Port Utilization in Unified CCX

- Port Utilization Table Columns, on page 1
- System Services Port Utilization, on page 2
- Unified CCX and IP IVR Port Utilization, on page 5
- Finesse Port Utilization, on page 8
- Unified Intelligence Center Port Utilization, on page 10
- Port Utilization in Cisco Cloud Connect, on page 11

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
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
DBMON	TCP 1501	—	—	Bidirectional	- This is an alternate port to bring up a second instance of IDS during upgrade. - Localhost traffic only

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
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.
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.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
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 5701	Intra-cluster communication	5701 **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 (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.
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.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
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 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
Informix Dynamic Server (IDS)	TCP 1504	External process like CUIC, WallBoard Client, External DB clients (like Squirrel or others for custom reporting) can connect	—	Bidirectional	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

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic direction	Purpose
Cisco Identity Service Data Grid	TCP 5701	Intra-cluster communication	5701 **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
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

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic direction	Purpose
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
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.
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.

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		

(Process or Application Protocol)	Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CherryPoint		Webex Experience Management	TCP 443		Get remote host address from the Webex Experience Management