IP Communications Required by Cisco Unity Connection

• IP Communications Required by Cisco Unity Connection, on page 1

IP Communications Required by Cisco Unity Connection

Service Ports

Table 1: TCP and UDP Ports Used for Inbound Connections to Cisco Unity Connection 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 Unity Connection.

Table 1: TCP and UDP Ports Used for Inbound Connections to Cisco Unity Connection

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 20500, 20501, 20502, 19003, 1935	Open only between servers in a Unity Connection cluster. Port 1935 is blocked and is for internal use only.	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Servers in a Unity Con must be able to connec on these ports.
TCP: **21000–21512**	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	IP phones must be able this range of ports on Connection server for client applications.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: **5000**	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Opened for port-status mo read-only connections. M must be configured in Connection Administratio any data can be seen on th (Monitoring is off by defa Administration workstatio to this port.
TCP and UDP ports allocated by administrator for SIP traffic. Possible ports are **5060–5199**	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Unity Connection SIP Co Traffic handled by conver manager. SIP devices must be able to these ports.
TCP: 20055	Open only between servers in a Unity Connection cluster	CuLicSvr/Unity Connection License Server	culic	Restricted to localhost on remote connections to this are needed).
TCP: 1502, 1503 ("ciscounity_tcp" in /etc/services)	Open only between servers in a Unity Connection cluster	unityoninit/Unity Connection DB	root	Servers in a Unity Connect must be able to connect to on these database ports. For external access to the use CuDBProxy.
TCP: **143, 993, 7993, 8143, 8993**	Open	CuImapSvr/Unity Connection IMAP Server	cuimapsvr	Client workstations must connect to ports 143 and 9 IMAP inbox access, and I SSL inbox access.
TCP: **25, 8025**	Open	CuSmtpSvr/Unity Connection SMTP Server	cusmtpsvr	Servers delivering SMTP Connection port 25, such servers in a UC Digital N
TCP: 4904	Blocked; internal use only	SWIsvcMon (Nuance SpeechWorks Service Monitor)	openspeech	Restricted to localhost on remote connections to this are needed).
TCP: 4900:4904	Blocked; internal use only	OSServer/Unity Connection Voice Recognizer	openspeech	Restricted to localhost on remote connections to this are needed).
UDP: **16384–21511**	Open	CuMixer/Unity Connection Mixer	cumixer	VoIP devices (phones and must be able to send traffi UDP ports to deliver inbo streams.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
UDP: 7774–7900	Blocked; internal use only	CuMixer/ Speech recognition RTP	cumixer	Restricted to localhost remote connections to are needed).
TCP: 22000 UDP: 22000	Open only between servers in a Unity Connection cluster	CuSrm/ Unity Connection Server Role Manager	cusrm	Cluster SRM RPC. Servers in a Unity Con must be able to connec on these ports.
TCP: 22001 UDP: 22001	Open only between servers in a Unity Connection cluster	CuSrm/ Unity Connection Server Role Manager	cusrm	Cluster SRM heartbea Heartbeat event traffic encrypted but is MAC Servers in a Unity Con must be able to connec on these ports.
TCP: **20532**	Open	CuDbProxy/ Unity Connection Database Proxy	cudbproxy	If this service is enabl administrative read/wr connections for off-bo example, some of the ciscounitytools.com to port. Administrative workst connect to this port.
TCP: **22**	Open	Sshd	root	Firewall must be open connections for remot and serving SFTP in a Connection cluster. Administrative workst able to connect to a U Connection server on Servers in a Unity Con must be able to connec on this port.
UDP: **161**	Open	Snmpd Platform SNMP Service	root	—
UDP: **500**	Open	Raccoon ipsec isakmp (key management) service	root	Using ipsec is optiona default. If the service is enable Unity Connection clus able to connect to eac port.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: **8500** UDP: **8500**	Open	clm/cluster management service	root	The cluster manager servi of the Voice Operating Sy Servers in a Unity Connect must be able to connect to on these ports.
UDP: **123**	Open	Ntpd Network Time Service	ntp	Network time service is e keep time synchronized b servers in a Unity Connec cluster. The publisher server can u the operating system time publisher server or the tim separate NTP server for ti synchronization. Subscrib always use the publisher s time synchronization. Servers in a Unity Connect must be able to connect to on this port.
TCP: 5007	Blocked; internal use only.	Tomcat/Cisco Tomcat (SOAP Service)	tomcat	Servers in a Unity Connect must be able to connect to on these ports.
TCP: 1500, 1501	Open only between servers in a Unity Connection cluster	cmoninit/Cisco DB	informix	These database instances information for LDAP int users, and serviceability d Servers in a Unity Connect must be able to connect to on these ports.
TCP: 1515	Open only between servers in a Unity Connection cluster	dblrpm/Cisco DB Replication Service	root	Servers in a Unity Connect must be able to connect to on these ports.
TCP: 8001	Open only between servers in a Unity Connection cluster	dbmon/Cisco DB Change Notification Port	database	Servers in a Unity Connect must be able to connect to on these ports.
TCP: 2555, 2556	Open only between servers in a Unity Connection cluster	RisDC/Cisco RIS Data Collector	ccmservice	Servers in a Unity Connect must be able to connect to on these ports.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 1090, 1099	Open only between servers in a Unity Connection cluster	Amc/Cisco AMC Service (Alert Manager Collector)	ccmservice	Performs back-end ser data exchanges 1090: AMC RMI Obj AMC RMI Registry P Servers in a Unity Con must be able to connec on these ports.
TCP: **80, 443, 8080, 8443**	Open	tomcat/Cisco Tomcat	tomcat	Both client and admin workstations need to co ports. Servers in a Unity Con must be able to connec on these ports for com that use HTTP-based i like REST. **Note** These por both the I addresses the IPv6 a only whe platform i in Dual (I mode. Cis Connectio Remote S SRSV sup ports for I communi
TCP: 8081, 8444	Open only between servers in HTTPS Networking	tomcat/Cisco Tomcat	tomcat	Servers in HTTPS Net be able to connect to e these ports for commu Unity Connection HT Feeder service uses th directory synchronizat **Note** Unity Co HTTPS D Feeder se only IPv4
TCP: 5001-5004, 8005	Blocked; internal use only	tomcat/Cisco Tomcat	tomcat	Internal tomcat servic axis ports.
TCP: **32768–61000** UDP: **32768–61000**	Open	—	—	Ephemeral port range anything with a dynan allocated client port.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 7443	Open	jetty/Unity Connection Jetty	jetty	Secure Jabber and Web In notifications **Note** You can enab port using "u jetty ssl enab command.
TCP: 7080	Open	jetty/Unity Connection Jetty	jetty	*Exchange 2010 only, sing only:* Jabber and Web Inb notifications of changes to Connection voice messag
UDP: 9291	Open	CuMbxSync/ Unity Connection Mailbox Sync Service	cumbxsync	*Single inbox only:* WebD notifications of changes to Connection voice messag
TCP: 6080	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Video server must be able to Unity Connection on th communications.

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

Outbound Connections Made by Unity Connection

Table 2: TCP and UDP Ports Unity Connection Uses to Connect With Other Servers in the Network lists the TCP and UDP ports that Cisco Unity Connection uses to connect with other servers in the network.

Table 2: TCP and UDP Ports 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	Unity Connection SCCP client co to Cisco Unified CM when they a integrated using SCCP.
UDP: 16384–32767* (RTP) * Many devices and applications allow configurable RTP port allocations.	CuMixer	cumixer	Unity Connection outbound audio traffic.
UDP: 69	CuCsMgr	cucsmgr	When you are configuring encryp encrypted SIP, or encrypted media Unity Connection makes a TFTP connection to Cisco Unified CM to security certificates.

Ports and Protocols	Executable	Service Account	Comments
TCP: 6972	CuCsMgr	cucsmgr	When you are configuring enc encrypted media streams, Uni makes the HTTPS client conn Cisco Unified CM to downloa certificates.
TCP: 53 UDP: 53	any	any	Used by any process that need DNS name resolution.
TCP: 53, and either 389 or 636	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	Used when Unity Connection for unified messaging with Ex one or more unified messagin configured to search for Excha Unity Connection uses port 38 select LDAP for the protocol u communicate with domain con Unity Connection uses port 63 select LDAPS for the protocol communicate with domain con
TCP: 80, 443 (HTTP and HTTPS)	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	**Note** These ports suppo IPv4 and IPv6 ad
TCP: 80, 443, 8080, and 8443 (HTTP and HTTPS)	CuCsMgr tomcat	cucsmgr tomcat	Unity Connection makes HTT client connections to: • Other Unity Connection Digital Networking auton • Cisco Unified CM for AX synchronization. **Note** These ports the IPv4 and addresses. **Note** Cisco Unity Survivable R Voicemail SI these ports f communicat
TCP: 143, 993 (IMAP and IMAP over SSL)	CuCsMgr	cucsmgr	Unity Connection makes IMA to Microsoft Exchange servers text-to-speech conversions of e in a Unity Connection user's E mailbox.

Ports and Protocols	Executable	Service Account	Comments
TCP: 25,587 (SMTP)	CuSmtpSvr	cusmtpsvr	Unity Connection makes client co to SMTP servers and smart hosts, Unity Connection servers for feat as VPIM networking or Unity Co Digital Networking. **Note** Cisco Unity Connect supports STARTTLS 25. With Release 14S later, STARTTLS is a supported over port 5
TCP: 21 (FTP)	ftp	root	The installation framework perfor connections to download upgrade when an FTP server is specified.
TCP: 22 (SSH/SFTP)	CiscoDRFMaster sftp	drf root	The Disaster Recovery Framework SFTP connections to network back to perform backups and retrieve ba restoration. The installation framework perfor connections to download upgrade when an SFTP server is specified
UDP: 67 (DHCP/BootP)	dhclient	root	Client connections made for obtain addressing. Although DHCP is supported, Cis recommends that you assign static addresses to Unity Connection ser
TCP: 123 UDP: 123 (NTP)	Ntpd	root	Client connections made for NTP synchronization.
UDP: 514 TCP: 601	Syslog/Cisco Syslog Server	syslog	Unity Connection server must be a audit logs to remote syslog server these ports

Securing Transport Layer

Unity Connection uses Transport Layer Security(TLS) protocol and Secure Sockets Layer(SSL) protocol for signaling and client server communication. Unity Connection supports TLS 1.0, TLS 1.1 and TLS 1.2 for secure communication across various interfaces of Cisco Unity Connection. TLS 1.2 is the most secure and authenticated protocol for communication.

Depending upon the organization security policies and deployment capabilities, Unity Connection 11.5(1) SU3 and later allows you to configure the minimum TLS version. After configuring the minimum version of TLS, Unity Connection supports the minimum configured version and higher versions of TLS. For example, if you configure TLS 1.1 as a minimum version of TLS, Unity Connection uses TLS 1.1 and higher versions

for communication and rejects the request for a TLS version that is lower than the configured value. By default, TLS 1.0 is configured.

Before configuring minimum TLS version, ensure that all the interfaces of Unity Connection must be secured and use configured minimum TLS version or higher version for communication. However, you can configure the minimum TLS version for inbound interfaces of Unity Connection.

Table 3 lists the supported interfaces for which you can configure the minimum TLS version on Unity Connection.

Table 3: Supported Interfaces for secure Communication

Ports	Executable, Service or Application	Service Account	Comments
8443, 443, 8444	• Cisco HAProxy	• haproxy	Both client and administrative workstations must connect to these ports. Servers in a Unity Connection cluster must be able to connect to each other on these ports for communications that use HTTP-based interactions like REST.
7443	jetty/Unity Connection Jetty	jetty	Secure Jabber and Web Inbox notifications. Cisco Unity Connection 14SU3 and later, supports only TLS version 1.2 for secure communication
993	CuImapSvr/Unity Connection IMAP Server	cuimapsvr	Client workstations must be able to connect to port 993 for IMAP over SSL inbox access.
25,587	CuSmtpSvr/Unity Connection SMTP Server	cusmtpsvr	Servers delivering SMTP to Unity Connection port 25 or 587, such as other servers in a UC Digital Network.
5061-5199	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Unity Connection SIP Control Traffic handled by conversation manager. SIP devices must be able to connect to these ports.
LDAP *(outbound interface)*	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	Unity Connection uses port 636 when you select LDAPS for the protocol used to communicate with domain controllers.
20536	Cisco HAProxy	haproxy	If this service is enabled it allows administrative secure read/write database connections for off-box clients.

For more information on supported inbound interfaces of Cisco Unity Connection, see "Service Ports" section.

Configuring Minimum TLS Version

To configure the minimum TLS version in Cisco Unity Connection, execute the following CLI command:

- set tls min-version <tls minVersion>

In cluster, you must execute the CLI command on both publisher and subscriber.

In addition to this, you can execute the following CLI command to check the configured value of minimum TLS version on Unity Connection:

- show tls min-version

For detailed information on the CLI, see *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Caution After configuring minimum TLS version, the Cisco Unity Connection server restart automatically.