Port Utilization Guide for Cisco Unified Contact Center Express Solution, Release 12.5(1)

First Published: 2020-01-31

Americas 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: 408 527-0883

CONTENTS

Preface

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
		January 2020
Initial Release of Document for Release 12.5(1)		
Cisco SocialMiner (SM) has been renamed as Customer Collaboration Platform (CCP).	Port Utilization in Customer Collaboration Platform >> Customer Collaboration Platform Port Utilization	
Introduced Cloud Connect.	Port Utilization in Unified CCX >> Cloud Connect Port Utilization	
Unified CCX and IP IVR Port related information has been updated.	Port Utilization in Unified CCX >> Unified CCX and IP IVR Port Utilization	
Updated notes for TCP 7071 and 5222.	Port Utilization in Unified CCX >> Finesse Port Utilization	

Change	See	Date
		January 2020
Added the port 8447.	Port Utilization in Unified CCX >> Unified CCX and IP IVR Port Utilization Port Utilization in Unified CCX >> Unified Intelligence Center Port Utilization	

About this Guide

This document provides a list of the TCP and UDP ports that Cisco Unified Contact Center products use. You use this information to configure Quality of Service (QoS) and Firewall/VPN solutions. Proper configuration is important on a network with an Architecture for Voice, Video, and Integrated Data (AVVID) solution.

Audience

This document is intended primarily for network administrators.

Conventions

This manual uses the following conventions.

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find** • Click **Finish**.

Convention	Description
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • An argument for which you must supply values. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco Unified Contact Center Express Installation Guide*.

`window` font	Window font, such as Courier, is used for the following:
	• Text as it appears in code or information that the system displays. Example:
	`<html><title> Cisco Systems,Inc. </title></html>`
	• File names. Example: `tserver.properties`.
	• Directory paths. Example:
	`C:\Program Files\Adobe`

string	Nonquoted sets of characters (strings) appear in regular font. Do not use quotation marks around a string or the string will include the quotation marks.
[ ]	Optional elements appear in square brackets.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Convention	Description
^	The key labeled Control is represented in screen displays by the symbol ^. For example, the screen instruction to hold down the Control key while you press the D key appears as ^D.

Related Documents

Document or Resource	Link
Cisco Unified Contact Center Express Documentation Guide	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html
Cisco Unified CCX documentation	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
Cisco Unified Intelligence Center documentation	https://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html
Cisco Finesse documentation	https://www.cisco.com/en/US/products/ps11324/tsd_products_support_series_home.html
Cisco Customer Collaboration Platform documentation **Note** From Unified CCX Release 12.5(1), CCP documents are available in the Cisco Unified CCX documentation folder.	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
Cisco Unified CCX Virtualization Information	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html
Cisco Unified CCX Compatibility Information	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Documentation and Support

To download documentation, submit a service request, and find additional information, see *What's New in Cisco Product Documentation* at https://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Documentation Feedback

To provide your feedback for this document, send an email to:

contactcenterproducts_docfeedback@cisco.com

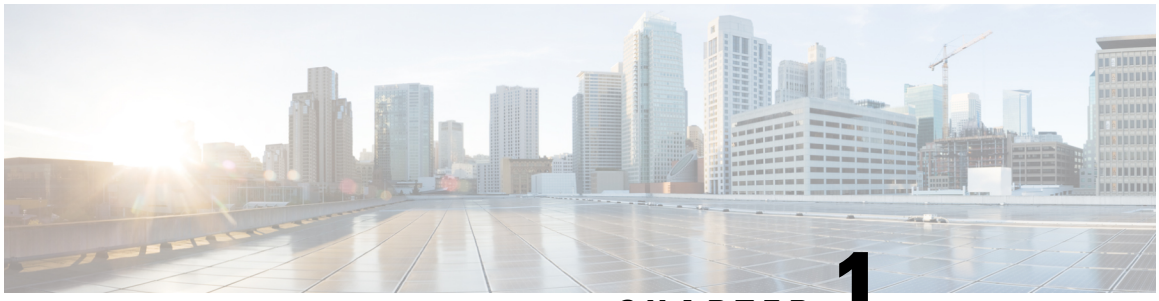
Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.



CHAPTER 1

Port Utilization in Unified CCX

Port Utilization Table Columns

The columns in the port utilization tables in this document describe the following:

Listener (Process or Application Protocol)

A value representing the server or application and where applicable, the open or proprietary application protocol.

Listener Protocol and Port

An identifier for the TCP or UDP port that the server or application is listening on, along with the IP address for incoming connection requests when acting as a server.

Remote Device (Process or Application Protocol)

The remote application or device making a connection to the server or service specified by the protocol.

Remote Port

The identifier for the TCP or UDP port that the remote service or application is listening on, along with the IP address for incoming connection requests when acting as the server.

Traffic Direction

The direction that traffic flows through the port: Inbound, Bidirectional, Outbound.

Note

- The operating system dynamically assigns the source port that the local application or service uses to connect to the destination port of a remote device. In most cases, this port is assigned randomly above TCP/UDP 1024.
- For security reasons, keep open only the ports mentioned in this guide and those required by your application. Keep the rest of the ports blocked.

System Services Port Utilization

Table 1: System Services Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
System Service	TCP 7	Editor	—	Bidirectional	- Echo for Editor - ICM Controller
System Service	TCP 22	—	—	Bidirectional	SFTP and SSH access
Tomcat (HTTP)	TCP 80	—	—	Bidirectional	- Web access
System Service	UDP 123	—	—	Bidirectional	NTP, network time sync
SNMP Agent	UDP 161	—	—	Bidirectional	Provide services for SNMP-based management applications
Tomcat (HTTPS)	TCP 443	—	—	Bidirectional	This port is used for communication between the subscriber and publisher during COP file installation in the subscriber node.
AON Management Console (AMC) Service	TCP 1090	Intracluster communication	—	Bidirectional	Provide RTMT data collecting, logging and alerting functionalities (AMC RMI Object Port)
AON Management Console (AMC) Service	TCP 1099	Intracluster communication	—	Bidirectional	Provide RTMT data collecting, logging and alerting functionalities (AMC RMI Registry Port)
DBMON	TCP 1500	—	—	Bidirectional	This is the port where the IDS engine listens for DB clients

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
DBMON	TCP 1501	—	—	Bidirectional	- This is an alternate port to bring up a second instance of IDS during upgrade. - Localhost traffic only
DBL RPC	TCP 1515	Intracluster communication	—	Bidirectional	DBL RPC, this is used during installation to set up IDS replication between nodes
Real-Time Information Server (RIS) Data Collector service (RISDC)	TCP 2555	Intracluster communication	—	Bidirectional	Used by the RISDC platform service. The Real-time Information Server (RIS) maintains real-time Cisco Unified CM information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RISDC service provides an interface for applications, such as RTMT, SOAP applications, Cisco Unified CM Administration and AMC to retrieve the information that is stored in all RIS nodes in the cluster.
RISDC	TCP 2556	Intracluster communication	—	Bidirectional	Allowed RIS client connection to retrieve real-time information
Disaster Recovery System (DRS)	TCP 4040	—	—	Bidirectional	Real-time service
Real-time service	TCP 5001	—	—	Bidirectional	SOAP Monitor Used by SOAP to monitor the Real Time Monitoring Service and fetch the Server information for selection of specific CM devices and other such activities.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
Perfmon service	TCP 5002	—	—	Bidirectional	SOAP Monitor Used by SOAP to monitor the Performance Monitor Service for opening and closing sessions, collecting session data and fetching various other data.
Control center service	TCP 5003	—	—	Bidirectional	SOAP Monitor Used by SOAP to monitor the Control Center Service for activities like getting the Service Status and performing service deployment.
Log Collection Service	TCP 5004	—	—	Bidirectional	SOAP Monitor
System Service	TCP 5007	—	—	Bidirectional	SOAP Monitor - a troubleshooting tool for SOAP infrastructure
Cisco Identity Service Data Grid	TCP 5702	Intra-cluster communication	5702 **Note:** The Cisco IdS server node in the cluster connects to this port.	Bidirectional	Data or Service grid to manage Cisco IdS cluster nodes.
DBMON (CN)	TCP 8001	Intracluster communication	—	Bidirectional	DB change notification port.
Tomcat	TCP 8005	—	—	—	Used for receiving shutdown requests, which would halt all applications within Tomcat
Tomcat (HTTP)	TCP 8080	Client Browser	—	Bidirectional	- Client browser trying to access any of the Administration interfaces or User Options interface. - Web services client using RTMT.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
Tomcat (HTTPS)	TCP 8443	Client Browser	—	Bidirectional	- Client browser trying to access any of the Administration interfaces or User Options interface. - Web services client using RTMT. - DB access via SOAP; Tomcat forwards the SOAP request to AXL.
IPSec Manager daemon	TCP 8500	—	—	Bidirectional	Connectivity testing. Uses a proprietary protocol.
IPSec Manager daemon	UDP 8500	—	—	Bidirectional	Cluster replication of platform data (hosts) certificates etc. Uses a proprietary protocol.
Cisco Identity Service (Cisco IdS)	TCP 8553	—	—	—	HTTPS for Cisco IdS

Unified CCX and IP IVR Port Utilization

Table 2: Unified CCX Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic direction	Purpose
Cisco Unified CCX Socket.IO Service	TCP 12014	—	—	Bidirectional	This is the port where live-data reporting clients can connect to the socket.IO server.
Cisco Unified CCX Socket.IO Service	TCP 12015	—	—	Bidirectional	This is the secure port where live-data reporting clients can connect to socket.IO server.
Unified CCX Engine	TCP 12499	—	—	Bidirectional	Unified CCX and Socket I/O service management port.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic direction	Purpose
Informix Dynamic Server (IDS)	TCP 1504	External process like CUIC, WallBoard Client, external clients such as Squirrel or custom reporting can connect	—	Bidirectional	Unified CCX database port.
Informix Dynamic Server (IDS)	TCP 9089	External process like CUIC, WallBoard Client, external clients such as Squirrel or custom reporting can connect	—	Bidirectional	This is the secured Unified CCX database port.
Informix Dynamic Server (IDS)	TCP 1516	—	—	Bidirectional	Intra-cluster communication.
JTAPI Client (QBE)	TCP 2789	Unified CM	2748	Bidirectional	Provide services to CTI applications.
Unified CCX Engine	UDP 5065 and TCP 5065	SIP gateway and MRCP server	—	Bidirectional	Used to communicate with SIP gateway and MRCP server.
Cisco Identity Service Data Grid	TCP 5702	Intra-cluster communication	5702 **Note:** The Cisco IdS server node in the cluster connects to this port.	Bidirectional	Data or Service grid to manage Cisco IdS cluster nodes.
CVD	TCP 5900	CVD of other node in cluster	—	Bidirectional	Heartbeats between CVDs in the cluster.
CVD ActiveMQ	TCP 6161	Internal	6161	Bidirectional	Publish JMS events across JMS network connectors in the cluster.
CVD	TCP 6999	Unified CCX Engine, Tomcat, CVD, and Editor	—	Bidirectional	RMI Port.
Cisco Unified Intelligence Center Tomcat (HTTP)	TCP 8081	Client Browsers	—	Bidirectional	Client browser trying to access the Cisco Unified Intelligence Center web interface.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic direction	Purpose
Cisco Unified Intelligence Center Tomcat (HTTPS)	TCP 8444	Client Browsers	—	Bidirectional	Client browser trying to access the Cisco Unified Intelligence Center web interface.
	TCP 8447	Browsers	—	—	HTTPS - Unified Intelligence Center Online Help.
Cisco Identity Service Tomcat (HTTPS)	TCP 8553	—	—	Bidirectional	Client browser trying to access the Cisco Identity Service Management web interface. Single Sign-On (SSO) components access this interface to know the operating status of Cisco IdS.
Unified CCX Engine	TCP 9080	—	—	Bidirectional	- Tomcat instance used by Unified CCX Engine. - Clients trying to access HTTP triggers or documents / prompts / grammars / live data.
Unified CCX Engine	TCP 9443	—	—	Bidirectional	Secure port used by the Unified CCX Engine to: - Respond to clients trying to access HTTPS triggers. - Authenticate the live data clients.
Unified CCX Engine	TCP 12028	—	—	Bidirectional	CTI Server.
Cisco IP Voice Media Streaming application (RTP RTCP)	UDP 24576 ~ 32767	—	—	Bidirectional	- Audio media streaming - Kernel streaming device driver.
	TCP 32768 ~ 61000	—	—	Bidirectional	Generic ephemeral TCP ports (see table note).
	UDP 32768 ~ 61000	—	—	Bidirectional	Generic ephemeral UDP ports (see table note).
Notification Service ActiveMQ	TCP 61616	Chat applications	—	Bidirectional	Notification Service—ActiveMQ OpenWire transport connector.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic direction	Purpose
Unified CCX	TCP 1994	—	—	Bidirectional	—
Unified IP IVR Cluster View Daemon (CVD)	TCP 1994	—	—	Bidirectional	—
Unified IP IVR Engine	TCP 5000	Unified ICM	—	Bidirectional	Using this port Unified ICM Subsystem listens to GED-125Clients. This port is modifiable.

Table Notes

1. Intra-cluster communication in the table represents communication between Unified CCX/IP-IVR servers in a cluster.
2. TCP Ephemeral ports are used to accept connections during Java RMI communication. Java RMI clients know which port it must connect, because RMI first connects to RMI Registry (well-known port - 6999) and get the information which ephemeral port client must connect to Unified CCX Administration page, Unified CCX Engine and CVD use RMI communication in CCX/IP-IVR, so TCP ephemeral port range is opened up for intra-cluster communication between these processes.
3. UDP Ephemeral ports are used to receive audio/video RTP streams; so UDP Ephemeral port range is opened for incoming connections for streaming RTP media from CTI ports.
4. Port 38983 is open only on Unified CCX systems that were upgraded from versions earlier than 9.0(1).

Finesse Port Utilization

Table 3: Cisco Finesse Server

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Cisco Unified Web Proxy Service (HTTPS)	TCP 8445	Browser and third-party REST clients	—	Bidirectional	Secure port used for Finesse administration console, Finesse agent and supervisor desktop, Finesse Desktop Modules (gadgets) with the Finesse desktop and Finesse IP Phone Agent. Secure port used to communicate between Unified CCX Publisher and Subscriber for synchronizing configurations.

Note Finesse desktop uses specific ports for communication between Finesse servers for intra-cluster traffic. For the complete list of the ports that are used, see *System Services Port Utilization*.

The Manage Digital Channel gadget uses HTTPS Port 443 to access the internet. The URI used will vary depending on the region. For more information on region-specific URI, see Manage Digital Channels gadget section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

Table 4: Cisco Finesse Notification Service

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
XMPP	TCP 5223	Browser and agent desktop	—	Bidirectional	Secure XMPP connection between the Finesse server and custom third-party applications. Secure XMPP connection between Unified CCX Publisher and Subscriber.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
BOSH (HTTPS)	TCP 7443	Browser and agent desktop	—	Bidirectional	Secure BOSH connection between the Finesse server and agent and supervisor desktops for communication over HTTPS.

Note Finesse desktop uses specific ports on CUIC and Live Data to render Live Data gadgets and reports. For the complete list of the ports that can be used, see *Unified Intelligence Center Port Utilization*.

Table 5: Primary and Secondary Node Communication

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
XMPP	TCP 5222	—	—	Bidirectional	The primary and secondary Finesse servers use this XMPP connection to communicate with each other to monitor connectivity.

Third-Party (External) Web Server

Note Gadgets hosted on a third-party (external) web server are fetched through the Finesse server on the port exposed by said web server.

Unified Intelligence Center Port Utilization

Table 6: Web Requests to Cisco Unified Intelligence Center

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Notes
Unified Intelligence Center	TCP 8081	Browser	—	—	HTTP - Unified Intelligence Center
	TCP 8444	Browser	—	—	HTTPS - Unified Intelligence Center
	TCP 8447	Browser	—	—	HTTPS - Unified Intelligence Center Online Help

Table 7: Intracluster Ports Between Cisco Unified Intelligence Center

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Notes
CUIC Reporting Process	UDP 54327 (Multicast)	Unified Intelligence Center Node	—	—	Hazelcast Discovery
CUIC Reporting Process	TCP 57011	Unified Intelligence Center Node	—	—	Hazelcast

For more information on other port usages, see: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Port Utilization in Cisco Cloud Connect

Table 8: Cisco Unified Web Proxy

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Cisco Unified Web Proxy Service (HTTPS)	TCP 8445	Applications	—	Inward from applications to Cloud Connect Services.	

Table 9: Cloud Connect Services

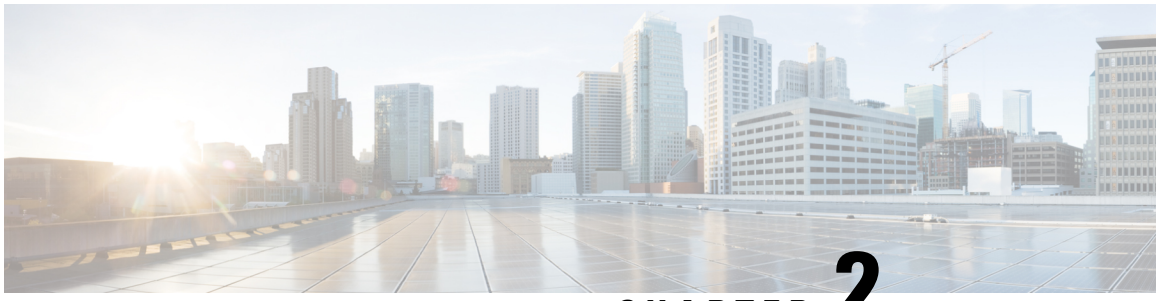
Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CherryPoint Service	TCP 3551	CherryPoint Service on the other node in the same cluster.		Bidirectional	CherryPoint services use this port for secure cluster management.
EvaPoint Service	TCP 4551	EvaPoint Service on the other node is the same cluster.		Bidirectional	EvaPoint services use this port for secure cluster management.
Certificate Management Service	UDP 6389 TCP 7237	–-	–-	Bidirectional	Ports are used for replicating data.

Cloud Connect External Connections

Note When using a proxy for Cloud Connect integration, ensure the domains and URLs listed in the table below are added to the proxy allowlist.

Table 10: Cloud Connect External Connections

(Process or Application Protocol)	Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CloudConnectMgmt		Fusion Management Service https://hercules-a.wbx2.com, https://hercules-k.wbx2.com, https://hercules-r.wbx2.com	TCP 443		
CloudConnectMgmt		WxCC Services https://*.ciscoservice.com	TCP 443		
CloudConnectMgmt		Webex Identity https://idbroker.webex.com	TCP 443		
CherryPoint		Webex Experience Management	TCP 443		Get remote host address from the Webex Experience Management



CHAPTER 2

Port Utilization in Customer Collaboration Platform

Port Utilization Table Columns

The columns in the port utilization tables in this document describe the following:

Listener (Process or Application Protocol)

A value representing the server or application and where applicable, the open or proprietary application protocol.

Listener Protocol and Port

An identifier for the TCP or UDP port that the server or application is listening on, along with the IP address for incoming connection requests when acting as a server.

Remote Device (Process or Application Protocol)

The remote application or device making a connection to the server or service specified by the protocol.

Remote Port

The identifier for the TCP or UDP port that the remote service or application is listening on, along with the IP address for incoming connection requests when acting as the server.

Traffic Direction

The direction that traffic flows through the port: Inbound, Bidirectional, Outbound.

Note

- The operating system dynamically assigns the source port that the local application or service uses to connect to the destination port of a remote device. In most cases, this port is assigned randomly above TCP/UDP 1024.
- For security reasons, keep open only the ports mentioned in this guide and those required by your application. Keep the rest of the ports blocked.

Customer Collaboration Platform Port Utilization

Table 11: Customer Collaboration Platform Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Destination Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Purpose
Email notifications	25	—	—	—	Outward, from Customer Collaboration Platform to the configured email server.	Customer Collaboration Platformcommunicates with the configured email server (that can be in the corporate intranet or on the internet) to send email notifications.
HTTP	80	—	—	—	Bidirectional	Used for unsecure (HTTP) traffic: • From the Customer Collaboration Platform user interface (browser) or APIs to the Customer Collaboration Platform server. • From the Customer Collaboration Platform server to the internet. Customer Collaboration Platform communicates outward to the internet to fetch social contact information (such as Facebook posts and tweets) over HTTP. • From the internet or corporate website to the Customer Collaboration Platform server. Customer Collaboration Platform receives incoming chat and callback requests from the internet or corporate website over HTTP.

Listener (Process or Application Protocol)	Listener Protocol and Port	Destination Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Purpose
HTTPS	Port 443	—	—	—	Bidirectional	Used for secure (HTTPS) traffic • From the Customer Collaboration Platform user interface (browser) or APIs to the Customer Collaboration Platform server. • From the Customer Collaboration Platform server to the internet. Customer Collaboration Platform communicates outward to the internet to fetch social contact information (such as Facebook posts and tweets) over HTTPS. • From the internet or corporate website to the Customer Collaboration Platform server. Customer Collaboration Platform receives incoming chat and callback requests from the internet or corporate website over HTTPS.
Email notifications SSL/TLS	Port 465 (configurable)		—	—	Outward, from Customer Collaboration Platform to the configured email server.	Customer Collaboration Platform communicates with the configured email server (that can be in the corporate intranet or on the internet) to send email notifications.

Listener (Process or Application Protocol)	Listener Protocol and Port	Destination Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Purpose
Email (SMTP)	Port 587 (configurable in Unified CCX Administration)		—	—	Outward, from Customer Collaboration Platform to the Exchange Server.	Used by the Email Reply API to send email. The Email Reply API uses SMTP to send a response to a customer email message.
Email (secure IMAP/IMAPS)	Port 993 (configurable in Unified CCX Administration)		—	—	Outward, from Customer Collaboration Platform to the Exchange Server.	Used by email feeds to retrieve email. IMAPS allows email feeds to fetch email from the Exchange Servers and allows the Email Reply API to retrieve email and save draft email messages.
Customer Collaboration Platform Chat Gateway webhook interface (HTTPS)	Port 10443		—	—	Unidirectional, Inward from the Internet to Cisco Customer Collaboration Platform server.	This TCP port is enabled for public access to the Customer Collaboration Platform Chat Gateway webhook interface.
XMPP (IM) notifications using an external XMPP server	Port 5222 (configurable)		—	—	Bidirectional	Customer Collaboration Platform communicates with the configured XMPP Notifications server (that can be in the corporate intranet or on the internet) to send XMPP (IM) notifications. Outward, from Customer Collaboration Platform to the configured XMPP Notifications server.

Listener (Process or Application Protocol)	Listener Protocol and Port	Destination Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Purpose
Notification Service (XMPP eventing over TCP sockets)	Port 5222		—	—	Bidirectional	Customer Collaboration Platform listens for incoming TCP socket connections to register and send XMPP events. Unified CCX uses this port to receive social contact events. Inward, from CCX to the Customer Collaboration Platform server.
Eventing and chat (BOSH)	Port 7071		—	—	Bidirectional	The unsecure BOSH connection supports eventing and chat communication between the Customer Collaboration Platform user interface and the Customer Collaboration Platform server.
Eventing and chat (secure BOSH)	Port 7443 is used for secure BOSH connections to the XMPP eventing server.	—	—	—	Bidirectional	The secure BOSH connection supports eventing and chat communication between the Customer Collaboration Platform user interface and the Customer Collaboration Platform server.