CHAPTER 1

IP Communications Required by Cisco Unity Connection

See the following sections:

Cisco Unity Connection Service Ports

Table 1-1 lists the TCP and UDP ports that are used for inbound connections to the Cisco Unity Connection server, and ports that are used internally by Connection.

Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 20500, 20501, 20502, 19003	Open only between servers in a Connection cluster	CuCsMgr/Connection Conversation Manager	cucsmgr	Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: **21000–21512**	Open	CuCsMgr/Connection Conversation Manager	cucsmgr	IP phones must be able to connect to this range of ports on the Connection server for some phone client applications.
TCP: **5000**	Open	CuCsMgr/Connection Conversation Manager	cucsmgr	Opened for port-status monitoring read-only connections. Monitoring must be configured in Connection Administration before any data can be seen on this port (Monitoring is off by default). Administration workstations connect to this port.

Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP and UDP ports allocated by administrator for SIP traffic Possible ports are **5060–5100**	Open	CuCsMgr/Connection Conversation Manager	cucsmgr	Connection SIP Control Traffic handled by conversation manager. SIP devices must be able to connect to these ports.
TCP: 20055	Open only between servers in a Connection cluster	CuLicSvr/Connection License Server	culic	Restricted to localhost only (no remote connections to this service are needed).
TCP: 1502, 1503 ("ciscounity_tcp" in /etc/services)	Open only between servers in a Connection cluster	unityoninit/Connection DB	root	Servers in a Connection cluster must be able to connect to each other on these database ports. For external access to the database, use CuDBProxy.
TCP: **143, 993, 7993, 8143, 8993**	Open	CuImapSvr/Connection IMAP Server	cuimapsvr	Client workstations must be able to connect to ports 143 and 993 for IMAP inbox access, and IMAP over SSL inbox access.
TCP: **25, 8025**	Open	CuSmtpSvr/Connection SMTP Server	cusmtpsvr	Servers delivering SMTP to Connection port 25, such as other servers in a UC Digital Network.
TCP: 4904	Blocked; internal use only	SWIsvcMon (Nuance SpeechWorks Service Monitor)	openspeech	Restricted to localhost only (no remote connections to this service are needed).
TCP: 4900:4904	Blocked; internal use only	OSServer/Connection Voice Recognizer	openspeech	Restricted to localhost only (no remote connections to this service are needed).
UDP: **16384–21511**	Open	CuMixer/Connection Mixer	cumixer	VoIP devices (phones and gateways) must be able to send traffic to these UDP ports to deliver inbound audio streams.
UDP: 7774–7900	Blocked; internal use only	CuMixer/ Speech recognition RTP	cumixer	Restricted to localhost only (no remote connections to this service are needed).
TCP: 22000 UDP: 22000	Open only between servers in a Connection cluster	CuSrm/ Connection Server Role Manager	cusrm	Cluster SRM RPC. Servers in a Connection cluster must be able to connect to each other on these ports.

Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 22001 UDP: 22001	Open only between servers in a Connection cluster	CuSrm/ Connection Server Role Manager	cusrm	Cluster SRM heartbeat. Heartbeat event traffic is not encrypted but is MAC secured. Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: **20532**	Open	CuDbProxy/ Connection Database Proxy	cudbproxy	If this service is enabled it allows administrative read/write database connections for off-box clients. For example, some of the ciscounitytools.com tools use this port. Administrative workstations would connect to this port.
TCP: **22**	Open	Sshd	root	Firewall must be open for TCP 22 connections for remote CLI access and serving SFTP in a Connection cluster. Administrative workstations must be able to connect to a Connection server on this port. Servers in a Connection cluster must be able to connect to each other on this port.
UDP: **161**	Open	Snmpd Platform SNMP Service	root	—
UDP: **500**	Open	Raccoon ipsec isakmp (key management) service	root	Using ipsec is optional, and off by default. If the service is enabled, servers in a Connection cluster must be able to connect to each other on this port.
TCP: **8500** UDP: **8500**	Open	clm/cluster management service	root	The cluster manager service is part of the Voice Operating System. Servers in a Connection cluster must be able to connect to each other on these ports.

Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
UDP: **123**	Open	Ntpd Network Time Service	ntp	Network time service is enabled to keep time synchronized between servers in a Connection cluster. The publisher server can use either the operating system time on the publisher server or the time on a separate NTP server for time synchronization. Subscriber servers always use the publisher server for time synchronization. Servers in a Connection cluster must be able to connect to each other on this port.
TCP: 5007	Open	Tomcat/Cisco Tomcat (SOAP Service)	tomcat	Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: 1500, 1501	Open only between servers in a Connection cluster	cmoninit/Cisco DB	informix	These database instances contain information for LDAP integrated users, and serviceability data. Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: 1515	Open only between servers in a Connection cluster	dblrpm/Cisco DB Replication Service	root	Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: 8001	Open only between servers in a Connection cluster	dbmon/Cisco DB Change Notification Port	database	Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: 2555, 2556	Open only between servers in a Connection cluster	RisDC/Cisco RIS Data Collector	ccmservice	Servers in a Connection cluster must be able to connect to each other on these ports.
TCP: 1090, 1099	Open only between servers in a Connection cluster	Amc/Cisco AMC Service (Alert Manager Collector)	ccmservice	Performs back-end serviceability data exchanges 1090: AMC RMI Object Port 1099: AMC RMI Registry Port Servers in a Connection cluster must be able to connect to each other on these ports.

Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: **80, 443, 8080, 8443**	Open	tomcat/Cisco Tomcat	tomcat	Both client and administrative workstations need to connect to these ports. Servers in a Connection cluster must be able to connect to each other on these ports for communications that use HTTP-based interactions like REST. **Note** These ports support both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Reconfiguration and Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrug051.html. **Note** Cisco Unity Connection Survivable Remote Site Voicemail SRSV supports these ports for IP communication.
TCP: 5001, 8005	Blocked; internal use only	tomcat/Cisco Tomcat	tomcat	Internal tomcat service control and axis ports.
TCP: **32768–61000** UDP: **32768–61000**	Open	—	—	Ephemeral port ranges, used by anything with a dynamically allocated client port.

Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 7080, 7443	Open	jetty/Connection Jetty	jetty	*Exchange 2007 and Exchange 2010 only, single inbox only:* EWS notifications of changes to Connection voice messages. With Cisco Unity Connection 9.1(2) and later, Comet notifications are now supported over the HTTP(S) or SSL notification mode at 7443 TCP port.
UDP: 9291	Open	CuMbxSync/ Connection Mailbox Sync Service	cumbxsync	*Exchange 2003 only, single inbox only:* WebDAV notifications of changes to Connection voice messages.

1. Bold port numbers are open for direct connections from off-box clients.

Outbound Connections Made by the Cisco Unity Connection Server

Table 1-2 lists the TCP and UDP ports that Cisco Unity Connection uses to connect with other servers in the network.

Table 1-2 TCP and UDP Ports That Cisco Unity Connection Uses to Connect With Other Servers in the Network

Ports and Protocols	Executable	Service Account	Comments
TCP: 2000* (Default SCCP port) Optionally TCP port 2443* if you use SCCP over TLS. * Many devices and applications allow configurable RTP port allocations.	CuCsMgr	cucsmgr	Connection SCCP client connection to Cisco Unified CM when they are integrated by using SCCP.
UDP: 16384–32767* (RTP) * Many devices and applications allow configurable RTP port allocations.	CuMixer	cumixer	Connection outbound audio-stream traffic.
UDP: 69	CuCsMgr	cucsmgr	When you are configuring encrypted SCCP, encrypted SIP, or encrypted media streams, Connection makes a TFTP client connection to Cisco Unified CM to download security certificates.
TCP: 53 UDP: 53	any	any	Used by any process that needs to perform DNS name resolution.

Table 1-2 TCP and UDP Ports That Cisco Unity Connection Uses to Connect With Other Servers in the Network

Ports and Protocols	Executable	Service Account	Comments
TCP: 53, and either 389 or 636	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	Used when Connection is configured for unified messaging with Exchange and one or more unified messaging services are configured to search for Exchange servers. Connection uses port 389 when you choose LDAP for the protocol used to communicate with domain controllers. Connection uses port 636 when you choose LDAPS for the protocol used to communicate with domain controllers.
TCP: 80, 443 (HTTP and HTTPS)	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	Connection makes HTTP and HTTPS client connections to other servers for communications for external services (in Connection 8.0) or unified messaging (in 8.5 and later), such as connections to Microsoft Exchange for single inbox and calendar integrations. **Note** These ports support both the IPv4 and IPv6 addresses.
TCP: 80, 443, 8080, and 8443 (HTTP and HTTPS)	CuCsMgr tomcat	cucsmgr tomcat	Connection makes HTTP and HTTPS client connections to: • Other Connection servers for Digital Networking automatic joins. • Cisco Unified CM for AXL user synchronization. **Note** These ports support both the IPv4 and IPv6 addresses. **Note** Cisco Unity Connection Survivable Remote Site Voicemail SRSV supports these ports for IP communication.
TCP: 143, 993 (IMAP and IMAP over SSL)	CuCsMgr	cucsmgr	Connection makes IMAP connections to Microsoft Exchange servers to perform text-to-speech conversions of email messages in a Connection user's Exchange mailbox.

Table 1-2 TCP and UDP Ports That Cisco Unity Connection Uses to Connect With Other Servers in the Network

Ports and Protocols	Executable	Service Account	Comments
TCP: 25 (SMTP)	CuSmtpSvr	cusmtpsvr	Connection makes client connections to SMTP servers and smart hosts, or to other Connection servers for features such as VPIM networking or Connection Digital Networking.
TCP: 21 (FTP)	ftp	root	The installation framework performs FTP connections to download upgrade media when an FTP server is specified.
TCP: 22 (SSH/SFTP)	CiscoDRFMaster sftp	drf root	The Disaster Recovery Framework performs SFTP connections to network backup servers to perform backups and retrieve backups for restoration. The installation framework will perform SFTP connections to download upgrade media when an SFTP server is specified.
UDP: 67 (DHCP/BootP)	dhclient	root	Client connections made for obtaining DHCP addressing. Although DHCP is supported, Cisco highly recommends that you assign static IP addresses to Connection servers.
TCP: 123 UDP: 123 (NTP)	Ntpd	root	Client connections made for NTP clock synchronization.