

Main page: [Cisco Unified MeetingPlace, Release 7.0](#)

Previous page: [System Requirements](#)

Contents

- [1 Media Server Administration](#)
- [2 Cisco Unified Communications Manager Requirements](#)
- [3 Cisco Security Agent \(CSA\)](#)
- [4 McAfee VirusScan Enterprise](#)
- [5 Directory Service Requirements](#)
- [6 License Requirements](#)
- [7 Reservationless Single Number Access \(RSNA\) Requirements](#)
- [8 Cisco WebEx Requirements](#)
 - ◆ [8.1 Hardware](#)
 - ◆ [8.2 Software](#)
 - ◆ [8.3 Limitations and Restrictions](#)
 - ◆ [8.4 Types of Cisco WebEx Service Contracts](#)
- [9 Load Balancing Requirements](#)
 - ◆ [9.1 Application Server Requirements](#)
 - ◆ [9.2 Internal Web Server Cluster Requirements](#)
 - ◆ [9.3 External Web Server Cluster Requirements](#)
 - ◆ [9.4 Mixed Cluster Requirements](#)
- [10 Segmented Meeting Access \(SMA\) Requirements](#)
 - ◆ [10.1 Hardware Requirements](#)
 - ◆ [10.2 Software Requirements](#)
 - ◆ [10.3 DNS Configuration Requirements](#)
 - ◆ [10.4 Additional Requirements](#)
 - ◇ [10.4.1 Related Information](#)
- [11 Cisco Unified MeetingPlace Conference Manager Requirements](#)
 - ◆ [11.1 Restrictions](#)

Media Server Administration

The Media Server Administration pages require Internet Explorer 6 or Internet Explorer 7.

Cisco Unified Communications Manager Requirements

Cisco Unified MeetingPlace Release 7.0 requires Cisco Unified Communications Manager Release 6.1(2) or later.

Note: The latest release of Cisco Unified MeetingPlace Release 7.0 (version 7.0.3 (MR2)) was tested against Cisco Unified Communications Manager Release 6.1.5.10000-10, 7.1.5.10000-12, and 8.0.2.40000-1.

Cisco Unified Communications Manager Release 6.1.x is automatically included with all shipments of Cisco Unified MeetingPlace Release 7.0.

In the following cases, you may connect Cisco Unified MeetingPlace to Cisco Unified Communications Manager Release 6.0(3) or later release:

- Video installations in which only Cisco Unified Video Advantage is used
- Audio-only installations

Cisco Security Agent (CSA)

| Cisco Unified MeetingPlace Release | CSA version for Application Server | CSA version for Web Server |
|------------------------------------|------------------------------------|----------------------------|
| Release 7.0.1 | Release 5.2.0.268 | Release 5.2.0.245 |
| Release 7.0.2 | Release 5.2.0.268 | Release 5.2.0.245 |
| Release 7.0.3 | Release 6.0 | Release 6.0.1.140 |

For information about Cisco Security Agent, see http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html.

McAfee VirusScan Enterprise

Cisco Unified MeetingPlace supports the following on the Web Server:

- McAfee VirusScan Enterprise versions 8.0i and later
- McAfee VirusScan Enterprise versions 8.7i and later as included in the McAfee Endpoint Protection Suite

If you install McAfee VirusScan Enterprise 8.7i or later, make sure that you uncheck the following settings in the Access Protection Rules (found in the Access Protection Properties window) so that Cisco Unified MeetingPlace Web will function properly:

- **Prevent programs registering as a service** found in the Common Maximum Protection category
- **Protect Cached files from password and email...** (4th Option) in the Anti-virus Maximum Protection category
- **Protect network settings** found in the Common Standard Protection category

If you are deploying an SMA-2S configuration, make sure that you also uncheck **Prevent HTTP Communication** found in the Common Maximum Protection category. Unchecking this setting ensures that the internal site will be able to communicate with the DMZ site.

To find out more information about McAfee VirusScan Enterprise use this link <http://www.mcafee.com/us/products/virusscan-enterprise.aspx>

Directory Service Requirements

Directory Service enables the system to populate and synchronize the Cisco Unified MeetingPlace user database with the Cisco Unified Communications Manager user database. The Cisco Unified Communications Manager user database is typically integrated with an LDAP directory, the following of which are supported by Cisco Unified MeetingPlace Directory Service:

- Microsoft Windows Active Directory 2000
- Microsoft Windows Active Directory 2003
- Microsoft Windows Active Directory Windows 2008
- Netscape Directory Server Version 4.x
- iPlanet Directory Server Version 4.x
- SunONE Directory Server Version 5.1
- Sun Java Version 5.2
- Novell eDirectory Release 4.x, 5.x, 6.x

Note: Novell eDirectory requires a custom configuration. See <http://www.novell.com/coolsolutions/appnote/16752.html> for information about Novell eDirectory Release 4.x and <http://www.novell.com/communities/node/3028/> for information about Novell eDirectory Release 5.x and 6.x.

License Requirements

Cisco Unified MeetingPlace requires licenses depending on the features you use. For a list of all the licenses, see [About Licenses](#).

Reservationless Single Number Access (RSNA) Requirements

- To use Cisco Unified MeetingPlace with RSNA, you must use Cisco Unified Communications Manager Release 6.1.2 or later for use with the SIP REFER command.
- A maximum of two Cisco Unified MeetingPlace Release 7 systems may be deployed with the RSNA configuration with no Application Server redundancy at this time.
- A single Cisco Unified Communications Manager cluster must be configured to process both inbound and outdial calls to both Cisco Unified MeetingPlace RSNA systems. If the RSNA systems are in different locations, they share an IP address and hostname for database replication and the same VLAN must be configured to work in both data sites.
- Cisco Unified MeetingPlace Web Conferencing URLs will be different on both RSNA systems and are accessed using the profile number that matches the audio reservationless ID for meetings.
- The following maximum ports are possible:
 - ◆ 3000 audio (1500 on each system)
 - ◆ 2000 Web (1000 on each system)
 - ◆ 320 or 600 video (160 or 300 on each system) if the system has 16 (2x8) Audio Blades and 16 (2x8) Video Blades
 - ◆ 240 or 480 video (120 or 240 on each system) if the system has 12 (2x6) Audio Blades and 12 (2x6) Video Blades

- Cisco Unified MeetingPlace RSNA does not support Cisco WebEx today. However, we plan to support Cisco WebEx with multi-node (RSNA) Cisco Unified MeetingPlace systems in the future. We recommend that you become familiar with the Cisco WebEx requirements and pay special attention to the length restrictions for profile numbers.

Cisco WebEx Requirements

Note: Cisco Unified MeetingPlace Release 7.0.1 does not support Cisco WebEx. If you want to use Cisco WebEx in your deployment, upgrade to Cisco Unified MeetingPlace Release 7.0.2 or 7.0.3.

Hardware

- For Integration Option 1 (schedule and attend Cisco WebEx meetings from Cisco Unified MeetingPlace) only:
 - ◆ Cisco Unified MeetingPlace requires that your system contain at least one internal Cisco Unified MeetingPlace Web Server (or cluster). The system can optionally also contain an external Web Server(or cluster).
 - ◆ Part of the Cisco WebEx gateway software is installed on the Web Server.
- Cisco Unified MeetingPlace URLs are published in Cisco Unified MeetingPlace notifications that provide automatic redirect to the Cisco WebEx MeetingCenter upon joining, for both internal users and external guest users via the Cisco Unified MeetingPlace Web Servers deployed.
- A Cisco MCS-7835 can be used for web scheduling and up to 250 concurrent web redirect sessions.
- A Cisco MCS-7845 can be used for up to 500 concurrent web redirect per Web Server with a maximum of 100 meetings.
- No Cisco Unified MeetingPlace web user licenses are required or used with Cisco WebEx.

Software

Note: Cisco Unified MeetingPlace Release 7.0.1 does not support Cisco WebEx. If you want to use Cisco WebEx in your deployment, upgrade to Cisco Unified MeetingPlace Release 7.0.2 or 7.0.3.

- Cisco Unified MeetingPlace Release 7.0.2 and 7.0.3 require Cisco WebEx Release WBS 27 on the Cisco WebEx site.
- Cisco Unified MeetingPlace requires Cisco WebEx MeetingCenter or Cisco WebEx MeetingCenter Pro.

Limitations and Restrictions

- MeetingPlace Application Server Webex TSP only support SOCKS Web Proxy servers (Not HTTP Proxy) so please allow direct firewall access to Webex Site IPs directly. Often there are delay issues when proxy servers are used and the integration to Webex links must be able to be maintained continuously, otherwise it will affect user response times.

Cisco_Unified_MeetingPlace,_Release_7.0_--_Software_Requirements

- A Cisco WebEx integration can have a maximum of 1000 user ports per system.
- The Cisco WebEx integration on the Cisco Unified MeetingPlace Application Server does not support redundancy and failover deployments.
- The Media Servers may be redundant (which provides active DSP redundancy).
- Cisco WebEx is only supported for use with Cisco Unified MeetingPlace web conferencing and the Cisco Unified MeetingPlace for Microsoft Outlook integration. It cannot be used with the IBM Lotus Notes for Cisco Unified MeetingPlace integration.
- Cisco WebEx does not support Cisco Unified MeetingPlace for Microsoft Office Communicator.
- Cisco WebEx does not support Cisco Unified MeetingPlace RSNA.
- Cisco Unified MeetingPlace unique profile numbers must be eight digits or less. The profile number is typically the telephone number of an end user and usually does not include the country code or area code.
- If scheduling from the Cisco Unified MeetingPlace web user portal, the meeting scheduler can choose to define certain users as "alternate hosts". Alternate hosts can start the meeting if the meeting scheduler does not arrive on time.
 - ◆ If you schedule your meeting from an alternate scheduling interface, such as the Microsoft Outlook integration, you can still define certain users as alternate hosts from the Cisco Unified MeetingPlace web user portal.
 - ◆ Users must have their e-mail address, first name, and last name set in their user profiles in order to be listed as alternate hosts.
 - ◆ If any user who is defined as an alternate host does *not* have this information listed, the system marks the meeting invalid and locks it. This prevents any user from attending the meeting, including the meeting scheduler, even if all other alternate hosts and the meeting host have an e-mail address, first name, and last name set in their user profiles.
 - ◆ If a user defined as an alternate host does not have their e-mail address, first name, and last name set in their user profile, the system will set the accounts of all other users who are attempting to attend the *same* meeting to inactive on Cisco WebEx and remove their ability to attend any meetings. This includes users who have their e-mail address, first name, and last name set in their user profiles.
 - ◆ If you invite an alternate host whose Cisco WebEx user account is inactive, the system will "hang" and the alternate host will see a blank window.

Note: We highly recommend that you populate the user profile for anyone who will ever be invited to a Cisco WebEx meeting with an e-mail address, first name, and last name.

Types of Cisco WebEx Service Contracts

Minutes

With this model, Cisco WebEx charges the customer for web-meeting minutes consumed by attendees.

Concurrent Ports

With this model, the customer purchases a certain number of Cisco WebEx ports. A port corresponds to a web-meeting attendee. The number of attendees that can join meetings system-wide is limited to the number

of ports purchased; hence the term "concurrent ports".

Named Host

With this model, only someone who is explicitly named as a host can schedule a meeting.

The Named Host license requires a Cisco WebEx user account for each profiled user of Cisco Unified MeetingPlace. If there are more Cisco Unified MeetingPlace users than Cisco WebEx users, some users will be able to schedule but not actually join the meeting.

Load Balancing Requirements

Cisco Unified MeetingPlace Web Servers make use of an algorithmic formula to evenly distribute web-conferencing requests within a cluster of Web Servers.

Application Server Requirements

- All Web Servers within both internal and external clusters must point to the same Cisco Unified MeetingPlace Application Server.
- For primary and failover Application Server deployments, all Web Servers within both internal and external clusters must point to the "Shared IP/Hostname" of these servers.
- Cisco Unified MeetingPlace Web Servers can be deployed in geographically disbursed data centers with a network requirement of ~150 ms RRT over the network to the primary Application Server.
- You can attach a maximum of 16 Cisco MCSs running Cisco Unified MeetingPlace applications (for example, Cisco Unified MeetingPlace Web Conferencing, Cisco Unified MeetingPlace for Microsoft Outlook, etc.) to the same Cisco Unified MeetingPlace Application Server.

Internal Web Server Cluster Requirements

If you have an internal Web Server cluster in your load balancing configuration, ensure the following:

- All Web Servers within the internal cluster must share a single SQL Server database.
- The SQL Server 2000 local software is provided with the Cisco Unified MeetingPlace Web Server installation CD and will install locally. Customer can also provide the hardware and software for a "remote" SQL 2000 or SQL 2005 system.
- All Web Servers within the internal cluster must have access to a shared storage location for attachments.
- Install Cisco Unified MeetingPlace Web Conferencing on each Web Server sequentially (internal Web Server 1, internal Web Server 2, and so forth) with the following option: for Server Location,

choose Internal (Full Access).

- Make sure that all Web Servers within the internal cluster have the same deployment settings and configurations (for example, the same Replication Service and Audio Service parameters).

External Web Server Cluster Requirements

If you have an external Web Server cluster in your load balancing configuration, ensure the following:

- All Web Servers within the external cluster must share a single SQL Server database.
- The SQL Server 2000 local software is provided with the Cisco Unified MeetingPlace Web Server installation CD and will install locally. Customer can also provide the hardware and software for a remote SQL 2000 or SQL 2005 system. The remote SQL Server may be installed on your internal network (TCP port access through the firewall must be opened) or in your DMZ network with the Cisco Unified MeetingPlace Web Server or cluster.
Note: Make sure the internal cluster and external cluster use different SQL Server databases.
- All Web Servers within the external cluster must have access to a shared storage location (for attachments).
- Install Cisco Unified MeetingPlace Web Conferencing on each Web Server sequentially (external Web Server 1, external Web Server 2 and so forth) with the following option: for Server Location, choose External (Limited Access).
- Make sure that all Web Servers within the external cluster have the same deployment settings and configurations (for example, the same Replication Service and Audio Service parameters).

Mixed Cluster Requirements

A mixed cluster has at least one internal cluster and one external cluster. If you have a mixed cluster in your load balancing configuration, ensure the following:

- All requirements for internal Web Server clusters and external Web Server clusters are met.
- The database of the internal cluster and the database of the external cluster must contain identical system and site Globally Unique Identifiers (GUIDs).
- You have configured the redirection from the internal cluster to the external cluster.

Segmented Meeting Access (SMA) Requirements

Cisco Unified MeetingPlace Web Conferencing supports Segmented Meeting Access (SMA) deployments for external access.

Hardware Requirements

Two single Cisco MCSs or clusters of Cisco MCSs (in the case of load balancing):

- One Web Server (or cluster of Web Servers) deployed inside the private corporate network functioning as *internal* Web Servers.
- One Web Server (or cluster of Web Servers) deployed in a network segment, such as a DMZ, functioning as *external* Web Servers.

Software Requirements

- On internal Web Servers, Cisco Unified MeetingPlace Web Conferencing Release 7.0 installed with the "Internal (Full Access)" server location option.
- On external Web Servers, Cisco Unified MeetingPlace Web Conferencing Release 7.0 installed with the "External (Limited Access)" server location option.

DNS Configuration Requirements

- For segmented DNS, the same host name must resolve to the internal Web Server on the internal DNS and resolve to the external Web Server on the external DNS.
- The internal host names and IP addresses are accessible only from the internal network.
- The external host names or IP addresses are accessible from both the internal network and the Internet.

Additional Requirements

- Synchronized Globally Unique Identifiers (GUIDs) between internal and external Web Servers. The database of the internal Web Server and the database of the external Web Server must contain identical GUIDs.

Related Information

- For more information about SMA, see [About Web Deployment Options for Cisco Unified MeetingPlace Release 7.0](#).
- For information on installing an SMA configuration, see [How to Install Cisco Unified MeetingPlace Web Conferencing for a Segmented Meeting Access \(SMA\) Deployment](#).
- For information on configuring your system for SMA, see [Configuring External Access to Cisco Unified MeetingPlace Web Conferencing](#).

Cisco Unified MeetingPlace Conference Manager Requirements

Restrictions

- Sun Java JRE 6 update 16 and update 18 are not supported. Prior versions (updates) are supported. Later versions (updates) are supported if latest Conference Manager hotfix is installed.