



Installation and Upgrade Guide for Cisco Unified MeetingPlace Web Conferencing

Release 6.x
May 31, 2007

Corporate 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: 408 526-4100

Text Part Number: OL-13418-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Installation and Upgrade Guide for Cisco Unified MeetingPlace Web Conferencing Release 6.x
© 2007 Cisco Systems, Inc. All rights reserved.



Preface vii

Purpose	ii-vii
Audience	ii-vii
Naming Conventions	ii-viii
Documentation Conventions	ii-ix
Cisco Unified MeetingPlace Documentation	ii-x
Obtaining Documentation	ii-x
Cisco.com	ii-x
Product Documentation DVD	ii-x
Ordering Documentation	ii-x
Documentation Feedback	ii-xi
Cisco Product Security Overview	ii-xi
Reporting Security Problems in Cisco Products	ii-xi
Product Alerts and Field Notices	ii-xii
Obtaining Technical Assistance	ii-xii
Cisco Support Website	ii-xii
Submitting a Service Request	ii-xiii
Definitions of Service Request Severity	ii-xiii
Obtaining Additional Publications and Information	ii-xiv

CHAPTER 1

Introducing Cisco Unified MeetingPlace Web Conferencing 1-1

About Cisco Unified MeetingPlace	1-1
About Cisco Unified MeetingPlace Web Conferencing	1-1
Overview of Web Conferencing Components	1-2
Benefits of Web Conferencing	1-3
Overview of the Cisco MeetingPlace Agent Service	1-4
Terms of Use	1-7
Configuration Restrictions	1-7
Cisco Policy for Use of Third-Party Software	1-7
Terms for Single Sign On Software Integration	1-7
Terms of Support for Single Sign On Software Integration	1-8
New Feature and Enhancement Information	1-9

CHAPTER 2

Installing Web Conferencing 2-1

- Preinstallation Tasks: Web Conferencing 2-1
 - Installing Cisco Unified MeetingPlace Audio Server 2-2
 - Planning Web Conferencing License Usage 2-2
 - Installing SQL Server on a Remote Server 2-2
 - Gathering Web Conferencing Installation Values 2-3
- Installation Tasks: Web Conferencing 2-5
 - Installing the Operating System on the Cisco MCS Server 2-5
 - Configuring Network Settings on the Cisco MCS Server 2-5
 - Installing Web Conferencing 2-9
- Postinstallation Tasks: Web Conferencing 2-12
 - Defining the Web Conferencing Server Hostname Information 2-12
 - Testing the Web Conferencing Installation 2-13
 - Installing the Cisco Security Agent for Cisco Unified MeetingPlace Web Conferencing 2-14
 - Creating and Using a Least-Privileged SQL Account for Web Conferencing 2-14
 - Configuring SSL 2-16

CHAPTER 3

Installing Web Conferencing for a Segmented Meeting Access Configuration 3-1

- About Segmented Meeting Access 3-1
 - About the SMA-2S Configuration 3-2
 - About the SMA-2S Configuration with SSL and Segmented DNS 3-3
 - About the SMA-2S Configuration and Video-Enabled Systems 3-4
- Preinstallation Tasks: Web Conferencing in an SMA-2S Configuration 3-4
- Installation Tasks: Web Conferencing in an SMA-2S Configuration 3-5
 - Copying GUIDS from the Internal Web Server to the External Web Server 3-5
- Postinstallation Tasks: Web Conferencing in an SMA-2S Configuration 3-6

CHAPTER 4

Installing Web Conferencing in a Load Balancing Configuration 4-1

- About Installing Web Conferencing in a Load Balancing Configuration 4-1
 - Restrictions for Installing Web Conferencing in a Load Balancing Configuration 4-2
 - Web Conferencing Clusters 4-2
 - Web Conferencing Load Balancing and Failover Capability 4-4
 - Load Balancing Behavior with Internal and External Clusters 4-5
 - Recommendations for a Robust Cisco Unified MeetingPlace System 4-6
 - End-User Experience During Meeting Console Failover 4-6
- About Installing Web Conferencing in a Load Balancing Configuration for Video-Enabled Systems 4-7
- Preinstallation Tasks: Web Conferencing in a Load Balancing Configuration 4-7
 - Preparing the Internal Cluster 4-8

Preparing the External Cluster	4-8
Installation Tasks: Web Conferencing in a Load Balancing Configuration	4-9
Installing the First Internal Web Server	4-9
Installing Additional Internal Web Servers	4-10
Copying GUIDS from the Internal to the External Web Server	4-11
Installing the First External Web Server	4-12
Installing Additional External Web Servers	4-13
Linking the Internal and External Servers	4-14
Postinstallation Tasks: Web Conferencing in a Load Balancing Configuration	4-15
Synchronizing Purge Parameters	4-15
Configuring SSL (Optional)	4-15
Viewing the Web Conferencing Load on a Server	4-16

CHAPTER 5**Troubleshooting the Web Conferencing Installation 5-1**

Installation Problems	5-1
What to Do First	5-1
Checking That the Cisco MCS Operating System Version Meets the Requirement	5-2
Obtaining Additional Assistance	5-3
Server Connection Problems	5-3
Meeting Room Connection Problems	5-3

APPENDIX A**Uninstalling Web Conferencing or SQL Server Software A-1**

Uninstalling Web Conferencing Software	A-1
Uninstalling SQL Server Software and Removing MPWEB SQL Database Files	A-1

INDEX



Preface

This preface contains the following sections:

- [Purpose, page vii](#)
- [Audience, page vii](#)
- [Naming Conventions, page viii](#)
- [Documentation Conventions, page ix](#)
- [Cisco Unified MeetingPlace Documentation, page x](#)
- [Obtaining Documentation, page x](#)
- [Documentation Feedback, page xi](#)
- [Cisco Product Security Overview, page xi](#)
- [Product Alerts and Field Notices, page xii](#)
- [Obtaining Technical Assistance, page xii](#)
- [Obtaining Additional Publications and Information, page xiv](#)

Purpose

This guide describes how to install and upgrade Cisco Unified MeetingPlace Web Conferencing Release 6.x.

This guide does not describe how to configure or maintain Web Conferencing Release 6.x, nor does it describe how to install or use additional Cisco Unified MeetingPlace applications that can reside on the same server as Web Conferencing.

Audience

This guide is for Cisco Unified MeetingPlace system administrators. It assumes the following considerations:

- You have a thorough understanding of voice and data terminology and concepts.
- You are familiar with Cisco Unified MeetingPlace, networking concepts, and Microsoft Windows software-based web servers.

After you install Cisco Unified MeetingPlace Web Conferencing, you are also responsible for the following tasks:

- Installing and configuring third-party applications that are not currently available to Web Conferencing (for example, optional audio tools such as Windows Media Server).



Note Installation of third-party software is subject to the [“Cisco Policy for Use of Third-Party Software”](#) section on page 7.

- Working with others, such as the corporate web master and network administrator.
- Performing maintenance and troubleshooting on an ongoing basis.
- Planning storage and purging requirements.

Naming Conventions

Earlier releases of Cisco Unified MeetingPlace Audio Server were called “MeetingPlace Server” or “MeetingServer.” In this guide, “Cisco Unified MeetingPlace Audio Server” and “Audio Server” refer to all releases past and present.

[Table 1](#) describes other terms used throughout the Cisco Unified MeetingPlace set of documents.

Table 1 *Product Naming Conventions*

Term	Definition	Used in This Document As
Cisco Unified MeetingPlace 8100 series server	Includes Cisco Unified MeetingPlace 8106 and Cisco Unified MeetingPlace 8112 servers.	Cisco Unified MeetingPlace 8100 series
Cisco Unified MeetingPlace 8106 Server	Hardware on which Cisco Unified MeetingPlace Audio Server software runs.	Cisco Unified MeetingPlace 8106
Cisco Unified MeetingPlace 8112 Server	Hardware on which Cisco Unified MeetingPlace Audio Server software runs. (This server was called M3 in Releases 5.2 and earlier.)	Cisco Unified MeetingPlace 8112
Cisco Unified MeetingPlace Audio Server	Software that runs on the Cisco Unified MeetingPlace 8100 series server.	Cisco Unified MeetingPlace Audio Server
Cisco Unified MeetingPlace Audio Server system	Cisco Unified MeetingPlace 8106 or Cisco Unified MeetingPlace 8112 running Cisco Unified MeetingPlace Audio Server.	Cisco Unified MeetingPlace Audio Server system or Audio Server system
Cisco Unified MeetingPlace MeetingNotes	A Cisco Unified MeetingPlace Audio Server feature by which users record meetings and listen to meeting recordings.	MeetingNotes
Cisco Unified MeetingPlace MeetingTime	Windows desktop software through which system administrators can access and configure Cisco Unified MeetingPlace Audio Server.	MeetingTime

Table 1 *Product Naming Conventions (continued)*

Term	Definition	Used in This Document As
Cisco MCS Unified CallManager Appliance	Hardware on which Cisco Unified MeetingPlace applications are installed.	Cisco MCS
Cisco Unified MeetingPlace Web Conferencing server	A Cisco MCS installed with Cisco Unified MeetingPlace Web Conferencing.	web server All references to a “web server” in this guide refer to the Cisco Unified MeetingPlace Web Conferencing server.

Documentation Conventions

Table 2 *Conventions for Cisco Unified MeetingPlace Documentation*

Convention	Description
boldfaced text	Used for: <ul style="list-style-type: none"> • Commands that you must enter exactly as shown. • Key and button names. • Information that you enter.
<i>italicized text</i>	Used for arguments for which you supply values.
[] (square brackets)	Used for elements that are optional.
text in Courier font	Used for information that appears on the screen.
^ (caret)	Used to indicate use of the Control key. (For example, ^D means press the Control and D keys simultaneously.)
< > (angle brackets)	Used for nonprinting characters, such as passwords.

Cisco Unified MeetingPlace documentation also uses the following conventions:

**Note**

Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

**Caution**

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Cisco Unified MeetingPlace Documentation

For descriptions and locations of Cisco Unified MeetingPlace documentation on Cisco.com, see the *Documentation Guide for Cisco Unified MeetingPlace*. The document is shipped with Cisco Unified MeetingPlace and is available at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_documentation_roadmaps_list.html.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

<http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Introducing Cisco Unified MeetingPlace Web Conferencing

This chapter contains the following sections:

- [About Cisco Unified MeetingPlace, page 1-1](#)
- [About Cisco Unified MeetingPlace Web Conferencing, page 1-1](#)
- [Terms of Use, page 1-7](#)
- [New Feature and Enhancement Information, page 1-9](#)

About Cisco Unified MeetingPlace

Cisco Unified MeetingPlace provides a rich-media conferencing solution that includes the following:

- Voice, web, and video-conferencing capabilities.
- Centralized access.
- Real-time collaboration.
- Integrated-network security that uses the existing telephony or IP-based infrastructure of your organization.

For more information about Cisco Unified MeetingPlace, refer to the *Installation Planning Guide for Cisco Unified MeetingPlace*.

About Cisco Unified MeetingPlace Web Conferencing

Cisco Unified MeetingPlace Web Conferencing provides real-time collaboration functionality to an organization's intranet and extranet and integrates Cisco Unified MeetingPlace with a web server, thus providing users with a browser-based interface. Cisco Unified MeetingPlace Web Conferencing enables Windows, Mac, Linux, and UNIX users to schedule and attend conferences, access meeting materials, and collaborate on documents from common web browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

For more information about Cisco Unified MeetingPlace Web Conferencing, refer to the *Configuration Guide for Cisco Unified MeetingPlace Web Conferencing*.

This section provides information about the following Cisco Unified MeetingPlace Web Conferencing concepts:

- [Overview of Web Conferencing Components, page 1-2](#)
- [Benefits of Web Conferencing, page 1-3](#)
- [Overview of the Cisco MeetingPlace Agent Service, page 1-4](#)

Overview of Web Conferencing Components

Cisco Unified MeetingPlace Web Conferencing is implemented by using a combination of technologies, including the following:

- Hypertext Markup Language (HTML)
- JavaScript
- Adobe Flash
- Internet Server Application Program Interface (ISAPI)
- Windows services
- ASP.NET

[Table 1-1](#) describes the Cisco Unified MeetingPlace Web Conferencing components, which work with the Cisco Unified MeetingPlace Audio Server system and the Cisco IPVC Multipoint Control Unit (MCU) to fulfill user requests and deliver functionality.

Table 1-1 Cisco Unified MeetingPlace Web Conferencing Components

Component	Description
Cisco Unified MeetingPlace Agent Service	Maintains a constant connection between the web server and the Audio Server system. Priority = Normal (8). For more information, see the “Overview of the Cisco MeetingPlace Agent Service” section on page 1-4.
Cisco Unified MeetingPlace Audio Service	Converts Cisco Unified MeetingPlace Voice (.mpv) files. Priority = Normal (8).
Cisco Unified MeetingPlace Connect Application Service	Performs meeting load balancing functions and sends commands and events from the meeting room to other Cisco Unified MeetingPlace components. Priority = Normal (8).
Cisco Unified MeetingPlace Connect Gateway	Receives commands and events from the Agent Service and translates them into meeting room activity. Priority = Normal (8).
Cisco Unified MeetingPlace Flash Media Administration Server	Auxiliary service that provides web-conferencing capability. Priority = Normal (8).
Cisco Unified MeetingPlace Flash Media Server	Serves the web-conferencing meeting room client to end-users. Priority = Normal (8).
Cisco Unified MeetingPlace Replication Service	Synchronizes the local web server database with that of the Audio Server system. Priority = Low (4).

Table 1-1 Cisco Unified MeetingPlace Web Conferencing Components (continued)

Component	Description
Cisco MeetingPlace Video Service (optional)	Provides video conference integration by communicating with Cisco Unified MeetingPlace Video Administration, the Audio Server system, and the web server.
Cisco Unified MeetingPlace Web Conferencing	Priority = Normal (8).

All of these services are controlled by a master service called the Cisco MeetingPlace Web Conferencing Service.

Benefits of Web Conferencing

As part of an integrated rich-media conferencing solution, Cisco Unified MeetingPlace Web Conferencing provides four key benefits, which are described in the following sections:

- [Common Endpoints, page 1-3](#)
- [Server-Based Conferencing, page 1-3](#)
- [Increased Reliability, page 1-4](#)
- [Network Security, page 1-4](#)

Common Endpoints

Cisco Unified MeetingPlace Web Conferencing includes a Flash-based endpoint called the meeting console, which facilitates participation in Cisco Unified MeetingPlace web conferences. The meeting console is automatically loaded on the web browsers of users as soon as they join their meetings. Users can download the Cisco Unified Presenter Add-in to share their desktop or to upload and share documents and presentations from their desktop.

The use of these common endpoints allows meeting attendees to view any document being shared by the host regardless of whether they have the applications installed on their PCs. For example, if the host shares an Excel spreadsheet, all attendees are able to view the shared spreadsheet. If the host enables collaboration of the shared document, all attendees can then take control of the shared application and modify its contents—regardless of whether they have Excel installed.

Server-Based Conferencing

Cisco Unified MeetingPlace Web Conferencing takes advantage of server-based conferencing, which connects each user directly to the web server. To access a web conference, users either sign in through the Cisco Unified MeetingPlace Web Conferencing home page by using their user ID, user password, and meeting ID, or click the click-to-attend link in their meeting notification. Either action launches the meeting console, which connects users to their meeting. Because of server-based conferencing, users do not need to know the IP addresses of other PCs to connect.

Increased Reliability

Cisco Unified MeetingPlace Web Conferencing not only makes scheduling and attending meetings easy, it also increases the reliability of a meeting for the following reasons:

- The web server continues to host conferences even if an individual user's system crashes.
- Typically, the web server is a powerful system that can support a higher volume of transactions than a user's PC.
- You can locate the web server in the server room for redundant power backup.
- You can deploy multiple web servers in clusters to provide Web Conferencing load balancing and redundancy. (For more information on load balancing, see the [“Installing Web Conferencing in a Load Balancing Configuration”](#) chapter.)

Network Security

Cisco Unified MeetingPlace Web Conferencing provides increased network security when conducting web conferences with users outside your organization for the following reasons:

- Because the web server provides a central point of connection, you need to provide inbound network access only to one server rather than to all desktops in your organization.
- You can install Web Conferencing on an external web server with attend-only capability and deploy it in a publicly accessible network, such as in a demilitarized zone (DMZ).
- Web Conferencing supports Secure Sockets Layer (SSL), which allows the web server to send and receive encrypted data over your network.

Locking down Microsoft web servers by using the Microsoft Lockdown Utility is an increasingly popular way to close potential security holes. The Cisco MCS operating system used with Cisco Unified MeetingPlace Web Conferencing is already locked down. If you are using a legacy, non-Cisco MCS server, see the release note or readme file for the latest Cisco MCS OS to identify supported security settings.

Overview of the Cisco MeetingPlace Agent Service

The Cisco MeetingPlace Agent service maintains a constant connection between the web server and the Cisco Unified MeetingPlace Audio Server system. If you have the Cisco Unified MeetingPlace Video Integration installed, the Agent service also acts as a communicator between the Audio Server system and the Video service.

The Agent service processes all user-invoked transactions, including the following:

- Scheduling and attending meetings.
- Managing profile information.
- Requesting lists of meetings to which a user is invited.

This section contains the following information:

- [How Users Connect to Web Conferencing, page 1-5](#)
- [How Web Conferencing Fulfills Requests, page 1-5](#)

How Users Connect to Web Conferencing

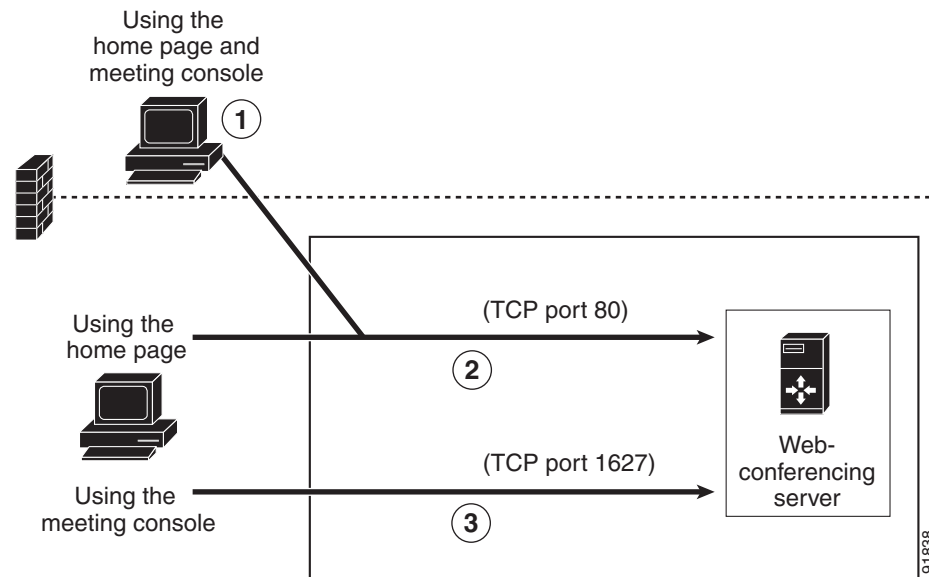
Users connect to the Web Conferencing home page to sign in, schedule or find meetings to attend, and update their profile settings. This connection uses the primary IP address (or hostname) configured on the Web Conferencing server and port 80.

When a meeting is scheduled to begin, the Cisco MeetingPlace Agent Service instructs the web engine to initiate the meeting. As users join the web component of the meeting, the Flash-based meeting console is downloaded on their desktops, allowing them to connect to the Flash Media Server running on the Web Conferencing system by using the secondary IP address (or hostname) configured on the server.

The meeting console communicates with the Flash Media Server on the Web Conferencing server through TCP port 1627, as shown in [Figure 1-1](#). If this port is blocked due to a firewall, the Flash client establishes a tunnel connection over HTTP through port 80. This process allows the meeting console to bypass firewall restrictions so that external users can participate in web conferences.

The web server also supports tunneling over HTTPS by using Secure Sockets Layer (SSL).

Figure 1-1 How Users Communicate with Cisco Unified MeetingPlace Web Conferencing

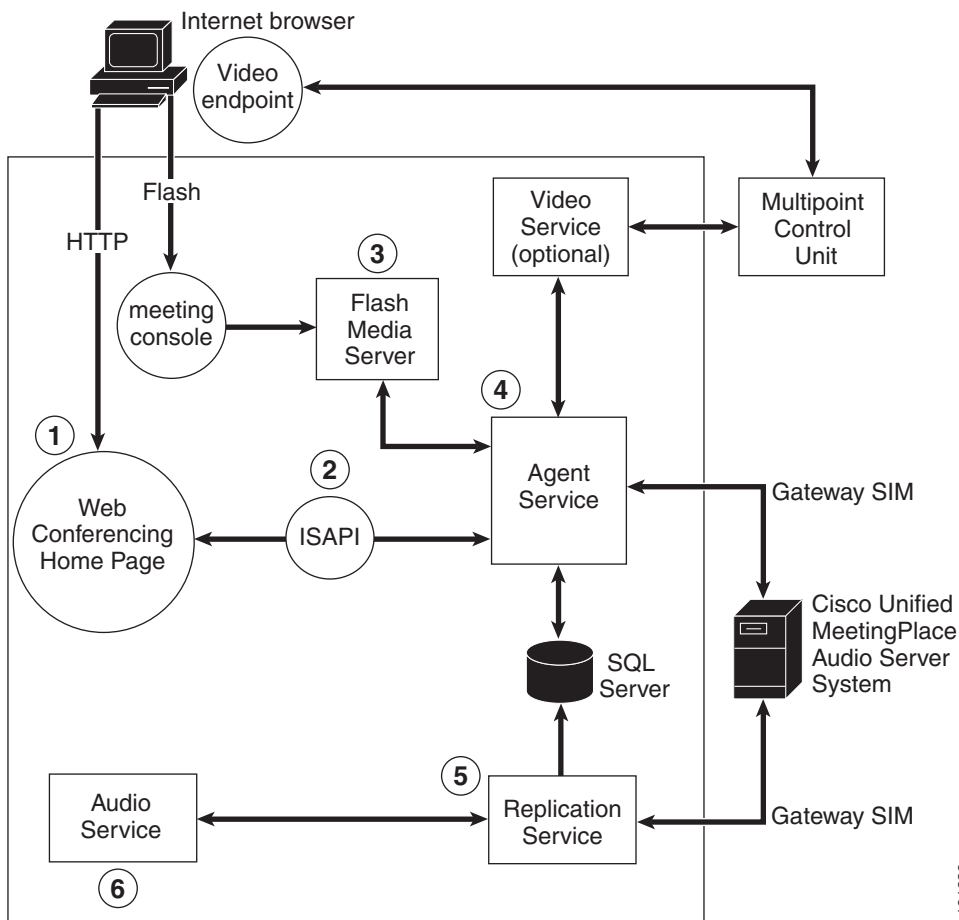


1. For external participants, the meeting console tunnels communication by using HTTP through TCP port 80.
2. Cisco Unified MeetingPlace Web Conferencing home page traffic (signing on, scheduling meetings, changing profile settings, etc.) for both internal and external participants uses port 80.
3. For internal participants using the meeting console, connection is made directly to the web server over TCP port 1627.

How Web Conferencing Fulfills Requests

[Figure 1-2](#) shows how Cisco Unified MeetingPlace Web Conferencing components work together to fulfill user requests.

Figure 1-2 Cisco Unified MeetingPlace Web Conferencing Components



191839

1. Users submit requests to schedule meetings, change their profile, and join meetings.
2. ISAPI processes user requests for the Cisco MeetingPlace Agent Service and generates HTML pages to display to users for meeting scheduling, meeting details, and account update pages.
3. When users join a meeting, their meeting consoles connect to the Flash Media Server on the Cisco Unified MeetingPlace Web Conferencing server.
4. The Agent Service manages all user requests from ISAPI and accomplishes the following:
 - Passes the scheduling requests and profile updates to the Cisco Unified MeetingPlace Audio Server system.
 - Coordinates between the meeting room components (Connect Gateway, Connect Application Service, Flash Media Administration Server, and Flash Media Server) and the rest of the Cisco Unified MeetingPlace system.
 - Acts as a communication channel between the Audio Server system and the Video Service. For information about the Video Service, refer to the *Administration Guide for Cisco Unified MeetingPlace Video Integration*.
 - Retrieves and stores information in the MPWEB database.

(For more information about the Agent Service, see the “[Overview of the Cisco MeetingPlace Agent Service](#)” section on page 1-4.)

5. The Replication Service copies meeting materials from the Audio Server system and stores them on the web server. Pointers to the data are kept in an SQL Server database. The Replication Service also forwards voice recordings to the Audio Service for file conversion.
6. The Audio Service converts voice recordings and passes the converted files back to the Replication Service.

Terms of Use

This section contains information on particular terms of agreement that you should be aware of when configuring or using this product:

- [Configuration Restrictions](#), page 1-7
- [Cisco Policy for Use of Third-Party Software](#), page 1-7
- [Terms for Single Sign On Software Integration](#), page 1-7
- [Terms of Support for Single Sign On Software Integration](#), page 1-8

Configuration Restrictions

Cisco Unified MeetingPlace Web Conferencing deployments that are customized beyond the built-in configuration capabilities of the product, or beyond the documented configuration settings, procedures or instructions, are not supported by Cisco Systems.

Examples of such customizations include, but are not limited to, the following: modifying web page templates, changing HTML or Javascript code, changing IIS running parameters or applying custom ASP pages or ISAPI filters, modifying SQL server configuration or authentication method, and modifying Windows OS security through IPsec policies and NTFS ACL.

Cisco Policy for Use of Third-Party Software

The Cisco Unified MeetingPlace Web Conferencing documentation describes the system, end user, and other requirements for the use of Web Conferencing software. Failure to meet these requirements or the introduction of certain third-party products may interfere with the operation of the Cisco Unified MeetingPlace Web Conferencing software, and may affect Cisco support for the Web Conferencing product.

Terms for Single Sign On Software Integration

- Customer Premise Equipment (CPE) customers who implement SSO software integrations on their Cisco Unified MeetingPlace web servers do so at their own risk and are responsible for understanding the technical implementations and feasibility of SSO integrations on their systems.
- By allowing SSO software integrations, we do not claim support for any SSO software packages or vendors.

- SSO software integrations require proper configuration of Cisco Unified MeetingPlace Web Conferencing systems through the Admin pages. If your SSO software integration requires a change in the Cisco Unified MeetingPlace Web Conferencing product source code, your SSO integration becomes an SSO customization, and we do not support customizations by either customers or any other parties.
- CPE customers who want to integrate SSO packages can contact Cisco Managed Services to obtain a Service Request to implement SSO. This service is offered as a convenience and does not change the scope of the SSO integration: this service is an integration and configuration of the Cisco Unified MeetingPlace Web Conferencing product, not a customization of the product code.
- Customers must first implement SSO software integrations on test or lab servers and verify that the integrated systems work, including Cisco Unified MeetingPlace Web Conferencing features and operations.
- Customers are responsible for ensuring stability of integrated Cisco Unified MeetingPlace Web Conferencing-SSO systems, including communicating with SSO software vendors for the following reasons:
 - To obtain necessary fixes and support
 - To troubleshoot functional problems and technical problems, including crashes triggered by the SSO package
- SSO software often includes a web-server extension, called the IIS ISAPI extension or filter. Cisco Unified MeetingPlace Web Conferencing installs and uses four IIS extensions. Any incompatibility between an SSO software extension and the Cisco Unified MeetingPlace Web Conferencing extensions can make IIS non-functional or unstable. Any crash of the SSO IIS extension can cause IIS to crash and can generate a full Cisco Unified MeetingPlace Web Conferencing outage, resulting in a full system reboot, ending of in-progress meetings, and disconnecting of web-conferencing users. Any memory leak in the SSO package or module can make IIS or the whole server unstable, as well.
- Although SSO software integration is productized for the Cisco Unified MeetingPlace Web Conferencing system, any changes in overall configuration, including Cisco Unified MeetingPlace Web Conferencing upgrades and SSO package upgrades, can potentially break integrated Cisco Unified MeetingPlace Web Conferencing-SSO systems.

Terms of Support for Single Sign On Software Integration

- Customers must inform Cisco TAC that their Cisco Unified MeetingPlace Web Conferencing servers have third-party SSO packages installed and configured with Cisco Unified MeetingPlace Web Conferencing when opening a service request for Cisco Unified MeetingPlace Web Conferencing, Cisco Unified MeetingPlace for Microsoft Outlook, or Cisco Unified MeetingPlace for Lotus Notes.
- Customers must be able to provide SSO integration details upon request. Inability to provide details can result in Cisco TAC not being able to proceed with service requests.
- If a service request is about troubleshooting the SSO integration, Cisco TAC can review the logs and identify if the problem is on the SSO side or the Cisco Unified MeetingPlace Web Conferencing side. If the problem is on the SSO side, information will be provided to customers, so they can further troubleshoot with their SSO vendors.
- If the service request is about troubleshooting a Cisco Unified MeetingPlace Web Conferencing problem that does not seem to be connected to the SSO integration, Cisco TAC will proceed per the normal support process. If TAC discovers that the SSO integration plays a role in the problem, information will be provided to customers, so they can further troubleshoot with their SSO vendors.

- If Cisco TAC believes the problem is triggered by an SSO package, Cisco TAC can require customers to disable the SSO package to troubleshoot further.
- Microsoft Debug Diagnostic tool, also called DebugDiag, may be required for troubleshooting IIS crashes and memory leaks to determine if these problems are produced by the SSO package.

New Feature and Enhancement Information

For information on new and changed functionality in Cisco Unified MeetingPlace Web Conferencing, refer to *Release Notes for Cisco Unified MeetingPlace Web Conferencing* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.



Installing Web Conferencing

This chapter describes how to complete a new installation of Cisco Unified MeetingPlace Web Conferencing. It does not describe upgrades.

This chapter contains the following sections:

- [Preinstallation Tasks: Web Conferencing, page 2-1](#)
- [Installation Tasks: Web Conferencing, page 2-5](#)
- [Postinstallation Tasks: Web Conferencing, page 2-12](#)



Note

Before reviewing this chapter, please read *System Requirements for Cisco Unified MeetingPlace Release 6.x* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html. All installations of Release 6.x require a Cisco MCS and a supported version of MCS OS 2003 software.

Preinstallation Tasks: Web Conferencing

Before attempting to install Cisco Unified MeetingPlace Web Conferencing, refer to *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html for updated system requirements. When reviewing the requirements, note the following considerations:

- If you are installing Web Conferencing in a segmented meeting access configuration, that is, allowing external access, also see the “[Installing Web Conferencing for a Segmented Meeting Access Configuration](#)” chapter in this guide.
- If you are installing Web Conferencing in a load balancing configuration, also see the “[Installing Web Conferencing in a Load Balancing Configuration](#)” chapter in this guide.

After reviewing system requirements, complete the following preinstallation tasks:

1. [Installing Cisco Unified MeetingPlace Audio Server, page 2-2](#)
2. [Planning Web Conferencing License Usage, page 2-2](#)
3. (Optional) [Installing SQL Server on a Remote Server, page 2-2](#)
4. [Gathering Web Conferencing Installation Values, page 2-3](#)

Installing Cisco Unified MeetingPlace Audio Server

You must install and configure Audio Server software on a Cisco Unified MeetingPlace 8100 series server before you begin the Web Conferencing installation. (Refer to the *Installation and Upgrade Guide for Cisco Unified MeetingPlace Audio Server* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.)

Planning Web Conferencing License Usage

Cisco Unified MeetingPlace Release 6.0 introduced a new license usage model for Web Conferencing. In this model, users joining a Cisco Unified MeetingPlace meeting from the web see one of two meeting console formats, with different license requirements:

Full meeting room	Includes tools for sharing and collaboration, in-session controls, and other features such as chat and polling. Requires an available web conferencing license for each participant.
Participant list only	Includes only the list of meeting participants and associated audio and video controls (such as mute audio and pause video). No web conferencing license is required to use this meeting console; it is included in the license for an audio port.

The meeting console format that participants see in a meeting depends on the Host Meetings With setting in the profile of the meeting scheduler. When planning for web conferencing license usage, consider the licensing capacity of your Web Conferencing server and determine which groups or individuals should have the capability to schedule meetings that utilize the full meeting room.

Files for license keys that you may add or upgrade are made available to you when you purchase a new Cisco Unified MeetingPlace system or upgrade to the current release. These files are loaded into your Cisco Unified MeetingPlace 8100 series server when it is purchased. To add additional web conferencing licenses to the Audio Server, refer to the “About Loading Cisco Unified MeetingPlace License Keys” section in the “Managing and Maintaining Cisco Unified MeetingPlace” chapter of the applicable *Administration Guide for Cisco Unified MeetingPlace Audio Server* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html.

Installing SQL Server on a Remote Server

Cisco Unified MeetingPlace Web Conferencing requires SQL Server. You can choose to install SQL Server on either the same machine as Web Conferencing or on a separate machine. If you choose to install SQL Server on the same machine as Cisco Unified MeetingPlace Web Conferencing, the installer will handle the installation of SQL Server 2000 and the appropriate service pack on your local system automatically; in this case, no pre-installation steps are required.

If you choose to install SQL Server on a separate machine, install both SQL Server 2000 and the appropriate service pack on a separate Windows machine before installing Web Conferencing. This can be a Cisco MCS or legacy non-Cisco MCS.

**Note**

Check *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html for the required service pack.


Gathering Web Conferencing Installation Values

Gather and record the information in [Table 2-1](#) to prepare for your installation of Cisco Unified MeetingPlace Web Conferencing.

Table 2-1 Installation Values for Cisco Unified MeetingPlace Web Conferencing

Parameter	Description and Value
Hostname of MeetingPlace Server	<p>This parameter refers to the Cisco Unified MeetingPlace Audio Server system hostname. If you are installing multiple web servers that share a database and point to the same Audio Server system, make sure that the Audio Server hostname on all of these web servers match.</p> <p>Note If a connection exists between the web server and the Audio Server system—that is, if there is no firewall between them, port 5003 is not blocked, and the Audio Server system is up and running—then you can use an IP address instead of a hostname. However, using an IP address prevents you from taking advantage of the Audio Server system’s reverse connection feature, which allows the Audio Server system to initiate a connection to the web server when port 5003 is blocked inbound.</p> <p>Hostname:</p> <p>IP address:</p> <p>Notes:</p>
Location of web server	<ul style="list-style-type: none"> Internal (Full Access)—Cisco Unified MeetingPlace Web Conferencing is installed with all features enabled, and this server is placed inside your corporate network. In Segmented Meeting Access-2 Server (SMA-2S) deployments, this server functions as the internal web server. External (Limited Access)—Cisco Unified MeetingPlace Web Conferencing is installed with attend-only capability. In SMA-2S deployments, this server is placed outside your corporate firewall in an Internet-accessible network, such as a DMZ, and functions as the external web server. <p>(For more information on SMA configurations, see the “Installing Web Conferencing for a Segmented Meeting Access Configuration” chapter.)</p> <p>Web server location:</p> <p>Notes:</p>

Table 2-1 Installation Values for Cisco Unified MeetingPlace Web Conferencing (continued)

Parameter	Description and Value
Hostname or static IP address of web server	<p>After installing the operating system on the web server, you will enable two IP interfaces for the server on the same subnet. During installation of the Web Conferencing software, you will enter the information for the primary IP interface. List either the primary IP address of the web server or the hostname associated with this IP address.</p> <p>Web server primary hostname:</p> <p>Web server primary IP address:</p> <p>Notes:</p>
Location of SQL Server 2000 database	<p>If you are installing SQL Server 2000 on the web server, enter Local Server.</p> <p>If you are pointing the web server to a version of SQL Server previously installed on a separate machine, enter Existing Remote Server.</p> <p>If you are connecting to a remote SQL Server, also enter its hostname or IP address.</p> <p>SQL Server location:</p> <p>(Optional) Remote SQL Server hostname:</p> <p>(Optional) Remote SQL Server IP address:</p> <p>Notes:</p>
Your SQL Server 2000 user name and password	<p>If you are completing a new installation of Cisco Unified MeetingPlace Web Conferencing with a local install of the SQL Server, use sa as your user name.</p> <p> Caution The Web Conferencing installer does not create or verify the existence of the SQL account or check the validity of its user name and password combination. If the Web Conferencing installer will be installing SQL Server locally on the Web Conferencing server, you must use sa as the user name. To ensure that the Web Conferencing server functions correctly after installation, we strongly recommend that you use sa as the user name during the installation even if you have preinstalled SQL Server on a remote server. After the installation, you can configure a least-privileged SQL account and configure Web Conferencing to use this account instead.</p> <p>Note You must enter a password. Web Conferencing does not support a blank password. The password you enter during this installation will override any blank or previously entered SQL Server password.</p> <p>User name:</p> <p>Password:</p> <p>Notes:</p>

Installation Tasks: Web Conferencing

The Cisco Unified MeetingPlace Web Conferencing installation is completed in three parts:

1. [Installing the Operating System on the Cisco MCS Server, page 2-5](#)
2. [Configuring Network Settings on the Cisco MCS Server, page 2-5](#)
3. [Installing Web Conferencing, page 2-9](#)

Installing the Operating System on the Cisco MCS Server

Before you begin, confirm that your system meets the network and system requirements. (Refer to *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.)

To Install the Operating System on the Cisco MCS Server

Step 1 Dedicate a networked Cisco MCS on which to install Cisco Unified MeetingPlace Web Conferencing.

Step 2 Install the required Cisco MCS operating system on the Cisco MCS server.

The operating system CD was shipped with your Cisco Unified MeetingPlace application software.

Follow the installation procedure in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*, which is included with the operating system software. Although the document refers to Cisco Unified CallManager and other applications, it also applies to Cisco Unified MeetingPlace integration applications.



Note Return to this document before performing the Post-Installation Tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*.

Step 3 Continue with the next section, “[Configuring Network Settings on the Cisco MCS Server](#)”.

Configuring Network Settings on the Cisco MCS Server

Once the operating system is installed, you must configure the network interfaces. Cisco Unified MeetingPlace Web Conferencing has the following networking requirements:

- Two separate IP addresses are required.
- The IP addresses must be on the same network segment. (Both must be connected to the same Layer 3 subnet and the same Layer 2 Ethernet broadcast domain.)
- The two IP interfaces cannot share the same hostname or be aliased to each other in DNS. (Hostnames are only required if the server will be configured for Secure Sockets Layer.)

Cisco Unified MeetingPlace Web Conferencing supports assigning the two required IP addresses by using the following Network Interface Card (NIC) configurations:

<p>One NIC enabled and configured with two IP addresses; second NIC is disabled</p>	<ul style="list-style-type: none"> • Only utilizes one of the two NICs on the system. • The NIC is a single point of failure. • This configuration is available for both HP and IBM MCS server models • To configure this option, perform the “To Configure a Single NIC with Both IP Addresses on the Cisco MCS Server” procedure on page 2-7.
<p>Both NICs enabled, one IP address per NIC</p>	<ul style="list-style-type: none"> • Each NIC on the system is used, although one NIC may be more heavily used than the other. • Each NIC is a single point of failure. If either NIC fails, Web Conferencing will be unavailable. • If the Web Conferencing server is connected to a 100 MB/sec. network, the NIC capacity may be exceeded in large meetings with heavy application sharing. • This configuration is available for both HP and IBM MCS server models. • To configure this option, perform the “To Configure One IP Address per NIC on the Cisco MCS Server” procedure on page 2-8.

<p>Both NICs enabled, teamed, configured in Transmit Load Balancing (TLB) mode</p>	<ul style="list-style-type: none"> • The two NICs act together to handle traffic for both IP addresses; one NIC receives inbound traffic, both NICs send outbound traffic. • If either NIC fails, the other NIC can take over. • We strongly recommend this configuration if the Web Conferencing server is connected to a 100 MB/sec. network. • This configuration is available only for HP MCS server models. • To configure this option, perform the “To Configure NIC Teaming on the Cisco MCS Server (HP Models Only)” procedure on page 2-8
<p>Both NICs enabled, teamed, configured in Network Fault Tolerance (NFT) mode</p>	<ul style="list-style-type: none"> • One NIC is active, handling traffic for both IP addresses. • The other NIC is passive and takes over if the primary NIC fails. • This configuration is available only for HP MCS server models. • To configure this option, perform the “To Configure NIC Teaming on the Cisco MCS Server (HP Models Only)” procedure on page 2-8

To Configure a Single NIC with Both IP Addresses on the Cisco MCS Server

- Step 1** Follow the procedure for “Configuring Network Settings” in the post-installation tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*. In this procedure, configure the primary NIC on the system with a static IP address and with DNS, WINS, or the LMHosts file for hostname resolution.
- Step 2** Add the secondary IP address to the primary NIC:
- On the Start menu, click **Settings > Network Connections**.
 - Right-click **Local Area Connection**, then click **Properties**.
 - Double-click **Internet Protocol (TCP/IP)**.
 - Click **Advanced**.
 - On the IP Settings tab, in the IP Addresses area, click **Add**.
 - Enter the secondary IP address and subnet mask and click **Add**.
 - Click **OK** three times to close the Local Area Connection Properties window.
- Step 3** (Optional) Continue performing the post-installation tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*.



Note We highly recommend that you configure the duplex of your network adapters for Full Duplex (either 100/Full or 1000/Full, as applicable). Autonegotiation may impact Web Conferencing traffic flow.

Step 4 Proceed to the [“Installing Web Conferencing” section on page 2-9](#).

To Configure One IP Address per NIC on the Cisco MCS Server

Step 1 Follow the procedure for “Configuring Network Settings” in the post-installation tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*. In this procedure, configure the primary NIC on the system with a static IP address and with DNS, WINS, or the LMHosts file for hostname resolution.

Step 2 Repeat [Step 1](#) for the secondary NIC on the system, using a different IP address on the same subnet, with the same subnet mask and default gateway. If you receive a warning about using the same default gateway, click OK to accept the warning and continue.

Step 3 Enable the secondary NIC:

- a. On the Start menu, click **Settings > Network Connections**.
- b. Right click **Local Area Connection 2** and click **Enable**.

Step 4 (Optional) Continue performing the post-installation tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*.



Note We highly recommend that you configure the duplex of your network adapters for Full Duplex (either 100/Full or 1000/Full, as applicable). Autonegotiation may impact Web Conferencing traffic flow.

Step 5 Proceed to the [“Installing Web Conferencing” section on page 2-9](#).

To Configure NIC Teaming on the Cisco MCS Server (HP Models Only)


Step 1 Follow the procedure for “Configuring Network Settings” in the post-installation tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*. In this procedure, configure the primary NIC on the system with a static IP address and with DNS, WINS, or the LMHosts file for hostname resolution.



Note If you are using the LMHosts file for hostname resolution, add an entry for both the primary and secondary IP addresses and hostnames.

Step 2 Enable the secondary NIC:

- a. On the Start menu, click **Settings > Network Connections**.
- b. Right click **Local Area Connection 2** and click **Enable**.

- Step 3** Configure network teaming by using the HP Network Configuration Utility, available by choosing **Start > Settings > Control Panel > HP Network**. Refer to the HP Network Configuration Utility online help for instructions.
- Step 4** Add the primary IP address to the NIC team:
- On the Start menu, click **Settings > Network Connections**.
 - Right-click **Local Area Connection 3**, then click **Properties**.
 - Double-click **Internet Protocol (TCP/IP)**.
 - Click **Use the following IP address**; in the appropriate fields, enter the server primary IP address, subnet mask, and default gateway that you used in [Step 1](#).
 - If you configured DNS or WINS for the primary NIC by using the procedure in [Step 1](#), repeat the procedure for the team. If you configured the LMHosts file, skip to [Step 5](#) substep d.
- Step 5** Add the secondary IP address to the NIC team:
- On the Start menu, click **Settings > Network Connections**.
 - Right-click **Local Area Connection 3**, then click **Properties**.
 - Double-click **Internet Protocol (TCP/IP)**.
 - Click **Advanced**.
 - On the IP Settings tab, in the IP Addresses area, click **Add**.
 - Enter the secondary IP address and subnet mask and click **Add**.
 - Click **OK** three times to close the Local Area Connection Properties window.
- Step 6** Verify that the team is configured correctly:
- On the Start menu, click **Run**.
 - Type **cmd** and press **Enter**. The command window opens.
 - Type **ipconfig /all** and press **Enter**. The connection information displays in the command window. The Local Area Connection 3 (for the network team) should show two IP addresses.
- Step 7** (Optional) Continue performing the post-installation tasks in *Installing the Operating System on the Cisco Unified Communications Server (version 2003.1.1 or later)*.
-  **Note** We highly recommend that you configure the duplex of your network adapters for Full Duplex (either 100/Full or 1000/Full, as applicable). Autonegotiation may impact Web Conferencing traffic flow.
- Step 8** Proceed to the [“Installing Web Conferencing” section on page 2-9](#).

Installing Web Conferencing

The Cisco Unified MeetingPlace Web Conferencing executable takes approximately 45 minutes to install the following components:

- Cisco Unified MeetingPlace Gateway SIM.
- Cisco Unified MeetingPlace Web Conferencing software. This requires an automatic reboot.

- (If the local server option is chosen) SQL Server 2000. This requires an automatic reboot.
- (If the local server option is chosen) The appropriate release of the SQL Server 2000 service pack. This requires an automatic reboot.
- Cisco Unified MeetingPlace Web Conferencing engine. This requires an automatic reboot.

Note that there are a total of four automatic reboots if you are installing SQL Server 2000 locally, or two if you are using a remote SQL server.

**Note**

Check *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html for the required SQL Server 2000 service pack.

**Note**

The installation executable disables antivirus software for the duration of the installation.

Before You Begin

- Confirm that the Cisco MCS server is configured with the correct time zone and daylight savings time settings. The installation may fail if you do not configure the system to automatically observe daylight savings time in a time zone that requires it.
- Confirm that your installation drive has sufficient disk space to allow for the storage of applications, attachments, recordings, and meeting and profile database information, which will grow over time. (Refer to *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.)
- Confirm that the Cisco Unified MeetingPlace 8100 series server has Cisco Unified MeetingPlace Audio Server Release 6.0 or later installed.
- Have the information that you gathered in the “[Gathering Web Conferencing Installation Values](#)” section on page 2-3 available.
- Complete the “[Installing the Operating System on the Cisco MCS Server](#)” section on page 2-5.

Restriction

We do not support installing or upgrading to Web Conferencing Release 6.x by using Terminal Services.

**Caution**

Do not interrupt the server during program installation or during automatic system shutdown or reboot.

To Install Cisco Unified MeetingPlace Web Conferencing

- Step 1** Exit any open applications.
- Step 2** Insert the Cisco Unified MeetingPlace Web Conferencing DVD into the DVD-ROM drive and double-click the **CiscoUnifiedMeetingPlaceWebConferencing.exe** file to begin installation.

**Note**

The Cisco Unified MeetingPlace Web Conferencing CD contains multiple executable files. Verify that you are double-clicking the correct executable file.

- Step 3** After the install files are extracted, click **Next** and follow the instructions in the installer windows using the information you gathered in the “[Gathering Web Conferencing Installation Values](#)” section on page 2-3. Note the following considerations:
- If you enter an IP address instead of a hostname for the Audio Server system, a warning message appears regarding reverse connection.
 - If this machine is in a network segment, such as a DMZ, and you are interested in reverse connection, enter a hostname instead of an IP address, then proceed with the installation.
 - If this machine has a connection to the Audio Server system—that is, if they are in the same network segment, port 5003 is open, and the Audio Server system is running—and you are not interested in reverse connection, then use the IP address and proceed with the installation.
- Step 4** The installer installs the Gateway SIM first. When the InstallShield Wizard Complete window appears, click **Finish**. The Gateway SIM is installed.




Note If a Missing Server Version error message appears, confirm that Audio Server Release 6.0 or later is installed on the Cisco Unified MeetingPlace 8100 series server. If the correct version is installed, proceed with the Web Conferencing installation. If not, click **Cancel** and upgrade the Audio Server software to version 6.0 or later before proceeding.

- Step 5** Continue following the instructions in the installer windows using information from the “[Gathering Web Conferencing Installation Values](#)” section on page 2-3.



Note If you chose Local Server as your SQL Server location, after the first reboot, you must log in to the system as an administrator in order for the installer to begin installing SQL Server. When SQL Server installation is complete, the server reboots automatically.

During installation, remember the following information:

- If the installer detects a local SQL Server installation, after the second reboot, the installer begins installing the SQL Server service pack. When the service pack installation is complete, the server reboots automatically.
 - Installations of SQL Server and the SQL Server service pack are slow, and depending on your server hardware, installations may take 40 minutes or more to complete. Status updates appear from the Cisco Unified MeetingPlace icon in the system tray during the installation.
 - The Cisco Unified MeetingPlace icon appears as an orange door .
 - If the SQL Server installation appears to be taking too long (over 35 minutes), check Task Manager to confirm that SQLInstall.exe is running.
 - After the server reboots, the installer invokes SQLInstall.exe to create the MPWEB SQL database. This process may take 5 to 10 minutes.
 - After creating the database and installing the Web Conferencing engine, the server reboots automatically.
- Step 6** After the final automatic reboot (the fourth reboot if you are installing SQL Server 2000 locally, or the second if you are using a remote SQL server), open the Gateway SIM event log to monitor Web Conferencing application activities.
- While the system is coming up, you should see the event text, “Waiting for Connect.”
 - When the Web Conferencing engine is ready, you should see response text similar to the following:

```
MPConnect (0x14B0) Debug: Response: <?xml version="1.0" encoding="utf-8"?>
<results><status code="ok" /></results>
```

Step 7 Continue with the next section, “[Postinstallation Tasks: Web Conferencing](#).”

Postinstallation Tasks: Web Conferencing

We recommend that you complete the following optional tasks as applicable after installing the web conferencing software:

- [Defining the Web Conferencing Server Hostname Information, page 2-12](#)
- [Testing the Web Conferencing Installation, page 2-13](#)
- [Installing the Cisco Security Agent for Cisco Unified MeetingPlace Web Conferencing, page 2-14](#)
- [Creating and Using a Least-Privileged SQL Account for Web Conferencing, page 2-14](#)
- [Configuring SSL, page 2-16](#)

Defining the Web Conferencing Server Hostname Information

If you want users to be able to access the Web Conferencing server by using the fully qualified domain name (FQDN) of the server, or if you plan to configure SSL for this server, do the following procedure.



Note

If the web server is not in a Domain Name Server (DNS), do not perform this procedure.

To Define the Cisco Unified MeetingPlace Web Conferencing Server Hostname Information

- Step 1** Open your web browser, and enter the URL of your web server.
- For internal web servers, the default URL structure is `http://<server>`, where `<server>` is the name of your internal web server.
- For external web servers, the default URL structure is `http://<server>/mpweb/admin/`, where `<server>` is the name of your external web server.
- Step 2** When the Web Conferencing home page appears, sign in by using your System Manager-level user ID and password, then click **Sign In Now**.
- If you are on an internal web server, the Welcome page appears with your name displayed at the top. To access the administrative page, click **Admin**.
- If you are on an external web server, the administrative page appears.
- Step 3** From the Admin page, click **Web Server**.
- Step 4** From the View section of the page, click the name of the web server that you want to configure.
- Information about this web server populates the Edit section of the page.
- Step 5** For Hostname [Home Page], enter the fully qualified domain name (FQDN) of the primary network interface on the web server, for example, **hostname.domain.com**. Note the following considerations:
- To use SSL, you must enter the FQDN.

- This hostname must be resolvable by its intended users. (For details, see the “[Testing the Web Server Home Page Connection](#)” section on page 2-13.)
- Step 6** For Hostname [Web Conferencing], enter the FQDN of the secondary network interface on the web server, for example, **hostnamewc.domain.com**. Note the following considerations:
- To use SSL, you must enter the FQDN.
 - This hostname must be resolvable by its intended users. (For details, see the “[Testing the Meeting Console Connection](#)” section on page 2-13.)
- Step 7** Click **Submit**.
-

Testing the Web Conferencing Installation

After you install Cisco Unified MeetingPlace Web Conferencing, test the installation by completing the following tasks:

1. [Testing the Web Server Home Page Connection, page 2-13](#)
2. [Testing the Meeting Console Connection, page 2-13](#)

Testing the Web Server Home Page Connection

Confirm that the web server can resolve itself using the hostname configured on the Web Server administrative page. This is the hostname that you configured in [Step 5](#) of the preceding section, “[Defining the Web Conferencing Server Hostname Information](#),” and is also the hostname that end users use to connect to this web server.

To Test the Web Server Home Page Connection

- Step 1** From the web server, use a web browser to connect to **http://hostname.domain.com**, the Fully Qualified Domain Name, or FQDN, of the web server.
- or
- If the web server is not in a Domain Name Server (DNS), use a web browser to connect to an IP address from the web server.
- Step 2** If the Cisco Unified MeetingPlace Web Conferencing home page appears, the connection is successful. If an error message appears, see the “[Server Connection Problems](#)” section on page 5-3
-

Testing the Meeting Console Connection

To Test the Meeting Console Connection

- Step 1** From an end-user system, open a web browser and enter the Cisco Unified MeetingPlace Web Conferencing URL in the address field and click **Enter**.
- Step 2** Sign in by using your System Manager-level user ID and password.
- Step 3** From the Welcome page, click **Schedule Meeting**.

- Step 4** From the New Meeting scheduling page, fill in your meeting details, then click **Schedule**.
- Step 5** Return to the Welcome page and enter the meeting ID of the meeting you just scheduled, then click **Attend Meeting**.
- Step 6** Confirm that the meeting console loads properly.
-

Installing the Cisco Security Agent for Cisco Unified MeetingPlace Web Conferencing

For instructions on installing the Cisco Security Agent, refer to the applicable *Release Notes for Cisco Security Agent for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

Creating and Using a Least-Privileged SQL Account for Web Conferencing

By default, the Cisco Unified MeetingPlace Web Conferencing installer suggests using the SQL built-in sa administrator account as the SQL Server user name. Often, a strong password for the sa account is sufficiently secure to protect your system from unauthorized access. However, if you do not want to continue to use a SQL account that has full administration rights after the installation is complete, you can create a SQL account with minimal privileges that is dedicated to Web Conferencing use, and configure the Web Conferencing server to use this account.

To create and use a least-privileged SQL account, do the following tasks in the order presented:

1. [Creating a Least-Privileged SQL Account for Web Conferencing, page 2-14](#)
2. [Updating SQL Account Access from the MeetingPlace Gateway Configurations Utility, page 2-15](#)

Creating a Least-Privileged SQL Account for Web Conferencing



Caution

If you choose to create a SQL account that is dedicated to Web Conferencing use, ensure that it meets all the specified database role requirements in this procedure. Failure to do so can cause a database connection failure between Web Conferencing and the SQL Server and result in a total outage or broken features.



Note

If Cisco TAC determines that your SQL account does not meet requirements, you will be asked to reconfigure your SQL account and to delete any existing Cisco Unified MeetingPlace Web Conferencing database so that a new database can be created once the account problem is remedied.

To Create a Least-Privileged SQL Account for Web Conferencing

- Step 1** Open the SQL Server Enterprise Manager and create a new login:
- a. On the Start menu, click **Programs > SQL Server 2000 > Enterprise Manager**.
 - b. Click a server group to expand it, then click the name of a server.

- c. Click **Security** to expand it.
 - d. Click **New Login**. The SQL Server Login Properties window opens.
 - Step 2** On the General tab, enter a name for the login.
 - Step 3** Click **SQL Server Authentication**, then enter a password for the account.
 - Step 4** In the Database drop-down menu, click **MPWEB** to set the MPWEB database as the default database.
 - Step 5** Click the **Database Access** tab.
 - Step 6** Specify the database roles for the MPWEB database:
 - a. In the Databases table, click the check box for the **MPWEB** database.
 - b. In the Database Roles table, click the check boxes for the following roles:
 - **db_datareader**
 - **db_datawriter**
 - **db_ddladmin**
 - Step 7** Repeat [Step 6](#) for each additional MPWEB slave database. The slave databases have names that begin with “MPWEB_”. Depending on your deployment, your SQL Server will have either one or two slave databases.
 - Step 8** Click **OK** to complete the account configuration.
-

Updating SQL Account Access from the MeetingPlace Gateway Configurations Utility

The MeetingPlace Gateway Configurations utility allows you to update the web server with the least-privileged SQL login account that you created in the [“To Create a Least-Privileged SQL Account for Web Conferencing” procedure on page 2-14](#). It does not create a SQL Server login for you.

To Update SQL Account Access from the MeetingPlace Gateway Configurations Utility

- Step 1** Stop the Cisco Unified MeetingPlace Web Conferencing Service:
 - a. From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
 - b. Right-click Cisco Unified MeetingPlace Web Conferencing and choose **Stop**.
 - c. (Optional) To stop other Cisco Unified MeetingPlace gateway services, including Gateway SIM, right-click the service and choose **Stop**.
 - d. If the IIS Admin Service is still running, right-click the service and choose **Stop**.
 - e. Close the Services control panel.
- Step 2** Open the MeetingPlace Gateway Configurations utility:
 - a. From your system tray, right-click the Cisco Unified MeetingPlace icon.
 - b. Choose **Properties**.
- Step 3** Click the **Web Conferencing** tab.
- Step 4** For Server, enter the hostname or IP address of the SQL Server you want to update. For a local server, enter **local**.

- Step 5** For Username and Password, enter the login account username and password you applied to the SQL Server in the “[To Create a Least-Privileged SQL Account for Web Conferencing](#)” procedure on page 2-14.
- Step 6** Click **OK**.
- Step 7** Restart the Cisco Unified MeetingPlace Web Conferencing Service:
- a. From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
 - b. Right-click Cisco Unified MeetingPlace Web Conferencing and choose **Start**.
 - c. If you stopped any other gateway services, restart them by right-clicking the applicable service and choosing **Start**.
 - d. Close the Services control panel.
-

Configuring SSL

For instructions on configuring SSL, refer to the “Configuring External Access to Cisco Unified MeetingPlace Web Conferencing” chapter of the *Configuration Guide for Cisco Unified MeetingPlace Web Conferencing, Release 6.x* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html.



Installing Web Conferencing for a Segmented Meeting Access Configuration

Cisco Unified MeetingPlace Web Conferencing supports a segmented meeting access configuration that allows you to provide external access to your users while maintaining network security. Although you can provide external access to Cisco Unified MeetingPlace web conferences by simply opening ports in your firewall, we do not recommend this option because it lacks security.

This chapter contains the following sections:

- [About Segmented Meeting Access, page 3-1](#)
- [Preinstallation Tasks: Web Conferencing in an SMA-2S Configuration, page 3-4](#)
- [Installation Tasks: Web Conferencing in an SMA-2S Configuration, page 3-5](#)
- [Postinstallation Tasks: Web Conferencing in an SMA-2S Configuration, page 3-6](#)



Note

Before reviewing this chapter, please read *System Requirements for Cisco Unified MeetingPlace Release 6.0* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.

About Segmented Meeting Access

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. SMA configurations 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.

Typically, a Cisco MCS is placed in the demilitarized zone, or DMZ, a network segment created between the private corporate network and the Internet to host meetings for external access.



Note

The Segmented Meeting Access-1 Server (SMA-1S) configuration supported in previous releases of Cisco Unified MeetingPlace Web Conferencing is no longer supported in Release 6.x.

The following sections describe the supported SMA configurations:

- [About the SMA-2S Configuration, page 3-2](#)
- [About the SMA-2S Configuration with SSL and Segmented DNS, page 3-3](#)

- [About the SMA-2S Configuration and Video-Enabled Systems, page 3-4](#)

About the SMA-2S Configuration

**Note**

For requirements, refer to the “Segmented Meeting Access Requirements” sections of *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/us/products/sw/ps5664/ps5669/prod_installation_guides_list.html. New installations of Cisco Unified MeetingPlace Web Conferencing Release 6.0 require a Cisco MCS.

In the Segmented Meeting Access-2 Servers (SMA-2S) 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 DMZ. The internal server or cluster is accessible only from behind the firewall, while the external server or cluster is accessible from inside or outside the firewall.

While internal users have access to the full-access Web Conferencing user interface, external users have access to an attend-only web page that allows attendance only to external meetings.

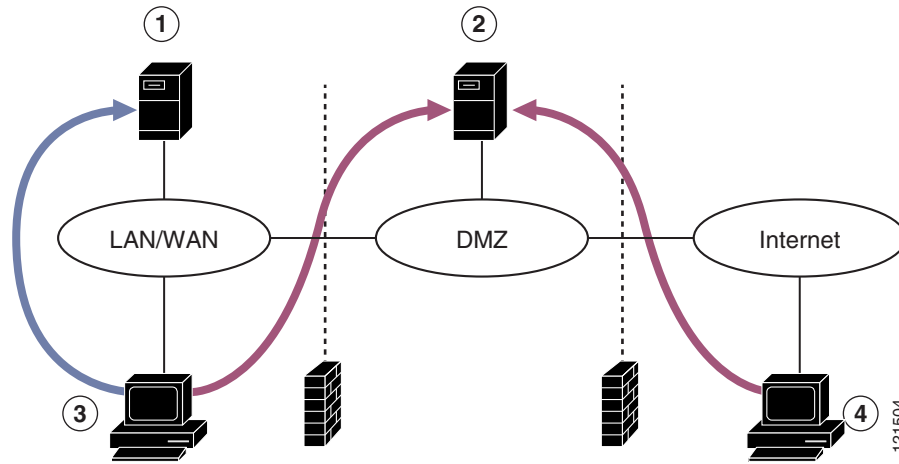
The SMA-2S configuration is the preferred and most secure deployment model if you want to provide external access to Cisco Unified MeetingPlace web conferences.

We highly 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 conference. (For more information, refer to the “Configuring External Access to Cisco Unified MeetingPlace Web Conferencing” chapter of the *Configuration Guide for Cisco Unified MeetingPlace Web Conferencing* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html.)

**Note**

If you configure SSL on an external web server and users will access the 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 server.

Figure 3-1 Segmented Meeting Access-2 Server Configuration



<p>1 Internal Cisco Unified MeetingPlace web server This web server sits inside the private corporate network.</p>	<p>2 External Cisco Unified MeetingPlace web server This web server sits in a network segment, such as a DMZ.</p>
<p>3 Internal user</p> <ul style="list-style-type: none"> • Internal users enter internal meetings through the internal web server. • Internal users enter external meetings through the external web server. 	<p>4 External user</p> <ul style="list-style-type: none"> • External users can enter external meetings only. • Users enter these meetings through the external web server.

About the SMA-2S Configuration with SSL and Segmented DNS

If your Cisco Unified MeetingPlace Web Conferencing 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 machine. See the following example for configuration guidelines.

Example

You have an SMA-2S configuration in which SSL is required for external users but is not required for internal users who are accessing the internal or external machine.

- The segmented DNS name is meetingplace.company.com.
- The SSL certificate name for the external machine is meetingplace1.company.com.
- The hostname for the external machine from the internal machine 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 machine will automatically redirect them to HTTPS plus whatever hostname is configured in the database—in this case, meetingplace1.



Note

If you force SSL on all users, both internal and external users will be forced to use SSL when they access the external web server.

About the SMA-2S Configuration and Video-Enabled Systems

In a Segmented Meeting Access-2 Server (SMA-2S) deployment, note the following considerations:

- If the Video Integration is deployed on the internal web server, users can schedule internal video-enabled meetings from the web. Requests to schedule external video meetings are denied. (In this case, users must make sure the Allow External Web Participants parameter on the New Meeting scheduling page is set to No.)
- If the Video Integration is deployed on the external web server, users can schedule external video meetings from the web. Requests to schedule internal video meetings are denied. (In this case, users must make sure the Allow External Web Participants parameter on the New Meeting scheduling page is set to Yes.)

Preinstallation Tasks: Web Conferencing in an SMA-2S Configuration

**Note**

If you are installing either an internal cluster or external cluster as part of your SMA-2S deployment, see [Chapter 4, “Installing Web Conferencing in a Load Balancing Configuration”](#) and follow the preinstallation, installation, and post-installation tasks in that chapter rather than the tasks in this chapter.

Before attempting to install Cisco Unified MeetingPlace Web Conferencing, refer to *System Requirements for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html for updated system requirements.

After reviewing system requirements, complete the following preinstallation tasks:

1. Install and configure the Audio Server, which will be used by both the internal and external servers. See the [“Installing Cisco Unified MeetingPlace Audio Server”](#) section on page 2-2.
2. Determine the licenses needed for Web Conferencing. See the [“Planning Web Conferencing License Usage”](#) section on page 2-2.
3. Determine the SQL Server instances that the internal and external Web Conferencing servers will be using. SQL Server can be installed locally on the web server or remotely on a separate, dedicated SQL server; however, the internal and external Web Conferencing servers must use separate SQL Server instances.

For the internal server, complete the following tasks:

4. If you will be using a remote SQL Server instance for the internal server, install it. See the [“Installing SQL Server on a Remote Server”](#) section on page 2-2.
5. Gather the values needed for the installation of the internal server. This must be a Cisco MCS inside your private corporate network. See the [“Gathering Web Conferencing Installation Values”](#) section on page 2-3

For the external server, complete the following tasks:

6. If you will be using a remote SQL Server instance for the external server, install it. See the [“Installing SQL Server on a Remote Server”](#) section on page 2-2.

7. Gather the values needed for the installation of the external server. This must be a Cisco MCS in a network segment, such as a DMZ. See the [“Gathering Web Conferencing Installation Values” section on page 2-3](#).

Installation Tasks: Web Conferencing in an SMA-2S Configuration

1. Install the operating system on the internal web server. See the [“Installing the Operating System on the Cisco MCS Server” section on page 2-5](#).
2. Configure network settings on the internal web server. See the [“Configuring Network Settings on the Cisco MCS Server” section on page 2-5](#).
3. Install the Web Conferencing software on the internal web server. For Server Location, choose **Internal (Full Access)**. See the [“Installing Web Conferencing” section on page 2-9](#).
4. Install the operating system on the external web server. See the [“Installing the Operating System on the Cisco MCS Server” section on page 2-5](#).
5. Configure network settings on the external web server. See the [“Configuring Network Settings on the Cisco MCS Server” section on page 2-5](#).
6. Copy the GUIDS from the internal web server to the external server, and run the file on the external server to install registry entries. See the [“Copying GUIDS from the Internal Web Server to the External Web Server” section on page 3-5](#).
7. Install the Web Conferencing software on the external web server. For Server Location, choose **External (Limited Access)**. See the [“Installing Web Conferencing” section on page 2-9](#).

Copying GUIDS from the Internal Web Server to the External Web Server

The GUIDS entries for site and system must match between the internal and external web servers. Make sure that you run the GUIDS.reg file on each external web server before installing Cisco Unified MeetingPlace Web Conferencing.

To Copy GUIDS from the Internal Web Server to the External Web Server

-
- Step 1** Copy the **GUIDS.reg** file from the internal web server (located in the Program Files\Cisco Systems\MPWeb directory).
 - Step 2** Paste the **GUIDS.reg** file to the Temp directory on the external web server.
 - Step 3** On the external web server, double-click the **GUIDS.reg** file to install it.
 - Step 4** When prompted to add the information from the GUIDS.reg file to the registry, click **OK**.
-

Postinstallation Tasks: Web Conferencing in an SMA-2S Configuration

1. Perform the following postinstallation tasks as appropriate for both the internal and external web servers:
 - (Optional) [Installing the Cisco Security Agent for Cisco Unified MeetingPlace Web Conferencing, page 2-14](#)
 - (Optional) [Creating and Using a Least-Privileged SQL Account for Web Conferencing, page 2-14](#)
2. Configure the SMA-2S deployment. Refer to the “Configuring External Access to Cisco Unified MeetingPlace Web Conferencing” chapter of the *Configuration Guide for Cisco Unified MeetingPlace Web Conferencing* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html.



Installing Web Conferencing in a Load Balancing Configuration

This chapter describes how to install Cisco Unified MeetingPlace Web Conferencing in a load balancing configuration. It does not describe upgrades.

This chapter contains the following sections:

- [About Installing Web Conferencing in a Load Balancing Configuration, page 4-1](#)
- [About Installing Web Conferencing in a Load Balancing Configuration for Video-Enabled Systems, page 4-7](#)
- [Preinstallation Tasks: Web Conferencing in a Load Balancing Configuration, page 4-7](#)
- [Installation Tasks: Web Conferencing in a Load Balancing Configuration, page 4-9](#)
- [Postinstallation Tasks: Web Conferencing in a Load Balancing Configuration, page 4-15](#)



Note

Before reviewing this chapter, please read *System Requirements for Cisco Unified MeetingPlace Release 6.x* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.

About Installing Web Conferencing in a Load Balancing Configuration

Load balancing in Cisco Unified MeetingPlace Web Conferencing makes use of a cluster of Web Conferencing servers to spread the active meeting load, allowing you to scale the number and size of meetings that your deployment can support. It also provides failover capabilities for meetings—if one Cisco Unified MeetingPlace Web Conferencing server is unavailable or unreachable, meeting clients will reconnect to another server, even if they are currently connected to a meeting that is in progress when the connection is interrupted.

You can view the amount of web-conferencing load per server from the Web Server administrative page. This information is displayed only on internal web servers.

To configure load balancing, you should understand the following concepts in this section:

- [Restrictions for Installing Web Conferencing in a Load Balancing Configuration, page 4-2](#)
- [Web Conferencing Clusters, page 4-2](#)
- [Web Conferencing Load Balancing and Failover Capability, page 4-4](#)

- [Load Balancing Behavior with Internal and External Clusters](#), page 4-5
- [Recommendations for a Robust Cisco Unified MeetingPlace System](#), page 4-6
- [End-User Experience During Meeting Console Failover](#), page 4-6

Restrictions for Installing Web Conferencing in a Load Balancing Configuration

- Microsoft Network Load Balancing is not supported.
- Third-party web server load balancing is not supported.

Web Conferencing Clusters

With Cisco Unified MeetingPlace Web Conferencing, you can configure up to three web servers into a cluster, and you can configure clusters as either internal or external.

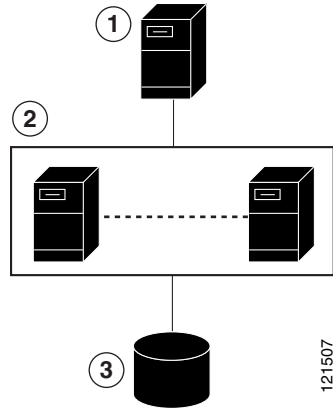
Internal cluster—Places all web servers behind the firewall inside the private corporate network. Typically, all web servers in an internal cluster display the full-access Cisco Unified MeetingPlace Web Conferencing interface

External cluster—Places all web servers between the private corporate network and the Internet, such as in a DMZ. For increased security, all web servers in an external cluster typically display the attend-only Cisco Unified MeetingPlace Web Conferencing interface.

You can attach a maximum of three web servers (including both internal and external servers) to a single Cisco Unified MeetingPlace Audio Server system. The two databases (one for the internal server or cluster, one for the external server or cluster) must have identical GUIDS.

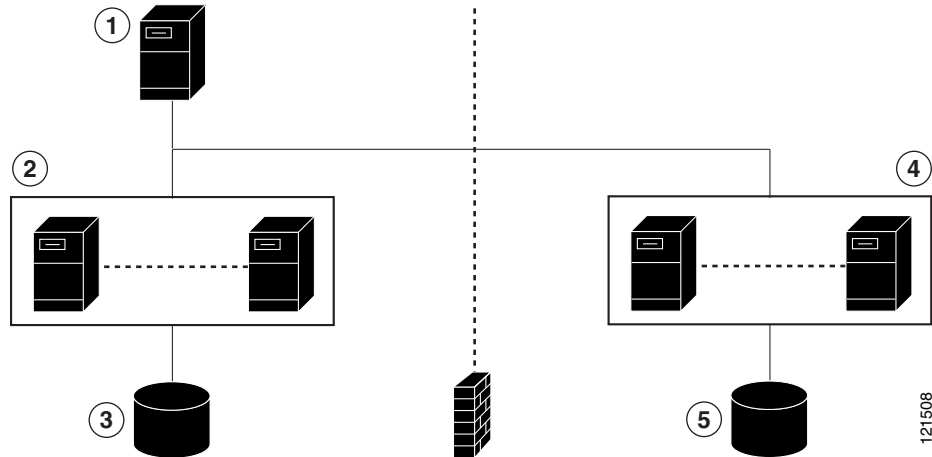
Web Conferencing supports five potential load balancing configurations, as shown in [Figure 4-1](#), [Figure 4-2](#), and [Figure 4-3](#).

Figure 4-1 One Cluster Configuration



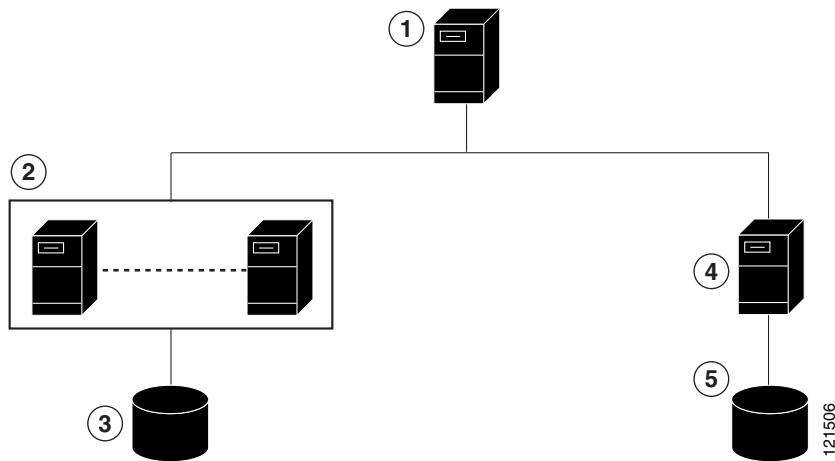
1	Cisco Unified MeetingPlace Audio Server system.	2	Cisco Unified MeetingPlace web server cluster—This can be an internal cluster or external cluster.
3	SQL Server—All web servers in a cluster must connect to the same SQL Server.		—

Figure 4-2 Mixed Configuration: Internal and External Clusters of Web Servers



1	Cisco Unified MeetingPlace Audio Server system.	2	Internal cluster of web servers.
3	SQL Server—All web servers in the internal cluster must connect to the same SQL Server.	4	External cluster of web servers.
5	SQL Server—All web servers in the external cluster must connect to the same SQL Server.		—

Figure 4-3 Mixed Configuration: One Web Server and a Cluster of Web Servers



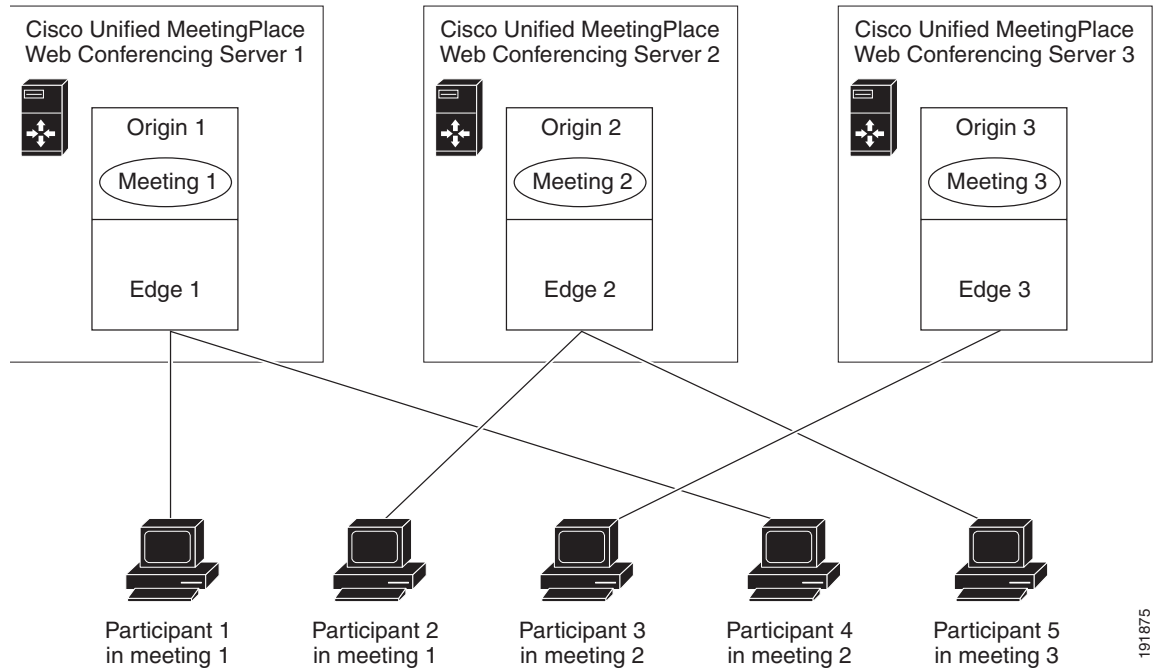
1	Cisco Unified MeetingPlace Audio Server system.	2	Cluster of web servers—This can be an internal cluster or an external cluster.
3	SQL Server—All web servers in a cluster must connect to the same SQL Server.	4	Single web server—This can be an internal or external web server.
5	SQL Server—The single web server must connect to a separate SQL Server.		—

Web Conferencing Load Balancing and Failover Capability

Each Web Conferencing server comprises two separate load balancing components, known as the origin server and edge server. Meetings are hosted on the origin server. Participants connect to the edge server when joining a meeting. These components interact to provide load balancing and failover capability as follows:

- When a meeting starts, the Web Conferencing server assigns a primary and backup origin server to the meeting room based on current active meeting load.
- As participants join the meeting, they are load balanced across the edge servers in the cluster based on the number of participants currently connected to each edge server at that time. The edge server internally makes a connection to the origin server that is hosting the meeting.
- Each client is given the primary edge/origin and backup edge/origin information by the server when the meeting room is launched. No configuration is needed on the clients.

Figure 4-4 shows an example load balancing topology with a cluster of Web Conferencing servers. Meetings are spread across the three origin servers in the cluster based on the current meeting load on each. Participants are spread across the three edge servers based on the participant load on each. Note that participants are not necessarily connected to the edge server on the machine hosting the meeting they are attending.

Figure 4-4 Web Conferencing Load Balancing for Meetings and Participants

Load Balancing Behavior with Internal and External Clusters

All users attend a Cisco Unified MeetingPlace web conference by opening their browsers and signing in through the Cisco Unified MeetingPlace Web Conference home page. When the first meeting participant attempts to join the web conference, the Cisco MeetingPlace Agent Service determines if the meeting should be held on an internal web server or external web server by checking the Allow External Web Participants parameter. This parameter is visible only if the Cisco Unified MeetingPlace system has an external site or cluster configured.

[Table 4-1](#) describes load-balancing behavior for load-balancing configuration options.

Table 4-1 Load Balancing Behavior in Cisco Unified MeetingPlace Web Conferencing

If...	Then...
Allow External Web Participants is set to No	This meeting is reserved for internal attendees only. When the first attendee launches the meeting console, Cisco Unified MeetingPlace Web Conferencing directs the web-conferencing session to the web server with the fewest currently active meetings in the internal cluster. This web server now owns the meeting. Subsequent attendees may be directed to any internal web server when they join the web conference.
Allow External Web Participants is set to Yes	<p>This meeting is accessible to external attendees, that is, participants attending from outside the firewall.</p> <p>If the first attendee attempts to join the web conference from an external web server, Cisco Unified MeetingPlace Web Conferencing directs the web-conferencing session to the web server with the fewest currently active meetings in the external cluster. This web server now owns the meeting.</p> <p>If the first attendee attempts to join the web conference from an internal web server, Cisco Unified MeetingPlace Web Conferencing determines if it has an associated external web server. Such information is found on the Web Server Properties administrative page in the DMZ Web Server field.</p> <ul style="list-style-type: none"> • If there is an entry in the DMZ Web Server field, Cisco Unified MeetingPlace Web Conferencing performs a redirection to that external server. • If Cisco Unified MeetingPlace Web Conferencing does not find an entry in the DMZ Web Server field, the web-conferencing session is directed to the least loaded internal server as described for internal meetings. All subsequent attendees are directed to an internal web server for their web conference.

Internal users can join both internal meetings and external meetings. If a meeting is designated as external, internal users who log in to an internal web server are redirected to an external web server.

External users can join only external meetings on external web servers.

Recommendations for a Robust Cisco Unified MeetingPlace System

To ensure a robust system with redundancy and failover, we recommend that you have the following:

- An internal web cluster.
- An external web cluster.
- A dedicated remote SQL Server system for each cluster.
- Remote storage location with an appropriately sized RAID array and a comprehensive backup policy.

End-User Experience During Meeting Console Failover

When failover occurs on a system that is configured for redundancy and failover, users will experience the following behavior:

1. The web server to which the participant is connected stops responding (for example, the computer loses power or the Web Conferencing services are shut down).
2. Users who are connected to the edge server on that web server lose their connection to the meeting.

3. Each meeting console client automatically tries to reconnect the user to the edge server. If this attempt fails, the meeting console attempts to connect to the edge server designated as the backup for that meeting. (The Web Conferencing server sends the assigned primary and backup edge server information to each client when the client first connects to a meeting.)

About Installing Web Conferencing in a Load Balancing Configuration for Video-Enabled Systems

If your Cisco Unified MeetingPlace Audio Server system is licensed for video, all of the web servers connected to it will display video-related fields. These fields appear on the following pages for those users who have video scheduling privileges:

- New Meeting scheduling page
- Meeting Details pages
- Account Basics page

In order for users to schedule their video meetings on a web server in a load balancing configuration, you must install the Cisco Unified MeetingPlace Video Integration on the server. Users receive an error if they attempt to reserve video ports while scheduling a meeting on a server which does not have the Video Integration installed.

Although in a load balancing configuration you install the Cisco Unified MeetingPlace Video Integration on each web server that users will use to schedule video meetings, you activate the Video Integration on only one web server in the cluster. We recommend that you activate the Video Integration on a server that is not used for scheduling, in order to minimize the load on the server.

If a meeting is scheduled with video ports reserved, video features will be available for end-users who use their video endpoints to dial in to the meeting regardless of which server hosts the meeting. If a meeting is scheduled without video ports reserved, ad hoc video may be available for end-users who dial in with a video endpoint if video ports are available at the time of the meeting.

Preinstallation Tasks: Web Conferencing in a Load Balancing Configuration

Before You Begin

- Read the [“About Installing Web Conferencing in a Load Balancing Configuration”](#) section on page 4-1.
- If applicable, read the [“About Installing Web Conferencing in a Load Balancing Configuration for Video-Enabled Systems”](#) section on page 4-7.

Complete the following tasks, as applicable, before you begin the installation:

- [Preparing the Internal Cluster, page 4-8](#)
- [Preparing the External Cluster, page 4-8](#)

Preparing the Internal Cluster

Before You Begin

Review the “Load Balancing Requirements” section in *System Requirements for Cisco Unified MeetingPlace* at

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html.

To Prepare the Internal Cluster

Step 1 Determine and create a common domain Windows administration account.

This account is used by all of the web servers in this cluster. It starts Web Conferencing services and allows all web servers in this cluster to access the shared storage location by using a Universal Naming Convention (UNC) path.

After creating the account, write down the value, which you will need later.



Note Enter different values for your internal and external clusters.

Step 2 Determine and create a shared storage location.

You can create this folder on the same machine as your first internal web server, or on a separate machine. Keep in mind that this shared storage location is where attachments are stored and, therefore, where all web servers in this cluster go to find attachments.

After creating the location, write down the value as a UNC path, for example, \\servername\shared folder\MPWeb.

Preparing the External Cluster

Before You Begin

(Optional) Read the “[Installing Web Conferencing for a Segmented Meeting Access Configuration](#)” chapter to understand the difference between internal and external servers.

To Prepare the External Cluster

Step 1 Determine and create a common domain Windows administration account.

This account is used by all of the web servers in this cluster. It starts Web Conferencing services and allows all web servers in this cluster to access the shared storage location using a UNC path.

After creating this account, write down the value, which you will need later.



Note Enter different values for your internal and external clusters.

Step 2 Determine and create a shared storage location.

You can create this folder on the same machine as your first external web server, or on another machine. Keep in mind that this shared storage location is where attachments are stored and, therefore, where all web servers in this cluster go to find attachments.

After creating the location, write down the value as a UNC path, for example, \\servername\shared folder\MPWeb.

Installation Tasks: Web Conferencing in a Load Balancing Configuration

The installation is completed in six parts:

- [Installing the First Internal Web Server, page 4-9](#)
- [Installing Additional Internal Web Servers, page 4-10](#)
- [Copying GUIDS from the Internal to the External Web Server, page 4-11](#)
- [Installing the First External Web Server, page 4-12](#)
- [Installing Additional External Web Servers, page 4-13](#)
- [Linking the Internal and External Servers, page 4-14](#)

Installing the First Internal Web Server

Before You Begin

- Read the “[Installing Web Conferencing](#)” chapter and have it available to assist you with this section.
- Complete the “[Preparing the Internal Cluster](#)” section on page 4-8.

To Install the First Internal Web Server

- Step 1** Install Cisco Unified MeetingPlace Web Conferencing on the first internal machine.
- For Server Location, choose **Internal (Full Access)**.
 - For Database Location, choose the applicable option:
 - If there is a full SQL Server installed elsewhere, choose **Existing remote server**.
 - To have the installer install SQL Server 2000 on this machine for you, choose **Local server**.
 - When you reach the final installer window, choose to reboot your computer later, then click **Finish**.
- Step 2** Configure the shared storage for this web server by performing the following sub-steps:
- a. Open your web browser to access the Web Conferencing home page.
 - b. Use your System Manager-level user ID and password to sign in.
 - c. Click **Admin**, then **Shared Storage**.
 - d. For Enabled, click **Yes**.
 - e. For Shared Storage Path, enter the path of the shared storage location that you determined in [Step 2](#) of the “[To Prepare the Internal Cluster](#)” procedure on page 4-8.

- f. For Content Cache Size, enter a value between 0 and 100 for the percentage of total disk space to use to cache content on the local server.
- g. In the appropriate fields, enter a domain, username, and password for a Windows account that will be used to access the shared storage location. If the account is a local account, enter the machine name in the Domain field.



Note All Cisco Unified MeetingPlace Web Conferencing services will be configured to "Log On As" the account you choose in this sub-step.

- h. Re-enter the password in the Confirm Password field.
- i. Click **Save Changes**.
- j. To put the changes into effect, click Reboot Server, then click **OK** to confirm the reboot. The server shuts down and restarts.

Step 3 Continue with the next task as applicable:

- If you have additional internal web servers, see the [“Installing Additional Internal Web Servers” section on page 4-10](#).
 - If you do not have additional internal web servers, see the [“Copying GUIDS from the Internal to the External Web Server” section on page 4-11](#).
-

Installing Additional Internal Web Servers

Before You Begin


Complete the [“Installing the First Internal Web Server” section on page 4-9](#).

Restrictions

When installing two or more web servers that share a single database and point to the same Cisco Unified MeetingPlace Audio Server system, the MeetingPlace Server hostname that you specify during the installation of all web servers must match. By default if the MeetingPlace Server hostnames do not match, a second site is created with a WebConnect configuration.

To Install Additional Internal Web Servers

-
- Step 1** Copy the **GUIDS.reg** file from the first internal web server to the next machine in your internal cluster:
- a. Copy the *drive:\Program Files\Cisco Systems\MPWeb\GUIDS.reg* file from the first server.
 - b. Place the **GUIDS.reg** file in the next web server’s *drive:\Temp* directory.
 - c. On the next web server, double-click the **GUIDS.reg** file to install it.
 - d. When prompted to add the information from the GUIDS.reg file to the registry, click **OK**.
- Step 2** Install Cisco Unified MeetingPlace Web Conferencing on the next machine in your internal cluster.
- For Server Location, choose **Internal (Full Access)**.
 - For Database Location, choose **Existing remote server** and specify the SQL Server that you used in the [“Installing the First Internal Web Server” section on page 4-9](#).

- Step 3** Configure the shared storage for this web server by performing the following sub-steps:
- On the Web Conferencing server, open a web browser and browse to **http://localhost:8002**. When you access this URL on the server, you are automatically signed in to Cisco Unified MeetingPlace Web Conferencing as a technician.
 - Click **Admin**, then **Shared Storage**.
 - In the appropriate fields, enter a domain, username, and password for a Windows account that will be used to access the shared storage location. If the account is a local account, enter the machine name in the Domain field.
-  **Note** All Cisco Unified MeetingPlace Web Conferencing services will be configured to "Log On As" the account you choose in this sub-step.
- Re-enter the password in the Confirm Password field.
 - Click **Save Changes**.
 - To put the changes into effect, click Reboot Server, then click **OK** to confirm the reboot. The server shuts down and restarts.
- Step 4** Repeat this procedure until you have installed all of your internal web servers.
- Step 5** Continue with the [“Copying GUIDS from the Internal to the External Web Server”](#) section on page 4-11.

Copying GUIDS from the Internal to the External Web Server

The GUIDS entries for site and system must match between internal and external web servers. Make sure that you run the GUIDS.reg file on each external web server before installing Cisco Unified MeetingPlace Web Conferencing.



Caution

You must complete this step before running the Web Conferencing installer on the external web server. If this step is skipped or completed incorrectly, Presentation mode will not work for internal users in external meetings, and recovering from this problem requires that you rebuild the SQL Server database.

Before You Begin

Complete installing and configuring at least one internal Cisco Unified MeetingPlace web server.

To Copy GUIDS from the Internal to the External Web Server

- Step 1** Copy the **GUIDS.reg** file from the first internal web server (located in *drive:\Program Files\Cisco Systems\MPWeb*).
- Step 2** Place the **GUIDS.reg** file in the first external web server's *drive:\Temp* directory.
- Step 3** On the external web server, double-click the **GUIDS.reg** file to install it.
- Step 4** When prompted to add the information from the GUIDS.reg file to the registry, click **OK**.
- Step 5** Continue with the [“Installing the First External Web Server”](#) section on page 4-12.

Installing the First External Web Server

Before You Begin

- Read the “[Installing Web Conferencing](#)” chapter and have it available to assist you with this section.
- Complete the “[Preparing the External Cluster](#)” section on page 4-8.
- Complete the “[Copying GUIDS from the Internal to the External Web Server](#)” section on page 4-11.



Note The GUIDS entries for site and system must match between internal and external web servers. Make sure that you run the GUIDS.reg file on each external web server before installing Cisco Unified MeetingPlace Web Conferencing.

To Install the First External Web Server

- Step 1** Install Cisco Unified MeetingPlace Web Conferencing on the first web server in your external cluster.
- For Server Location, choose **External (Limited Access)**.
 - For Database Location, choose the applicable option:
 - If the SQL Server is installed locally, choose **Local Server**.
 - If there is a full SQL Server installed elsewhere, choose **Existing Remote Server**.
 - When you reach the final installer window, choose to reboot your computer later, then click **Finish**.
- Step 2** Configure the shared storage for this web server by performing the following sub-steps:
- a. Open your web browser to access the Web Conferencing home page.
 - b. Use your System Manager-level user ID and password to sign in.
 - c. Click **Admin**, then **Shared Storage**.
 - d. For Enabled, click **Yes**.
 - e. For Shared Storage Path, enter the path of the shared storage location that you determined in [Step 2](#) of the “[To Prepare the External Cluster](#)” procedure on page 4-8.
 - f. For Content Cache Size, enter a value between 0 and 100 for the percentage of total disk space to use to cache content on the local server.
 - g. In the appropriate fields, enter a domain, username, and password for a Windows account that will be used to access the shared storage location. If the account is a local account, enter the machine name in the Domain field.



Note All Cisco Unified MeetingPlace Web Conferencing services will be configured to "Log On As" the account you choose in this sub-step.

- h. Re-enter the password in the Confirm Password field.
- i. Click **Save Changes**.
- j. To put the changes into effect, click Reboot Server, then click **OK** to confirm the reboot. The server shuts down and restarts.



- Step 3** If you have additional external web servers, continue with the “[Installing Additional External Web Servers](#)” section on page 4-13.
- If you do not have additional external web servers, continue with the “[Linking the Internal and External Servers](#)” section on page 4-14.
-

Installing Additional External Web Servers

Before You Begin

- Complete the “[Installing the First External Web Server](#)” section on page 4-12

To Install Additional External Web Servers

- Step 1** Copy the **GUIDS.reg** file from the first external web server to the next external web server:
- a. Copy the *drive:\Program Files\Cisco Systems\MPWeb\GUIDS.reg* file from the first server.
 - b. Place the **GUIDS.reg** file in the next web server’s *drive:\Temp* directory.
 - c. On the next web server, double-click the **GUIDS.reg** file to install it.
 - d. When prompted to add the information from the GUIDS.reg file to the registry, click **OK**.
-  **Note** The GUIDS entries for site and system must match between internal and external web servers. Make sure that you run the GUIDS.reg file on each external web server before installing Cisco Unified MeetingPlace Web Conferencing.
-
- Step 2** Install Cisco Unified MeetingPlace Web Conferencing on the next external web server.
- For Server Location, choose **External (Limited Access)**.
 - For Database Location, choose **Existing remote server** and specify the SQL Server used in the “[Installing the First External Web Server](#)” section on page 4-12.
 - When you reach the final installer window, choose to reboot your computer later, then click **Finish**.
- Step 3** Configure the shared storage for this web server by performing the following sub-steps:
- a. On the Web Conferencing server, open a web browser and browse to **http://localhost:8002**. When you access this URL on the server, you are automatically signed in to Cisco Unified MeetingPlace Web Conferencing as a technician.
 - b. Click **Admin**, then **Shared Storage**.
 - c. In the appropriate fields, enter a domain, username, and password for a Windows account that will be used to access the shared storage location. If the account is a local account, enter the machine name in the Domain field.
-  **Note** All Cisco Unified MeetingPlace Web Conferencing services will be configured to "Log On As" the account you choose in this sub-step.
-
- d. Re-enter the password in the Confirm Password field.
 - e. Click **Save Changes**.

- f. To put the changes into effect, click Reboot Server, then click **OK** to confirm the reboot. The server shuts down and restarts.

Step 4 Repeat this procedure until you have installed all the external web servers.

Step 5 Continue with the “[Linking the Internal and External Servers](#)” section on page 4-14.

Linking the Internal and External Servers

External meetings are held on an external web server so that users can access their meetings from the Internet. Rather than have all of your users log in to a particular external web server, configure automatic redirection of all external meetings from your internal web servers to a designated external web server.

The internal and external servers (or clusters of servers) each operate as completely separate units until you link them by configuring automatic redirection.

Before You Begin

You must have properly installed Cisco Unified MeetingPlace Web Conferencing on all of your internal and external web servers.

To Configure Redirection of External Meetings

Step 1 From an internal web server, sign in to Cisco Unified MeetingPlace Web Conferencing.

Step 2 From the Welcome page, click **Admin**, then **Web Server**.

Step 3 From a blank Web Server Name field, enter the name of a new web server to represent your designated external web server.

Step 4 For Hostname, enter the fully qualified domain name (FQDN) of your external web server (for example, *hostname.domain.com*). If your web server is not in a Domain Name Server (DNS), enter the IP address instead. Note the following considerations:

- You must be able to resolve this hostname from the internal web server.
- If you plan to use SSL, make sure that the hostname on the SSL certificate resolves to the external web server’s IP address.
- If you plan to use SSL and a segmented DNS, make sure that the DNS name and the SSL certificate name differ.

Step 5 To add this web server to the database, click **Submit**.

This server now appears as part of your list of web servers on the bottom portion of the page.

Step 6 If you have only one internal web server and one external web server, you are finished with this procedure.

If you have more than one internal web server, continue with [Step 7](#).

Step 7 Return to the main Admin page and click **Site**.

The Site administrative page appears.

Step 8 Click the Site Name that represents your cluster of internal web servers. Note the following considerations:

- There should be only one site indicated on this page unless you deployed WebConnect.

- Site Name should have a default value equal to the NetBIO name of the first web server you installed in this cluster.

Step 9 For DMZ Web Server, choose the external web server you just added.

This configures the internal web servers in this cluster to point to this external web server in the case of external meetings.

Step 10 Click **Submit**.



Tip The external cluster does not require any additional SQL Server database configurations.

Step 11 (Optional) If one of your web servers has Cisco Unified MeetingPlace Video Integration activated, review the information on load balancing video-enabled systems in the “[About Installing Web Conferencing in a Load Balancing Configuration for Video-Enabled Systems](#)” section on page 4-7.

Postinstallation Tasks: Web Conferencing in a Load Balancing Configuration

This section contains information on the following tasks:

- [Synchronizing Purge Parameters](#), page 4-15
- [Configuring SSL \(Optional\)](#), page 4-15
- [Viewing the Web Conferencing Load on a Server](#), page 4-16

Synchronizing Purge Parameters

When you install multiple web servers, make sure that you synchronize the Purge parameters. For more information, see the “About the MeetingNotes Purge Parameter and SMA-2S Configurations” section in the “Configuring Cisco Unified MeetingPlace Web Conferencing for Optimal Data Storage” chapter of the *Configuration Guide for Cisco Unified MeetingPlace Web Conferencing* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html.

Configuring SSL (Optional)

Refer to the “How to Configure Secure Sockets Layer” section in the “Configuring External Access to Cisco Unified MeetingPlace Web Conferencing” chapter of the *Configuration Guide for Cisco Unified MeetingPlace Web Conferencing* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html.

Viewing the Web Conferencing Load on a Server

The amount of web conferencing load on a web server is indicated in the Current Server Load Index field as a number between 0 and 1. This number is a weighed average among several factors, such as CPU, memory, and disk usage. The higher the value, the heavier the load on this web server.

To View the Web Conferencing Load on a Server

Step 1 Sign in to Cisco Unified MeetingPlace Web Conferencing.

Step 2 From the Welcome page, click **Admin**, then **Web Server**.

Step 3 From the View section of the page, locate the web server you want to view.

The amount of web-conferencing load on this web server is indicated in the Current Server Load Index field.



Troubleshooting the Web Conferencing Installation

This chapter describes how to troubleshoot common problems that can occur while installing Cisco Unified MeetingPlace Web Conferencing.

This chapter contains the following sections:

- [Installation Problems, page 5-1](#)
- [Server Connection Problems, page 5-3](#)
- [Meeting Room Connection Problems, page 5-3](#)

Installation Problems

This section contains the following information:

- [What to Do First, page 5-1](#)
- [Checking That the Cisco MCS Operating System Version Meets the Requirement, page 5-2](#)
- [Obtaining Additional Assistance, page 5-3](#)

What to Do First

If the web server is not working properly, try the following troubleshooting tasks:

1. Restart the Cisco Unified MeetingPlace Web Conferencing services:
 - a. From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
 - b. Right-click **Cisco MeetingPlace Web Conferencing** and choose **Start**.
 - c. If you stopped any other gateway services, reboot them by right-clicking the service and choosing **Start**.
 - d. Close the Services control panel.
2. If the server is still not working properly, check the debug log for a possible time zone/daylight savings setting problem. Perform the [“To Check For a Time Zone/Daylight Savings Time Conflict” procedure on page 5-2](#).
3. If the server is still not working properly, reboot the server.

4. If the server is still not working properly, run the Cisco Unified MeetingPlace Web Conferencing installer again in Repair mode.
5. If the server is still not working properly, collect the following installation logs and contact your Cisco support representative:
 - mpwebstp.log
 - mpwebstp-sql.log
 - mpwebstp-sql2ksp4.log

Web Conferencing installation logs are in the C:\Winnt directory.

To Check For a Time Zone/Daylight Savings Time Conflict

- Step 1** In Windows Explorer, browse to the <drive>:\Program Files\Cisco Systems\MPWeb\WebConf\logs\support directory.
- Step 2** Open the **debug.log** file.
- Step 3** Look for a pair of messages similar to the following:
- ```
brze (d) <status code="invalid"><invalid field="time-zone-id" type="id"
subcode="missing" /></status>
brze (d) com.macromedia.airspeed.StatusException$Invalid$Missing: <status
code="invalid"><invalid field="time-zone-id" type="id" subcode="missing" /></status>
```
- Step 4** If you see these messages, open the Date and Time Properties window by double-clicking the system time in the Windows menu bar. If all of the areas in your time zone regularly observe daylight savings time, you may need to check **Automatically Adjust Clock for Daylight Saving Changes**.
- Step 5** If you made changes to the date and time properties, restart the Cisco Unified MeetingPlace Web Conferencing services:
- e. From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
  - f. Right-click **Cisco MeetingPlace Web Conferencing** and choose **Start**.
  - g. If you stopped any other gateway services, reboot them by right-clicking the service and choosing **Start**.
  - h. Close the Services control panel.
- 

## Checking That the Cisco MCS Operating System Version Meets the Requirement

You must have the required operating system version installed on a Cisco MCS before attempting to install Cisco Unified MeetingPlace Web Conferencing. Refer to *System Requirements for Cisco Unified MeetingPlace Release 6.0* at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html).

#### To Check That the Cisco MCS Operating System Version Meets the Requirement

---

- Step 1** From the Windows Start menu, click **Cisco OS Version**. The MCS Version Utility opens.

- Step 2** In the OS Image field, verify the operating system version.
  - Step 3** Click **OK** to close the MCS Version Utility.
- 

## Obtaining Additional Assistance

If there is a problem with a Windows service or the web server loses its connection, go to the *drive:\Program Files\Cisco Systems\MPWeb\datasvc* directory and run *Dcdiags.bat* as soon as possible to generate a server log. All diagnostic information is stored in the *Cisco Systems\MPWeb\Diagnostics* directory.

Zip these files, and send them to your Cisco support representative for additional assistance.

## Server Connection Problems

The web server must be able to connect to itself by using the hostname you configured on the Web Server administrative page. This is also the hostname used by end users to connect to this web server.

Connection problems are most likely caused by firewall-related configurations.

The following procedure uses *hostname.domain.com* as an example. Replace *hostname.domain.com* with your web server's actual FQDN.

### To Resolve HTTP Connection Problems

---

- Step 1** From the web server, use a web browser to connect to *http://hostname.domain.com*.
  - Step 2** If you receive an error message, add the following line to the *C:\WINNT\System32\drivers\etc\hosts* file:  
**127.0.0.1 hostname.domain.com**
  - Step 3** Try to connect to *http://hostname.domain.com* again.
- 

## Meeting Room Connection Problems

If users are not able to access the full meeting room after upgrading the Audio Server from a previous release, it is possible that the Full Web Conferencing Ports setting on the Audio Server is incorrect. Perform the following procedure to configure the Full Web Conferencing Ports setting to match the number of web conferencing licenses available on your Audio Server.

### To Configure the Full Web Conferencing Ports Setting

---

- Step 1** Start MeetingTime and log in to the Cisco Unified MeetingPlace Audio Server.
- Step 2** Click **Administration > Configure**.
- Step 3** Click **Server Configuration**, then click **Query**.
- Step 4** Click the value for **Full Web Conferencing Ports** and enter the number of web conferencing licenses purchased.

**Step 5** Click **OK**.

**Step 6** Click **Save Changes**.

---



## APPENDIX **A**

# Uninstalling Web Conferencing or SQL Server Software

---

This appendix contains the following sections:

- [Uninstalling Web Conferencing Software, page A-1](#)
- [Uninstalling SQL Server Software and Removing MPWEB SQL Database Files, page A-1](#)

## Uninstalling Web Conferencing Software

### To Uninstall Web Conferencing Software

---

- Step 1** From the Windows Start menu, choose **Settings > Control Panel > Add/Remove Programs**.
  - Step 2** From the Add/Remove Programs window, click **Cisco Unified MeetingPlace Web Conferencing**.
  - Step 3** Click **Change/Remove**.
  - Step 4** When prompted to completely remove Web Conferencing and all its components, click **Yes**.
  - Step 5** From Windows Explorer, manually delete the storage locations for converted audio files (for example, drive:\wma\_files).
- 

## Uninstalling SQL Server Software and Removing MPWEB SQL Database Files

If you are no longer using SQL Server for any other applications, you can uninstall it manually.

### Restrictions

Uninstalling SQL Server does not remove the MPWEB SQL database files. To completely remove all database files associated with Cisco Unified MeetingPlace Web Conferencing, you must manually locate and delete the files.

### To Remove SQL Server Software

---

- Step 1** From the Windows Start menu, choose **Settings > Control Panel > Administrative Tools > Services**.
- Step 2** Stop the **Microsoft SQL Server** service.
- Step 3** From the Start menu, choose **Settings > Control Panel > Add/Remove Programs**, then choose **Microsoft SQL Server**.
- Step 4** Click **Remove**.
- Step 5** Reboot the server.
-



---

## A

account, least privileged SQL, creating [2-14](#)

### Audio Server

hostname [2-3](#)

installation requirement [2-2](#)

---

## B

### behavior

failover [4-6](#)

load balancing [4-5](#)

load balancing in video-enabled systems [4-7](#)

---

## C

checking, Cisco MCS operating system version [5-2](#)

### Cisco MCS

operating system, installing [2-5](#)

operating system version, checking [5-2](#)

product key [2-5](#)

Cisco MeetingPlace Agent service, about [1-4](#)

Cisco Unified MeetingPlace, about [1-1](#)

### clusters

#### external

about [4-2](#)

common administration account (load balancing) [4-8](#)

common storage location (load balancing) [4-8](#)

preparing (load balancing) [4-8](#)

#### internal

about [4-2](#)

common administration account (load balancing) [4-8](#)

common storage location (load balancing) [4-8](#)

preparing (load balancing) [4-8](#)

### common administration account

external cluster (load balancing) [4-8](#)

internal cluster [4-8](#)

### common storage location

external cluster (load balancing) [4-8](#)

internal cluster (load balancing) [4-8](#)

components installed with Web Conferencing [2-9](#)

### configuring

redirection of external meetings (load balancing) [4-14](#)

### connections

HTTP problems, resolving [5-3](#)

tunnel, about [1-5](#)

### copying

GUIDS from internal to external web server [4-11](#)

GUIDS from internal to external web server (SMA-2S) [3-5](#)

### creating

least privileged SQL account [2-14](#)

---

## D

defining web server [2-12](#)

demilitarized zone. *See* DMZ

DMZ, about [3-1](#)

---

## E

endpoints, common [1-3](#)

### external clusters

about [4-2](#)

common administration account (load balancing) [4-8](#)

- common storage location (load balancing) [4-8](#)
- preparing (load balancing) [4-8](#)
- external web servers
  - copying GUIDS to (load balancing) [4-11](#)
  - installing additional (load balancing) [4-13](#)

---

## F

- fully qualified domain name, entering [2-12](#)

---

## G

- Gateway System Integrity Manager (SIM), installing [2-11](#)
- GUIDS
  - copying from internal to external web server (load balancing) [4-11](#)
  - copying from internal to external web server (SMA-2S) [3-5](#)

---

## H

- hostnames
  - Audio Server [2-3](#)
  - SQL Server [2-4](#)
  - web server [2-4](#)
- HTTP
  - connection, testing web server [2-13](#)
  - resolving connection problems [5-3](#)

---

## I

- icon, Cisco Unified MeetingPlace [2-11](#)
- installation
  - Audio Server requirement [2-2](#)
  - gathering values [2-3](#)
  - tasks [2-5](#)
  - Terminal Services restriction [2-10](#)
  - testing [2-13](#)
- installing

- additional external web servers (load balancing) [4-13](#)
- additional internal web servers (load balancing) [4-10](#)
- first external web server (load balancing) [4-12](#)
- first internal web server (load balancing) [4-9](#)
- operating system on Cisco MCS [2-5](#)
- SQL Server on remote server, about [2-2](#)
- troubleshooting [5-1](#)
- Web Conferencing
  - software [2-9](#)

### internal clusters

- about [4-2](#)
- common administration account (load balancing) [4-8](#)
- common storage location (load balancing) [4-8](#)
- preparing (load balancing) [4-8](#)

### internal web servers

- additional, installing (load balancing) [4-10](#)
- copying GUIDS from (load balancing) [4-11](#)
- first, installing (load balancing) [4-9](#)

- IP address, web server [2-4](#)

---

## L

- load, viewing web conferencing on server (load balancing) [4-16](#)
- load balancing
  - about [4-1](#)
  - behavior [4-5](#)
  - configuring
    - redirection of external meetings [4-14](#)
  - copying GUIDS from internal to external web server [4-11](#)
  - failover [4-6](#)
  - installation tasks [4-9](#)
  - installing
    - additional external web servers [4-13](#)
    - additional internal web servers [4-10](#)
    - first external web server [4-12](#)
    - first internal web server [4-9](#)

- mixed cluster and single configuration, illustration [4-3](#)
- mixed cluster configuration, illustration [4-3](#)
- one cluster configuration, illustration [4-3](#)
- postinstallation tasks [4-15](#)
- preinstallation tasks [4-7](#)
- preparing external cluster [4-8](#)
- preparing internal cluster [4-8](#)
- recommendations for robust system [4-6](#)
- restrictions [4-2](#)
- video-enabled systems [4-7](#)
- viewing web conferencing load on server [4-16](#)
- Web Conferencing clusters, about [4-2](#)

#### locations

- SQL Server [2-4](#)
- web server [2-3](#)

---

## M

#### meeting console

- common endpoint [1-3](#)
- connection, testing [2-13](#)

#### meetings

- external, configuring redirection of (load balancing) [4-14](#)
- reliability, about [1-4](#)

---

## N

NetMeeting, common endpoint [1-3](#)

network security, about [1-4](#)

---

## O

operating system, installing on Cisco MCS [2-5](#)

---

## P

preinstallation tasks [2-1, 3-4](#)

product key, Cisco MCS [2-5](#)

---

## R

#### redirection

- external meetings, configuring (load balancing) [4-14](#)

remote server, about installing SQL Server [2-2](#)

#### removing

- SQL Server software [A-1](#)
- Web Conferencing software [A-1](#)

#### restrictions

- installing additional internal web servers (load balancing) [4-10](#)
- installing Web Conferencing in load balancing configuration [4-2](#)

---

## S

Secure Socket Layer. *See* SSL

#### security

- network, about [1-4](#)
- SMA-2S configuration [3-2](#)

Segmented Meeting Access. *See* SMA

server-based conferencing, about [1-3](#)

#### SMA

- about [3-1](#)
- video meetings, considerations [3-4](#)

#### SMA-2S configuration

- about [3-2](#)
- illustration [3-3](#)
- with SSL and segmented DNS [3-3](#)

software, installing Web Conferencing [2-9](#)

#### SQL Server

- hostname [2-4](#)
- installing on remote server, about [2-2](#)
- least privileged account, creating [2-14](#)
- location [2-4](#)
- removing software [A-1](#)
- username [2-4](#)

## SSL

SMA-2S configuration with segmented DNS [3-3](#)

**T**

## tasks

installation [2-5](#)  
 installation for load balancing [4-9](#)  
 postinstallation for load balancing [4-15](#)  
 preinstallation [2-1, 3-4](#)  
 preinstallation for load balancing [4-7](#)  
 testing installation [2-13](#)

Terminal Services, installation restriction [2-10](#)

terms of use, Web Conferencing [1-7](#)

## testing

meeting console connection [2-13](#)  
 web server over HTTP connection [2-13](#)

## troubleshooting

checking Cisco MCS operating system version [5-2](#)  
 installation problems [5-1](#)  
 server connection problems [5-3](#)

tunnel connection, about [1-5](#)

**U**

## uninstalling

SQL Server software [A-1](#)  
 Web Conferencing software [A-1](#)

username, SQL Server [2-4](#)

**V**

## video meetings

load balancing, behavior [4-7](#)  
 load balancing considerations [4-7](#)  
 SMA considerations [3-4](#)

**W**

## Web Conferencing

about [1-1](#)  
 benefits [1-3](#)  
 Cisco MeetingPlace Agent service [1-4](#)  
 common endpoints [1-3](#)  
 components, overview [1-2](#)  
 connecting procedure [1-5](#)  
 fulfilling user requests, illustration [1-5](#)  
 meeting reliability [1-4](#)  
 network security [1-4](#)  
 server based [1-3](#)  
 terms of use [1-7](#)

components installed with [2-9](#)

software, installing [2-9](#)

software, uninstalling [A-1](#)

web conferencing load, viewing (load balancing) [4-16](#)

## web servers

copying GUIDS from internal to external (SMA-2S) [3-5](#)

defining [2-12](#)

## external

installing additional (load balancing) [4-13](#)

installing first (load balancing) [4-12](#)

hostname or static IP address [2-4](#)

location [2-3](#)

testing over HTTP connection [2-13](#)

troubleshooting connection [5-3](#)

viewing web conferencing load on (load balancing) [4-16](#)