Cisco Unified Workforce Optimization

Firewall Configuration Guide Version 10.5

First Published: June 18, 2014

Last Updated: June 18, 2014

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.

Firewall Configuration Guide

Contents

Introduction

This document lists the firewall configuration requirements for the following Cisco products:

- Cisco Quality Management, version 10.5
- Workforce Management (WFM), version 10.5

Cisco Quality Management Port Usage

The following tables list the inbound port requirements for the Cisco Quality Management server components and the server connections to external integration points. All outbound communications uses dynamic ports unless otherwise listed. A server may contain one or more components and not all ports are required for all recording types. Ports marked with an * are the default port and can be changed in the configuration.

See Windows Firewall or Internet Connection Sharing Service for additional information on Microsoft SQL Server and Informix JDBC Driver ports.

Cisco Quality Management Jetty Component

The Monitoring and Recording Jetty service uses TCP ports 80, 443, and 7001. Make sure that you do not have any other web service that use these ports installed on the Base server and Site Upload server or the Jetty service might fail.

> **Example:** Microsoft SQL Server 2008 Reporting Services and Microsoft Internet Information Services (IIS) might use these ports.

Port 7001 is reserved exclusively for Cisco Quality Management for encrypted data transfer.

The SQL Server 2008 Reporting Services is a tool that provides a web-based GUI to present SQL performance information. You can configure this tool to use another port so it does not interfere with the Jetty service.

Consult your SQL Server documentation for instructions on changing the port used by SQL Server 2008 Reporting Services.

Base Component

The following table lists the inbound ports on the base server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
80	TCP	Jetty service (Jetty port)	All servers and clients
443	TCP	Jetty service (Jetty SSL port)	All servers and clients
7001	TCP	Jetty service (Jetty alternate port)	All servers and clients
8088	TCP	Jetty service (Automated Update)	Desktop Recording client
59011	TCP	Sync service	Quality Management Administrator client
59103	TCP	Jetty service (Data API service) **Note:** The surrogate port is located on the Base server. The Data API Service uses this port to communicate with the Surrogate through the Jetty service.	Data API

External Communication

Port	Type	Destination	Source
1504	TCP	Unified CCX Informix database	Sync for Unified CCX
8443, 443, or 80	TCP	Unified CM Publisher and Subscribers	MANA, Sync, and Quality Management Administrator
389* or 636*	TCP	Active Directory	Data API and Quality Management Administrator
25*	TCP	SMTP Server	MANA and Jetty

Port	Type	Destination	Source
*	TCP	SNMP	MANA
1433	TCP	SQL	System Configuration Setup (PostInstall.exe), Data API, and Sync

CTI Component

The following table lists the ports on the recording CTI server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
52102	TCP	CTI Service	All servers and clients
5060	UDP/TCP	CTI Service	Recording CTI service (SIP Messaging)
5061	TCP	CTI Service	Recording CTI service (secure SIP Messaging)

External Communication

Port	Type	Destination	Source
1433*	TCP	SQL database	DB Proxy
	TCP	Unified CM CTI Manager	CTI service

CUBE SIP CTI Component

The following table lists the ports on the CUBE SIP CTI server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
5060	UDP/TCP	CUBE SIP CTI service	CUBE Voice Gateway
59106	TCP	CUBE SIP CTI service	All servers

External Communication

None

Database Component

The following table lists the ports on the Database server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
52103	TCP	DB Proxy service	All servers

External Communication

Port	Type	Destination	Source
1433* or 1434*	TCP	SQL database **Note:** This port can be changed or be dynamic if you are using a named instance.	DB Proxy

MediaSense Subscription Component

The following table lists the ports on the MediaSense Subscription server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
59104	TCP	MediaSense Subscription service	All servers
59105	TCP	MediaSense Subscription service	All servers

External Communication

Port	Type	Destination	Source
8440*	TCP	MediaSense API Server	MediaSense Subscription Service

Monitor Server Component

The following table lists the ports on the Monitor server that must be opened in the Windows Firewall for Server Recording deployments.

Inbound Ports

Port/Program	Type	Destination	Source
59101	TCP	Monitor service	All servers
All	All	Monitoring NIC	SPAN Session

External Communication

None

Voice Record Component

If you are not using Windows Firewall, the following table lists the ports on the Voice Record server that must be opened.

Inbound Ports

Port	Type	Destination	Source
59102	TCP	Network Recording service	All servers
39500 to 41500	UDP	Network Recording service	BiB RTP stream from phones or RTP stream from CUBE

External Communication

Port	Type	Destination	Source
8440*	TCP	MediaSense Record Server	Voice Record Server

Site Component

The following table lists the ports on the Site Upload server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
80	TCP	Jetty service (Jetty port)	All servers and clients
443	TCP	Jetty service (Jetty SSL port)	All servers and clients
7001	TCP	Jetty service (Jetty alternate port)	Used for both site and base server
2303	TCP	PROXY Pro Gateway service	Web clients (Screen Playback)
59100	TCP	Upload Controller service	All servers and clients

Port	Type	Destination	Source
59108	TCP	Jetty service	Jetty API

External Communication

Port	Type	Destination	Source
135 to 139 and 445	TCP	Storage Location	Jetty Service (File Transfer)

Media Encoder Component

The following table lists the ports on the Media Encoder server that must be opened in the Windows Firewall.

Inbound Ports

Port	Type	Destination	Source
52109	TCP	Media Encoder service	All servers

External Communication

Port	Type	Destination	Source
135 to 139 and 445	TCP	Storage Location	Jetty Service (File Transfer)

Reconciliation Component

The following table list the ports for the Reconciliation service that must be opened in the Windows Firewall.

Inbound Ports

None

External Communication

Port	Type	Destination	Source
8443, 443, or 80	TCP	Unified CM Publisher and Subscribers	Reconciliation
1433*	TCP	SQL	Reconciliation
1504	TCP	Unified CCX Informix database	Reconciliation for Unified CCX

Desktop Client, Citrix Server, or Windows Terminal Services Component

The following table lists ports that must be opened in the Windows Firewall on the desktop client, Citrix server for thin client users, or Windows Terminal Services if you want to use the Live Screen Monitoring feature.

Inbound Ports

Port	Type	Destination	Source
1505	TCP		Screen Recording
49152 to 65535	TCP	Thin Client Screen Recording service	Live Screen Monitoring Client

WFM Port Usage

The following table lists the ports used by WFM and its components.

Note: The port numbers listed are defaults. They can be changed as needed.

Server Application	Destination Port (Listening)	Client Application
CTI service **Note**: You can set this port number in the System Parameters window of the Unified CCX Administration web page. The parameter name for the port number is RmCm TCP Port. For more information, see “Managing System Parameters”, *Cisco Customer Response Solutions Administration Guide*.	TCP 12028 Side A TCP 12028 Side B	WFM Sync service WFM RTE service
Unified CCX instance of Informix		WFM Capture service

Server Application	Destination Port (Listening)	Client Application
WFM instance of SQL Server	TCP 1433 TCP 1434 **Note**: Port numbers for named instances of SQL Server might vary. Addition ports might need to be opened.	WFM ACC service WFM Capture service WFM Compile service WFM Configuration Setup WFM Forecast service WFM iCalendar service WFM MANA service WFM Product Adapter service WFM Reports WFM RTE service WFM Request service WFM Schedule service WFM Sync service
WFM iCalendar service	TCP 444 (HTTPS) TCP 8086 (HTTP)	Any iCalendar client
WFM Jetty service	TCP 59103 (surrogate)	WFM Product Adapter service
	TCP 443 (HTTPS) TCP 80 (HTTP)	Web browser

WFM Jetty Service Ports

The WFM Jetty service uses TCP ports 80 and 443. Make sure that you do not have any other web service installed on the server that hosts the WFM Transaction services that uses these ports, or the Jetty service might fail.

Examples of other web services include Microsoft SQL Server 2008 Reporting Services and Microsoft Internet Information Services (IIS).

The SQL Server 2008 Reporting Services is a tool that provides a web-based GUI to present SQL performance information. You can configure this tool to use another port and so not interfere with the Jetty service.

Consult your SQL Server documentation for instructions on changing the port used by SQL Server 2008 Reporting Services.

Windows Firewall or Internet Connection Sharing Service

For Unified Workforce Optimization to function correctly, the ports listed in this document must be opened in Windows Firewall.

If Windows Firewall or the Internet Connection Sharing (ICS) service is running when Unified Workforce Optimization is installed, the installation process opens the necessary firewall ports except those in the following table, which must be opened manually.

Product	Open Manually
Cisco Quality Management	Microsoft SQL Server: ports 1433 and 1434 Informix JDBC Driver: port 1504 (Unified CCX environment only)
WFM	iCalendar service: 444 (HTTPS) or 8086 (HTTP)

See "Adding Firewall Exclusions by Program" in the *Server Installation Guide* for information on adding Windows Firewall exclusions and allowing remote connections for Microsoft SQL Server and Informix JDBC Driver .

Ports must be opened manually in these situations:

- If another firewall is used
- If you turn on the Windows Firewall after Unified Workforce Optimization is installed

See your firewall documentation for instructions on configuring manual port exceptions.

Note: Any non-Unified Workforce Optimization services that use the ports listed in this document must be configured to use a different port.

Index