Main page: Cisco Unified MeetingPlace, Release 7.0

Previous page: System Requirements

Contents

- 1 TCP/UDP Ports for Cisco Unified MeetingPlace
  - 1.1 Table: Incoming Ports Used by Cisco Unified MeetingPlace
  - 1.2 Table: Outgoing Ports Used by Cisco Unified MeetingPlace
- 2 Application Server to Media Server Connectivity
- 3 Application Server to Web Server Connectivity
- 4 Failover Requirements

TCP/UDP Ports for Cisco Unified MeetingPlace

Table: Incoming Ports Used by Cisco Unified MeetingPlace lists the incoming ports, and Table: Outgoing Ports Used by Cisco Unified MeetingPlace lists the outgoing ports, used by Cisco Unified MeetingPlace. Use these lists 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.

Note: 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.

Table: Incoming Ports Used by Cisco Unified MeetingPlace

Protocol	Port Type	Ports	Port Usage	Special Requirements
Application Server				
SSH	TCP	22	Secure access	Expose to system administrators.
HTTP, HTTPS	TCP	80, 443	Administrator web access	Expose to system administrators.
NTP	UDP	123	Network Time Protocol communication from the Web Servers and Media Servers	Expose to Web Server in the DMZ.
SNMP	UDP	161	SNMP configuration	Expose to system administrators.
MP_REPL	TCP	2008	Database replication between the active and standby servers for Application Server failover	-

GWSIM	TCP	5003	Attachments between the external Web Server and the Application Server	Expose to all Web Servers in the DMZ. You can set up port 5003 to traverse the firewall either inbound or outbound. **NOTE:** Port 5003 must be closed inbound (that is, communication from the DMZ Web Server to the Application Server must be closed) to allow the Application Server to consistently use a reverse connection successfully.
SIP	TCP UDP	5060	SIP B2BUA	-
HTTP	TCP	8080	HTTP services	-
HTTP	TCP	9090	Media Server Administration	Expose to system administrators.
SIP	TCP UDP	61002	Recording signaling	-
Recording control	TCP	61003	Recording control	-
HTTP	TCP	61004	Communication from the external Web Server to the Application Server for prompts, recordings, attachment access, and login service for remote users	Expose to all Web Servers in the DMZ.
RTP, RTCP	UDP	16384-32767	Recording media	-
Media Server				
FTP	TCP	21	Retrieving log files	Expose to system administrators.
Telnet	TCP	23	Telnet	Expose to system administrators.
HTTP	TCP	80	Web user interface	Expose to system administrators.
NTP	UDP	123	Network Time Protocol	-
SNMP	UDP	161	SNMP configuration	Expose to system administrators.
MPI	TCP	2010	MPI (Pompa control protocol)	-
DCI	TCP	3333	DCI (DCS control protocol)	-
XML control	TCP	3336	XML control	-
XML cascading	TCP	3337	XML cascading	-
File server	TCP	3340	File server	-
SIP	TCP UDP	5060	SIP	-
RTP/RTCP	UDP	16384-16683	Audio Blades	Expose to system administrators and end users.
RTP/RTCP	UDP	20000-21799	Video Blades	Expose to system administrators and end users.
	TCP	2944-2945	Video Blade control (H.248)	-

Video Blade control				
Web Server				
HTTP	TCP	80	User web access Cisco Unified MeetingPlace for Microsoft Outlook client	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	TCP	443	Secure user web access Cisco Unified MeetingPlace for Microsoft Outlook client	(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.
RTMP	TCP	1627	Web meeting room	(Optional but recommended for best performance) 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.
DCOM	TCP	Dynamically open 1024 to 65535	Cisco Unified MeetingPlace for Microsoft Outlook to Microsoft Exchange uses the CDO API	Required only for Release 7.0.1 systems using the *back-end* Microsoft Outlook integration.
SQL	TCP	1433	Communication between the Web Server and the SQL Server database	-
Control connection	TCP	5003	Control connection between Web Servers and the Application Server	Expose to Application Server.
Microsoft Office Communicator				
SIP/TLS	TCP	5060-5069	Live Communication Server (LCS) gateway service	-
IBM Lotus Sametime				
TCP/UDP	TCP UDP	8083	Java RMI[1] lookup service for IBM Lotus Sametime	-
TCP	TCP	8086	RMI calls (JRMP[2]) for IBM Lotus Sametime web conferencing	-

Footnote 1: RMI = Remote Method Invocation

Footnote 2: JRMP = Java Remote Method Protocol

Note: Table: Outgoing Ports Used by Cisco Unified MeetingPlace contains only a partial list of outgoing ports.

Table: Outgoing Ports Used by Cisco Unified MeetingPlace

Service	Port Type	Port	Purpose	Source	Destination
Microsoft Exchange					
HTTP	TCP	80	Microsoft Exchange integration	Application Server	Microsoft Exchange server
HTTPS	TCP	443	Microsoft Exchange integration when SSL is enabled	Application Server	Microsoft Exchange server
SMTP	TCP	25	E-mail notification	Application Server	SMTP server or Microsoft Exchange server
SOCKS	TCP	1080	Optional configuration for connecting to Cisco WebEx via a proxy configuration	Application Server	Cisco WebEx

Note: The SOCKS configuration is an optional configuration and is not used unless you specifically configure it. The standard SOCKS port is 1080 but you can configure a different port. Other types of proxies (such as HTTP) are not supported by Cisco Unified MeetingPlace for Cisco WebEx connectivity.

Application Server to Media Server Connectivity

- The Media Server should be on the same local network segment as the Application Server. Cisco Unified MeetingPlace does not support Media Server blades that are remotely located.
- If Primary and Failover Application Servers are deployed, all Media Server hardware can be shared if deployed in a single datacenter.
- If Primary and Failover Application Servers are deployed in different locations, then Media Server hardware must be duplicated at the second site and is only utilized when that "Failover" Application Server is made "Active".

Application Server to Web Server Connectivity

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 a host name instead of an IP address during the

Cisco Unified MeetingPlace Web Conferencing 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.

Failover Requirements

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

- Both the active and the standby Application Servers must be licensed exactly the same. Each Application Server license key is applied separately based on the MAC address of the Cisco MCS where the software is installed.

- If the active and standby Application Server are deployed in different locations, then the same VLAN configuration must be spanned between data centers to accomodate the shared IP address and hostname on both Application Servers.

- Informix database replication is buffered via the LAN/WAN and the heartbeat is done every 60 seconds. If there is no response, it does a ping. For latency, there is no minimum requirement. Network bandwidth is 128kbps minimum between Application Servers.

- Replication happens asynchronously for each configuration change related to users, groups, or meetings. The source server captures the configuration changes and reliably transmits each transaction to the other server. In case the target server or the link between them is down, the configuration changes are queued up on the source server and are synced with the target server when the connection is re-established.

- Data for user profiles; groups; and past, present, and future meetings is replicated.