Port Utilization Guide for Cisco Unified Contact Center Solutions, Release 12.6(2)

First Published: 2023-04-28

Last Modified: 2025-11-30

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 1994–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface v

Change History v

About This Guide v

Audience v

Obtaining Documentation and Submitting a Service Request v

Field Notice v

Documentation Feedback vi

Conventions vi

CHAPTER 1 **Port Utilization in System Services** 1

Port Utilization Table Columns 1

System Services Port Utilization 2

CHAPTER 2 **Port Utilization in Contact Center Enterprise** 7

Unified CCE and Packaged CCE Port Utilization 7

Unified CCMP Port Utilization 22

Unified CRM Connectors Port Utilization 24

CHAPTER 3 **Port Utilization in Cisco Cloud Connect** 25

Port Utilization in Cisco Cloud Connect 25

CHAPTER 4 **Port Utilization in CVP** 29

Unified CVP Port Utilization 29

CHAPTER 5 **Port Utilization in Cisco VVB** 37

Cisco VVB Port Utilization 37

CHAPTER 6 **Port Utilization in Finesse** 39

Finesse Port Utilization 39

CHAPTER 7 **Port Utilization in Customer Collaboration Platform** 43

Customer Collaboration Platform Port Utilization 43

CHAPTER 8 **Port Utilization in Unified Intelligence Center** 47

Unified Intelligence Center Port Utilization 47

Preface

Change History

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

Change	See	Date
Initial Release of Document for Release 12.6(2)		April, 2023
Added a note for deprecated ports for OMAP and Live Data.	OAMP and CUIC Live Data table	
Added the TCP 6379 port for the Digital Routing service.	Cloud Connect 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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

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.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

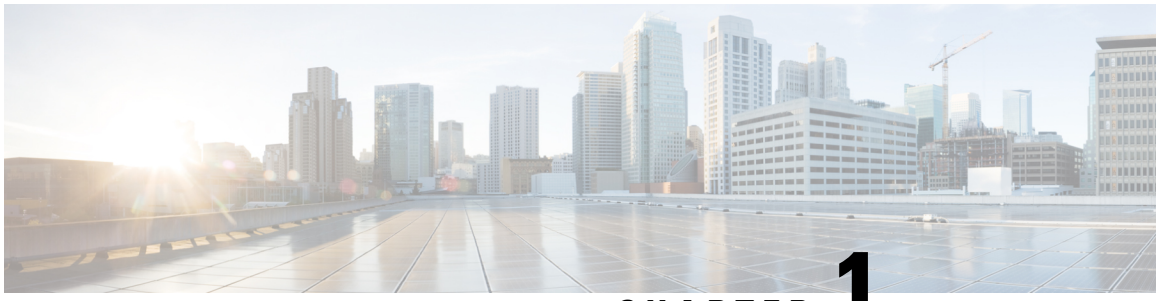
Conventions

This document uses the following conventions:

Table 2: Conventions

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
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. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`

Convention	Description
< >	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.



CHAPTER 1

Port Utilization in System Services

- Port Utilization Table Columns, on page 1
- System Services 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 remote port is used to make an outgoing connection to the corresponding listener port.

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 from unused ports in the ephemeral port range 1024 - 65535.
- 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.

Note The preceding column descriptions apply to all the tables in this Port Utilization guide.

System Services Port Utilization

Table 3: 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 - Call recording server - Unified CCMP Web server and AXL provisioning - CRM Connector server - Default port for voice browsers to fetch media and "external VXML" files from media server
System Service	UDP 123	—	—	Bidirectional	NTP, network time sync
SNMP Agent	UDP 161	—	—	Bidirectional	Provide services for SNMP-based management applications
IIS	TCP 443	Client Browser Unified CCE Admin (AW-HDS) Web Setup	—	Bidirectional	Web access for CCE Web Administration, Web Setup, and Internet Script Editor - Unified CCMP clients - Default port for voice browsers to fetch media and "external VXML" files from media server
AON Management Console (AMC) Service	TCP 1090	Intracluster communication	—	Bidirectional	Provide RTMT data collecting, logging and alerting functionalities (AMC RMI Object Port)

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

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

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic direction	Purpose
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, configuration APIs, and mobile supervisor applications. - Data replication for call recording server - OAMP for Live Data - CRM Connector for SAP (adjustable through registry)
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, configuration APIs, and mobile supervisor applications. - 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) [1]	TCP 8553	—	—	—	HTTPS for Cisco IdS

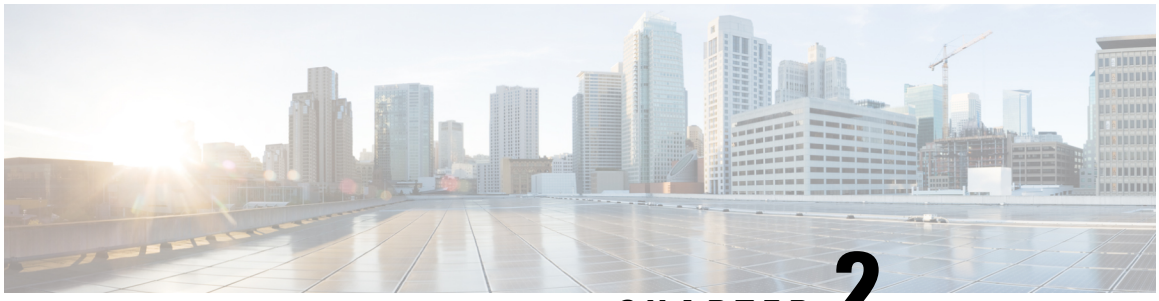
[1] Not applicable to Cisco Virtualized Voice Browser.

SOAP Port Considerations

The following considerations apply to the Simple Object Access Protocol (SOAP) ports:

- SOAP monitor uses specific ports to send the corresponding SOAP API requests.

- Access to the ports are always authenticated with the Username and Password authentication.



CHAPTER 2

Port Utilization in Contact Center Enterprise

- Unified CCE and Packaged CCE Port Utilization, on page 7
- Unified CCMP Port Utilization, on page 22
- Unified CRM Connectors Port Utilization, on page 24

Unified CCE and Packaged CCE Port Utilization

This table includes information for Unified CCE and CTI OS.

Some port definitions use a formula. For example:

```
TCP 40007 + (Instance Number * 40)
```

In this example, instance 0 uses port 40007, instance 1 uses port 40047, instance 2 uses port 40087, and so on.

Note In the following table, PG1, PG2, and PG3 are not specific PG numbers or DMP IDs. They are the order in which the PGs get installed.

Note This document does not include the Enterprise Chat and Email (ECE) port details. For more information on ECE ports, see the ECE documentation at: https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/tsd-products-support-series-home.html.

Table 4: Unified CCE Port Utilization: Routers, PGs, Administration & Data Servers, and Loggers

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Router (side B) (MDS)	**Private low:** • TCP 41004 + (instance number * 40) **Private medium:** • TCP 41016 + (instance number * 40) **Private high:** • TCP 41005 + (instance number * 40) **State Xfer for CIC:** • TCP 41022 + (instance number * 40) **State Xfer for HLGR:** • TCP 41021 + (instance number * 40) • TCP 41032 + (instance number * 40) **State Xfer for RTR:** • TCP 41020 + (instance number * 40) UDP 39500–39999 **State Xfer for DBAgent:** • TCP 41033 + (instance number * 40)	Router (side A) (MDS)		Bi-directional	Private network at the central controller site **Note** UDP ports are not used, if QoS is enabled on the router private interface.
Router (side B) (MDS)	MDS process port TCP 41000	MDS process client		Bi-directional	
Router (side B) (MDS)	MDS state transfer port TCP 41001	MDS process client (synchronized)		Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Router (side A and B) (DB Worker)	DB Worker process port UDP 445	DB Worker process client		Bi-directional	
ICM PG1 (side A and B) (pgagent)	TCP 43006 + (instance number * 40)	ICM PG1 (Opposite Side: A or B) (pgagent)		Bi-directional	Public network (test-other-side)
ICM PG2 (side A and B) (pgagent)	TCP 45006 + (instance number * 40)	ICM PG2 (Opposite Side: A or B) (pgagent)		Bi-directional	Public network (test-other-side)
ICM PG3 (side A and B) (pgagent)	TCP 47506 + (instance number * 40)	ICM PG3 (Opposite Side: A or B) (pgagent)		Bi-directional	Public network (test-other-side)
ICM PG1 (side A and B) (MDS)	• Private low: TCP 43004 + (instance number * 40) • Private medium: TCP 43016 + (instance number * 40) • Private high: TCP 43005 + (instance number * 40) • State Xfer for OPC: TCP 43023 + (instance number * 40) UDP 39500–39999	ICM PG1 (Opposite Side: A or B)		Bi-directional	Private network **Note** UDP ports are not used, if QoS is enabled on the ICM PG private interface.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
ICM PG2 (side A and B) (MDS)	• Private low: TCP 45004 + (instance number * 40) • Private medium: TCP 45016 + (instance number * 40) • Private high: TCP 45005 + (instance number * 40) • State Xfer for OPC: TCP 45023 + (instance number * 40) UDP 39500–39999	ICM PG2 (Opposite Side: A or B)		Bi-directional	Private network **Note** UDP ports are not used if QoS is enabled on the ICM PG private interface.
ICM PG3 (side A and B) (MDS)	• Private low: TCP 47504 + (instance number * 40) • Private medium: TCP 47516 + (instance number * 40) • Private high: TCP 47505 + (instance number * 40) • State Xfer for OPC: TCP 47523 + (instance number * 40) UDP 39500–39999	ICM PG3 (Opposite Side: A or B)		Bi-directional	Private network **Note** UDP ports are not used if QoS is enabled on the ICM PG private interface.
ICM PG1 (side B) (MDS)	MDS process port TCP 43000	MDS process client		Bi-directional	
ICM PG1 (side B) (MDS)	MDS state transfer port TCP 43001	MDS process client (synchronized)		Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
ICM PG2 (side B) (MDS)	MDS process port TCP 45000	MDS process client		Bi-directional	
ICM PG2 (side B) (MDS)	MDS state transfer port TCP 45001	MDS process client (synchronized)		Bi-directional	
ICM PG3 (side B) (MDS)	MDS process port TCP 47500	MDS process client		Bi-directional	
ICM PG3 (side B) (MDS)	MDS state transfer port TCP 47501	MDS process client (synchronized)		Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Router (side A) (MDS)	**Private low:** • TCP 41004 + (instance number * 40) **Private medium:** • TCP 41016 + (instance number * 40) **Private high:** • TCP 41005 + (instance number * 40) **State Xfer for CIC:** • TCP 41022 + (instance number * 40) **State Xfer for HLGR:** • TCP 41021 + (instance number * 40) • TCP 41032 + (instance number * 40) **State Xfer for RTR:** • TCP 41020 + (instance number * 40) UDP 39500–39999 **State Xfer for DBAgent:** • TCP 41033 + (instance number * 40)	Router (side B) (MDS)		Bi-directional	Private network at the central controller site **Note** UDP ports are not used if QoS is enabled on the router private interface.
Router (side A) (MDS)	MDS process port TCP 40000	MDS process client		Bi-directional	
Router (side A) (MDS)	MDS state transfer port TCP 40001	MDS process client (synchronized)		Bi-directional	
ICM PG1 (side A) (MDS)	MDS process port TCP 42000	MDS process client		Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
ICM PG1 (side A) (MDS)	MDS state transfer port TCP 42001	MDS process client (synchronized)		Bi-directional	
ICM PG2 (side A) (MDS)	MDS process port TCP 44000	MDS process client		Bi-directional	
ICM PG2 (side A) (MDS)	MDS state transfer port TCP 44001	MDS process client (synchronized)		Bi-directional	
ICM PG3 (side A) (MDS)	MDS process port TCP 46000	MDS process client		Bi-directional	
ICM PG3 (side A) (MDS)	MDS state transfer port TCP 46001	MDS process client (synchronized)		Bi-directional	
Router (side A) DMP (ccagent)	**Secure mode enabled** • Public low: TCP 40002 + (instance number * 40) • Public medium: TCP 40017 + (instance number * 40) • Public high: TCP 40003 + (instance number * 40) UDP 39500–39999	ICM PG (pgagent)		Bi-directional	Public network connecting the PG to the central controller Router to pre-5.0 PG communication. **Note** UDP ports are not used if QoS is enabled on the ICM PG private interface.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Router (side B) DMP (ccagent)	• Public low: TCP 41002 + (Instance Number * 40) • (instance number Public medium: TCP 41017 + (instance number * 40) • Public high: TCP 41003 + (instance number * 40) UDP 39500–39999	ICM PG (pgagent)		Bi-directional	Public network connecting the PG to the central controller Router to pre-5.0 PG communication. **Note** UDP ports are not used if QoS is enabled on the ICM PG private interface.
Router A (rtfeed)	TCP 40007 + (instance number * 40)	Administration & Data Server		Bi-directional	Real-time feed
Router B (rtfeed)	TCP 41007 + (instance number * 40)	Administration & Data Server		Bi-directional	Real-time feed
Router A (DB Agent)	TCP 40019 + (instance number * 40)	Administration & Data Server		Bi-directional	Secure EMT port to DB Agent
Router B (DB Agent)	TCP 41019 + (instance number * 40)	Administration & Data Server		Bi-directional	Secure EMT port to DB Agent
Router A (DB Agent)	TCP 40019 + (instance number * 40)	Administration client		Bi-directional	Secure EMT port to DB Agent
Logger (side A)	• TCP 40026 + (instance number * 40) • TCP 40028 + (instance number * 40)	Administration & Data Server Historical Data Server (HDS)		Bi-directional	Replication
Logger (side A)	**Secure mode enabled** TCP 40032 + (instance number * 40)	Dialer and Import		Bi-directional	Campaign Manager EMT port to Dialer
Logger (side B)	• TCP 41026 + (instance number * 40) • TCP 41028 + (instance number * 40)	Administration & Data Server Historical Data Server (HDS)		Bi-directional	Replication

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Logger (side B)	TCP 41036 + (instance number * 40)	Dialer and Import		Bi-directional	Campaign Manager EMT port to Dialer
Logger (side A)	TCP 40024 + (instance number * 40)	Logger (side B)		Bi-directional	Secure Campaign Manager EMT port to other side of Campaign Manager
Primary Administration & Data Server (rtfeed)	TCP 48008 + (instance number * 40)	Administration client		Bi-directional	Real-time feed
Secondary Administration & Data Server (rtfeed)	TCP 49008 + (instance number * 40)	Administration client		Bi-directional	Real-time feed
Primary Administration & Data Server (rtfeed)	TCP 48007 + (instance number * 40)	Administration client		Bi-directional	RTD to RTC secure port
Secondary Administration & Data Server (rtfeed)	TCP 48007 + (instance number * 40)	Administration client		Bi-directional	RTD to RTC secure port
Contact Sharing	TCP 61616	Active MQ for Live Data	TCP 61616	Bidirectional	
CICM Router (side A) (INCRPNIC)	UDP 40025 + (instance number * 40)	NAM Router (CIC)		Bi-directional	Public network connecting the NAM to the CICM
CICM Router (side B) (INCRPNIC)	UDP 41025 + (instance number * 40)	NAM Router (CIC)		Bi-directional	Public network connecting the NAM to the CICM
CSFS	TCP 40015	CSFS duplexed peer		Bi-directional	CSFS event synchronization link
Logger Recovery Process (side A)	41013 + (instance number *40)			Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Logger Recovery Process (side B)	40013 + (instance number *40)			Bi-directional	
Diagnostic framework	TCP 7890	Any client that is requesting information from the diagnostic service.		Bi-directional	This serviceability component is installed on major CCE component servers (e.g. router, logger, PG, and Administration and Data Servers)

Table 5: Unified CCE Port Utilization: Administration & Data Servers and Logger

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
MSSQL	TCP 1433(Default)	Logger Distributor		Bi-directional	Ensure the chosen custom SQL Server port does not overlap with the reserved ports used by CCE services as defined in this document.

Table 6: Unified CCE Port Utilization: CCE Outbound Option Dialer

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Dialer	58800 + instNum *instNum* is the instance number for the Dialer.	Voice Gateway	UDP 58800	Bi-directional	Set in the **SIPDialerPortBaseNumber** registry key.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
RTP for SIP	UDP ports in a range based on these formulas: • RangeStart = RTPPortRangeStart + (*instNum* * 2000) • RangeEnd = RangeStart + 2000 You can set RTPPortRangeStart in the registry key: **RTPPortRangeStart**.	Voice gateway		Bi-directional	Receive ports for reservation calls. Use the following registry key to select and configure UDP ports: **RTPPortRangeStart**
MR PG	TCP 38001+ (instance number)	Dialer		Bi-directional	The MR PG connects to the SIP Dialer using this port.
Dialer (SIP)	5060 and "SIPDialerPortBaseNumber + instance number"	Voice Gateway or SIP Proxy		Bi-directional	Set in the **SIPServerPortNumber** registry key.

Table 7: Unified CCE Port Utilization: CTI and CTI Object Server

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
GED-188 (CTI Server) unsecured	Side A TCP 42027 + (instance number * 40) Side B TCP 43027 + (instance number * 40)	Finesse Cisco Outbound Dialer ARM Interface CTI OS Server		Bi-directional	CTI OS is only supported for TDM and System PG.
GED-188 (CTI Server) secured	Side A TCP 42030 + (instance number * 40) Side B TCP 43030 + (instance number * 40)	Finesse Cisco Outbound Dialer ARM Interface CTI OS Server		Bi-directional	CTI OS is only supported for TDM and System PG.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CTI OS Server	TCP 42028	CTI OS Client CTI OS Server Peers CAD Desktop Cisco Sync Service		Bi-directional	Applicable to first CTI OS instance. Multi-instance CTI OS require a custom port be defined.
CTI OS Server	TCP 42028	CTI OS Client CTI OS Server Peers Cisco Sync Service		Bi-directional	CTI OS is only supported for TDM and System PG. Applicable to first CTI OS instance. Multi-instance CTI OS require a custom port be defined.
CTI OS Supervisor Desktop	UDP 39200	CTI OS Client		Bi-directional	Desktop Silent Monitoring
CTI OS Supervisor Desktop	UDP 39200	CTI OS Client		Bi-directional	Desktop Silent Monitoring CTI OS Supervisor Desktop is only supported for System PG.
CTI OS Silent Monitor Service	TCP 42228			Bi-directional	
CTI OS Silent Monitor Service	TCP 42228	CTI OS Client		Bi-directional	CTI OS Silent Monitor Service is only supported for System PG.

Table 8: Unified CCE Port Utilization: TDM/IP Peripherals

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
IP Process Communications					
CTI/QBE			TCP 2748	Bi-directional	JTAPI

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Customer Voice Portal — Call Server Cisco Unified IP-IVR		PG, VRU PIM (GED-125)	TCP 5000–5001	Bi-directional	Unified ICM/IVR message interface, VRU PIM
CCE PG	TCP 2789	Unified CM		Bi-directional	JTAPI application server
Media Routing process		MR PIM	TCP 38001	Bi-directional	
TDM Process Communications **Note** For more information on peripheral communication, see the "ACD Supplement" user documentation for the specific switch you are using.					
Avaya ACD CMS	TCP 6060–6070	Avaya PIM	TCP 5678	Bi-directional	Event link
UCCE System PG / CTI Server	TCP 42027	UCCE Gateway PIM		Bi-directional	Port number is configurable

Note For port utilization information about Network Interface Controllers (NICs), refer to the TCP/IP-based NIC System Management Guide Supplements and setup parameters of the NIC or SCP connections.

Table 9: Unified CCE Port Utilization: Windows Authentication and Remote Administration Ports

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
RPC	TCP 135 UDP 135			Bi-directional	
NetBIOS Session	TCP 139			Bi-directional	
NetBIOS Name Resolution	TCP 137 UDP 137			Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
NetBIOS Netlogon/ Browsing	UDP 138			Bi-directional	
SMB	TCP 445 UDP 445[2]			Bi-directional	
LDAP	TCP 389 UDP 389			Bi-directional	
LDAP SSL	TCP 636			Bi-directional	
LDAP GC	TCP 3268			Bi-directional	
LDAP GC SSL	TCP 3269			Bi-directional	
Active Directory Web Services	TCP 9389 UDP 9389			Bi-directional	Powershell uses this port.
DNS	TCP 53 UDP 53			Bi-directional	
Kerberos	TCP 88 UDP 88			Bi-directional	

[2] DB Worker uses UDP 445. This port is also used for named pipes connectivity.

Note For more information on Windows authentication, see Service overview and network port requirements for the Windows in Microsoft documentation.

Table 10: Unified CCE Port Utilization: Network Management and Remote Administration

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
SNMP–Trap	UDP 162			Bi-directional	
Syslog	UDP 514			Bi-directional	
Telnet	TCP 23			Bi-directional	

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
RDP (Terminal Services)	TCP 3389			Bi-directional	
pcAnywhere	TCP 5631 UDP 5632			Bi-directional	
VNC	TCP 5900 TCP 5800 (Java HTTP)			Bi-directional	RealVNC

Table 11: Unified CCE Port Utilization: Live Data

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Notes
Router (side A and B) (TIP Event)	Router A: 40034 + (instance number * 40) Router B: 41034 + (instance number * 40)	CUIC/Live Data		Bi-directional	Public network Live Data Events.
Router (side A and B) (TIP TOS)	Router A: 40035 + (instance number * 40) Router B: 41035 + (instance number * 40)	CUIC/Live Data		Bi-directional	Public network Live Data Test Other Side.
ICM PG1 (side A and B) (TIP Event) [3]	Side A: 42034 + (instance number * 40) Side B: 43034 + (instance number * 40)	CUIC/Live Data		Bi-directional	Public network Live Data Events.
ICM PG2 (side A and B) (TIP Event)	Side A: 44034 + (instance number * 40) Side B: 45034 + (instance number * 40)	CUIC/Live Data		Bi-directional	Public network Live Data Events.
ICM PG1 (side A and B) (TIP TOS)	Side A: 42035 + (instance number * 40) Side B: 43035 + (instance number * 40)	CUIC/Live Data		Bi-directional	Public network Live Data Test Other Side.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Notes
ICM PG2 (side A and B) (TIP TOS)	Side A: 44035 + (instance number * 40) Side B: 45035 + (instance number * 40)	CUIC/Live Data		Bi-directional	Public network Live Data Test Other Side.

[3] The ports for TIP/TOS connections are assigned based on the order in which the PG pair (side A/B) is installed on the same server. For example, the first PG pair (PG1 Side A/B) installed, is assigned TIP base ports 42034 and 43034 respectively. The second PG pair (PG2 Side A/B) installed, is assigned ports 44034 and 45034 respectively. The same assignment is applicable to TOS ports as well.

Table 12: Unified CCE Port Utilization: External Connections

Process or Application Protocol	Protocol and Port	Remote Device	Remote Port	Traffic Direction	Notes
AW Tomcat	—	Hybrid Services on cloud	443	Bi-directional	Following URLs must be included in the allowed list of network: *.wbx2.com *.ciscoccservice.com

Unified CCMP Port Utilization

Table 13: Cisco Unified Contact Center Management Portal Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CCMP Web/Application server A/B					
LDAP (Domain Controller)	UDP 389 TCP 389	Integrated Configuration Environment (ICE)			Used to read AD account information for supervisor provisioning
CCMP Database server A/B					

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
SQL	TCP 1433(Default)	CCMP DB server A/B			Standard SQL Connection and for SQL replication
	TCP 1433(Default)	CCE/CCH Administration and Data server side A/B			For import of CCE/CCH dimension data
*MSDTC	TCP 135	CCMP DB sever A/B	TCP 1024-5000		For the CCMP audit archive job
SMB over IP (CVP Media Server)	UDP 445* TCP 445	Integrated Configuration Environment			For CVP file upload file replication
* Also used for named pipes connectivity.					

These assume the Server Name field in ICE is configured with either a TCP/IP address or DNS name (hence no NETBIOS port requirements).

Ports are also required to access all Unified Contact Center Management Portal servers for support reasons (either pcAnywhere or terminal services).

Note This list does not include standard Windows ports such as DNS and Kerberos.

* MSDTC response ports by default use a dynamically allocated port in the range of 1024 to 5000. You can configure this range creating the HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet location registry key and adding the following registry values:

- Ports (REG_MULTI_SZ) - specify one port range per line, for example, 3000-3005
- PortsInternetAvailable (REG_SZ) - always set this value to "Y" (do not include the quotes)
- UseInternetPorts (REG_SZ) - always set this value to "Y" (do not include the quotes)

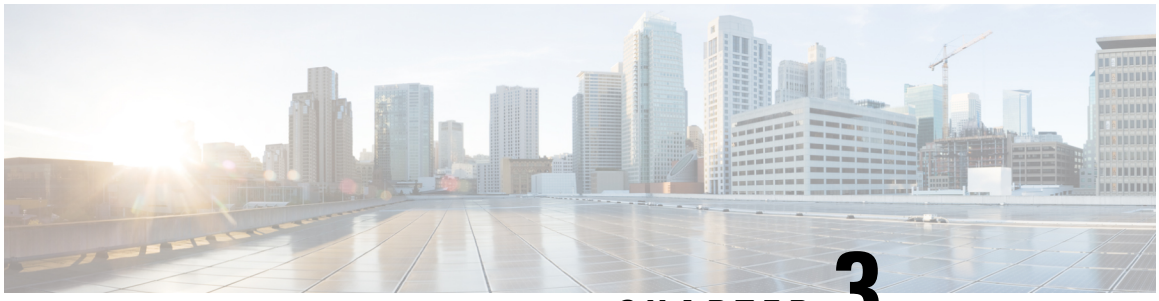
Unified CRM Connectors Port Utilization

Table 14: Cisco Unified CRM Connector for SAP

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Notes
CRM DataStore for SAP	TCP 42029	CRM Connector for SAP			

Table 15: Cisco Unified CRM Connector for Microsoft CRM, Oracle PeopleSoft, Salesforce.com

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Protocol and Port	Traffic Direction	Notes
MSCRM Server	TCP 81	MSCRM Client			MSCRM only.
CRM Connector Server	TCP 5666	CRM Adapters			Configurable in \Program Files\Cisco\CRM Connector\MCIS\Config.ini
.NET Adapter	TCP 5558	Agent Desktop			Remoting Port.
CRM Connector Server	TCP 42027	Cisco CTI Server			Default port for side A. Configurable in the Config.ini file [CTIModule Setting] Port_A.
CRM Connector Server	TCP 44027	Cisco CTI Server			Default port for side B. Configurable in the Config.ini file [CTIModule Setting] Port_B.
CRM Connector Server	TCP 65372	Server Administration Tool			Configurable under \Program Files\Cisco\CRM Connector\MCIS\Config.ini and \Program Files\Cisco\CRM Connector\ Server Administration Tool\WebComponent\ server.config



CHAPTER 3

Port Utilization in Cisco Cloud Connect

• Port Utilization in Cisco Cloud Connect, on page 25

Port Utilization in Cisco Cloud Connect

Table 16: 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 17: Cloud Connect Services

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Dataconn Service	TCP 2551	Dataconn Service on the other node in the same cluster.	—	Bidirectional (between two nodes in the same cluster)	Services use this port for secure cluster management.
CherryPoint Service	TCP 3551	CherryPoint Service on the other node in the same cluster.	—	Bidirectional	CherryPoint services use this port for secure cluster management.
Inventory Service	TCP 5551	Inventory Service on the other node in the same cluster.	—	Bidirectional	Inventory services use this port for secure cluster management.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CloudConnectMgmt Service	TCP 6551	CloudConnectMgmt Service on the other node in the same cluster.	—	Bidirectional	CloudConnectMgmt services use this port for secure cluster management.
Digital Routing Service (Redis Service)	TCP 6379	Digital Routing Service on the other node in the same cluster.	—	Bidirectional	Default Redis service port that is used by Digital Routing Service to connect locally, and for Redis instances on Publisher and Subscriber to replicate data between both the nodes.
Ansible Controller	—	SSH Server on Orchestration target node	TCP 22	Outward from Ansible Controller to SSH Server on Orchestration target node	Used for connecting to target node for Orchestration.
Ansible Controller	—	SMTP Relay Server	TCP 25	Outward from Ansible Controller to SMTP Relay Server	Used for sending email notification.

Cloud Connect External Connections

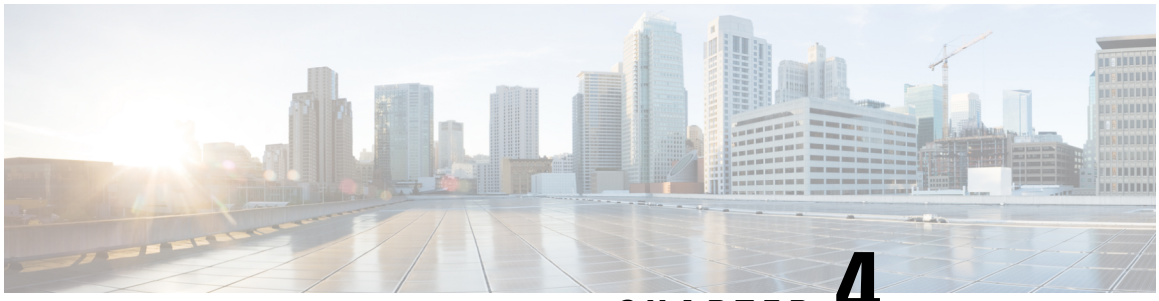
Note When using a proxy for Cloud Connect integration, ensure the domains and URLs listed in the table below are added to the proxy allowlist.

Table 18: Cloud Connect External Connections

(Process or Application Protocol)	Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Dataconn Service	—	Webex Engage API endpoints for user sync. US region—https://api-us-site-1.imiengage.io, https://api-us-site-1.us.webexengage.com, and https://engage-api.produs1.ciscoccservice.com London / UK—https://api-uk-site-1.imiengage.io, https://api-uk-site-1.uk.webexengage.com, and https://engage-api.produeu1.ciscoccservice.com EU region [illegible] and https://engage-api.produeu2.ciscoccservice.com ANZ region—https://api-syd-site-1.imiengage.com.au, https://api-syd-site-1.anz.webexengage.com, and https://engage-api.prodanz1.ciscoccservice.com Canada region—https://api-ca-site-1.imiengage.io, https://api-ca-site-1.ca.webexengage.com, and https://engage-api.prodca1.ciscoccservice.com India region—https://engage-api.prodin1.ciscoccservice.com[4]	TCP 443	Outbound traffic	—
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 https://idbroker-eu.webex.com https://idbroker-b-us.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
Digital Routing	—	Webex Connect tenant specific Webhook endpoint	TCP 443	Outbound traffic	Asynchronous Webhook notifications sent from Digital Routing service to Webex Connect to invoke flows
Digital Routing	—	Region-specific OAuth access token URL of Webex Connect. For the list of URLs based on the location of Webex Connect data center, see the *Integrate Cloud Connect with Webex Connect* section in the Cisco Unified Contact Center Enterprise Features Guide	TCP 443	Outbound traffic	Used to generate tokens for Webhook notifications.
Ansible Controller	—	Cisco Devhub Artifactory	TCP 443	Outward from Ansible Controller to Cisco Devhub Artifactory	Used for communicating with Cisco Devhub Artifactory.
Feature Flag Mgmt	—	Split.io	Both	Outbound traffic	—

[4] India region does not require *.webexengage.com or *.imiengage.io URLs.



CHAPTER 4

Port Utilization in CVP

• Unified CVP Port Utilization, on page 29

Unified CVP Port Utilization

Table 19: Cisco Unified Customer Voice Portal Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
TCP	2000-2002			Bi-directional	Call Manager and gateway interface communication
Call Server JMX	2098	JConsole	Random	Bi-directional	JMX access by JConsole into Call Server
Call Server JMX RMI port	2097	JConsole	Random	Bi-directional	JMX access by JConsole into Call Server
WSM JMX	TCP 10002	JConsole	Random	Bi-directional	JMX access by JConsole into WSM
WSM JMX RMI	TCP 10003	JConsole	Random	Bi-directional	JMX access by JConsole into WSM
OAMP JMX	TCP 10001	JConsole	Random	Bi-directional	JMX access by JConsole into OAMP
OAMP JMX RMI	TCP 10000	JConsole	Random	Bi-directional	JMX access by JConsole into OAMP
CVP Messaging Layer	TCP 23000 - 28000 (First available)	CVP Subsystem		Bi-directional	CVP Message Bus communications

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
7960-CUVA Video	UDP 5445	7960-CUVA		Bi-directional	Cisco 7960-CUVA Video Phone
CVP SIP Subsystem, SIP Proxy Server, Gateway, Unified CM: SIP (Session Initiation Protocol)	UDP 5060 TCP 5060 TLS 5061	SIP endpoints	Local / Remote between CVP components	Bi-directional	Listen port for incoming SIP requests. Port is configurable.
SIP Heartbeat Local Listen Port	UDP 5067 TCP 5067 **Note** This port must be different from the default SIP port which is 5060/5061 (see aforementioned row).	SIP endpoints	Random	Bi-directional	Listen port for incoming Heartbeat.
VXML Server: HTTP	TCP 7000	IOS VXML gateways/VVB	Random	Bi-directional	VXML over HTTP. Calls/sessions answered on port 7000 by HTTP server which relays request to WAS on local system port 9080.
VXML Server: HTTPS	TCP 7443	IOS VXML gateways/VVB	Random	Bi-directional	VXML over HTTPS. Calls/sessions answered on port 7443 by HTTPS server.
VXML Server with Tomcat	TCP 7005	Local machine		Bi-directional	Port restricted to local access only
	TCP 7009			Bi-directional	AJP/1.3 Connector
VXML Server JMX	TCP 9696	JConsole		Bi-directional	JMX access by JConsole into VXML Server
VXML Server JMX RMI port	TCP 9697	JConsole	Random	Bi-directional	JMX access by JConsole into VXML Server

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
VXML Server	TCP 10100	Local VXML Server Administration Scripts		Bi-directional	Port restricted to local access only
CVP Call Server Tomcat: HTTP	TCP 8000	Browser	Random	Bi-directional	HTTP
CVP Call Server Tomcat: HTTPS	TCP 8443	Browser	Local / Remote Random	Bi-directional	HTTPS
CVP IVR Server	TCP 8002	VXML Server		Bi-directional	Message over TCP
CVP Call Server: HTTP	TCP 8005			Bi-directional	Port restricted to local access only
CVP OPSConsole: HTTP	TCP 9000	Web Browser	Random	Bi-directional	Web-based interface for configuring CVP components
CVP OPSConsole: HTTPS	TCP 9443	Web Browser	Random	Bi-directional	Web based interface for configuring CVP components with SSL
CVP OPSConsole	TCP 9005	Local machine		Bi-directional	Port restricted to local access only
CVP OPSConsole	TCP 9009			Bi-directional	AJP/1.3 Connector
CVP OPSConsole	TCP 1529	Local machine		Bi-directional	Port restricted to local access only
CVP Resource Manager FTP Server	TCP 21	Content Services Switch	Random	Bi-directional	Only opened by Resource Manager residing on the same machine as the CVP OPSConsole
CVP Resource Manager	TCP 2099	CVP OPSConsole	Random	Bi-directional	JMX communication from OPSConsole to CVP Resource Manager on remote device

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CVP Resource Manager RMI Port	TCP 3000	CVP OPSConsole	Random	Bi-directional	JMX communication from OPSConsole to CVP Resource Manager on remote device
CVP Resource Manager Java Service Wrapper	TCP 32000 - 32999 (first available)	JVM instance launched by wrapper	Random	Bi-directional	CVP Resource Manager Service Wrapper will no longer accept connections after the first JVM instance is connected.
MRCP V1 (RTSP)	TCP 554	VXML gateway			MRCP session between gateway voice browser and MRCP server. This is the signaling path; the media path uses RTP. Also, Helix streaming audio/ ASR/TTS (MRCP/RTSP)
MCRP V2 (SIP)	TCP 5060	VXML gateway			MRCP session between gateway voice browser and MRCP server. This is the signaling path; the media path uses RTP.
CVP SNMP SubAgent	UDP 5517, 5519, 5521, 5523, 5525, 5527, 5529, 5531, 5533, 5535, 5537, 5539, 5541, 5543, 5545, 5547, 5549, 5551, 5553, 5555	CVP SNMP subsystem		Bi-directional	CVP SNMP SubAgent services local requests from CVP SNMP subsystem
CVP SNMP subsystem	UDP 5516, 5518, 5520, 5522, 5524, 5526, 5528, 5530, 5532, 5534, 5536, 5538, 5540, 5542, 5544, 5546, 5548, 5550, 5552, 5554	CVP SNMP SubAgent		Bi-directional	CVP SNMP subsystem services local requests from CVP SNMP SubAgent

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CVP ICM Subsystem	TCP 5000	IPCC Enterprise VRU CTI (ICM/IVR message interface)	Random	Bi-directional	Between CVP ICM Subsystem (Call Server) and Unified CCE/ICM VRU PG. Port is configurable.
Web Server: HTTP	TCP 80	Voice Browsers	Random	Bi- directional	Voice browsers fetches media and "External VXML" files from media server. This port is configurable.
Web Server: HTTPS	TCP 443	Voice Browsers	Random	Bi- directional	Voice browsers fetches media and "External VXML" files from media server. This port is configurable.
IBM Informix	TCP 1526	CVP Reporting Subsystem	Random	Bi-directional	Database Connection
IBM Informix Storage Manager	TCP 7939 - 7942 TCP 111	IBM Informix		Bi-directional	IBM Informix Storage Manager Services
IBM WAS Console	TCP 9043, 9060	IBM Informix	Random for remote desktop	Bi-directional	
CVP Web Services Manager: HTTP/HTTPS	TCP 8101, 8110, 8111 TCP 10000, 10001, 10002, 10003	Unified System CLI, Diagnostic Portal, Custom Agent Desktop	Random	Bi-directional	REST Web Services TCP 10000, 10001, 10002, 10003 OAMP ports are used for transferring data related to the configuration and administration of VXML Server and Call Server.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
CVP OPSConsole	TCP 443	Hybrid Services on Cloud	Random	Bidirectional	Following URLs must be included in the allowed list of network : *.wbx2.com *.ciscoccservice.com

Table 20: Network Management and Remote Administration

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
SNMP Primary Agent	TCP 7161	Local SNMP subagents		Bi-directional	SNMP Primary Agent listens for TCP connections from local SNMP subagents.
SNMP–Trap	UDP 162	SNMP Primary Agent	Random	Bi-directional	SNMP Primary Agent sends SNMP traps to SNMP management application.
Syslog	UDP 514		Random	Bi-directional	Syslog protocol provides a transport to allow a machine to send event notification messages across IP network to event message collectors. Port is configurable.
Telnet	TCP 23				
RDP (Terminal Services)	TCP 3389		Random	Bi-directional	
pcAnywhere	TCP 5631 UDP 5632				
VNC	TCP 5900 TCP 5800				

Table 21: Windows Authentication and Remote Administration Ports

Listener (Process or Application Protocol)	Listener Protocol and Port	Notes
RPC	TCP 135	
NetBIOS Session	TCP 139	
NetBIOS NameResolution	TCP 137 UDP 137	
NetBIOS Netlogon/Browsing	UDP 138	
SMB	TCP 445 UDP 445	Microsoft CIFS
DNS	TCP 53 UDP 53	
optima-vnet	TCP 1051	TCP Optima VNET
optima-vnet	UDP 1051	UDP Optima VNET

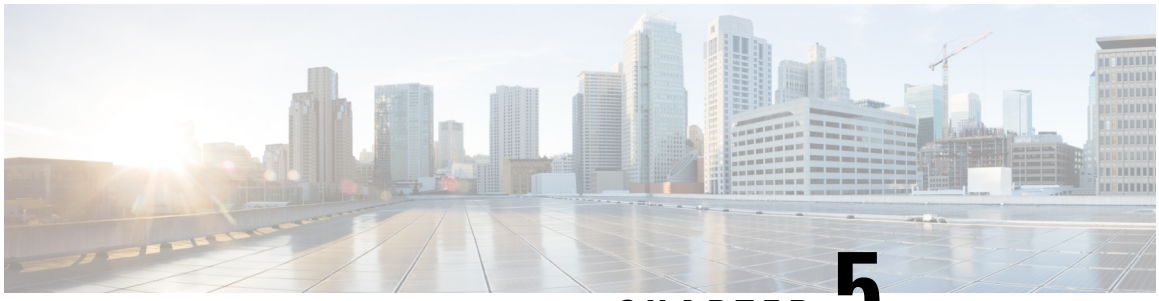
Note

- Ephemeral loopback client ports may be opened locally for CVP services to talk to port 1529 for communications with Derby database.
- Similarly, ephemeral loopback client/server ports may be opened locally by CVP services for internal calls.
- Ephemeral loopback client ports may also be opened by local subagents for talking to the SNMP primary agent running on port 7161.

The above ports are closed when the services concerned are shut down.

From a security perspective, it is recommended to review the ports opened by the underlying Windows operating system or other services running on a machine and close all ports except those required for system operation.

Note For more information on Windows authentication and remote administration ports, see Service overview and network port requirements for the Windows Server in Microsoft documentation.



CHAPTER 5

Port Utilization in Cisco VVB

• Cisco VVB Port Utilization, on page 37

Cisco VVB Port Utilization

Table 22: Cisco VVB Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
VBONINIT	TCP 1504	External process such as External DB clients (like Squirrel or others for custom reporting) can connect	—	Bidirectional	Cisco VVB database port
VVB_ Engine	SIP over TCP, SIP over UDP 5060	SIP	—	Bidirectional	Communicates with SIP gateway
VVB_ Engine	SIP over TLS 5061	SIP	—	Bidirectional	Communicates with SIP gateway
VVB_CVD	TCP 6161	Internal	6161	Bidirectional	Publishes JMS events across JMS network connectors in the cluster
CVD	TCP 6295	CVD of other node in cluster	—	Bidirectional	Bootstrap HTTPD service port
VVB_CVD	TCP 6999	Engine, Tomcat, CVD, and Editor	—	Bidirectional	RMI Port

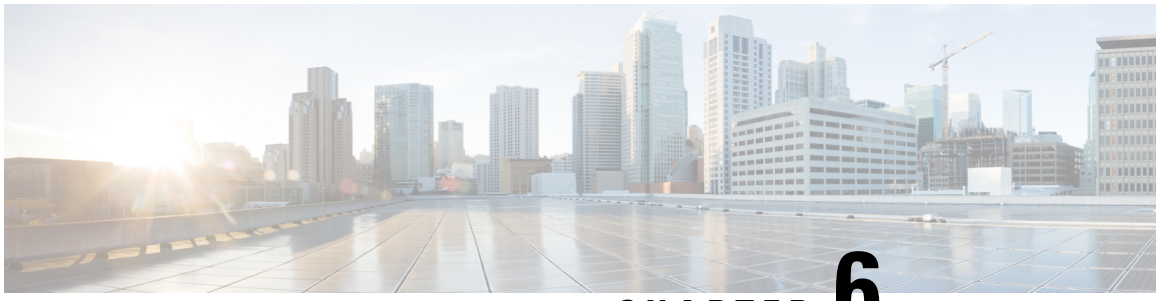
Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
VVB_Engine	TCP 9080	—	—	Bidirectional	- Clients trying to access HTTP triggers, documents, prompts, or grammars - Tomcat instance used by Cisco VVB engine
Cisco IP Voice Media Streaming application	UDP 24576 ~ 32767	—	—	Bidirectional	- Audio media streaming. - Kernel streaming device driver

Table 23: Cisco VVB Ephemeral Port Utilization

Ephemeral (Process or Application Protocol)	Ephemeral Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Generic Ports	TCP, UDP 32768 ~ 61000	—	—	Bidirectional	Generic ephemeral TCP and UDP ports

Note SIP signalling is possible over TCP or TLS. For RTP, underlying protocol is UDP always (not configurable). If TLS is used for SIP signalling, then the same exchanged keys will be used to encrypt and decrypt the RTP packets - for SRTP

To view the system services for port utilization for Cisco Virtualized Voice Browser, see System Services Port Utilization, on page 2



CHAPTER 6

Port Utilization in Finesse

• Finesse Port Utilization, on page 39

Finesse Port Utilization

Table 24: 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 443, 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.

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 25: 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.
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** In Cisco Finesse Release 12.5(1) and later, BOSH (long polling) notifications are disabled by default. Applications must use either WebSocket-based notifications (over 8445 port) or direct XMPP notifications (over TCP). Support for port 7443 (BOSH) is planned for removal in a future release.

Note

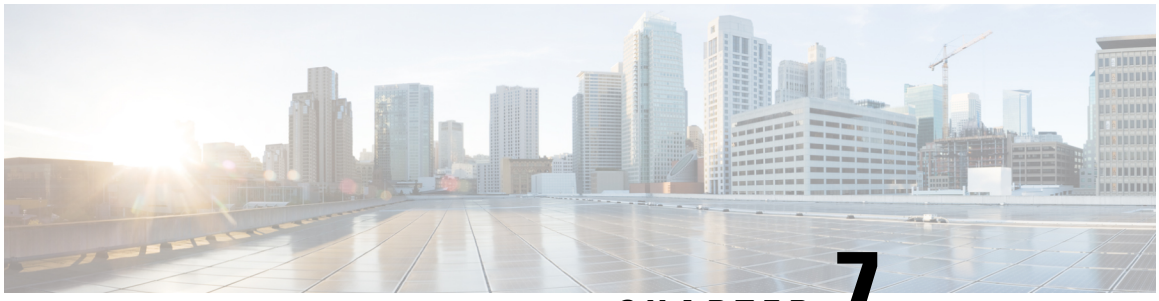
- A network connection is required to open between the Finesse Server and the ECE Web server.
- Finesse desktop uses specific ports on CUIC and Live Data to render Live Data gadgets and reports. For the complete list of the ports that can be used, see *Unified Intelligence Center Port Utilization*.

Table 26: 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.



CHAPTER 7

Port Utilization in Customer Collaboration Platform

• Customer Collaboration Platform Port Utilization, on page 43

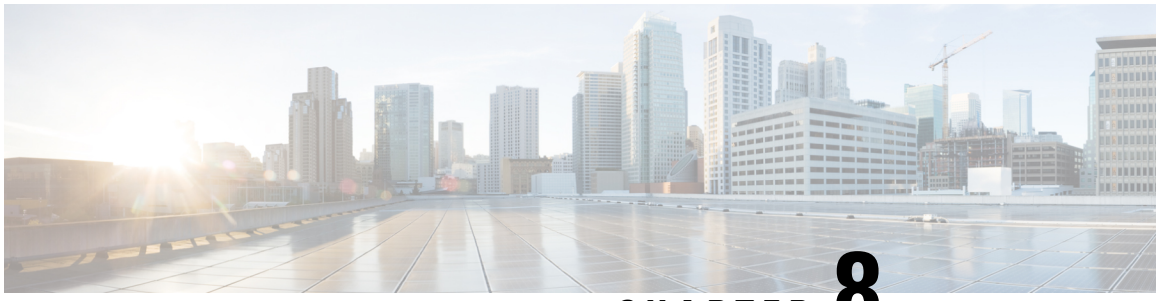
Customer Collaboration Platform Port Utilization

Table 27: Customer Collaboration Platform Port Utilization

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
HTTP	Port 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 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	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
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 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.
XMPP (IM) notifications using an external XMPP server	Port 5222 (configurable)			Outward, from Customer Collaboration Platform to the configured XMPP Notifications server.	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.
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.

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Media routing (in CCE deployments)	Port 38001 (configurable)			Inward, from the CCE MR PG to the Customer Collaboration Platform server.	The CCE Media Routing Peripheral Gateway (MR PG) communicates over a socket connection to Customer Collaboration Platform to support the media routing connection.



CHAPTER 8

Port Utilization in Unified Intelligence Center

• Unified Intelligence Center Port Utilization, on page 47

Unified Intelligence Center Port Utilization

Table 28: Web Requests to Cisco Unified Intelligence Center and Operation Administration Maintenance and Provisioning (OAMP)

Listener (Process or Application Protocol)	Listener Protocol and Port	Remote Device (Process or Application Protocol)	Remote Port	Traffic Direction	Notes
Web Proxy for Unified Intelligence Center	TCP 8444/TCP 443	Browser	Random	Bi-Directional	HTTPS - Unified Intelligence Center Online Help and Unified Intelligence Center.
	TCP 8447	Browser	Random	Bi-Directional	HTTPS - Unified Intelligence Center - Online Help
OAMP	TCP 8080	Browser	Random	Bi-Directional	HTTP - OAMP
	TCP 8443/TCP 443	Browser	Random	Bi-Directional	HTTPS - OAMP

Note The port 8447 is deprecated and will be removed in future releases. Unified Intelligence Center Online Help will be available on Port 8444.

Table 29: Cisco Unified Intelligence Center and Live Data

Listener (Process or Application Protocol)	Listener Protocol and port	Remote Device (Process or Application protocol)	Remote Port	Traffic Direction	Notes
CCE Live Data Cassandra Service	TCP 12000	CCE Live Data Cassandra Service (other side)	Random	Bi-Directional	Used for replicating Cassandra data
CCE Live Data Zookeeper Service	TCP 2181	CCE Live Data Zookeeper Service (other side)	Random	Bi-Directional	Used for replicating zookeeper data
Web Proxy for CCE Live Data Web Service	TCP 12005	Browser	Random	Bi-Directional	Live Data web service
Web Proxy for CCE Live Data Socket IO Service	TCP 12008	Browser	Random	Bi-Directional	Live Data Socket.IO listening port
CCE Live Data Active MQ Service	TCP 61616	CCE Live Data Active MQ Service (other side)	Random	Bi-Directional	Live Data ActiveMQ Openwire transport connector port
CCE Live Data Active MQ Service	TCP 61612	CCE Live Data Active MQ Service (other side)	Random	Bi-Directional	Live Data ActiveMQ Stomp transport connector port
Web Proxy for CCE Live Data Web Service and Web Proxy for CCE Live Data Socket IO Service	TCP 443	Browser	Random	Bi-Directional	Live Data Web Service and Live Data Socket.IO listening port.

Note The ports 12005 and 12008 are deprecated and will be removed in future releases. The port 443 will be used for Live Data Web Service and Live Data Socket.IO Service.

Table 30: Intracluster Ports Between Cisco Unified Intelligence Center

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

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

Cisco Unified Intelligence Center, which runs on the Cisco VOS operating system uses the following ports: TCP 5001, TCP 5002, and TCP 5003 for SOAP monitoring. For more information on these ports, see *Port Utilization for System Services* section.

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