Unified MeetingPlace and Cisco WebEx Deployments

Introduction to Cisco WebEx

Cisco WebEx is an off-premise service that integrates Cisco WebEx-based web conferencing with Cisco Unified MeetingPlace-based voice conferencing within a single meeting.

Cisco Unified MeetingPlace Release 7.0 includes three web deployments as described in Table: Web Deployment Options.

Table: Web Deployment Options

Web Deployment	Scheduling Interface	Web Meeting Interface	Voice	Video
Cisco Unified MeetingPlace only	MeetingPlace	MeetingPlace	MeetingPlace (scheduled and reservationless)	MeetingPlace
Cisco WebEx only	WebEx	WebEx	MeetingPlace (reservationless only)	WebEx
Combination of Cisco Unified MeetingPlace and Cisco WebEx	MeetingPlace	WebEx	MeetingPlace (scheduled and reservationless)	Cisco WebEx has video but the video terminals only receive audio from Cisco Unified MeetingPlace

Meetings that use Cisco WebEx for web conferencing do not use Cisco Unified MeetingPlace web licenses or ports.

Cisco WebEx provides a variety of APIs including a teleconferencing service provider (TSP) API. This API allows third-party bridges, in this case Cisco Unified MeetingPlace, to provide voice conferencing to Cisco WebEx web meetings. Cisco Unified MeetingPlace provides a variety of APIs including a conference technology provider (CTP) API that allows third-party conferencing providers, in this case Cisco WebEx, to plug in to the Cisco Unified MeetingPlace application.

Cisco WebEx Restrictions

- Cisco IP PhoneView and IBM Lotus Notes do not support Cisco WebEx integration at this time.
- Cisco Unified MeetingPlace systems that use Cisco WebEx support US English only.

Considerations for Using Cisco WebEx with Video

In Cisco Unified MeetingPlace Release 7.0.1, users may join Cisco WebEx meetings with video, but only through web cameras that are installed on their computers. Users cannot use other Cisco Unified applications with Cisco Unified MeetingPlace meetings. Video is displayed in the video panel within the Cisco WebEx meeting interface and is included in Cisco WebEx meeting recordings.

In Cisco Unified MeetingPlace Release 7.0.2 and later, Cisco WebEx meetings support Cisco Unified MeetingPlace video conferencing, which displays video through the video endpoints, for example, Cisco Unified Personal Communicator, Cisco Unified Video Advantage, and video terminals.

For all releases, note the following:

- When you obtain your Cisco WebEx account and site, you choose between Cisco Unified MeetingPlace video conferencing and Cisco WebEx webcam video. The Cisco WebEx site cannot support both types of video at the same time.
- Cisco Unified MeetingPlace video conferencing is not included in the Cisco WebEx recordings.
- Cisco Unified MeetingPlace video conferencing is available only to users with video privileges. Configure the Video usage user profile field appropriately for your users.

Cisco Unified MeetingPlace Deployment without Cisco WebEx

This deployment uses a Cisco Unified MeetingPlace Web Server for both scheduling and attending web meetings. There is no interaction at all with Cisco WebEx. Deployments require a minimum of 2 MeetingPlace Web servers on MCS platforms to provide both internal and external guest access for web conferences on premisis. The Internal Web server is deployed behind the company firewall and is used for Internal Meetings that users schedule for internal employees only. This is held on the internal web server only. The second MeetingPlace Web server is deployed in the companies DMZ to provide outside guest users access. All internal and external guest users are sent to the DMZ web server for meetings. The MeetingPlace Web server in DMZ is a locked down version that supports joining a meeting only. Users click on a MeetingPlace URL provided in the meeting email notification and can be password protected.

Cisco WebEx Deployment without Cisco Unified MeetingPlace Web

This deployment uses Cisco WebEx for both scheduling and attending web meetings with reservationless audio conferencing. Features include Cisco WebEx cloud web conferencing, scheduling with various calendar programs such as Microsoft Outlook, IBM Lotus Notes, IM Clients, Microsoft Office and many Cisco UC Clients and WebEx Connect clients. The WebEx Cloud also provides audio/web network based

recordings(NBR provides all secure storage in the Webex Site)and email notifications. There is no ability to record audio-only conferences with this deployment model.

Cisco Unified MeetingPlace uses an Application Server to provide the voice portion of the meeting but does not use any Cisco Unified MeetingPlace Web Servers. You do not need any Cisco Unified MeetingPlace web licenses for this deployment.

Cisco WebEx Scheduling Model ? Audio Experience

Cisco Unified MeetingPlace provides reservationless meetings to all profiled users. Reservationless meetings are initiated by the host or another profiled user (if allowed) and have the following special characteristics:

1. The meeting ID for a reservationless meeting is the profile number of the meeting owner.
2. The meeting owner starts the meeting from the telephone user interface (TUI) by entering their profile number and PIN.
3. The meeting owner can also start the meeting by joining the Cisco WebEx meeting.
4. Participants who join a reservationless meeting before the owner does are placed in a waiting room (where they cannot communicate with each other).
5. Participants are moved from the waiting room to the main audio meeting in the following circumstances:
    1. When the host joins the meeting or
    2. If the **Allow any profiled user to initiate** field on the Usage Configuration Page is set to Yes and a profiled user starts the meeting from the telephone user interface (TUI)

Note: Additional audio (TUI) passwords for guests are NOT supported for this deployment model.

Reservationless Meetings and Logs

1. A meeting instance is created on demand when someone joins a meeting with a reservationless meeting ID.
2. The meeting is terminated immediately when the last participant leaves.
3. The system treats each instance of a reservationless meeting as a separate entity with its own unique conference ID, displayed as ConfNum in reports and exported data.

Note: For more information about reservationless meetings, see the *User Guide for Cisco Unified MeetingPlace* at [1].

Auto Attend Feature

The auto attend feature simplifies how users join meetings or log in over the phone. It is an optional feature but highly recommended for reservationless systems.

If a user calls the system from a phone number in the user profile, then the user is immediately authenticated and placed into the relevant meeting based on their CallerID in Cisco Unified Communications Manager.

You can enable or disable the auto attend feature for specific user profiles and user groups. When enabled, you can also specify the following:

- Whether users are automatically logged in as Hosts.
- Whether users must enter their profile passwords.

Note: Not requiring the profile password is easier for end-users, but less secure.

The feature works as follows:

1. A user calls Cisco Unified MeetingPlace.
2. The system reads the automatic number ID (ANI), which is the phone number from which the user called.
3. The system modifies the ANI according to the translation rules on the Auto Attend Translation Configuration Page, if any apply.
4. If the (modified) ANI exactly matches the Main phone number or Alternate phone number in one user profile, then the system checks all meetings (except continuous meetings) as follows:
    - ♦ Whether the user owns or is invited to any meetings that are in session or that are scheduled to begin.
    - ♦ Whether the user was a participant in any meetings that are still in session.
    - ♦ Whether anyone is in the waiting room of the reservationless meeting owned by the user.
5. If multiple meetings or no meetings are found, then the system authenticates the user and lets the user select the meeting.
6. If only one meeting is found, then the caller hears the meeting ID confirmation and is prompted to do one of the following:
    - ♦ Press **1** to attend the meeting.
    - ♦ Press ***** to hear menu options for authenticated users.
7. The caller may hear additional prompts in the following situations:
8. You configure the **Auto attend requires profile password user profile** field to Yes.
9. Meeting requires a password.
10. Caller needs to record a name or location.

Note: End users can access the Cisco WebEx site to retrieve audio/web recordings by clicking the **My Cisco WebEx** link. Retrieving recordings is the only action end users can take on the Cisco WebEx site. Attempting to complete any other actions will disconnect the voice bridge.

Combination Cisco Unified MeetingPlace and Cisco WebEx Deployment

This deployment uses Cisco Unified MeetingPlace to schedule web meetings and Cisco WebEx for holding the meetings. It includes Cisco WebEx network-based web conferencing and Cisco Unified MeetingPlace scheduled and reservationless voice conferencing, web conferencing, scheduling, notifications, and Microsoft Outlook integration. Users can be given permissions for MP Web use only, Webex web use only or both. This deployment option may cause confusion to end users based on which web conference type they are defaulted to and it requires more Help Desk support and is not recommended to combine both types of web conferencing.

To use this deployment, you must obtain a Cisco WebEx account and site, such as cisco.webex.com. MeetingPlace Web license would also be used as well based on what permissions were allowed per user or group settings.

About MeetingPlace Scheduling Model - Segmented Meeting Access for web conferencing (SMA)

Cisco Unified MeetingPlace Scheduling model using MeetingPlace Web conferencing supports a Segmented Meeting Access (SMA) configuration that allows you to provide external access to your users while maintaining network security. This is not used when deploying the Webex Scheduling Model.

Firewalls and SMA

A firewall is a security device set up to protect a local area network (LAN) from unwanted Internet access. However, you can provide limited access by opening specific TCP ports to allow inbound access to public servers while leaving other portions of the network protected. For example, when a user on the Internet connects to a company home page, the user must pass through TCP port 80 of the company firewall to access the Web Server.

While external participation is possible by controlling port access through a firewall, we highly recommend that you consider a segmented meeting access (SMA) configuration instead. Configurations that use SMA isolate some meetings on the private corporate network while exposing others, designated as external, to the Internet. Users designate their meetings as internal or external during the scheduling process by setting the Allow External Web Participants parameter on the New Meeting scheduling page.

SMA Configuration

In a Segmented Meeting Access (SMA) configuration, Cisco Unified MeetingPlace Web Conferencing is deployed on two separate Web Servers or two separate clusters of Web Servers. One is on the internal network, behind the firewall; the other is on another network segment, such as a demilitarized zone (DMZ). The internal Web Server or cluster is only accessible from behind the firewall while the external Web Server or cluster is accessible from inside or outside the firewall.

While internal users have access to the full Cisco Unified MeetingPlace web interface, external users have access to an external meeting, attend-only web page.

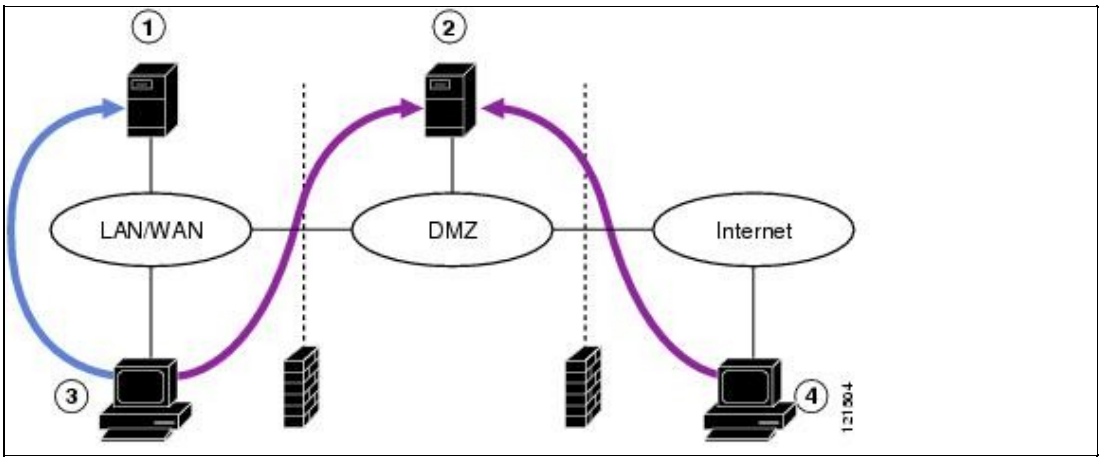
The SMA configuration is the preferred and most secure deployment model if you want to provide external access to Cisco Unified MeetingPlace web meetings.

Note: We recommend that you configure external Web Servers to use Secure Sockets Layer (SSL). This provides optimum security and resolves proxy server issues that can prevent users from joining a web meeting.

- If you configure SSL on an external Web Server and users will access the Web Server through a firewall, make sure that TCP port 443 is open inbound on your firewall for both of the hostnames or IP addresses on the Web Server.

- For SSL configuration instructions, see the *Configuration Guide for Cisco Unified MeetingPlace Release 7.0* or the online help in the administrator interface.

Figure: Segmented Meeting Access (SMA) Configuration



1	Internal Cisco Unified MeetingPlace Web Server. Sits inside the private corporate network.	2	External Cisco Unified MeetingPlace Web Server. Sits in a network segment, such as a DMZ.
3	Internal user. • Internal users enter internal meetings through the internal Web Server. • Internal users enter external meetings through the external Web Server.	4	External user. • External users can enter external meetings only. • Users enter these meetings through the external Web Server.

SMA with SSL and Segmented DNS

If your Cisco Unified MeetingPlace system has SSL configured on the external Web Server and a segmented DNS, the segmented DNS name cannot be the same as the SSL certificate name on the external or internal system. See the following example for configuration guidelines.

Example

You have an SMA configuration where SSL is required for external users, but not required for internal users who are accessing the internal or external system.

- The segmented DNS name is *meetingplace.company.com*.
- The SSL certificate name for the external system is *meetingplace1.cisco.com*.
- The hostname for the external system from the internal system is *meetingplace1*.

- All URLs and click-to-attend links are in the form of http://*meetingplace.company.com*.

When users access http://*meetingplace.company.com* from the external network, the external system will automatically redirect them to an HTTPS URL that uses the hostname configured in the system database, in this case, https://*meetingplace1.company.com*.

Note: If you force SSL on all users, both internal and external users will be required to use SSL when they access the external Web Server.

Related Topics

For information on configuring your system for SMA, see Configuration.

Reservationless Single Number Access (RSNA)

The Reservationless Single Number Access (RSNA) feature allows multiple Cisco Unified MeetingPlace systems to appear as one system to the user community. Users who host or attend a reservationless meeting can join their meeting by dialing the access phone number of their local Cisco Unified MeetingPlace system, regardless of which system is hosting the meeting. Users are then redirected to the system that is hosting the meeting. Webex cannot be used with the RSNA deployment model which is supported for Audio/Video only conferences.

The RSNA Reserved Meeting Server feature allows a single Application Server to host reserved meetings within an RSNA-based network. Typically, all meeting reservations are hosted on the one designated Reserved Meeting Server. When users access their local server to attend meetings and the local server does not recognize the meeting ID, it transfers the user to the Reserved Meeting Server.

Note: The server times must be synchronized between the local Application Server and the Reserved Meeting Server.

The local server attempts to transfer calls to the Reserved Meeting Server if all of the following conditions are true:

- The Reserved Meeting Server feature has been configured on the local server.
- The meeting ID that the user entered does not match the meeting ID of any meetings scheduled around that time on the local server.
- The meeting ID that the user entered does not match any user profile, active or not.
- The user confirms the meeting ID.

In addition, consider the following behavior of the RSNA Reserved Meeting Server feature:

- This feature does not prevent meetings from being scheduled locally and will not warn or transfer a user who attempts to schedule a meeting locally.
- If a meeting is scheduled on a server other than the Reserved Meeting Server, this feature will not facilitate attendance of that meeting.
- A locally-scheduled meeting always takes precedence over a remote one. This rule applies even if a local meeting recently ended and the user hears that meeting is over.
- If the meeting does not exist on the remote system, the system reprompts the user for a meeting ID after the transfer.
- Users choose which server to schedule the meeting on from the Server drop-down box on the Scheduling page. To restrict users from choosing a server other than the Reserved Meeting Server, you may need to disable the Server drop-down box from the scheduling page. This restriction does not apply if the user dials into a local server and uses the TUI to schedule the meeting. In that case the meeting will be scheduled on a local server.

Related Topics

For information on configuring your system for RSNA, see Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace