Main page: Cisco Unified MeetingPlace Release 8.5

One page up: System Requirements

Print PDF: Cisco Unified MeetingPlace Release 8.5 -- Print System Requirements

The following information assumes that you are migrating to Cisco Unified MeetingPlace Release 8.5 from a previous release. Release 8.5 does not support deployments with MeetingPlace-scheduling for new installations. If you are completing a new installation for an audio-only deployment, see system requirements for Audio-Only deployments.

The MeetingPlace-scheduling deployment supports a maximum of two nodes in an active/standby configuration.

Contents

Hardware and Software Requirements

Note: Cisco Unified MeetingPlace Release 8.5 does not support interoperability between different releases. All servers within a system must be running the same version of software.

MeetingPlace-scheduled deployments require the following components:

Component	Requirement

Cisco Unified MeetingPlace Application Server	**Hardware** See the Application Server Requirements. The Cisco Unified MeetingPlace Application Server WebEx TSP supports SOCKS Web Proxy servers (HTTP proxy). Allow direct firewall access to WebEx Site IPs directly. Note that there are often delay is proxy servers are used. Make sure that the integration to Cisco WebEx is continuously maintained via I without delays, otherwise it will affect user response times. **Software** • Cisco Unified MeetingPlace Application Server Release 8.5/Express Media Server (EMS) • Cisco Security Agent Release 6.0.1.112 **Notes:** • One Application Server is deployed as "Primary" and one optionally deployed as "Standby" (m deployment is not supported with the MeetingPlace-scheduling model) • The Cisco Unified MeetingPlace integration for Microsoft Outlook scheduling is included on th Server. • The Express Media Server is a set of software modules that reside on the Application Server. D installation, you will have the option to choose either the Hardware Media Server or the Expres Server. For details about the EMS, see the Express Media Server Requirements. • The Cisco Security Agent software is packaged and installed during the Application Server inst details, see the "Using Cisco Security Agent (CSA) on the Application Server" in the *Configura for Cisco Unified MeetingPlace Release 8.5* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configurat
Cisco Unified Communications Manager	**Hardware** Cisco Media Convergence Server (MCS) • Make sure that the specific Cisco MCS model supports the number of SIP sessions that are requ Cisco Unified MeetingPlace system. • For information about physically installing the Cisco MCS, see the documentation at this locati http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_installation_guides_list.html **Software** • CUCM 6.1(5), 7.0(2), 7.1(5), 8.0(1), 8.0(2), 8.0(3), 8.5(1), 8.6(1), 9.0(1), 9.1(1) • CUCM-SME 7.1(3), 8.0, 8.5 **Notes:** • CUCM 9.1(1) is supported in Cisco Unified MeetingPlace Release 8.5.5. • CUCM 8.6 is supported in Cisco Unified MeetingPlace Release 8.5.2 and later. • Ad-hoc (SCCP) meetings are supported in Cisco Unified MeetingPlace Release 8.5.2 and later. meetings are not supported with CUCM 8.5.

	• CUCM 8.0(3) is the only release that supports SIP Refers for multinode Cisco Unified Meeting (WebEx-scheduling deployments). If you require this support, open a case with Cisco TAC aga Unified Communications Manager to obtain the latest Engineering Special (ES) or Service Upd version of CUCM 8.0(3).
Hardware Media Server (HMS)	If your deployment requires a HMS, see the Hardware Media Server Requirements. • During installation, you will have the option to choose either the Hardware Media Server or the Media Server. You do not require both. • The Hardware Media Server should be on the same local network segment as the Application S Unified MeetingPlace does not support Hardware Media Server blades that are remotely located
MeetingPlace Conference Manager	Java JRE 6.0 or later and Java Web Start **Note:** For best performance, we recommend that you install the latest Java JRE.
Cisco Unified MeetingPlace Web Server	**Hardware** See the Web Server Requirements. **Software** • Cisco Unified MeetingPlace Web Server Release 8.5 • (Optional) Cisco Security Agent Release 6.0.1.117 for Cisco Unified MeetingPlace • (Customer provided option) McAfee VirusScan Enterprise 8.0 or 8.5 **SQL Server** • Microsoft SQL Server 2008 Express Edition and .NET Framework 3.5 SP1 This version is included with Cisco Unified MeetingPlace Web Release 8.5 and is supp SQL Server deployments. • Microsoft SQL Server 2008 Standard Edition This version is supported for remote SQL Server deployments only. **Notes:** • You must install and configure your SQL Server to be case-insensitive. If you configure your S be case-sensitive, the Web Server will not function properly. • All SQL Servers are required to be local to the Cisco Unified MeetingPlace server that is handli replication. SQL Servers can be ?remote? in that they are installed on separate machines within center. However, this release of Cisco Unified MeetingPlace does not support attaching to an S remote data center.

	Additional Requirements • Make sure that all corporate fonts and standard Microsoft fonts, including Microsoft PowerPoin installed. • Web Server software does not support "thin clients" (Citrix or Terminal Server).
Cisco WebEx Node **Note:** This is an optional component.	**Hardware** Release 8.5 supports Cisco WebEx Node for both MCS/UCS and ASR. If your deployment requires a C Node, see the Cisco WebEx Node Requirements. • Cisco WebEx Node does not support any HTTP or SOCKS proxy servers. Allow direct accesss Site IPs directly through firewall settings. • Cisco WebEx Node is currently not supported with the WebEx Global Site Backup system. If y fully redundant option with GSB, submit a new WebEx Node request to WebEx Provisioning to redundant node that is ?homed? to the GSB data center instead of the primary. You must deploy UCS with the Cisco WebEx Node for MCS software for this function in your network. **Software** Cisco WebEx Node Release 8.5
Cisco WebEx integration	• Cisco WebEx Meeting Center, Cisco WebEx Meeting Center Pro, or Cisco WebEx Enterprise E (supports Meeting Center, Event Center and Training Center) ♦ Event Center and Training Center are not supported on Apple Mac systems. ♦ Event Center supports the Audio Broadcast feature that reduces the need for all particip into a MeetingPlace audio meeting. Connection to the audio system is limited to those p designated as Speakers. All other attendees receive the audio, video, and web conferenc components in multiple HTTPS streams via their PC. • WebEx Business Suite (WBS)27 SP27 or later • WebEx XML API Release 5.7 or later • WebEx Federated SSO is supported with WebEx XML API. For information about WebEx Fed see http://developer.webex.com/web/meetingservices/sso **Notes:** • If your site is on a version earlier than WBS 27 SP25, contact your Cisco WebEx Customer Sup (CSE) to request an upgrade to the minimum version required for use with Cisco Unified Meeti Release 8.5. • You must have both WBS 27 SP27 and WebEx XML API Release 5.7 or later to use the WebEx-MeetingPlace Automatic Configuration feature. • WBS27 FR23 and later offers a new capability for supporting Dual Audio vendors on the same For more information, see the "New Features" section of the *Release Notes for Cisco Unified M Release 8.5*. The WebEx end-user client interface supports any HTTP or SOCKS proxy server based on browser sett

Cisco Unified MeetingPlace PhoneView	Cisco Unified MeetingPlace PhoneView is available only to Cisco Unified IP Phones that are registered Unified Communications Manager. Cisco Unified MeetingPlace PhoneView is not supported with the following: • Cisco Unified CallManager Express • Cisco Unified Communications Manager Express • Cisco Unified MeetingPlace Web Servers with SSL enabled • Cisco Unified MeetingPlace Application Servers with SSL enabled **Hardware** For a list of supported Cisco Unified IP Phones, see Audio Endpoint Compatibility.
Video options	See Video Requirements.

Failover Requirements

To configure failover, you need two Application Servers with a high-speed network connection (preferably 100Mpbs or better) between them. Failover configuration requires the following:

- When you configure the Application Server for the Express Media Server, both the primary and secondary failover Express Media Servers must have the same licenses and port distribution for scheduled and ad-hoc meetings.
- The time must be synchronized between the two Application Servers. This is required to resolve conflicts when the same piece of data is modified simultaneously in both Application Servers.
- If the primary and failover Application Servers share a common set of Audio and Video Blades, you must add all the Audio Blades to both Applications Servers. Be sure to use the same passwords and SNMP community names on the two systems or the failover mechanism will not work.

Note: Directory Service between two Application Servers is not supported in a failover deployment.

Directory Services Requirement

Cisco Unified MeetingPlace Directory Service enables you to populate and synchronize the Cisco Unified MeetingPlace user database with the contents of the Cisco Unified Communications Manager (CUCM) user database, as well as provide encrypted end-user authentication. The CUCM user database is typically integrated with an LDAP directory. CUCM end-user authentication also supports secure LDAP (sLDAP) configuration. The following LDAP directories are supported by Cisco Unified Communications Manager to MeetingPlace Directory Service:

- Microsoft Windows Active Directory 2000
- Microsoft Windows Active Directory 2003
- Microsoft Windows Active Directory 2007
- Microsoft Windows Active Directory 2008
- ADAM 2003/2008 (ADLDS) with CUCM 7.1.3
- iPlanet Directory Server Version 4.*x*
- SunONE Directory Server Version 5.*1*
- Sun Java Directory Server Version 5.2
- Sun Java Directory Server Version 6.0
- OpenLDAP 2.3.39/2.4 with CUCM 7.1.3

- Novell eDirectory Release 4.x, 5.x, 6.x

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

Cisco Unified MeetingPlace Directory Service (via Cisco Unified Communications Manager LDAP integration) may also be optionally configured to work with WebEx to provide on-premises end-user authentication and automatic profile propegation to WebEx for "host" accounts. This must be requested upon provisioning of the WebEx Site at installation. The MeetingPlace to WebEx LDAP integration is called Directory Service "SSO" Single Sign On, which is optional based on customer requirements for LDAP use. No passwords are stored on WebEx nor passed to the WebEx cloud for authentication.

All "Host" users must be able to resolve to the Cisco Unified MeetingPlace Application Server fully qualified domain name (FQDN) which is deployed behind the company firewall, for instance they must be on the corporate network and VPN connection before "hosting" any meetings. If your profiled users cannot access the corporate network, then a non-Directory Service implementation is advised. MeetingPlace profiles can be exported and imported into the WebEx Site via Administration interface using Excel CSV formatted files.

To enable secure end-user authentication via MeetingPlace/WebEx SSO integration, you must install an SSL certificate on the Application Server for secure user ID and password authentication to LDAP (via Cisco Unified Communications Manager AXL interfaces). End-user authentication may also be done via the internal MeetingPlace Web Server with the following five options:

- MeetingPlace local username/password
- LDAP - this supports multidomain environments
- LDAP, then MeetingPlace - this supports single domain environments only
- Windows Integrated Authentication (WIA) - all MeetingPlace profiled users must use Windows OS and the MeetingPlace Web server must be able to join the domain.
- Third Party Authentication Servers - supports Siteminder and others
- Web HTTP

License Requirements

This release of Cisco Unified MeetingPlace uses active host-based licensing. The system uses an audit mechanism to track the number of users who have actively created meetings and compares that to the number of licenses that are installed. An alarm is raised when the number of users who create meetings exceeds the number of licenses installed.

Licenses are for both audio conferencing and standards-based video conferencing in Cisco Unified MeetingPlace.

Notes:

- System capacity is directly affected if you use Cisco Unified MeetingPlace video. For more information, see System Capacity Quick Reference Tables.
- If you have no licenses installed the system will allow only a single meeting at a time.
- If you are completing a Cisco UCS installation under VMware, note that the Cisco Unified MeetingPlace system produces a randomly generated 12-digit "MAC address" that you will require for licensing. To obtain the MAC address, make sure that you install the Meeting Directors first. You

can then obtain the randomly generated MAC address and register your license key.

Network Requirements

DNS Recommendations

- All FQDNs of Meeting Director Nodes (if applicable), Conferencing Nodes and Cisco WebEx Nodes are required for DNS resolution between all servers
- No multiple names to IPs
- Reverse IP lookup required
- Classless DNS not supported
- CUCM needs to have DNS enabled to resolve the MP hostnames for the SIP Refer commands to be sucessful.

Ports

This section lists the incoming and outgoing ports that are used by the various components of the Cisco Unified MeetingPlace Release 8.5 system. The information refers to MeetingPlace-scheduling deployment options.

Use these tables to make sure that your firewalls do not block access to Cisco Unified MeetingPlace from users or integrated systems, and to make sure that you do not block communication among the Cisco Unified MeetingPlace components and servers.

The ports that you do *not* need to expose to system administrators or end users are used for local communication between the Cisco Unified MeetingPlace elements or between Cisco Unified MeetingPlace and local services such as Cisco Unified Communications Manager or Microsoft Exchange. Such ports should be blocked in the DMZ or external firewall, but should not be blocked between internal components of the Cisco Unified MeetingPlace solution.

Note: Signaling between Cisco Unified MeetingPlace and Cisco Unified Communications Manager must be TCP.

Incoming Ports Used in MeetingPlace-Scheduling Deployments

Protocol	Source	Destination	Port Type	Ports	Port Usage	Special Requirements
Application Server/Express Media Server						
SSH	Administrator PC	Application Server	TCP	22	Secure access	Expose to system administrators
HTTP, HTTPS	Administrator PC	Application Server	TCP	80, 443	Administrator web access for both MeetingPlace Applications Admin and Cisco WebEx	Expose to system administrators

					Site Admin	
SNMP	Administrator PC	Application Server	UDP	161	SNMP configuration	Expose to system administrators; optional
MP_REPL	Application Server 1	Application Server 2	TCP	2008	Database replication between the active and standby servers for Application Server failover	Optional; only if failover is configured
GWSIM	External Web Server	Application Servers	TCP	5003, 5005	Receive attachments from the external Web Server to Application Servers (active server and standby server, if one exists) in segmented meeting access configurations.	Expose to Web Server in the DMZ. Used in segmented meeting access configurations. If you configured your network for reverse connection, where your Web Servers are configured with a Cisco Unified MeetingPlace hostname instead of an IP address, the Application Server can initiate a reverse connection to the Web Server in the DMZ when port 5003 inbound is blocked.
SIP	Cisco Unified Communications Manager (CUCM)	Application Server	TCP UDP	5060	SIP B2BUA; UDP optional	--
SIP over TLS				5061		--

	Cisco Unified Communications Manager (CUCM)	Application Server	TCP UDP		SIP B2BUA; UDP optional	
--	WebEx Node for MCS TSP (Telephony Agent)	Application Server (Telephony Adapter)	TCP	7676	Telephony service connection, exchange telephony event and so on	--
HTTP	Cisco IP Phones PhoneView XML application	Application Server	TCP	8080	HTTP services used by Cisco Unified MeetingPlace PhoneView XML on IP Phones (optional)	--
HTTP	Application Server	Hardware Media Server	TCP	9090	Media Server Administration	Expose to system administrators
SIP	External Web Server	Application Server	TCP UDP	61002	Recording signaling	-
Recording control	External Web Server	Application Server	TCP	61003	Recording control	For remote RSS servers only
HTTP	External Web Server	Application Server	TCP	61004	Communication for prompts, recordings, attachment access, and login service for remote users	Expose to Web Server in the DMZ Used in segmented meeting access configurations
RTP/RTCP	Phones, video devices, gateway	Application Server/EMS, HMS	UDP	16384-32767	Recording media for both Hardware Media Server and Express Media Server	-
Hardware Media Server						
FTP	Application Server	HMS	TCP	21	Retrieving log files	Expose to system administrators
Telnet	Application Server	HMS	TCP	23	Telnet	Expose to system administrators
HTTP	Application Server	HMS	TCP	80	Web user interface	Expose to system

						administrators
NTP	Application Server	HMS	UDP	123	Network Time Protocol	Expose to Web Server in the DMZ
SNMP	Application Server	HMS	UDP	161	SNMP configuration	Expose to system administrators
MPI	Application Server	HMS	TCP	2010	MPI (Pompa control protocol)	--
DCI	Application Server	HMS	TCP	3333	DCI (DCS control protocol)	--
XML control	Application Server	HMS	TCP	3336	XML control	--
XML cascading	Application Server	HMS	TCP	3337	XML cascading	--
File server	Application Server	HMS	TCP	3340	File server	--
SIP	Application Server	HMS	TCP UDP	5060	SIP	--
RTP/RTCP	Phones	HMS	UDP	16384-16683	Audio Media	Expose to system administrators and end users
RTP/RTCP	--	HMS	UDP	20000-21799	Video Media	Expose to system administrators and end users
Video Blade control	HMS - Audio Blade	HMS - Video Blade	TCP	2944-2945	Video Blade control (H.248)	--
SSH	--	Application Server NFS	TCP	61003	Recording control used for NFS remote mount, file system sharing between Cisco WebEx Node and MeetingPlace Application Server machine. Port numbers are configurable.	Hardware Media Server only
SSH	--	Application Server NFS	TCP	61002	Recording signaling used for NFS remote mount, file system sharing	Hardware Media Server only

					between Cisco WebEx Node and MeetingPlace Application Server machine. Port numbers are configurable.	
Web Server						
HTTP	Administrator PC	Web Server	TCP	80	Client communication for user web access	Expose to system administrators and end users For external users to participate in web meetings, access must be granted from the Internet to the Web Server in the DMZ. However, access to port 80 may be closed if the Web Server is configured for HTTPS and you open TCP port 443.
HTTPS	Administrator PC	Web Server	TCP	443	Client communication for secure user web access	(Optional) Expose to system administrators and end users. If you have external users, then grant access from the Internet to the Web Server in the DMZ.
SQL	Web Server	SQL Server database	TCP	1433	Communication between the Web Server and the SQL Server database	--
Control connection	Web Servers		TCP	5003		

		Application Servers			Control connection between Web Servers and the Application Server	Expose to Application Server
Cisco WebEx Node for MCS (including WebEx Cloud)						
HTTP/HTTPS/WebEx Meeting Protocol	Meeting client, browser	Meeting Server in Cisco WebEx Node	TCP	443	Check meeting status, internal Checking time from the NTP server	The Cisco WebEx Site will redirect to the Cisco WebEx Node if configured.
HTTP/HTTPS/WebEx Meeting Protocol	Meeting client, browser	Meeting Server in Cisco WebEx Node	TCP	443	Meeting connection, internal	--
TCP/WebEx Meeting Protocol	Meeting client	Meeting Server in Cisco WebEx Node	TCP	1270-1279	Meeting connection	Internal network use only
HTTP/WebEx Meeting Protocol	Meeting client	Meeting Server in Cisco WebEx Node	TCP	2000-2009	Meeting connection	Internal network use only
UDP SNMP	SNMP client	Cisco WebEx Node	UDP	161	SNMP events (optional)	--
NTP	Application Server	Cisco WebEx Node	UDP	123	Network Time Protocol communication	--
User PC/Phones/Gateways						
RTP/RTCP	Application Server	Cisco Unified Personal Communicator (CUPC), IP Phones, Gateways	UDP	16384-32526	Voice and video	--
Cisco Unified Communications Manager (CUCM)						
SIP	Application Server	CUCM	TCP UDP	5060	SIP	--
SIP over TLS	Application Server	CUCM	TCP UDP	5061	SIP	--
SCCP	Phones	CUCM	TCP	2000	--	--
SIP	CUPC	CUCM	TCP UDP	5060	--	--
SIP over TLS	CUPC	CUCM	TCP UDP	5061	--	--
AXL	Application Server	CUCM	TCP	8443	AXL SOAP connection	--

Outgoing Ports Used in MeetingPlace-Scheduling

Note: This section contains a partial list of outgoing ports only.

Protocol	Source	Destination	Port Type	Port	Usage	Special Requirements
Application Server/Express Media Server						
SMTP	Application Server	SMTP or Microsoft Exchange Server	TCP	25	Send information for email notification	--
HTTP	Application Server	Microsoft Exchange Server	TCP	80	Send information for Microsoft Exchange integration	--
SOCKS	--	--	TCP	1080	Optional configuration for connecting to Cisco WebEx via a proxy configuration.	This is an optional configuration that is not used unless you specifically configure it. The standard SOCKS port is 1080 but is configurable. Other types of proxies (such as HTTP) are not supported by Cisco Unified MeetingPlace for Cisco WebEx connectivity.
--	External Web Server	Application Servers	TCP	5003, 5005	Control connection between the external Web Server and Application Servers (active server and standby server, if one exists) in segmented meeting access configurations	Open bidirectional If you configured your network for reverse connection, where your Web Servers are configured with a Cisco Unified MeetingPlace hostname instead of an IP address, the Application Server can initiate a reverse connection to the Web Server in the DMZ when port 5003 inbound is blocked.
Cisco WebEx Node for MCS (including Cisco WebEx Cloud)						
HTTPS	Cisco WebEx Node for	Cisco WebEx cloud	TCP	443	Tunnel control and meeting information from the Cisco WebEx Node to the Cisco	Only outbound firewall to Internet, these TCP connections also check

	MCS				WebEx cloud. Multiple outbound TCP 443 connections will be created to the Cisco WebEx cloud as external meetings are started. Shared content is sent to the Cisco WebEx cloud for guest users to view during meetings. No Web HTTPS or SOCKS proxy is allowed from the Cisco WebEx Node to the Cisco WebEx cloud.	for NTP clocking to synch to the Cisco WebEx cloud for correct conferencing time coordination.	
--	Cisco WebEx Node for MCS	Application Server	TCP	22	Recording use	--	
--	Cisco WebEx Node for MCS	Application Server	TCP	7676	Accept the connection from the Cisco WebEx Node	--	
Web Server							
NTP	Web Servers	Application Servers	UDP	123	Time synchronization	--	
Control connection	Web Servers	Application Server	TCP	5003	Control connection between Web Servers and the Application Server	--	
--	External Web Server	Application Servers	TCP	5003, 5005	Control connection between the external Web Server and Application Servers (active server and standby server, if one exists) in segmented meeting access configurations	Open bidirectional If you configured your network for reverse connection, where your Web Servers are configured with a Cisco Unified MeetingPlace hostname instead of an IP address, the Application Server can initiate a reverse connection to the Web Server in the DMZ when port 5003 inbound is blocked.	
HTTP	--	--	TCP	61004	Recording control	--	
HTTPS	--	--	TCP	443	Communication with Cisco WebEx	--	
Users							
	--	--	TCP	443			--

Cisco WebEx cloud					Outbound TCP 443 (HTTPS) requests to join and schedule meetings. Any profiled users on Cisco Unified MeetingPlace must be allowed to access the Cisco WebEx cloud outbound.	Only outbound firewall to Internet	

Application Server to Web Server Connectivity

Note: Cisco Unified MeetingPlace Web Servers are only required in MeetingPlace-scheduling deployments. They are optional in audio-only deployments depending on your deployment requirements.

Confirm that the system meets the following requirements so that the Web Server can communicate with the Application Server:

- The Web Server must be able to communicate with the Application Server on TCP port 5003. This can be achieved by opening port 5003 inbound from the Web Server to the Application Server, in which case the normal registration mechanism will operate. Alternately, the Application Server can initiate a reverse (outbound) connection to the Web Server. For the reverse connection to be initiated, you must enter the MeetingPlace Server name as an IP address instead of a hostname during the Web Server installation. You will also have to manually configure this Web Server unit on the Application Server.
- Connectivity between the Web Server and the Application Server is of high quality and not subject to interruptions because of traffic congestion. Any time the round-trip latency exceeds 100 ms or there is more than 1 percent packet loss, you should expect a noticeable reduction in service quality.
- TCP port 61004 must be open inbound from the Web Server to the Application Server. There is no "reverse" connection mechanism for this port.
- Cisco recommends opening UDP port 123 (NTP) bidirectionally between the Web Server and the Application Server. This is used for time synchronization. Alternate time synchronization mechanisms may be used, but any significant clock drift will result in failures.

Integration Requirements

Note: The Cisco Unified MeetingPlace integrations for IBM Lotus Notes and Microsoft Outlook are only supported if your deployment is configured for MeetingPlace-scheduling or audio-only. Deployments configured for WebEx-scheduling use WebEx Productivity Tools.

For more information about deployment options, see Planning Your Deployment.

IBM Lotus Notes Integration with Cisco Unified MeetingPlace Release 8.5

Notes:

- This integration is only supported with MeetingPlace-scheduled and audio-only deployments.

- Multiple clusters are not supported for the IBM Lotus Notes for Cisco Unified MeetingPlace integration.

The IBM Lotus Notes with Cisco Unified MeetingPlace integration requires the following servers:

- Cisco Unified MeetingPlace Application Server
- Cisco Unified MeetingPlace Web Server (which also hosts the integration)
- IBM Lotus Domino Server

Component	Requirement
Cisco Unified MeetingPlace Application Server	See the Application Server Requirements.
Cisco Unified MeetingPlace Web Server **Note:** The IBM Lotus Notes for Cisco Unified MeetingPlace integration is installed on the Web Server.	**Hardware** See the Web Server Requirements. **License** The Cisco Unified MeetingPlace *lotusnotes* license. **Software** • IBM Lotus Notes client Release 6.0.x, 6.5.x, 7.0.x, 8.0.x, 8.5.x • Microsoft Internet Information Server (IIS) Release 6.0. **Note:** Microsoft IIS Release 6.0 is installed and configured on the Cisco MCS when the operating system is installed.
IBM Lotus Domino Server	**Hardware** Microsoft Windows computer **Operating system** Windows **Software** IBM Lotus Domino Release 6.0.x, 6.5.x, 7.0.x, 8.0.x, 8.5.x
End-User System	**Hardware** Microsoft Windows computer

	Software Templates 6.0.5, 6.5.4, 6.5.5, 6.5.6, 7.0.2, 7.0.3, 8.0, 8.5.x Users of IBM Lotus Domino Server Release 6 require: • IBM Lotus Notes Release 6.0.5 • Template of the same release as the client Users of IBM Lotus Domino Server Release 6.5 require: • IBM Lotus Notes Release 6.5.6 or earlier • Template of the same release as the client Users of IBM Lotus Domino Server Release 7 require: • IBM Lotus Notes Release 7.0.3 or earlier • Template of the same release as the client Users of IBM Lotus Domino Server Release 8 require: • IBM Lotus Notes Release 8.0 or earlier • Template of the same release as the client Users of IBM Lotus Domino Server Release 8.5 require: • IBM Lotus Notes Release 8.5 or earlier • Template of the same release as the client **Operating system** One of the following: • Windows 7 • Windows ME • Windows Vista • Windows 2000 Professional • Windows 2000 Server Edition (SP2 or later) • Windows 2000 Advanced Server Edition (SP2 or later) • Windows XP

Microsoft Outlook Integration with Cisco Unified MeetingPlace Release 8.5

Notes:

- This integration is only supported with MeetingPlace-scheduling and audio-only deployments.

- In Release 8.5.2 and later, the Audio-Only deployment and migrated MeetingPlace-Scheduling deployment support the Cisco Unified MeetingPlace plug-in for Microsoft Outlook 2010.
- Cisco Unified MeetingPlace for Microsoft Outlook does not support "thin clients" (Citrix or Terminal Server).

There are two options for Microsoft Outlook integrations:

- *Front-end* integration: Enables users to schedule, reschedule, and cancel meetings from the Microsoft Outlook calendar. For information, see the "Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook" module in the *Configuration Guide for Cisco Unified MeetingPlace*.
- *Back-end* integration: Enables Cisco Unified MeetingPlace to send Microsoft Outlook calendar notifications for meetings that are scheduled from the Cisco Unified MeetingPlace end-user web interface. For more information, see the "Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface" module in the *Configuration Guide for Cisco Unified MeetingPlace*.

Component	Requirement
Cisco Unified MeetingPlace Application Server	See the Application Server Requirements.
Microsoft Exchange Server	**Hardware** See the Web Server Requirements for hardware specifications. **Software** • Microsoft Exchange Server 2010 or Microsoft Exchange Server 2010 Service Pack 1 or Service Pack 2 (Release 8.5.5 [8.5 MR3] only) ♦ Microsoft Exchange Server 2010 has SSL encryption turned on by default. Make sure that the proper SSL certificate is generated or that SSL is turned off on the Exchange server. ♦ Enable EWS access from Cisco Unified MeetingPlace to the Client Access server role and SNMP access to the Hub Transport server role. • Microsoft Exchange Server 2007 SP1 ♦ Enable EWS access from Cisco Unified MeetingPlace and use the Client Access server role. • Microsoft Exchange Server 2003 SP2 ♦ Enable WebDAV access from Cisco Unified MeetingPlace.
End-User System	**Hardware** Microsoft Windows computer **Software** • Microsoft Office 14 • Microsoft Outlook XP, 2003, or 2007

	• Microsoft Outlook 2010 32-Bit or 64-Bit Edition (Supported in Release 8.5.2 (or later) audio-only and migrated MeetingPlace-scheduling deployments only) An HTTP or HTTPS connection to Cisco Unified MeetingPlace for Microsoft Outlook. **Operating system** One of the following: • Windows 7 32-Bit or 64-Bit Edition (Professional, Business, or Ultimate) • Windows ME • Windows Vista 32-Bit or 64-Bit Edition (Enterprise, Business, or Ultimate) • Windows 2000 Professional • Windows 2000 SE with SP2 • Windows 2000 AS with SP2 • Windows XP • Windows Server 2003

Cisco WebEx Mobile Integration with Cisco Unified MeetingPlace Release 8.5

- Cisco WebEx offers integrations with iPhone and Blackberry mobile devices.
- Currently this integration does not support any level of SSO or LDAP integration capability.
- iPad is currently not supported with MeetingPlace audio systems because iPAD is VoIP enabled only via internet.

End-user Requirements for Web Conferencing

See the following link for supported web browser and operating system information:
http://support.webex.com/support/system-requirements.html

(Optional) For audio recording playback, make sure that you have an audio player that plays WAV, WMA, or MP3 files.