



# Port Utilization in Customer Collaboration Platform

---

- [Port Utilization Table Columns, on page 1](#)
- [Customer Collaboration Platform Port Utilization, on page 2](#)

## 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 1: 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 Platform communicates 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: <ul style="list-style-type: none"> <li>• From the Customer Collaboration Platform user interface (browser) or APIs to the Customer Collaboration Platform server.</li> <li>• 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.</li> <li>• 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.</li> </ul>

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	<p>Used for secure (HTTPS) traffic</p> <ul style="list-style-type: none"> <li>• From the Customer Collaboration Platform user interface (browser) or APIs to the Customer Collaboration Platform server.</li> <li>• 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.</li> <li>• 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.</li> </ul>
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.
HTTPS	8442	—	—	—	Bidirectional	Used for secure (HTTPS) traffic: <ul style="list-style-type: none"> <li>• From the client browser to Customer Collaboration Platform through the VPN-less reverse-proxy</li> </ul>

**Note**

- 
- In VPN-less deployment, port mapping can be configured between upstream servers and reverse-proxy servers. For example, CCP openfire port 7743 can be mapped to 7442 at the reverse-proxy side. However, ensure that these ports aren't blocked from the client system.
  - Microsoft 365 categorizes the endpoints to help organizations manage network traffic for better performance and security. CCP uses the endpoints [outlook.office365.com](https://outlook.office365.com), [smtp.office365.com](https://smtp.office365.com), and [login.microsoftonline.com](https://login.microsoftonline.com). These endpoints are categorized as
    - [outlook.office365.com](https://outlook.office365.com)—Optimize Required
    - [smtp.office365.com](https://smtp.office365.com)—Allow Optional
    - [login.microsoftonline.com](https://login.microsoftonline.com)—Allow Required

For details on category descriptions, please refer to the Microsoft 365 URLs and IP address ranges document at

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>.

---