



***REVIEW DRAFT - CISCO CONFIDENTIAL***



## **Cisco Jabber Guest Server 10.6 Installation and Configuration Guide**

**First Published:** December 12, 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.

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Prepare to Install 1

- Server Requirements 1
  - Cisco Product Requirements 1
  - Virtual Machine Requirements 2
    - Hardware and System Requirements 2
    - Supported Storage Models 3
    - Virtual Machine Specifications 3
    - VMware vSphere Feature Support 3
  - Reverse Proxy Server Requirements 4
- License Requirements 4
- Client Requirements 6
  - Client Hardware and System Requirements 6
  - Cisco Jabber Guest Plug-in Requirement 7
  - Supported Mobile Devices 7
- Deployment Options 7
- Network Topology 8
  - Call Control Flow 9
  - Media Flow 10
    - Media Flow: Cisco Expressway-E with Single NIC Deployment 11
    - Media Flow: Cisco Expressway-E with Dual NIC Deployment 12
- Ports and Protocols 13
  - Ports and Protocols: Cisco Expressway-E with Single NIC Deployment 13
  - Ports and Protocols: Cisco Expressway-E with Dual NIC Deployment 15
- Clustering Options 17
- Load Balancing Methods Available 18

---

### CHAPTER 2

#### Install Cisco Jabber Guest Server 21

- Overview 21

## ***REVIEW DRAFT - CISCO CONFIDENTIAL***

Install Server	21
Install Server to vCenter Server	22
Install Server to ESXi Hypervisor	23
Sign In to Cisco Jabber Guest Administration	23
Install Certificate	24
Install Certificate Signed by a Certificate Authority	24
Install Certificate with Additional Distinguished Name Information	25
Install Certificate That Includes the Intermediate Certificate or the Entire Certificate Trust Chain	26
Generate New Self-Signed Certificate	28
Sign In to Cisco Jabber Guest Server CLI	28
Change Time Zone on Server	28

---

### **CHAPTER 3**

#### **Perform Initial Setup 31**

Configure Cisco Expressway-E and Cisco Expressway-C	31
Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment	31
Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Dual NIC Deployment	33
Change MTU Size	36
Configure Signaling and Media	36
Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment	36
Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment	37
Configure Static NAT Mode on Cisco Expressway-E	39
Configure TURN Credential Provisioning	39
Set Up TURN Server Information	40
Set FQDN of Cisco Jabber Guest Server	40
Set Domain Used for Links	40
Customize Cisco Jabber Guest Clients	41

---

### **CHAPTER 4**

#### **Upgrade Cisco Jabber Guest Server 43**

Upgrade Cisco Jabber Guest Server	43
-----------------------------------	----

---

### **CHAPTER 5**

#### **Configure High Availability and Scalability 45**

Cluster	45
---------	----

## ***REVIEW DRAFT - CISCO CONFIDENTIAL***

Create Cluster	45
Change IP Address or Hostname of Server in Cluster	46
Demote Primary Server to Secondary Server	47
Upgrade Cluster	48
Remove Server from Cluster	50
Configure Load Balancing	51
Configure Round-Robin DNS Load Balancing	51
Change the SIP Call Throttle Limit	52
Configure Round-Robin CSV Loading Balancing	52
Configure HTTP Load Balancing	53
Configure Round-Robin TURN Port Range Load Balancing	53

---

### **CHAPTER 6**

#### **Post-Install Configuration Changes 55**

Change Virtual Machine Properties of a vCenter-hosted Server	55
Change Virtual Machine Properties of an ESXi-hosted Server	55

---

### **CHAPTER 7**

#### **Troubleshoot 57**

Locate chip.log File	57
Locate chip.dmp File	58
Reset Admin Password for Cisco Jabber Guest Administration	58
Reset Root Password for Cisco Jabber Guest Server	58
Audio and Video Issues	60
One-Way Video When Using VPN	60
No Audio or Video on Single NIC Deployment	60
Plug-in Crashes	61
Error Messages	61

---

### **CHAPTER 8**

#### **Documentation Reference 65**

Cisco Unified Communications Manager	65
Cisco TelePresence Video Communication Server	65

***REVIEW DRAFT - CISCO CONFIDENTIAL***



## CHAPTER

# 1

## Prepare to Install

---

Cisco Jabber Guest can be deployed in combination with Cisco Expressway-E and Cisco Expressway-C or in combination with Cisco VCS-E and VCS-C. To simplify the documentation, we reference only Cisco Expressway-E and Cisco Expressway-C throughout this guide.

The mobile and web clients use the same interfaces when interacting with Cisco Expressway/Cisco TelePresence Video Communication Server (VCS) and Cisco Jabber Guest. To simplify the documentation, we reference only the web client throughout this guide.

- [Server Requirements, page 1](#)
- [License Requirements, page 4](#)
- [Client Requirements, page 6](#)
- [Deployment Options, page 7](#)
- [Network Topology, page 8](#)
- [Ports and Protocols, page 13](#)
- [Clustering Options, page 17](#)
- [Load Balancing Methods Available, page 18](#)

## Server Requirements

### Cisco Product Requirements

Make sure that supporting infrastructure is in place before you begin to deploy and configure Cisco Jabber Guest. Deploy Cisco Jabber Guest with an existing Cisco Unified Communications Manager installation.

To allow Cisco Jabber Guest to access devices located inside the enterprise firewall, deploy the following:

- Cisco Unified Communications Manager 8.6.x or later  
Cisco Jabber Guest requires that your Cisco Unified Communications Manager be configured to work with Cisco TelePresence Video Communication Server.
- Cisco Jabber Guest Server

## REVIEW DRAFT - CISCO CONFIDENTIAL

- Cisco Expressway-C 8.2 or later
- Cisco Expressway-E 8.2 or later

**Important**

- Without Cisco Expressway-C and Cisco Expressway-E, you are limited to testing with clients that can directly access the network on which the Cisco Jabber Guest server is homed.
- You cannot use the same Cisco Expressway-C and Cisco Expressway-E pair or cluster for both Cisco Jabber Guest and Expressway for Mobile and Remote Access.

For more information, download the *Cisco Expressway Administrator Guide*, deployment guides, and release notes or see the online help for complete information on configuring the options available on your Cisco Expressway.

**Related Topics**

[Cisco VCS and CUCM Deployment Guide](#)

[Cisco Expressway Series on \*www.cisco.com\*](#)

## Virtual Machine Requirements

Cisco Jabber Guest is deployed as a virtual server using the Open Virtualization Format (OVF) standard for packaging and distributing virtual appliances that run in a virtual environment. It requires VMware vSphere as the hypervisor. Cisco publishes the distribution as an OVF file with the file extension .OVA, which stands for Open Virtual Appliance. This file contains the OVF template for the application. The OVF template defines the virtual machine's hardware and is preloaded with required software.

## Hardware and System Requirements

- A server platform that meets VMware's Compatibility Guide for VMware vSphere 5.x or later is required. The Cisco Jabber Guest virtual machine uses a 64-bit distribution of CentOS 6.5. Make sure that the server platform uses CPUs that are capable of 64-bit instructions.
- Cisco Jabber Guest is supported on any Full UC Performance CPU, beginning with Intel Xeon Processor 5600 with a minimum physical core speed of 2.53 GHz or higher. Cisco Jabber Guest is not supported on Restricted UC Performance CPUs. For more information on Full UC performance CPUs and Restricted UC Performance CPUs, see the *Processors/CPUs* section in *UC Virtualization Supported Hardware*.
- Cisco Jabber Guest is allowed on server models meeting required specifications; however, support of Cisco Jabber Guest is identical to UC on UCS rules and subject to application co-residency/TRC support policy. If a performance issue is encountered in the context of Cisco Business Edition 6000 (BE6000), Cisco Business Edition 7000 (BE7000), or otherwise, Cisco Jabber Guest is required to move off-box.
- In a BE6000 or BE7000 deployment, Cisco Jabber Guest is considered a non-Business Edition application. For more information, see the *Cisco Business Edition 6000 and Cisco Business Edition 7000 Co-residency Policy Requirements*.



## REVIEW DRAFT - CISCO CONFIDENTIAL

- See the VMware developer documentation for additional configuration and hardware requirements. We highly recommend using the Cisco Unified Computing System (CUCS) to simplify and maximize performance.

### Related Topics

[Cisco UCS](#)

[Processors/CPUs section in UC Virtualization Supported Hardware](#)

[Cisco Business Edition 6000 and Cisco Business Edition 7000 Co-residency Policy Requirements](#)

## Supported Storage Models

## Virtual Machine Specifications

*Table 1: Virtual Machine Specifications*

RAM	CPU	Storage	Operating System	CPU Resource Allocation	Memory Resource Allocation
4 GB	2 logical CPUs with 1 core each	100 GB	CentOS 6.5 64-bit	Default (not defined)	Default (not defined)

## VMware vSphere Feature Support

The following VMware vSphere features are supported:

- VM OVA template deployment (using the Cisco-provided Cisco Jabber Guest OVA)
- VMware vMotion
- VMware vSphere Distributed Switch (vDS)
- VMware Dynamic Resource Scheduler (DRS)
- VMware Storage vMotion (Storage DRS)
- VMware Virtual Machine Snapshots

You can restart Cisco Jabber Guest on a different VMware ESXi host and create or revert VMware Snapshots as long as the application was shut down without any issues before moving or taking a snapshot.

The following VMware vSphere features have not been tested with Cisco Jabber Guest:

- VMware Site Recovery Manager (SRM)
- VMware Consolidated Backup (VCB)
- VMware Data Recovery (VDR)
- VMware Dynamic Power Management (Cisco Jabber Guest must be configured to run 24/7)

## ***REVIEW DRAFT - CISCO CONFIDENTIAL***

- Long Distance vMotion (vMotion over a WAN)
- VMware Fault Tolerance (FT)

The following VMware vSphere and third-party features are not supported with Cisco Jabber Guest:

- VMware Hot Add
- Copying a Cisco Jabber Guest virtual machine (must use OVA to deploy new server)
- Configuring Cisco Jabber Guest with multiple virtual network interface controllers (vNICs)
- Third-party Virtual to Physical (V2P) migration tools
- Third-party deployment tools

## **Reverse Proxy Server Requirements**

The Cisco Expressway-E and Cisco Expressway-C can be used to tunnel HTTP from the Cisco Jabber Guest client to the Cisco Jabber Guest server. If a third-party reverse proxy is used in front of the Expressway, configure it to proxy only the following URL types:

- /call
- /jabberc
- /jc

Configure the reverse proxy to redirect any HTTP requests to HTTPS.

## **License Requirements**

Cisco Jabber Guest is licensed and obtained through User Connect Licensing (UCL), Cisco Unified Workspace Licensing (CUWL), and other ordering mechanisms. Contact a sales representative from a Cisco partner or from Cisco for ordering details. No license keys are provided or required for the Cisco Jabber Guest software.

The following table describes the license requirements for using Cisco Expressway with Cisco Jabber Guest.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 2: License Requirements for Using Cisco Expressway with Cisco Jabber Guest**

License	Requirement	Note
Rich Media Session licenses	<p>2 Rich Media Session licenses are required per Cisco Jabber Guest session:</p> <ul style="list-style-type: none"> <li>• 1 Rich Media Session license on the Cisco Expressway-E for each Cisco Jabber Guest session</li> <li>• 1 Rich Media Session license on the Cisco Expressway-C for each Cisco Jabber Guest session</li> </ul>	
TURN relay license	TURN licensed on Cisco Expressway	When you order Cisco Expressway, a TURN relay license is included.
Advanced Networking (AN) license	If Cisco Jabber Guest is installed in a dual-NIC deployment, an AN license is required on Cisco Expressway.	When you order Cisco Expressway, an AN license is included.

The following table describes the license requirements for using Cisco TelePresence Video Communication Server (VCS) with Cisco Jabber Guest.

**Table 3: License Requirements for Using Cisco VCS with Cisco Jabber Guest**

License	Requirement	Note
Traversal call licenses	<p>2 traversal call licenses are required per Cisco Jabber Guest session:</p> <ul style="list-style-type: none"> <li>• 1 traversal call license on the VCS-E for each Cisco Jabber Guest session</li> <li>• 1 traversal call license on the VCS-C for each Cisco Jabber Guest session</li> </ul>	
TURN relay license	TURN licensed on Cisco VCS	When you order Cisco VCS, a TURN relay license is included.
Dual Network Interface (DI) license	If Cisco Jabber Guest is installed in a dual-NIC deployment, a DI license is required on Cisco VCS.	When you order Cisco VCS, a DI license is not included. Specifically select this license.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

# Client Requirements

## Client Hardware and System Requirements

Callers require a multimedia-capable computer with a camera and microphone that support the following software and hardware requirements:

**Table 4: Client Requirements**

	PC Requirements	Mac Requirements
Operating system	Microsoft Windows Vista Service Pack 2 (SP2) or later	Apple Mac OS X 10.7 (Lion) or later
Hardware	GPU capable of OpenGL 1.2 or later Minimum CPU supporting SSE2 (Pentium IV or newer) Encoding at 720p 30fps requires Intel Core2Duo @ 1.2 GHz or better Encoding at VGA 30fps can be done on as low-end CPUs as the Intel Atom @ 1.6 GHz	Apple computer with Intel x86 processor Encoding at 720p 30fps requires Intel Core2Duo @ 1.2 GHz or better. For optimal experience Core2Duo @ 2GHz with 2 MB L2 cache per core is recommended.
Browsers	Mozilla Firefox 10 or later Google Chrome 18 or later Microsoft Internet Explorer 8 or later (32-bit only) <b>Note</b> On Windows 8 or later, only the desktop version is supported. The Metro version does not work. <a href="#">1</a>	Apple Safari 5 or later Mozilla Firefox 10 or later <sup>2</sup> Google Chrome 18 or later

<sup>1</sup> To configure Internet Explorer on Windows 8 or later to open the desktop version by default, do the following:

- 1 Open Microsoft Internet Explorer.
- 2 From the **Tools** menu, click **Internet options**.
- 3 Click the **Programs** tab.
- 4 Under **Opening Internet Explorer**, choose **Always in Internet Explorer on the desktop**.

<sup>2</sup> Currently, a known issue with Firefox on Mac OS X prevents full-screen video. This option is not offered for this combination of browser and operating system.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Cisco Jabber Guest Plug-in Requirement

The Cisco Jabber Guest solution includes a browser plug-in that is downloaded and installed by the caller on the local machine. For Google Chrome, the web page prompts the user to install the Cisco Jabber Guest Add-on and Cisco Jabber Guest Extension. For all other browsers, the Cisco Jabber Guest web page prompts the caller to download and install the plug-in the first time the service is used.

New plug-ins are periodically made available with fixes and new functionality. The caller is prompted to download and install the new plug-in the next time an attempt is made to place a call.

## Supported Mobile Devices

Cisco Jabber Guest for iOS is supported on iOS 7.0 or later.

The following table lists the iOS mobile devices that Cisco Jabber Guest supports.

**Table 5: iOS Mobile Devices**

<b>iPad</b>	<b>iPhone</b>
iPad 4	iPhone 6 Plus
iPad 3	iPhone 6
iPad 2	iPhone 5s
iPad Air 2	iPhone 5c
iPad Air	iPhone 5
iPad mini 3	iPhone 4S
iPad mini	
iPad mini with Retina display	

## Deployment Options

Cisco Jabber Guest supports two deployments:

- Cisco Expressway-E with a single NIC—SIP traffic goes to the Cisco Expressway-C and media flows over a port range between the Cisco Expressway-E and the Cisco Expressway-C.
- Cisco Expressway-E with dual NIC—SIP traffic goes to the Cisco Expressway-E and media flows through the traversal zone between the Cisco Expressway-E and the Cisco Expressway-C.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Important**

Only the Cisco Expressway-E with dual NIC deployment supports NAT/PAT between the Cisco Expressway-E and the Cisco Expressway-C.

## Network Topology

### Overview of Cisco Expressway-E with Single NIC Deployment

- SIP traffic is sent to the Cisco Expressway-C.
- Cisco Expressway-E is single NIC only.
- Cisco Expressway-E in static NAT mode is optional and requires additional configuration on the Cisco Jabber Guest server.
- Cisco Expressway-E is used for TURN services and reverse proxy, not call control.
- Media flows between the Cisco Expressway-E and the Cisco Expressway-C over port range, not a traversal zone.

### Overview of Cisco Expressway-E with Dual NIC Deployment

- SIP traffic is sent to the Cisco Expressway-E.
- Cisco Expressway-E is dual NIC only.
- Cisco Expressway-E in static NAT mode is optional and requires additional configuration on the Cisco Jabber Guest server.
- Cisco Expressway-E is used for TURN services, reverse proxy, and call control.
- Media flows between the Cisco Expressway-E and the Cisco Expressway-C through a traversal zone.

In a production environment, Cisco Jabber Guest requires that your Cisco Unified Communications Manager be configured to work with Cisco Expressway.

Cisco Jabber Guest can be pointed directly to Cisco Unified Communications Manager for lab deployments only; configure a SIP trunk on Cisco Unified Communications Manager for this deployment. This option is best suited to a lab deployment in which the goal is to familiarize yourself with Cisco Jabber Guest without the additional overhead of configuring Expressway. However, without configuring Expressway, Cisco Jabber Guest is not supported in a production environment.

**Note**

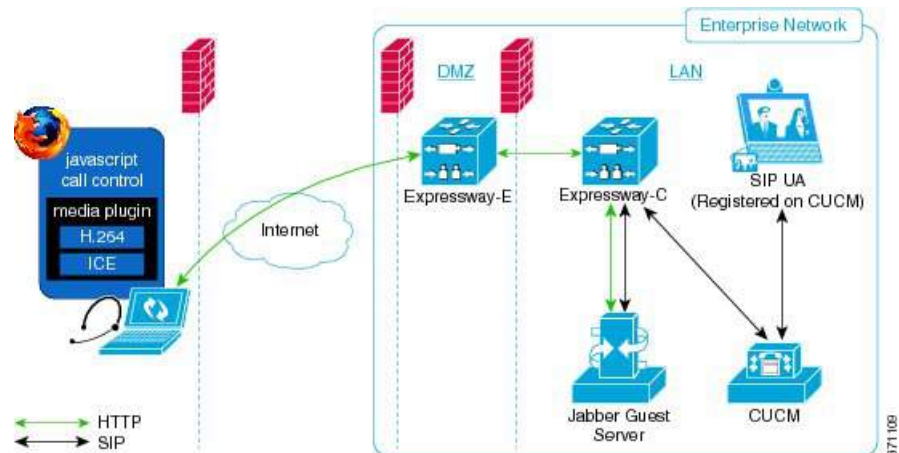
If Cisco Expressway-E is used for reverse proxy functionality, the Cisco Jabber Guest URL looks like `https://expressway-e.example.com/call` where *expressway-e.example.com* is the FQDN of Cisco Expressway-E.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

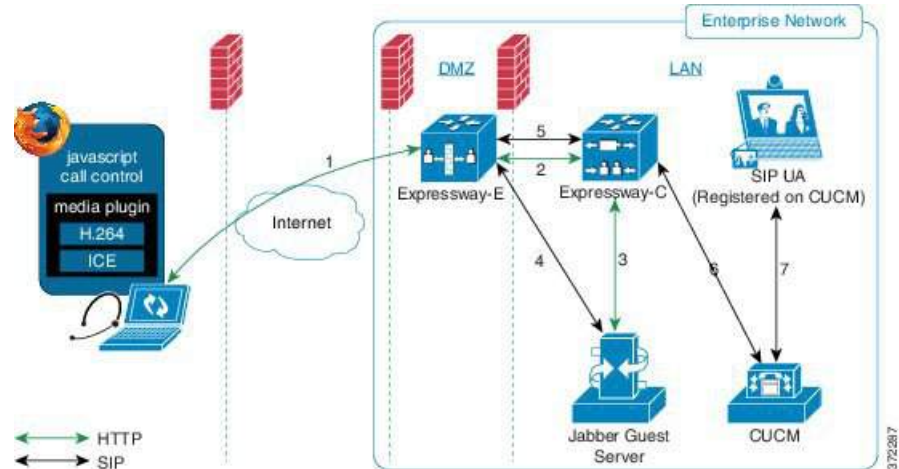
## Call Control Flow

The following are examples of call control flow for the two supported deployments of Cisco Jabber Guest Server.

**Figure 1: Cisco Jabber Guest Call Control: Cisco Expressway-E with Single NIC Deployment**



**Figure 2: Cisco Jabber Guest Call Control: Cisco Expressway-E with Dual NIC Deployment**



### Cisco Expressway-E with Dual NIC Deployment

SIP flows between the Cisco Jabber Guest server and the Cisco Expressway-E. This requires bi-directional TCP traffic between the two servers over 5060 (SIP over TCP) or 5061 (SIP over TLS). The SIP traffic then goes over the traversal zone to the Cisco Expressway-C.

We recommend that you disable SIP and H.323 application-level gateways on routers/firewalls carrying network traffic to or from a Cisco Expressway-E.

## REVIEW DRAFT - CISCO CONFIDENTIAL

**Important**

Because media hairpins between the two Cisco Expressway-E NICs, the TURN traffic and SIP traffic must reside on the same Cisco Expressway-E server. You must configure the static NAT address, DMZ external address, and DMZ internal address of the Cisco Expressway-E on the Cisco Jabber Guest server.

**Related Topics**

[Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment, on page 36](#)

[Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment, on page 37](#)

## Media Flow

The web client uses TURN relays allocated on the Cisco Expressway-E to tunnel media into the enterprise. Media is sent and received in STUN encapsulated packets to the TURN server through UDP port 3478.

TURN relay credentials are acquired and used as follows:

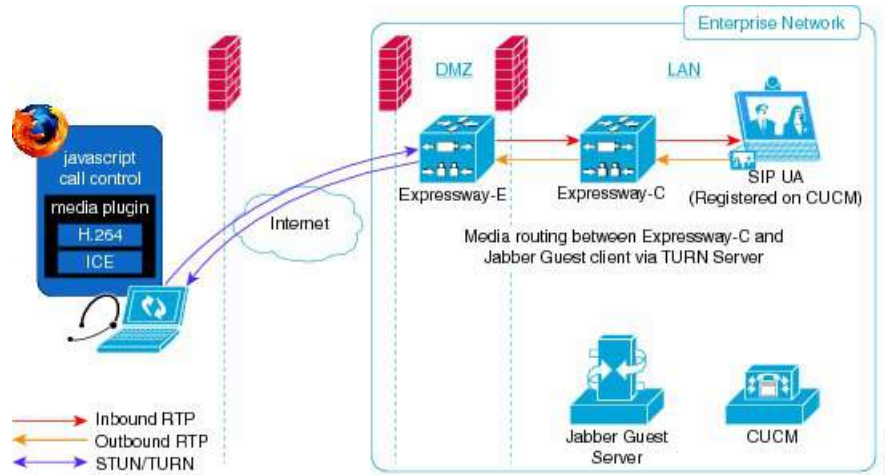
- The Cisco Jabber Guest client allocates a call resource through HTTP to the Cisco Jabber Guest server.
- The Cisco Jabber Guest server requests short-term TURN credentials from the Cisco Expressway-C through a secure HTTP request. Administrator credentials are used for authentication. The configured domain must be on the Cisco Expressway-C with Jabber Guest service enabled.
- The Cisco Expressway-C creates the TURN credential and passes it to the Cisco Jabber Guest server.
- The Cisco Expressway-C propagates the TURN credential to the Cisco Expressway-E through the SSH tunnel (port 2222).
- The Cisco Jabber Guest server responds to the Cisco Jabber Guest client with the TURN credential and TURN server (Cisco Expressway-E) address (DNS or IP).
- The Cisco Jabber Guestclient uses the TURN credential to allocate the TURN relay on the TURN server.



**REVIEW DRAFT - CISCO CONFIDENTIAL****Media Flow: Cisco Expressway-E with Single NIC Deployment**

The following diagram is an example of the media flow for a Cisco Expressway-E with single NIC deployment of Cisco Jabber Guest.

**Figure 3: Cisco Jabber Guest Media Flow: Cisco Expressway-E with Single NIC Deployment**



Cisco Jabber Guest media does not go through the traversal link between Cisco Expressway-E and Cisco Expressway-C.

**Important**

If the Cisco Expressway-E is behind a NAT, additional configuration is required on the Cisco Jabber Guest server to avoid the media flowing to the static NAT address. Turn on **Static NAT mode** and configure the static NAT address and DMZ external address of the Cisco Expressway-E on the Cisco Jabber Guest server. This allows media to be sent to the DMZ external address of the Cisco Expressway-E, avoiding NAT reflection on the outside firewall.

**Related Topics**

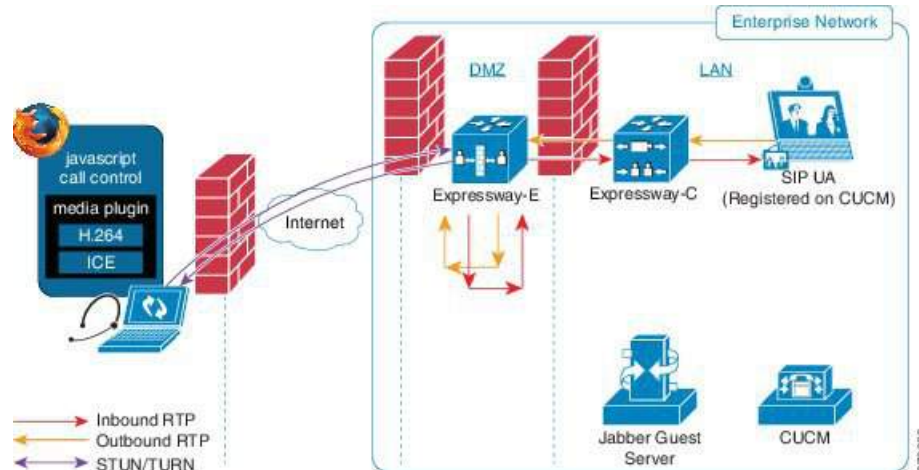
[Configure Static NAT Mode on Cisco Expressway-E, on page 39](#)

## REVIEW DRAFT - CISCO CONFIDENTIAL

### Media Flow: Cisco Expressway-E with Dual NIC Deployment

The following diagram is an example of the media flow for a Cisco Expressway-E with dual NIC deployment of Cisco Jabber Guest.

**Figure 4: Cisco Jabber Guest Media Flow: Cisco Expressway-E with Dual NIC Deployment**



Media flows through the traversal zone between the Cisco Expressway-C and the internal NIC of the Cisco Expressway-E. It hairpins on the Cisco Expressway-E to the external NIC of the Cisco Expressway-E, and then is STUN/TURN wrapped before being sent to the client browser.

#### Important

If the Cisco Expressway-E is behind a NAT, additional configuration is required on the Cisco Jabber Guest server to avoid the media flowing to the static NAT address. Turn on **Static NAT mode** and configure the static NAT address, DMZ external address, and DMZ internal address of the Cisco Expressway-E on the Cisco Jabber Guest server. This allows media to be sent to the DMZ external address of the Cisco Expressway-E, avoiding NAT reflection on the outside firewall.

#### Related Topics

[Configure Static NAT Mode on Cisco Expressway-E, on page 39](#)

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Ports and Protocols

**Important**

- HTTP and HTTPS traffic from Cisco Jabber Guest clients in the Internet is sent to ports 80 and 443 TCP respectively. Therefore the firewall between the Cisco Expressway-E and the public Internet must translate destination port 80 to 9980 and destination port 443 to 9443 for all TCP traffic that targets the Cisco Expressway-E address.
- The Cisco Expressway-E redirects HTTP requests on port 9980 to HTTPS on 9443.
- 80/443 TCP are the standard HTTP/S administration interfaces on the Expressway. If the Cisco Expressway-E is administered from systems located in the Internet, then the firewall translation must also distinguish by source address and must not translate the destination port of traffic arriving from those management systems.
- You also need to ensure that appropriate DNS records exist so that the Cisco Jabber Guest client can reach the Cisco Expressway-E. The FQDN of the Cisco Expressway-E in DNS must include the Cisco Jabber Guest domain. The Cisco Jabber Guest domain is the domain that is configured on the Cisco Expressway-C.

## Ports and Protocols: Cisco Expressway-E with Single NIC Deployment

*Table 6: Inbound from Public Internet to Cisco Expressway-E (DMZ)*

Purpose	Protocol	Internet Endpoint (Source)	Cisco Expressway-E (Listening)
HTTP	TCP	TCP source port	9980 (read the following <i>Important</i> note)
HTTPS proxy	TLS	TCP source port	9443 (read the following <i>Important</i> note)
TURN server control/media	UDP	UDP source port	3478–3483 (control and media sent to this port)

**Important**

- The Cisco Expressway-E administrator currently uses port 80 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 80 must be remapped to port 9980 using a firewall (or similar) in front of Cisco Expressway-E.
- The Cisco Expressway-E administrator currently uses port 443 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 443 must be remapped to port 9443 using a firewall (or similar) in front of Cisco Expressway-E.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 7: Outbound from Cisco Expressway-C (Private) to Cisco Expressway-E (DMZ)**

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Expressway-E (Destination)
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222 (not configurable)
Traversal zone SIP signaling	TLS	25000–29999	7001
Media <sup>3</sup>	UDP	36000–59999	24000–29999 <sup>4</sup> 60000–61799 <sup>5</sup>

<sup>3</sup> By default, media is sent to the NAT interface unless the Cisco Jabber Guest server is configured for static NAT mode.

<sup>4</sup> For fresh installs of Cisco Expressway-E 8.x.

<sup>5</sup> If you upgraded Cisco Expressway-E from 7.x.

**Table 8: Inbound from Cisco Expressway-E (DMZ) to Cisco Expressway-C (Private)**

Purpose	Protocol	Cisco Expressway-E (Source)	Cisco Expressway-C (Destination)
Media	UDP	24000–29999 <sup>6</sup> 60000–61799 <sup>7</sup>	36000–59999

<sup>6</sup> For fresh installs of Cisco Expressway-E 8.x.

<sup>7</sup> If you upgraded Cisco Expressway-E from 7.x.

**Important**

- Inbound firewall rules are required to allow media to flow from the Cisco Expressway-E to Cisco Expressway-C.
- You may find that two-way media can still be established even if the inbound from Cisco Expressway-E (DMZ) to Cisco Expressway-C (private) firewall rules are not applied. This is because the outbound media creates a pinhole in the firewall; however, these rules are required to support uni-directional media (that is, only from outside to inside).

**Table 9: From Cisco Expressway-C to Cisco Jabber Guest**

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Jabber Guest (Destination)
HTTP	TCP	Ephemeral port	80
HTTPS	TLS	Ephemeral port	443

**REVIEW DRAFT - CISCO CONFIDENTIAL**

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Jabber Guest (Destination)
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

**Table 10: From Cisco Jabber Guest to Cisco Expressway-C**

Purpose	Protocol	Cisco Jabber Guest (Source)	Cisco Expressway-C (Destination)
HTTPS	TLS	Ephemeral port	443
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

**Ports and Protocols: Cisco Expressway-E with Dual NIC Deployment****Table 11: Inbound from Public Internet to Cisco Expressway-E (DMZ)**

Purpose	Protocol	Internet Endpoint (Source)	Cisco Expressway-E (Listening)
HTTP	TCP	TCP source port	9980 (read the following <i>Important</i> note)
HTTPS proxy	TLS	TCP source port	9443 (read the following <i>Important</i> note)
TURN server control/media	UDP	UDP source port	3478–3483 (control and media sent to this port)

**Important**

- The Cisco Expressway-E administrator currently uses port 80 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 80 must be remapped to port 9980 using a firewall (or similar) in front of Cisco Expressway-E.
- The Cisco Expressway-E administrator currently uses port 443 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 443 must be remapped to port 9443 using a firewall (or similar) in front of Cisco Expressway-E.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 12: Outbound from Cisco Expressway-C (Private) to Cisco Expressway-E (DMZ)**

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Expressway-E (Destination)
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222 (not configurable)
Traversal zone SIP signaling	TLS	25000–29999	7001
Media  <b>Note</b> If the internal > DMZ firewall rules allow outgoing traffic, no rules are needed for media.	UDP	36002–59999 <sup>8</sup> 36002–59999 <sup>9</sup> 50000–54999 <sup>10</sup>	36000–36001 <sup>11</sup> 36000–36011 <sup>12</sup>

<sup>8</sup> For Cisco Expressway-C 8.1 or later.<sup>9</sup> For large deployments of Cisco Expressway-C 8.1 or later.<sup>10</sup> If Cisco Expressway-C is upgraded from 7.1.<sup>11</sup> For Cisco Expressway-E 8.1 or later.<sup>12</sup> For large deployments of Cisco Expressway-E 8.1 or later.**Table 13: Outbound from Cisco Jabber Guest (Private) to Cisco Expressway-E (DMZ)**

Purpose	Protocol	Cisco Jabber Guest (Source)	Cisco Expressway-E (Destination)
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

**Table 14: Inbound from Cisco Expressway-E (DMZ) to Cisco Jabber Guest (Private)**

Purpose	Protocol	Cisco Expressway-E (Source)	Cisco Jabber Guest (Destination)
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

**Table 15: From Cisco Expressway-C to Cisco Jabber Guest**

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Jabber Guest (Destination)
HTTP	TCP	Ephemeral port	80

**REVIEW DRAFT - CISCO CONFIDENTIAL**

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Jabber Guest (Destination)
HTTPS	TLS	Ephemeral port	443

**Table 16: From Cisco Jabber Guest to Cisco Expressway-C**

Purpose	Protocol	Cisco Jabber Guest (Source)	Cisco Expressway-C (Destination)
HTTPS	TLS	Ephemeral port	443

## Clustering Options

Cisco Jabber Guest supports a three-server cluster. Three operational servers are required for full redundancy. Cisco Jabber Guest functions properly with two operational servers in the cluster; however, we recommend to only run with two operational servers for short periods of time, for example, when upgrading the servers in a Cisco Jabber Guest cluster. Cisco Jabber Guest does not function properly if only one server in the cluster is operational.

### Recommended Deployment

Configure the reverse proxy to send requests to only one server in the cluster at a time. You set the order in which requests are sent on the Cisco Expressway-C, from the **Priority** field in **Configuration > Unified Communications > Configuration > Configure Jabber Guest servers**. Give each Cisco Jabber Guest server a different priority. Requests are sent to a different server only if a server becomes unresponsive.

Cisco Jabber Guest can be administered from any server in the cluster; however, to simplify troubleshooting, we recommend that you use one server in the cluster for administration purposes.

### Data Replication

The following table describes which data replicates in a cluster.

**Table 17: Cluster Data Replication**

Data That Replicates	Data That Does Not Replicate
Users	Settings > Local SSL Certificate
Links	Settings > Call Control and Media (Local)
Services > Passwords	Logs
Settings > Links	
Settings > Mobile	

**REVIEW DRAFT - CISCO CONFIDENTIAL**

Data That Replicates	Data That Does Not Replicate
Settings > Secure SIP Trust Certificate	
Settings > Call Control and Media	

**Cluster Latency**

The upper latency limit is 15 milliseconds.

**Related Topics**

[Cluster](#), on page 45

## Load Balancing Methods Available

You can balance the load on your Cisco Expressway-C, Cisco Expressway-E, and Cisco Jabber Guest server clusters.

The following table describes the methods of load balancing that are available to distribute different types of traffic across the network.

**Table 18: Load Balancing Methods**

Network Traffic		Method of Load Balancing Available
SIP for call control	Send SIP to the Cisco Expressway-C server cluster	<ul style="list-style-type: none"> <li>• Round-robin DNS</li> <li>• Round-robin comma-separated values (CSV)</li> <li>• HTTP</li> </ul>
	Send SIP to the Cisco Expressway-E server cluster	Send SIP to the Cisco Expressway-E server that provided TURN service  <b>Important</b> For a clustered Cisco Expressway-E with dual NIC deployment, you must send SIP to the Cisco Expressway-E server that provided TURN service.
TURN credential provisioning requests to the Cisco Expressway-C server cluster		<ul style="list-style-type: none"> <li>• Round-robin DNS</li> <li>• Round-robin CSV</li> <li>• HTTP</li> </ul>
HTTPS from the Cisco Jabber Guest client to the Cisco Expressway-E server cluster		Round-robin DNS



**REVIEW DRAFT - CISCO CONFIDENTIAL**

Network Traffic	Method of Load Balancing Available
TURN for media between the Cisco Jabber Guest client and the Cisco Expressway-E server cluster	<ul style="list-style-type: none"><li>• Round-robin DNS for the Cisco Expressway-E server IP address and port range for round-robin TURN port range</li><li>• Round-robin CSV for the Cisco Expressway-E server IP address and port range for round-robin TURN port range</li></ul> <p><b>Important</b> TURN port ranges are only supported when you use the large Cisco Expressway-E virtual machine.</p>
HTTP between the Cisco Expressway-E and Cisco Jabber Guest server clusters	Configure Cisco Jabber Guest server priorities on the Cisco Expressway-C server.

**Related Topics**

[Round-Robin DNS Load Balancing](#)

[Configure Round-Robin CSV Load Balancing, on page 52](#)

[Configure HTTP Load Balancing, on page 53](#)

[Configure Round-Robin TURN Port Range Load Balancing, on page 53](#)

***REVIEW DRAFT - CISCO CONFIDENTIAL***



## Install Cisco Jabber Guest Server

---

- [Overview, page 21](#)
- [Install Server, page 21](#)
- [Sign In to Cisco Jabber Guest Administration, page 23](#)
- [Install Certificate, page 24](#)
- [Sign In to Cisco Jabber Guest Server CLI, page 28](#)
- [Change Time Zone on Server, page 28](#)

### Overview

Cisco Jabber Guest is deployed as a virtual server and requires a VMware server to act its host. The server operating system is CentOS. Cisco Jabber Guest is an on-premises deployment: all services are set up, managed, and maintained on your corporate network.

Cisco Jabber Guest is delivered as an OVA image and deployed manually.

### Install Server

Do one of the following:

- [Install Server to vCenter Server, on page 22](#)
- [Install Server to ESXi Hypervisor, on page 23](#)

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Install Server to vCenter Server

### Procedure

---

- Step 1** Download the .OVA or copy the .OVA to a location on your drive that is accessible to vSphere.
- Step 2** Open the vSphere Client.
- Step 3** Choose **File > Deploy OVF Template**.
- Step 4** In the **Source** screen, browse to location of the OVA package, and then click **Next**.  
You can enter the URL if you know it.
- Step 5** Verify the details in the **OVF Template Details** screen, and then click **Next**.
- Step 6** In the **Name and Location** screen, enter a name for the virtual machine, select its location, and then click **Next**.
- Step 7** In the **Host / Cluster** screen, select the virtual machine deployment cluster, and then click **Next**.
- Step 8** In the **Storage** screen, select the virtual machine storage usage, and then click **Next**.
- Step 9** In the **Disk Format** screen, select a Virtual Machine Disk (VMDK) provisioning format, and then click **Next**.
- Step 10** In the **Networking Mapping** screen, select the appropriate Destination Networks for OVA deployment, and then click **Next**.
- Step 11** In the **Properties** screen, enter the network settings, and then click **Next**.  
The virtual machine is set up with DHCP by default. You must provide the following to configure the virtual machine with a static IP address:
- IP address
  - Network mask
  - Hostname
  - Gateway IP address
  - At least one DNS server IP address

**Important** Do not add leading zeros to the IP addresses. The addresses won't resolve as intended.

- Step 12** Click **Finish**.
- 

### What to Do Next

To turn on the virtual machine after it has been created, in the console window select **Power On**.

Configure the appropriate SIP trunk in Cisco Unified Communications Manager or zones in Cisco TelePresence Video Communication Server depending on the type of server deployed in your network.

**Note**

If the virtual machine cannot acquire the IP address of your VLAN, it shows a bootup failure related to network `eth0`.

---

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Install Server to ESXi Hypervisor

### Procedure

- 
- Step 1** Download the .OVA or copy the .OVA to a location on your drive that is accessible to vSphere.
- Step 2** Open the vSphere Client.
- Step 3** Choose **File > Deploy OVF Template**.
- Step 4** In the **Source** screen, browse to location of the OVA package, and then click **Next**.  
You can enter the URL if you know it.
- Step 5** Verify the details in the **OVF Template Details** screen, and then click **Next**.
- Step 6** In the **Name and Location** screen, enter a name for the virtual machine, select its location, and then click **Next**.
- Step 7** In the **Disk Format** screen, select a Virtual Machine Disk (VMDK) provisioning format, and then click **Next**.
- Step 8** Click **Finish**.
- 

### What to Do Next

To turn on the virtual machine after it has been created, in the console window, select **Power On**.



**Note** The virtual machine is set up with DHCP by default. If you want to configure the virtual machine with a static IP address, you must edit the following properties: IP address, network mask, hostname, gateway IP address, and at least one DNS server IP address.

Configure the appropriate SIP trunk in Cisco Unified Communications Manager or zones in Cisco TelePresence Video Communication Server depending on the type of server deployed in your network.



**Note** If the virtual machine cannot acquire the IP address of your VLAN, it shows a boot up failure related to network `eth0`.

### Related Topics

[Change Virtual Machine Properties of an ESXi-hosted Server, on page 55](#)

## Sign In to Cisco Jabber Guest Administration

The Cisco Jabber Guest server is set up with default credentials.

### Before You Begin

You can access Cisco Jabber Guest Administration on Windows with:

- Google Chrome 18 or later

## REVIEW DRAFT - CISCO CONFIDENTIAL

- Microsoft Internet Explorer 8 or later (32-bit only)
- Mozilla Firefox 10 or later

You can access Cisco Jabber Guest Administration on Mac with:

- Apple Safari 5 or later
- Google Chrome 18 or later
- Mozilla Firefox 10 or later

Your session times out after 30 minutes of inactivity.

### Procedure

- 
- Step 1** From a compatible browser, navigate to the IP address or host name of your Cisco Jabber Guest server and append `/admin/` to the URL.
- Step 2** For **Alias**, enter admin.
- Step 3** For **Password**, enter jabbercserver.  
The first time that you sign in you must change your password.
- Step 4** Enter a new password.
- 

## Install Certificate

When you install Cisco Jabber Guest, a self-signed certificate is installed by default. If you want, you can:

- Install a certificate that is signed by a third party (a trusted certificate authority).
- Install a certificate with additional distinguished name information.
- Install a certificate that includes the intermediate certificate or the entire certificate trust chain.

Cisco Jabber Guest supports installing DER encoded certificates and PEM encoded certificates.



### Important

The certificate signing request must be generated on the server on which you install the certificate. For this reason, we recommend that you obtain a new CA-signed certificate for your new install of Cisco Jabber Guest or use a self-signed certificate.

If you choose to use the certificate that is installed by default, you must generate a new self-signed certificate if the hostname of the server changes.

## Install Certificate Signed by a Certificate Authority

The following procedure creates a certificate signing request in which the Distinguished Name (DN) information is composed of Common Name=<ip address> only. If your organization requires you to include additional

## REVIEW DRAFT - CISCO CONFIDENTIAL

DN information in your request, follow the instructions in the procedure, *Install Certificate with Additional Distinguished Name Information*.

If you have deployed a Cisco Jabber Guest cluster, you must install a certificate on each server in the cluster.

When you create the new certificate signing request, the current certificate becomes invalid.

### Procedure

---

- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
  - Step 2** Click **Settings**, and then click **Local SSL Certificate**.
  - Step 3** Under **Certificate Signing Request Options**, click **Create a New Certificate Signing Request**.
  - Step 4** Click **Download a certificate signing request**.  
A 4096-bit certificate signing request named `csr.pem` downloads.
  - Step 5** Send the certificate signing request to a trusted certificate authority.
  - Step 6** After you receive the signed certificate from the certificate authority:
    - a) Click **Choose File**.
    - b) Open the signed certificate.
    - c) Click **Install a Certificate Authority Signed Certificate**.Under **Certificate Status**, the following message appears:  
This system has a certificate authority signed certificate
  - Step 7** Restart the virtual machine:
    - a) Open vSphere Client.
    - b) In the virtual machines and templates inventory tree, right-click the virtual machine.
    - c) Choose **Power > Restart Guest**.
- 

### Related Topics

[Install Certificate with Additional Distinguished Name Information, on page 25](#)

## Install Certificate with Additional Distinguished Name Information

If you use Cisco Jabber Guest Administration to create a certificate signing request, the Distinguished Name (DN) information in the request is composed only of Common Name=<*ip address*>. If your organization requires you to include additional DN information, such as organization name and locality name, use the following procedure.

If you have deployed a Cisco Jabber Guest cluster, you must install a certificate on each server in the cluster.

When you create the new certificate signing request, the current certificate becomes invalid.

### Procedure

---

- Step 1** Sign in to the server as root.
- Step 2** Change directory to `/opt/cisco/webcommon/scripts`:  
`/opt/cisco/webcommon/scripts`

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- Step 3** Execute the `createcsr` script:  
`./createcsr.sh`
- Step 4** Follow the instructions on the screen to enter additional DN information, including country name, state or province name, locality name, organization name, organizational unit name, and common name.  
 After you enter the information, the `csr` file is saved in a location from which you download it in Step 7.
- Step 5** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 6** Click **Settings**, and then click **Local SSL Certificate**.
- Step 7** Under **Certificate Signing Request Options**, click **Download a certificate signing request**.  
 A 4096-bit certificate signing request named `csr.pem` downloads.
- Step 8** Send the certificate signing request to a trusted certificate authority.
- Step 9** After you receive the signed certificate from the certificate authority:
- Click **Choose File**.
  - Open the signed certificate.
  - Click **Install a Certificate Authority Signed Certificate**.
- Under **Certificate Status**, the following message appears:  
 This system has a certificate authority signed certificate
- Step 10** Restart the virtual machine:
- Open vSphere Client.
  - In the virtual machines and templates inventory tree, right-click the virtual machine.
  - Choose **Power > Restart Guest**.
- 

## Install Certificate That Includes the Intermediate Certificate or the Entire Certificate Trust Chain

You can upload a combined certificate file that includes the Cisco Jabber Guest server certificate and your intermediate certificate or that includes the Cisco Jabber Guest server certificate, your intermediate certificate, and your root certificate.

If you have deployed a Cisco Jabber Guest cluster, you must install a certificate on each server in the cluster.

When you create the new certificate signing request, the current certificate becomes invalid.

### Procedure

---

- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 2** Click **Settings**, and then click **Local SSL Certificate**.
- Step 3** Under **Certificate Signing Request Options**, click **Create a New Certificate Signing Request**.
- Step 4** Click **Download a certificate signing request**.



**REVIEW DRAFT - CISCO CONFIDENTIAL**

A 4096-bit certificate signing request named `csr.pem` downloads.

- Step 5** Send the certificate signing request to a trusted certificate authority.
- Step 6** After you receive the signed certificate from the certificate authority, open it in a text editor, such as Notepad.
- Step 7** Download your intermediate certificate.
- Step 8** In the Cisco Jabber Guest certificate, after `-----END CERTIFICATE-----`, paste the entire body of your intermediate certificate.

**Note** Make sure that you include the beginning and end tags of both certificates. The result should look like this:

```
-----BEGIN CERTIFICATE-----
(Cisco Jabber Guest certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your intermediate certificate)
-----END CERTIFICATE-----
```

- Step 9** (Optional) If you want to include the root certificate in the combined certificate file:

- Download your root certificate.
- In the Cisco Jabber Guest certificate, after `-----END CERTIFICATE-----` for the intermediate file, paste the entire body of your root certificate.

**Note** Make sure that you include the beginning and end tags of all three certificates. The result should look like this:

```
-----BEGIN CERTIFICATE-----
(Cisco Jabber Guest certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your intermediate certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your root certificate)
-----END CERTIFICATE-----
```

- Step 10** Make sure that there is no additional formatting in the file.
- Step 11** Save the combined certificate file.
- Step 12** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 13** Click **Settings**, and then click **Local SSL Certificate**.
- Step 14** Click **Choose File**, open the combined certificate file, and click **Install a Certificate Authority Signed Certificate**.  
Under **Certificate Status**, the following message appears:  
This system has a certificate authority signed certificate
- Step 15** Restart the virtual machine:
- Open vSphere Client.
  - In the virtual machines and templates inventory tree, right-click the virtual machine.
  - Choose **Power > Restart Guest**.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Generate New Self-Signed Certificate

If you are using the self-signed certificate that is installed by default and the hostname of the server changes, you must generate a new self-signed certificate.

When you generate a new self-signed certificate, the current certificate becomes invalid.

### Procedure

---

- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
  - Step 2** Click **Settings**, and then click **Local SSL Certificate**.
  - Step 3** Click **Generate a New Self-Signed Certificate**.  
The message `Update successful` appears.
  - Step 4** Restart the virtual machine:
    - a) Open vSphere Client.
    - b) In the virtual machines and templates inventory tree, right-click the virtual machine.
    - c) Choose **Power > Restart Guest**.
- 

## Sign In to Cisco Jabber Guest Server CLI

The Cisco Jabber Guest server command-line interface (CLI) is set up with default credentials.

### Procedure

---

- Step 1** For the user ID, enter `root`.
  - Step 2** For the password enter `jabbercserver`. The first time that you sign in, you must change the password.
  - Step 3** Enter a new password.
- 

## Change Time Zone on Server

By default, the server time zone is set to Coordinated Universal Time (UTC). To change the time zone, use the following procedure.

The time zone change takes effect immediately.

### Procedure

---

- Step 1** Sign in to the server as `root`.
- Step 2** Check the current time zone by executing the command: `date`.

***REVIEW DRAFT - CISCO CONFIDENTIAL***

The date and time appear in the format: *ddd mmm dd hh:mm:ss UTC yyyy*. For example: Fri Dec 20 16:57:18 UTC 2013.

**Step 3** Change directory to `/opt/cisco/webcommon/scripts`:

```
cd /opt/cisco/webcommon/scripts
```

**Step 4** Execute the `timezone` script:

```
./timezone
```

**Step 5** Follow the on-screen instructions.

**Step 6** At the confirmation message, type 1 for Yes.

**Step 7** Verify that the server is set to your time zone by executing the command: `date`.

**Step 8** Restart Tomcat:

```
service tomcat-as-standalone.sh restart
```

---

***REVIEW DRAFT - CISCO CONFIDENTIAL***



## CHAPTER

# 3

## Perform Initial Setup

---

- [Configure Cisco Expressway-E and Cisco Expressway-C, page 31](#)
- [Change MTU Size, page 36](#)
- [Configure Signaling and Media, page 36](#)
- [Configure Static NAT Mode on Cisco Expressway-E, page 39](#)
- [Configure TURN Credential Provisioning, page 39](#)
- [Set Up TURN Server Information, page 40](#)
- [Set FQDN of Cisco Jabber Guest Server, page 40](#)
- [Set Domain Used for Links, page 40](#)
- [Customize Cisco Jabber Guest Clients, page 41](#)

## Configure Cisco Expressway-E and Cisco Expressway-C

Do one of the following:

- [Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment, on page 31](#)
- [Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Dual NIC Deployment, on page 33](#)

## Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment

Cisco Expressway-E and Cisco Expressway-C provide the following functionality:

- Both provide reverse proxy for HTTPS traffic.
- Cisco Expressway-E provides TURN relays.
- Cisco Expressway-C routes calls to Cisco Unified Communications Manager through a SIP trunk.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Before You Begin**

Follow the instructions in the Cisco Expressway documentation to set up Cisco Expressway security certificates and a Unified Communications traversal zone. Configure the traversal zone type between the Cisco Expressway-C and Cisco Expressway-E as *Unified Communications traversal*.

**Procedure**

- 
- Step 1** On the Cisco Expressway-E, enable Cisco Jabber Guest support:
- Choose **Configuration > Unified Communications > Configuration**.
  - From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
  - Click **Save**.
- Step 2** On the Cisco Expressway-E, enable TURN service:
- Choose **Configuration > Traversal > TURN**.
  - From the **TURN services** drop-down list, select **On**.
  - Click **Save**.
- Step 3** On the Cisco Expressway-C, enable Cisco Jabber Guest support:
- Choose **Configuration > Unified Communications > Configuration**.
  - From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
  - Click **Save**.
- Step 4** On the Cisco Expressway-C, configure the domain for which HTTP traffic will be routed to the Cisco Jabber Guest server:
- This domain is the outward-facing domain that is used to route the call on the Internet when users click a link.
- Choose **Configuration > Domains**.
  - Create a new domain if none exist or, in the row of the target domain, click **View/Edit**.
  - From the **Jabber Guest** drop-down list, select **On**.
  - Click **Save**.
  - Repeat Step 5.a. through Step 5.d. for each domain.
- Step 5** Make sure that the domain has an associated DNS record that resolves to the Cisco Expressway-E. The domain information is propagated from the Cisco Expressway-C to the Cisco Expressway-E through the SSH tunnel (port 2222). It is used by the Cisco Expressway-E to validate incoming HTTP requests for the Cisco Jabber Guest service.
- Step 6** On the Cisco Expressway-C, associate the Cisco Jabber Guest servers with the domain:
- This allows the Cisco Expressway-C to route HTTP requests with this domain to the appropriate Cisco Jabber Guest server.
- Choose **Configuration > Unified Communications > Configuration**.
  - In the **Advanced** section, click **Configure Jabber Guest servers**.
  - Click **New**.
  - For **Server hostname**, enter the FQDN of the Cisco Jabber Guest server.
  - For **Priority**, enter the priority of the Cisco Jabber Guest server. Lower numbers have higher priority. Make sure that all Cisco Jabber Guest servers have a different priority so that calls are only sent to one Cisco Jabber Guest server in the deployment at a time.
  - From the **Domain** drop-down list, select the Cisco Jabber Guest HTTP domain.
  - Click **Create entry**.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- h) Repeat Step 6.c. through Step 6.g. for each Cisco Jabber Guest server in the cluster.
- Step 7** Verify that the SSH tunnel is active:
- On either the Cisco Expressway-C or the Cisco Expressway-E, choose **Status > Unified Communications**.
  - Click **View ssh tunnel status**.
  - Make sure that the Cisco Jabber Guest domain is listed and that the SSH tunnel is active.
- Step 8** On the Cisco Expressway-C, create a neighbor zone for each Cisco Jabber Guest server:
- Choose **Configuration > Zones > Zones**.
  - Click **New**.
  - Enter the details. From the **Type** drop-down list, select **Neighbor**.
  - In the **H.323** section, from the **Mode** drop-down list, select **Off**.
  - In the **SIP** section, from the **Mode** drop-down list, select **On**.
  - For **Port**, enter 5061.
  - From the **Transport** drop-down list, select TLS.
  - From the **Media encryption mode** drop-down list, select **Best effort**.  
**Important** Selecting *Best effort* forces media from the Cisco Expressway-E to terminate on the Cisco Expressway-C.
  - From the **ICE support** drop-down list, select **Off**.
  - In the **Location** section, for **Peer 1 address**, enter the IP address or FQDN of the Cisco Jabber Guest server.
  - In the **Advanced** section, from the **Zone profile** drop-down list, select **Default**.
  - Click **Create zone**.
  - Repeat Step 7.b. through 7.l. for each Cisco Jabber Guest server in a Cisco Jabber Guest cluster.  
 Do not configure any search rules for these neighbor zones. These zones are used to receive traffic only.
- Step 9** On the Cisco Expressway-C, follow the steps in the *Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide* to set up a secure trunk to Cisco Unified Communications Manager.
- Step 10** Create a search rule on Cisco Expressway-C to route calls to Cisco Unified Communications Manager.
- Step 11** Force the protocol between the Cisco Jabber Guest server and the Cisco Expressway-C to be http:
- Sign in to the Cisco Expressway-C command-line interface as an administrator. In a clustered Cisco Expressway-C deployment, sign in to the master Cisco Expressway-C.
  - Enter the following command:  

```
xconf CollaborationEdge JabbercProxyProtocol: http
```

---

HTTP request goes from the Cisco Expressway-E to the Cisco Expressway-C to the Cisco Jabber Guest server.

**Related Topics**

[Cisco Expressway Series on www.cisco.com](http://www.cisco.com)

[Cisco Unified Communications Manager with Cisco Expressway \(SIP Trunk\) Deployment Guide](#)

## Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Dual NIC Deployment

Cisco Expressway-E and Cisco Expressway-C provide the following functionality:

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- Both provide reverse proxy for HTTPS traffic.
- Cisco Expressway-E provides TURN relays.
- Cisco Expressway-C routes calls to Cisco Unified Communications Manager through a SIP trunk.

**Before You Begin**

Follow the instructions in the Cisco Expressway documentation to set up Cisco Expressway security certificates and a Unified Communications traversal zone. Configure the traversal zone type between the Cisco Expressway-C and Cisco Expressway-E as *Unified Communications traversal*.

**Procedure**

- 
- Step 1** On the Cisco Expressway-E, enable Cisco Jabber Guest support:
- Choose **Configuration > Unified Communications > Configuration**.
  - From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
  - Click **Save**.
- Step 2** On the Cisco Expressway-E, enable TURN service:
- Choose **Configuration > Traversal > TURN**.
  - From the **TURN services** drop-down list, select **On**.
  - Click **Save**.
- Step 3** On the Cisco Expressway-C, enable Cisco Jabber Guest support:
- Choose **Configuration > Unified Communications > Configuration**.
  - From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
  - Click **Save**.
- Step 4** On the Cisco Expressway-C, configure the domain for which HTTP traffic routes to the Cisco Jabber Guest server:
- This domain is the outward-facing domain that is used to route the call on the Internet when users click a link.
- Choose **Configuration > Domains**.
  - Create a new domain if none exist or, in the row of the target domain, click **View/Edit**.
  - From the **Jabber Guest** drop-down list, select **On**.
  - Click **Save**.
  - Repeat Step 5.a. through Step 5.d. for each domain.
- Step 5** Make sure that the domain has an associated DNS record that resolves to the Cisco Expressway-E. The domain information is propagated from the Cisco Expressway-C to the Cisco Expressway-E through the SSH tunnel (port 2222). The information is used by the Cisco Expressway-E to validate incoming HTTP requests for the Cisco Jabber Guest service.
- Step 6** On the Cisco Expressway-C, associate the Cisco Jabber Guest servers with the domain:
- This allows the Cisco Expressway-C to route HTTP requests with this domain to the appropriate Cisco Jabber Guest server.
- Choose **Configuration > Unified Communications > Configuration**.
  - In the **Advanced** section, click **Configure Jabber Guest servers**.
  - Click **New**.
  - For **Server hostname**, enter the FQDN of the Cisco Jabber Guest server.
  - For **Priority**, enter the priority of the Cisco Jabber Guest server. Lower numbers have higher priority.



**REVIEW DRAFT - CISCO CONFIDENTIAL**

Give each Cisco Jabber Guest server a different priority so that calls are only sent to one Cisco Jabber Guest server in the deployment at a time.

- f) From the **Domain** drop-down list, select the Cisco Jabber Guest HTTP domain.
- g) Click **Create entry**.
- h) Repeat Step 6.c. through Step 6.g. for each Cisco Jabber Guest server in the cluster.

**Step 7** Verify that the SSH tunnel is active:

- a) On either the Cisco Expressway-C or the Cisco Expressway-E, choose **Status > Unified Communications**.
- b) Click **View ssh tunnel status**.
- c) Make sure that the Cisco Jabber Guest domain is listed and that the SSH tunnel is active.

**Step 8** On the Cisco Expressway-E, create a neighbor zone for each Cisco Jabber Guest server so that you can verify that the zone between the Cisco Expressway-E and the Cisco Jabber Guest server is active:

- a) Choose **Configuration > Zones > Zones**.
- b) Click **New**.
- c) Enter the details. From the **Type** drop-down list, select **Neighbor**.
- d) In the **H.323** section, from the **Mode** drop-down list, select **Off**.
- e) In the **SIP** section, from the **Mode** drop-down list, select **On**.
- f) For **Port**, enter 5061.
- g) From the **Transport** drop-down list, select **TLS**.
- h) From the **Media encryption mode** drop-down list, select **Best effort**.
- i) From the **ICE support** drop-down list, select **Off**.
- j) In the **Location** section, for **Peer 1 address**, enter the IP address or FQDN of the Cisco Jabber Guest server.
- k) In the **Advanced** section, from the **Zone profile** drop-down list, select **Default**.
- l) Click **Create zone**.
- m) Repeat Step 7.b. through 7.l. for each Cisco Jabber Guest server in a Cisco Jabber Guest cluster.  
Do not configure any search rules for these neighbor zones. These zones are used to receive traffic only.

**Step 9** Create a search rule for the traversal zone between the Cisco Expressway-E and the Cisco Expressway-C servers.

**Important** For proper call routing, the SIP domain that you specify (click **Settings**, click **Call Control and Media**) and the domain that you optionally specify for **Destination** when you create a link (click **Links**, click **New**) must be configured on the Cisco Expressway-E search rule to point to the traversal zone.

**Step 10** On Cisco Expressway-C, follow the steps in the *Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide* to set up a secure trunk to Cisco Unified Communications Manager.

**Step 11** Create a search rule on Cisco Expressway-C to route calls to Cisco Unified Communications Manager.

**Step 12** Force the protocol between the Cisco Jabber Guest server and the Cisco Expressway-C to be http:

- a) Sign in to the Cisco Expressway-C command-line interface as an administrator. In a clustered Cisco Expressway-C deployment, you must sign in to the master Cisco Expressway-C.
- b) Enter the following command:

```
xconf CollaborationEdge JabbercProxyProtocol: http
```

HTTP request goes from the Cisco Expressway-E to the Cisco Expressway-C to the Cisco Jabber Guest server.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Related Topics**

[Cisco Expressway Series on www.cisco.com](#)

[Cisco Unified Communications Manager with Cisco Expressway \(SIP Trunk\) Deployment Guide](#)

## Change MTU Size

In some call scenarios, such as when using VPN, the default Maximum Transmission Unit (MTU) on Cisco Expressway-E is too high and can cause packet loss. The default MTU is 1500 bytes. We recommend that you lower the MTU to 1400 bytes. If you do not, callers may experience problems, such as one-way video.

**Procedure**

- 
- Step 1** On Cisco Expressway-E, do one of the following:
- If you have Cisco Expressway-E 8.2, choose **System > IP**.
  - If you have Cisco Expressway-E 8.5 or later, choose **System > Network Interfaces > IP**.
- Step 2** In the **LAN 1** section, for **Maximum transmission unit (MTU)**, enter 1400.
- Step 3** Click **Save**.
- 

## Configure Signaling and Media

Do one of the following:

- [Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment, on page 36](#)
- [Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment, on page 37](#)

## Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment

We recommend enabling Session Initiation Protocol (SIP) over Transport Layer Security (TLS) for call control signaling and enabling Secure Real-Time Transfer Protocol (SRTP) for secure media. Secure media requires secure signaling.

**Procedure**

- 
- Step 1** To enable SIP over TLS, obtain the Cisco Expressway-C server certificate or the Cisco Expressway-C certificate authority certificate:
- If you have a single Cisco Expressway-C, obtain the Cisco Expressway-C server certificate.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- If Cisco Expressway-C is a cluster of servers, obtain the Cisco Expressway-C certificate authority certificate. This certificate must be uploaded to the Cisco Jabber Guest server so that Cisco Jabber Guest can communicate with all nodes in the Cisco Expressway-C cluster.

**Step 2** Upload the certificate to Cisco Jabber Guest Administration:

- a) Sign in to Cisco Jabber Guest Administration as an administrator.
- b) Click **Settings**, and then click **Secure SIP Trust Certificate**.
- c) Under **Secure SIP Trust Certificate**, click **Choose File**.
- d) Select the certificate that you obtained, and then click **Upload**.

**Step 3** Configure the **Call Control and Media** settings in Cisco Jabber Guest Administration:

- a) Click **Call Control and Media**.
- b) Select **Route calls using Cisco Expressway**.
- c) Check **Enable SIP over TLS**.
- d) Check **Enable SRTP**.
- e) For **SIP port**, enter 5061.
- f) For **SIP domain**, enter the SIP domain. This setting is used if the Cisco Jabber Guest link does not contain a SIP domain. In most cases, this is the enterprise SIP domain as configured in Cisco Unified Communications Manager.
- g) For **SIP server**, enter the IP address or FQDN of the Cisco Expressway-C.
- h) Specify whether SIP is sent to the Cisco Expressway-C that originated the HTTP call control or to the server entered above.

**Step 4** Click **Update**.

The message `Update successful` appears.

**Step 5** Restart Tomcat:

```
service tomcat-as-standalone.sh restart
```

**Step 6** On the Cisco Expressway-C, verify that the neighbor zones for each Cisco Jabber Guest server are active:

- a) Choose **Configuration > Zones > Zones**.
- b) View the **SIP status** column.

## Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment

We recommend enabling Session Initiation Protocol (SIP) over Transport Layer Security (TLS) for call control signaling and enabling Secure Real-Time Transfer Protocol (SRTP) for secure media. Secure media requires secure signaling.

### Procedure

**Step 1** To enable SIP over TLS, obtain the Cisco Expressway-E server certificate or the Cisco Expressway-E certificate authority certificate:

- If you have a single Cisco Expressway-E, obtain the Cisco Expressway-E server certificate.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- If Cisco Expressway-E is a cluster of servers, obtain the Cisco Expressway-E certificate authority certificate. This certificate must be uploaded to the Cisco Jabber Guest server so that Cisco Jabber Guest can communicate with all nodes in the Cisco Expressway-E cluster.

**Step 2** Upload the certificate to Cisco Jabber Guest Administration:

- Sign in to Cisco Jabber Guest Administration as an administrator.
- Click **Settings**, and then click **Secure SIP Trust Certificate**.
- Under **Secure SIP Trust Certificate**, click **Choose File**.
- Select the certificate that you obtained, and then click **Upload**.

**Step 3** Configure the **Call Control and Media** settings in Cisco Jabber Guest Administration:

- Click **Call Control and Media**.
- Select **Route calls using Cisco Expressway**.
- Check **Enable SIP over TLS**.
- Check **Enable SRTP**.
- For **SIP port**, enter 5061.
- For **SIP domain**, enter the SIP domain. This setting is used if the Cisco Jabber Guest link does not contain a SIP domain. In most cases, this is the enterprise SIP domain as configured in Cisco Unified Communications Manager.  
**Important** For proper call routing, the SIP domain must be configured on the Cisco Expressway-E search rule to point to the traversal zone.
- For a single Cisco Expressway-E server, for **SIP server**, enter the IP address or FQDN of the Cisco Expressway-E.
- Select where to send SIP traffic:

- For a single Cisco Expressway-E server, select **SIP server specified above**.
- For cluster of Cisco Expressway-E servers:

- 1 Select **Expressway-E server that provided TURN service**.

**Important** The TURN relay and SIP signaling must reside on the same server.

- 2 Under **Cisco Expressway-E Network Address Map**, enter the external IP addresses and internal IP addresses of each of the Cisco Expressway-E servers in the cluster. Mapping allows the Cisco Jabber Guest server to send the SIP to the same Cisco Expressway-E servers as the TURN relay.

If static NAT mode is enabled on Cisco Expressway-E with either single NIC deployment or dual NIC deployment, the Cisco Jabber Guest server must be configured for static NAT mode as well.

**Step 4** Click **Update**.

The message `Update successful` appears.

**Step 5** Restart Tomcat:

```
service tomcat-as-standalone.sh restart
```

**Step 6** On the Cisco Expressway-E, verify that the neighbor zones for each Cisco Jabber Guest server are active:

- Choose **Configuration > Zones > Zones**.
- View the **SIP status** column.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Configure Static NAT Mode on Cisco Expressway-E

If static NAT mode is enabled on Cisco Expressway-E with either single NIC deployment or dual NIC deployment, the Cisco Jabber Guest server must be configured for static NAT mode as well. This allows the media to flow within the DMZ, avoiding NAT reflection (sending media to the NATed address).

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration.
  - Step 2** Click **Settings**, and then click **Call Control and Media**.
  - Step 3** Under **Cisco Expressway-E Network Address Map**, check **Static NAT mode**.  
This check box appears only when the option, **Route calls using Cisco Expressway**, is selected.
  - Step 4** Under **Public IP (Static NAT)**, enter the static NAT IP address of the Cisco Expressway-E server.
  - Step 5** Under **External IP (DMZ)**, enter the external IP address of the Cisco Expressway-E server.
  - Step 6** Repeat Steps 4 and 5 for each of the Cisco Expressway-E servers in the cluster.
  - Step 7** Click **Update**.
- 

## Configure TURN Credential Provisioning

The Cisco Jabber Guest client needs TURN credentials to allocate TURN relays on the Cisco Expressway-E. The Cisco Jabber Guest server provisions these credentials on the Cisco Expressway-C when the Cisco Jabber Guest client connects.

The Cisco Jabber Guest server uses an HTTP-based XML API to communicate with Cisco Expressway-C.

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
  - Step 2** Click **Settings**, and then click **Call Control and Media**.
  - Step 3** Under **Cisco Expressway-C**, for **Expressway-C (IP address or DNS name)**, enter the Cisco Expressway-C IP address or DNS name.
  - Step 4** Specify whether short-term TURN credentials are requested from the Cisco Expressway-C that proxied the HTTP request from the Cisco Jabber Guest client or from the server entered in Step 3.
  - Step 5** For **HTTPS port**, specify the port.
  - Step 6** For **Domain**, enter the domain on Cisco Expressway-C that has Jabber Guest services enabled.
  - Step 7** For **Username** and **Password**, enter the username and password of the administrator account on Cisco Expressway-C that has read, write, and API access.
  - Step 8** Click **Update**.
-

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Set Up TURN Server Information

The Cisco Jabber Guest client needs to know which Cisco Expressway-E to use for TURN relays.

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 2** Click **Settings**, and then click **Call Control and Media**.
- Step 3** Under **Cisco Expressway-E**, for **Expressway-E TURN server (IP address or DNS name)**, enter the Cisco Expressway-E TURN server outside IP address or DNS name.
- Step 4** For **TURN port**, enter the UDP port. The port is typically 3478 but you can enter a range of ports, such as 3478-3483. The range is necessary if the Cisco Expressway-E supports multiple TURN ports.
- Important** The port must match the port specified on the Cisco Expressway-E (under **Configuration > Traversal > TURN**).
- Step 5** Click **Update**.
- 

## Set FQDN of Cisco Jabber Guest Server

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 2** Click **Settings**, and then click **Call Control and Media (Local)**.
- Step 3** Enter the FQDN of the Cisco Jabber Guest server.
- Important** The FQDN must match the value specified in the Cisco Jabber Guest **Server hostname** field on the Cisco Expressway-C. Cisco Expressway-C uses the FQDN to forward the per-session HTTP traffic to the appropriate Cisco Jabber Guest server in the cluster.
- Step 4** Click **Update**.
- 

### What to Do Next

Make sure that you populate the **Cisco Jabber Guest local FQDN** field for each node in the Cisco Jabber Guest cluster.

## Set Domain Used for Links

To create links on the Cisco Jabber Guest server, you must enter the domain that is configured on the Cisco Expressway.

## REVIEW DRAFT - CISCO CONFIDENTIAL

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
  - Step 2** Click **Settings**, and then click **Links**.
  - Step 3** For **Domain used for links**, enter the the public DNS name of the Cisco Expressway-E. You can add a subdomain for Cisco Jabber Guest service.

#### Example:

If `yourcompany.com` is configured as the domain on the Cisco Expressway and `yg.yourcompany.com` is configured on the Cisco Jabber Guest server, the format of the link is `https://yg.yourcompany.com/call/<directory number>`.

- Step 4** Click **Update**.
- 

## Customize Cisco Jabber Guest Clients



### Important

Do not to modify any files on the Cisco Jabber Guest server. For example, on the web client, editing the appearance of the Cisco Jabber Guest video window, such as the **Call** button, is not supported.

To change the appearance of the web page that contains the Cisco Jabber Guest video window, host the page on a server other than the Cisco Jabber Guest server.

The mobile client can be fully customized.

For more information about customizing Cisco Jabber Guest clients, go to the Cisco Jabber Guest SDK DevNet website.

### Related Topics

[Cisco Jabber Guest SDK DevNet](#)

***REVIEW DRAFT - CISCO CONFIDENTIAL***





## Upgrade Cisco Jabber Guest Server

- [Upgrade Cisco Jabber Guest Server, page 43](#)

## Upgrade Cisco Jabber Guest Server

Cisco Jabber Guest Server is upgraded through vSphere on the Microsoft Windows platform. The upgrade is delivered as an ISO file, and requires a CD or DVD drive that can be connected to the image.

### Procedure

- Step 1** Download JabberGuest-10.x.x.x.iso.
- Step 2** Open vSphere.
- Step 3** Browse to the virtual machine to upgrade.
- Step 4** Right-click the virtual machine and select **Open console**.
- Step 5** Connect the CD/DVD drive to the ISO image:
  - a) From the console of the virtual machine, click on the CD/DVD button whose icon image is a disk with a wrench.
  - b) Click the **CD/DVD drive 1** menu item and then select the **Connect to ISO image on local disk...** menu item.
  - c) In the **Open** window, browse to the ISO image downloaded in Step 1 and double-click it.
- Step 6** Click inside the virtual machine console and sign in as root.
- Step 7** Under the /mnt directory, create a new directory named `cdrom` to use as the mount location for the CD/DVD drive.

```
mkdir /mnt/cdrom
```
- Step 8** Mount the CD/DVD drive to /mnt/cdrom:

```
mount /dev/cdrom /mnt/cdrom
```
- Step 9** Change directory to /mnt/cdrom:

```
cd /mnt/cdrom
```
- Step 10** Execute the upgrade script:

```
bash upgrade
```

***REVIEW DRAFT - CISCO CONFIDENTIAL***

- Step 11** To ensure that the latest version of Cisco Jabber Guest Administration is loaded in your browser, refresh any browser instances that are signed in to Cisco Jabber Guest Administration or that have the Cisco Jabber Guest Administration sign-in page loaded.
-



## CHAPTER

# 5

## Configure High Availability and Scalability

- [Cluster, page 45](#)
- [Configure Load Balancing, page 51](#)

## Cluster

### Create Cluster

In this procedure, we refer to the primary server as *primary* and to the two secondary servers as *node A* and *node B*.

#### Before You Begin

When a secondary server joins a cluster, all of the data on the secondary server is discarded. If you need to retain the data for future use, back up the secondary server before joining it to the cluster.

#### Procedure

- 
- Step 1** Deploy the .OVA to all three servers.
- Step 2** Sign in to each server as root.
- Step 3** To establish the primary, on one of the three servers:
- Type `cluster initiate`, and follow the on-screen prompts.  
It takes a minute or two for the database to stabilize in its new configuration.
  - Verify that the database has stabilized by typing `cluster status`.  
When the database has stabilized, the status shows: `---> <IP address/hostname of primary> PRIMARY`.  
The symbol `--->` indicates the current server.
  - Restart Tomcat: `service tomcat-as-standalone.sh restart`.
- Step 4** To join node A to the cluster, on one of the remaining servers:
- Type `cluster join <IP address/hostname of primary>`, and follow the on-screen prompts.  
It takes a minute or two for the database to stabilize in its new configuration.
  - Verify that the database has stabilized by typing `cluster status`.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

When the database has stabilized, the status shows: ---> <IP address/hostname of node A> SECONDARY.

- c) Restart Tomcat: `service tomcat-as-standalone.sh restart`.

**Step 5** To join node B to the cluster, on the remaining server:

- a) Type `cluster join <IP address/hostname of primary>`, and follow the on-screen prompts.  
It takes a minute or two for the database to stabilize in its new configuration.
- b) Verify that the database has stabilized by typing `cluster status`.  
When the database has stabilized, the status shows as: ---> <IP address/hostname of node B> SECONDARY.
- c) Restart Tomcat: `service tomcat-as-standalone.sh restart`.

**Step 6** Allow node A to communicate with node B:

- a) Type `cluster allow <IP address/hostname of node B>`.
- b) Verify that communication is allowed by typing `cluster status`.  
When communication is allowed, the status of node B changes from ---> <IP address/hostname of node B> not reachable/healthy to ---> <IP address/hostname of node B> SECONDARY.

**Step 7** Allow node B to communicate with node A:

- a) Type `cluster allow <IP address/hostname of node A>`.
- b) Verify that communication is allowed by typing `cluster status`.  
When communication is allowed, the status of node A changes from ---> <IP address/hostname of node A> not reachable/healthy to ---> <IP address/hostname of node A> SECONDARY.

---

### What to Do Next

For each of the three servers in the cluster, configure the appropriate SIP trunk in Cisco Unified Communications Manager or zones in Cisco TelePresence Video Communication Server, depending on the type of servers deployed in your network.

## Change IP Address or Hostname of Server in Cluster

You can modify the IP address or hostname of a server in the cluster if it changes for any reason.

In this procedure, we refer to the server that we change the IP address or hostname of as the *target server*.

### Procedure

---

- Step 1** Make a note of the current IP address or hostname of the target server. You need to enter it during Step 4.b.
- Step 2** (Optional) If you are changing the IP address or hostname of the primary server, demote the primary server to a secondary server, otherwise proceed to Step 3:
- a) On the primary server, type `cluster stepdown`.
- b) Verify that the target server has been demoted from the primary server to a secondary server by typing `cluster status`.
- c) Make a note of which server is now the primary server.
- Step 3** Change the IP address or hostname of the target server.
- Step 4** In the cluster, change the IP address or hostname of the target server:
- a) Sign in to the primary server as root.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- b) Type `cluster move <old IP address/hostname of target server> <new IP address/hostname of target server>`.
  - c) Verify that the IP address or hostname of the target server has changed by typing `cluster status`.
- Step 5** On the other secondary server (node B), block communication from the old IP address or hostname of the target server and allow communication with the new IP address or hostname of the target server:
- a) Sign in to node B as root.
  - b) On node B, block communication from the old IP address or hostname of the target server by typing `cluster disallow <old IP address/hostname of target server>`.
  - c) On node B, allow communication with the new IP address or hostname of the target server by typing `cluster allow <new IP/hostname of target server>`.
- Step 6** Make sure that each server in the cluster is healthy by typing: `cluster status`.
- Step 7** On the target server, restart Tomcat:
- ```
service tomcat-as-standalone.sh restart
```
- Step 8** If you changed the IP address or hostname of the primary server, in Cisco Jabber Guest Administration, update the domain used for links:
- a) Sign in to Cisco Jabber Guest Administration as an administrator.
  - b) Click **Settings**, and then click **Links**.
  - c) For **Domain used for Links**, enter the IP address or hostname of the new primary server.
  - d) Click **Update**.

**What to Do Next**

If you are using a self-signed certificate, you must generate a new certificate after you change the IP address or hostname of the server.

**Related Topics**

- [Change Virtual Machine Properties of a vCenter-hosted Server, on page 55](#)
- [Change Virtual Machine Properties of an ESXi-hosted Server, on page 55](#)
- [Generate New Self-Signed Certificate, on page 28](#)

**Demote Primary Server to Secondary Server**

You can demote or stepdown a primary server to a secondary server. For example, if you need to do maintenance on the primary server.

A new primary server is elected from the remaining servers in the cluster.

**Procedure**

- Step 1** Sign in to the primary server as root.
- Step 2** Type `cluster stepdown`.
- Step 3** Verify that the server has been demoted to secondary by typing `cluster status`.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Upgrade Cluster

In this procedure, we refer to the primary server as *node A* and to the two secondary servers as *node B* and *node C*.

### Procedure

- 
- Step 1** Make a note of which nodes are the primary and secondary servers:
- Sign in to one of the Cisco Jabber Guest servers as root.
  - Type `cluster status`.
- Step 2** Make sure that you have backed up each server in the cluster.
- Step 3** Download `JabberGuest-10.x.x.x.iso`.
- Step 4** Open vSphere Client.
- Step 5** If a CD/DVD drive is not connected to the virtual machine, add one:
- In the **Virtual Machine Properties** window, click the **Hardware** tab, and then click **Add** to bring up the **Add Hardware** window.
  - In the **Add Hardware** window, select **CD/DVD Drive** as the device type, and then click **Next**.
  - For the **CD/DVD Media** type, click **Use physical drive**, and then click **Next**.
  - Accept the default CD/DVD drive when prompted to select a drive, and then click **Next**.
  - In the **Advanced Options** settings, accept the default values, and then click **Next**.
  - In the **Ready to Complete** window, click **Finish**.
  - In the **Virtual Machine Properties** window, click **OK**.
- Step 6** On each server, connect the CD/DVD drive to the ISO image:
- In the virtual machines and templates inventory tree, select the virtual machine.
  - Click the **Connect/disconnect the CD/DVD devices of the virtual machine** button. The button icon is a disk with a wrench.
  - Point to **CD/DVD drive 1**, and then click **Connect to ISO image on local disk**.
  - In the **Open** window, browse to the ISO image downloaded in Step 2 and double-click it.
- It takes a little while to connect to the ISO image. When connected, in the **Recent Tasks** list, the status of the **Connect** task shows **Completed**.
- Step 7** Prepare to upgrade node B by updating the reverse proxy so that call requests are sent to node A first, node C second, and no call requests are sent to node B:
- On Cisco Expressway-C, choose **Configuration > Unified Communications > Configuration**.
  - Under **Jabber Guest**, click **Configure Jabber Guest servers**.
  - In the row for node A, click **View/Edit**, change the value for **Priority** to 1, and click **Save**.
  - In the row for node B, click **View/Edit**, change the value for **Priority** to 0, and click **Save**.
  - In the row for node C, click **View/Edit**, change the value for **Priority** to 2, and click **Save**.
- Step 8** Make sure that there are no calls on node B:
- On Cisco Expressway-C, choose **Configuration > Zones > Zones**.
  - In the row for node B, wait until the **Calls** column show 0 calls.
- Step 9** Upgrade node B by doing the following:
- Sign in to the server as root.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- b) Under the `/mnt` directory, create a new directory named `cdrom` to be used as the mount location for the CD/DVD drive:

```
mkdir /mnt/cdrom
```

- c) Mount the CD/DVD drive to `/mnt/cdrom`:

```
mount /dev/cdrom /mnt/cdrom
```

When the CD/DVD drive is mounted, the following message appears: `mount: block device /dev/sr0 is write-protected, mounting read only.`

- d) Change directory to `/mnt/cdrom`:

```
cd /mnt/cdrom
```

- e) Execute the upgrade script:

```
bash upgrade
```

When the upgrade is complete, the following message appears: The log file, for this upgrade, can be found in `/var/log/webcommon/upgrade.log`.

- Step 10** Prepare to upgrade node C by updating the reverse proxy so that call requests are sent to node A first, node B second, and no call requests are sent to node C:

- a) On Cisco Expressway-C, choose **Configuration > Unified Communications > Configuration**.
- b) Under **Jabber Guest**, click **Configure Jabber Guest servers**.
- c) In the row for node A, leave the priority set to 1.
- d) In the row for node B, click **View/Edit**, change the value for **Priority** to 2, and click **Save**.
- e) In the row for node C, click **View/Edit**, change the value for **Priority** to 0, and click **Save**.

- Step 11** Make sure that there are no calls on node C:

- a) On Cisco Expressway-C, choose **Configuration > Zones > Zones**.
- b) In the row for node C, wait until the **Calls** column show 0 calls.

- Step 12** Upgrade node C by repeating Step 9.

- Step 13** Verify that node B and node C are back up and running by signing in to Cisco Jabber Guest Administration as an administrator.

- a) Confirm that the Cisco Jabber Guest version number to which you upgraded appears at the bottom of the screen.
- b) Check to make sure that all users and links look correct.

- Step 14** Prepare to upgrade node A by updating the reverse proxy so that call requests are sent to node C first, node B second, and no call requests are sent to node A:

- a) On Cisco Expressway-C, choose **Configuration > Unified Communications > Configuration**.
- b) Under **Jabber Guest**, click **Configure Jabber Guest servers**.
- c) In the row for node A, click **View/Edit**, change the value for **Priority** to 0, and click **Save**.
- d) In the row for node B, leave the priority set to 2.
- e) In the row for node C, click **View/Edit**, change the value for **Priority** to 1, and click **Save**.

- Step 15** Wait until there are no calls on node A:

- a) On Cisco Expressway-C, choose **Configuration > Zones > Zones**.
- b) In the row for node C, wait until the **Calls** column show 0 calls.  
This may take a few minutes because this server handled all of the calls while the other two servers were upgraded.

- Step 16** Demote node A to a secondary server:

- a) Type `cluster stepdown`.
- b) Verify that either node B or node C has been promoted to primary server by typing `cluster status`.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

Make sure that the status of either node B or node C shows: ---> <IP address/hostname of node B or node C> PRIMARY.

**Step 17** Upgrade node A by repeating Step 9.

**Step 18** Verify that node A is back up and running by signing in to Cisco Jabber Guest Administration as an administrator.

The Cisco Jabber Guest version number to which you upgraded appears at the bottom of the screen.

**Step 19** Promote node A to the primary server:

- a) On the server that is currently the primary, type `cluster stepdown`.
- b) Check to see if node A was promoted to primary by typing `cluster status`.  
If node A is the primary, the status shows: ---> <IP address/hostname of node A> PRIMARY.
- c) If node A was not promoted to primary, repeat Step 12.a until node A is promoted to the primary server.

**Step 20** Update the order of the reverse proxy.

**Step 21** To ensure that the latest version of Cisco Jabber Guest Administration is loaded in your browser, refresh any browser instances that are signed in to Cisco Jabber Guest Administration or that have the Cisco Jabber Guest Administration sign-in page loaded.

## Remove Server from Cluster



**Important** After a server is removed from a cluster, it cannot be run as a standalone Cisco Jabber Guest instance. To do this, the server must be reinstalled.

In this procedure, we refer to the secondary server that we want to remove as *node A*, and to the other secondary server as *node B*.

### Procedure

**Step 1** Sign in to each server in the cluster as root.

**Step 2** On the primary server:

- a) Type `cluster remove <IP address/hostname of node A>`, and follow the on-screen prompts.
- b) Verify that node A is removed from the cluster by typing `cluster status`.  
Node A is removed from the list of servers.

**Step 3** On node A, block communication from node B by typing `cluster disallow <IP address/hostname of node B>`.

**Step 4** On node B, block communication with node A by typing `cluster disallow <IP address/hostname of node A>`.



**REVIEW DRAFT - CISCO CONFIDENTIAL**

# Configure Load Balancing

## Configure Round-Robin DNS Load Balancing

With round-robin DNS load balancing, a DNS server returns an ordered list of IP addresses associated with a single host name. With each new query on that host name, the DNS server rotates through the list. Multiple servers at different IP addresses take turns handling new requests to provide the same service.

For TURN traffic, an advantage of round-robin DNS load balancing is that it also provides redundancy. If a TURN server is down or unreachable, the client tries another server.

**Note**

The order of the IP address list returned for a DNS lookup is difficult to predict if the DNS server is under any kind of load directed at the host name. The important thing to expect is that calls to the host name go to different servers over time.

**Procedure**

- Step 1** Make sure that the DNS server has round-robin enabled.
- Step 2** Make sure that the FQDNs for the Cisco Expressway-C and Cisco Expressway-E clusters are configured on the DNS server to round-robin through the IP addresses of the server cluster.
- Step 3** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 4** Click **Settings**, and then click **Call Control and Media**.
- Step 5** To set up round-robin DNS for the SIP server:
  - a) For **SIP server**, enter the FQDN of the Cisco Expressway-C cluster.
  - b) Next to **Send SIP traffic to**, click **SIP server specified above**.
- Step 6** To set up round-robin DNS to request short-term TURN credentials from Cisco Expressway-C:
  - a) For **Expressway-C (IP address or DNS name)**, enter the FQDN of the Cisco Expressway-C cluster.
  - b) Next to **Request short-term TURN credentials from**, click **Expressway-C server specified above**.
- Step 7** To set up round-robin DNS for the TURN server: For **Expressway-E TURN server (IP address or DNS name)**, enter the FQDN of the Cisco Expressway-E cluster.  
Successive clients making TURN requests to that cluster FQDN are directed to different servers in the Cisco Expressway-E cluster; however, whether and how a particular client uses round-robin DNS for subsequent calls can be influenced by DNS caching.
- Step 8** Click **Update**.

Round-robin DNS takes effect if the Cisco Jabber Guest call URL that is used by a client browser to make a Cisco Jabber Guest call uses the FQDN for the Cisco Expressway-E cluster.

**What to Do Next**

To ensure that the number of new call requests does not exceed the capacity of the Cisco Expressway-C, make sure that you change the SIP call throttle limit.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Change the SIP Call Throttle Limit**

To ensure that the rate of new call requests (SIP INVITES) does not exceed the capacity of the Cisco Expressway-C, the Cisco Jabber Guest server implements a call throttling mechanism.

For a clustered Cisco Expressway-C deployment in which load balancing is achieved by round-robin DNS, we recommend that you change the SIP call throttle limit to 10 multiplied by the number of servers in the Cisco Expressway-C cluster to which Cisco Jabber Guest sends SIP. For example, if there are two servers in the Cisco Expressway-C cluster, set the SIP call throttle limit to 20.

If the rate of new calls exceeds the throttle limit, Cisco Jabber Guest delays a small amount of time before processing those calls that exceed the throttle limit. This throttling should not be noticed by users.

**Procedure**

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
  - Step 2** Click **Settings**, and then click **Advanced Settings**.
  - Step 3** In the **SIP call throttle limit (new calls/second)** box, type or select the throttle limit.
  - Step 4** Click **Update**.
- 

**Configure Round-Robin CSV Loading Balancing**

With round-robin CSV load balancing, a Cisco Jabber Guest server can be configured to make requests, in round-robin order, across individually specified servers by using a CSV list. After a server is used, the next server on the list is used, until the choice rotates to the beginning of the list and then repeats.

**Procedure**

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
  - Step 2** Click **Settings**, and then click **Call Control and Media**.
  - Step 3** To set up a CSV list for the SIP server:
    - a) For **SIP server**, enter a list of IP addresses or FQDNs for individual Cisco Expressway-C servers. The list of IP addresses or FQDNs must be separated by commas and must not contain spaces.
  - Step 4** To set up a CSV list to request short-term TURN credentials from Cisco Expressway-C:
    - a) For **Expressway-C (IP address or DNS name)**, enter a list of IP addresses or FQDNs for individual Cisco Expressway-C servers. The list of IP addresses or FQDNs must be separated by commas and must not contain spaces.

**Example:**

*expressway-c-1.somedomain.com,expressway-c-2.somedomain.com,expressway-c-3.somedomain.com*

- b) Next to **Send SIP traffic to**, click **SIP server specified above**.

**Example:**

*expressway-c-1.somedomain.com,expressway-c-2.somedomain.com,expressway-c-3.somedomain.com*

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- b) Next to **Request short-term TURN credentials from**, click **Expressway-C server specified above**.
- Step 5** To set up a CSV list for the TURN server: For **Expressway-E TURN server (IP address or DNS name)**, enter a list of FQDNs for individual Cisco Expressway-E servers. The list of FQDNs must be separated by commas and must not contain spaces.
- Example:**  
*expressway-e-1.somedomain.com,expressway-e-2.somedomain.com,expressway-e-3.somedomain.com*
- Step 6** Click **Update**.
- 

## Configure HTTP Load Balancing

Cisco Jabber Guest server can take advantage of HTTP load balancing from the Cisco Expressway-C by sending SIP and TURN credential requests to the Cisco Expressway-C that sent the HTTP.

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 2** Click **Settings**, and then click **Call Control and Media**.
- Step 3** To send SIP to the Cisco Expressway-C that sent the HTTP, next to **Send SIP traffic to**, click **Expressway-C server that proxied the HTTP request from Jabber Guest client**.
- Step 4** To send TURN credential requests to the Cisco Expressway-C that sent the HTTP, next to **Request short-term TURN credentials from**, click **Expressway-C server that proxied the HTTP request from Jabber Guest client**.
- Step 5** Click **Update**.
- 

## Configure Round-Robin TURN Port Range Load Balancing

You can configure Cisco Jabber Guest to take advantage of the load-balancing potential for TURN requests by using different TURN ports for each successive TURN request.

On a large Cisco Expressway-E deployment, up to six TURN request ports can be specified as a range. When used in combination with round-robin DNS or round-robin CSV for TURN servers, this multiplies the number of TURN request ports in use.

### Procedure

- 
- Step 1** Sign in to Cisco Jabber Guest Administration as an administrator.
- Step 2** Click **Settings**, and then click **Call Control and Media**.
- Step 3** For **TURN port**, enter a hyphenated range of port numbers that matches the range of TURN request ports configured on Cisco Expressway-E (under **Configuration > Traversal > TURN**).

***REVIEW DRAFT - CISCO CONFIDENTIAL*****Example:**

3478-3483

**Step 4** Click **Update**.



## Post-Install Configuration Changes

---

- [Change Virtual Machine Properties of a vCenter-hosted Server, page 55](#)
- [Change Virtual Machine Properties of an ESXi-hosted Server, page 55](#)

### Change Virtual Machine Properties of a vCenter-hosted Server

You can change the properties of a virtual machine, such as its IP address or hostname.

#### Procedure

---

- Step 1** In the Virtual Machine tab of vSphere, click the Configure virtual machine link.
  - Step 2** Click the **Options** tab.
  - Step 3** Under **vApp Options**, click **Properties**.
  - Step 4** Edit the properties, as required.
  - Step 5** Click **OK**.
  - Step 6** Turn on the virtual machine:
    - a) In the virtual machines and templates inventory tree, right-click the virtual machine.
    - b) Choose **Power > Power On**.
- 

### Change Virtual Machine Properties of an ESXi-hosted Server

You can change the properties of a virtual machine, such as its IP address or hostname.

***REVIEW DRAFT - CISCO CONFIDENTIAL*****Procedure**

- 
- Step 1** Sign in to the virtual machine directly from the virtual machine console or by using a Secure Shell client such as SSH.
- Step 2** Change directory to `/etc/jabberguest`:
- ```
cd /etc/jabberguest
```
- Step 3** Copy the file `network.config.sample` to a file named `network.config`:
- ```
cp network.config.sample network.config
```
- Step 4** Edit the properties in `network.config`, as required.
- ```
vi network.config
```
- Step 5** Restart the virtual machine:
- ```
shutdown -r now
```
-



## CHAPTER

# 7

## Troubleshoot

---

- [Locate chip.log File, page 57](#)
- [Locate chip.dmp File, page 58](#)
- [Reset Admin Password for Cisco Jabber Guest Administration, page 58](#)
- [Reset Root Password for Cisco Jabber Guest Server, page 58](#)
- [Audio and Video Issues, page 60](#)
- [Plug-in Crashes, page 61](#)
- [Error Messages, page 61](#)

## Locate chip.log File

If you are asked to send the `chip.log` file, use the following procedure.

### Procedure

---

**Step 1** Do one of the following:

- For Windows, navigate to `%HOMEPATH%\Appdata\LocalLow\Cisco\chip`.  
**Note** `%HOMEPATH%` is generally of the form `'C:\Users\username'`.
- For Mac OS X, navigate to `~/Library/"Internet Plug-Ins"/"Cisco Jabber Guest Plug-in.version-number.plugin"/Contents/Frameworks/Logs`.
- For Chrome on Mac OS X, navigate to `~/Applications/"Cisco Jabber Guest Add-on.version-number"/Contents/Frameworks/Logs`

**Step 2** Compress the file and email it back to the requester.

---

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## Locate chip.dmp File

If your plug-in crashes, a dump file called `chip.dmp` is created. Currently, this file is created only for plug-in crashes on Microsoft Windows. If you are asked to send the `chip.dmp` file, follow this procedure.

### Procedure

---

**Step 1** Navigate to `%HOMEPATH%\Appdata\LocalLow\Cisco\chip`.

**Note** `%HOMEPATH%` is generally of the form  
`'C:\Users\username'`.

**Step 2** Compress the file and email it back to the requester.

---

## Reset Admin Password for Cisco Jabber Guest Administration

### Procedure

---

**Step 1** Sign in to the Cisco Jabber Guest server as root.

**Step 2** Change directory to `/opt/cisco/webcommon/scripts`:  
`cd /opt/cisco/webcommon/scripts`

**Step 3** Enter the following command:  
`python mongo_admin_reset.py`  
The password is reset to its default value: `jabbercserver`.

---

## Reset Root Password for Cisco Jabber Guest Server

### Procedure

---

**Step 1** Open a console session for the Cisco Jabber Guest server and restart the server.

**Step 2** Press any key to interrupt the start process.

**Step 3** Press `e` to edit.

**Step 4** From the entries, select **kernel** and press `e` to edit.



**REVIEW DRAFT - CISCO CONFIDENTIAL**

```
GNU GRUB version 0.97 (632K lower / 3140608K upper memory)

root (hd0,0)
kernel /vmlinuz-2.6.32-220.el6.x86_64 ro root=/dev/mapper/vg_kitllcbu-
initrd /initramfs-2.6.32-220.el6.x86_64.img

Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
```

- Step 5** Start the server in single-user mode:
- Add the word **single** to the end of the line.
  - Press the Enter key.

```
[ Minimal BASH-like line editing is supported. For the first word, TAB
lists possible command completions. Anywhere else TAB lists the possible
completions of a device/filename. ESC at any time cancels. ENTER
at any time accepts your changes.]

<ABEL=79d3d2d4 single
```

- Step 6** Press b to start the server.  
The Cisco Jabber Guest server starts in single-user mode.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

```

eth0: registered as PCnet/PCI II 79C978A
pcnet32: 1 cards found.
parport_pc 00:00: reported by Plug and Play ACPI
parport0: PC-style at 0x378, irq 7 [PCSP,TRISTATE]
ppdev: user-space parallel port driver

Setting hostname localhost.localdomain: [ OK ]
Checking filesystems [ OK ]
Remounting root filesystem in read-write mode: [ OK ]
mount: according to mtab, /dev/sda1 is already mounted on /

Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
Welcome to CentOS
Starting udev: [ OK ]
Setting hostname localhost.localdomain: [ OK ]
Checking filesystems [ OK ]
Remounting root filesystem in read-write mode: [ OK ]
mount: according to mtab, /dev/sda1 is already mounted on /

Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
[root@localhost ~]# _

```

**Step 7** Enter **passwd root**, and then enter a new password.

**Step 8** Restart the server.

## Audio and Video Issues

### One-Way Video When Using VPN

**Problem** Callers experience one-way video when using Cisco Jabber Guest over VPN.

**Possible Cause** The default Maximum Transmission Unit (MTU) on Cisco Expressway-E is too high and can cause packet loss.

**Solution** Change the MTU.

#### Related Topics

[Change MTU Size, on page 36](#)

### No Audio or Video on Single NIC Deployment

**Problem** No audio or video on single NIC deployment; media is terminating on the Cisco Expressway-E

**Possible Cause** On the Cisco Expressway-C, for the zone to the Cisco Jabber Guest server, **Media encryption mode** is not set to **Best effort**.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

**Solution** Set **Media encryption mode** to **Best effort**. *Best effort* forces media from the Cisco Expressway-E to terminate on the Cisco Expressway-C.

## Plug-in Crashes

**Problem** The plug-in crashes.

**Possible Cause** The video drivers may not be current.

**Solution** Make sure that the video drivers are up to date on the system.

## Error Messages

**Table 19: Error Messages**

| Location                                                                              | Error Message                                                                                                                                                                                                                                                                             | What It Means                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Jabber Guest webcommon logs                                                     | "IOException closing sock<br>javax.net.ssl.SSLHandshakeException:<br>General SSLEngine problem"<br>appears In the Cisco Jabber Guest<br>webcommon-tomcat.log file.                                                                                                                        | When one of these messages appears, it may indicate a problem with the Expressway certificate that is uploaded to Cisco Jabber Guest Administration.<br><br>Verify that the Expressway certificate that is uploaded to Cisco Jabber Guest Administration is either an Expressway certificate or the CA certificate that signed it:                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Cisco Expressway Event Log                                                            | tves: Event="Outbound TLS<br>Negotiation Error" Service="SIP"<br>Src-ip="<ip address>"<br>Src-port="27510" Dst-ip="<ip<br>address>" Dst-port="5061"<br>Detail="No SSL error available,<br>probably remote disconnect"<br>Protocol="TLS" Level="1"<br>UTCTime="yyyy-mm-dd<br>hh:mm:ss,732" | <ol style="list-style-type: none"> <li>1 Check the common name (CN) of the issuer and the subject of the certificate that is uploaded to Expressway: <ol style="list-style-type: none"> <li>1 On the Expressway, choose <b>Maintenance &gt; Security certificates &gt; Server certificate</b>.</li> <li>2 Click <b>Show (decoded)</b>.</li> </ol> </li> <li>2 Check the CN of the issuer and the subject of the certificate that is uploaded to Cisco Jabber Guest Administration: <ol style="list-style-type: none"> <li>1 Sign in to Cisco Jabber Guest Administration.</li> <li>2 Click <b>Settings</b>, and then click <b>Secure SIP Trust Certificate</b>.</li> </ol> </li> <li>3 Make sure that Tomcat was restarted:<br/>service tomcat-as-standalone.sh<br/>restart</li> </ol> |
| On Cisco Expressway, status of zone for Cisco Jabber Guest server shows <i>Failed</i> | SIP: Failed to connect to <IP<br>address>:5061 : TLS negotiation<br>failure                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**REVIEW DRAFT - CISCO CONFIDENTIAL**

| Location                  | Error Message                      | What It Means                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Jabber Guest client | Failed to acquire TURN credentials | <p>This message may mean that the call control and media settings for Cisco Expressway-C may not be configured correctly. Check the settings:</p> <ol style="list-style-type: none"> <li>1 Sign in to Cisco Jabber Guest Administration as an administrator.</li> <li>2 Click <b>Settings</b>, and then click <b>Call Control and Media</b>.</li> <li>3 Under Cisco Expressway-C, if <b>Request short-term TURN credentials from</b> is set to <b>Expressway-C server specified above</b>, make sure that the value in the <b>Expressway-C (IP address or DNS name)</b> field is correct.</li> <li>4 Check the value in the <b>HTTP port</b> field. The default value is 443.</li> <li>5 Check the values in the Cisco Expressway-C administrator <b>Username</b> and <b>Password</b> fields: <ul style="list-style-type: none"> <li>• The administrator account is created on the Cisco Expressway-C (<b>Users &gt; Administrator accounts</b>).</li> <li>• The Cisco Expressway-C administrator must have read-write and API access.</li> </ul> </li> </ol> |
| Cisco Jabber Guest client | Link Not Found                     | <p>Make sure that the link is active: Click <b>Links</b>, click the link, and check the <b>State</b> settings to make sure that the link has not expired.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Cisco Jabber Guest client | Link not valid                     | <p>This message may mean that the link that has not yet been replicated to the Cisco Jabber Guest server that handles the request.</p> <p>When you create a click-to-call link on a Cisco Jabber Guest server that is a member of a cluster, you must allow a small amount of time before that link is active on all servers in the cluster.</p> <p>If you deploy an application that creates links dynamically by using the link API and pushes them to the Cisco Jabber Guest client, we recommend that you factor this replication delay into your design.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## REVIEW DRAFT - CISCO CONFIDENTIAL

| Location                  | Error Message                                                                                           | What It Means                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Jabber Guest client | Missing SDP. There was a networking error between your device and the server.                           | This message may mean that Cisco Jabber Guest is unable to contact the TURN server. One possible cause is that multiple network interfaces are enabled, including SW VPN. Another possible cause is that a firewall or NAT blocking UDP port 3478 between the client and the Cisco Expressway-E (publicly accessible IP). Some home routers block all UDP.                                                                                                                                                                               |
| Cisco Jabber Guest client | Not found on Accelerator                                                                                | <p>You may see this message because the link between the Cisco Expressway-C and Cisco Expressway-E is down and domain information hasn't replicated from the Cisco Expressway-C to Cisco Expressway-E.</p> <p>On Cisco Expressway-E, when viewing Unified Communications status (choose <b>Status</b> &gt; <b>Unified Communications</b> and click <b>View ssh tunnel status</b>), make sure that:</p> <ul style="list-style-type: none"> <li>• The Cisco Jabber Guest domain is listed.</li> <li>• The SSH tunnel is active.</li> </ul> |
| Cisco Jabber Guest client | Server error: class java.lang.IllegalStateException: Error creating sipServletRequest<br>ROAP_EXCEPTION | <p>Apache Tomcat may not be running, perhaps after an upgrade or server interruption.</p> <p>Restart Tomcat on the Cisco Jabber Guest Server: <code>service tomcat-as-standalone.sh restart.</code></p>                                                                                                                                                                                                                                                                                                                                  |
| Cisco Jabber Guest client | SIP Error. The destination associated with this link is not reachable.                                  | <p>You may see this message for one of the following reasons:</p> <ul style="list-style-type: none"> <li>• The directory number (DN) embedded in the link or associated with the link, does not exist on the Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server.</li> <li>• The link contains a URI (<i>user@domain.com</i>) but the Cisco Unified Communications Manager is not configured to route calls by URI. Use a DN instead.</li> </ul>                                                       |

**REVIEW DRAFT - CISCO CONFIDENTIAL**

| Location                  | Error Message                                                                                                                                                                                              | What It Means                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Jabber Guest client | TURN Error. Your call attempt has failed due to incompatibility with your home or company security infrastructure. Please contact your network administrator or check your home network security settings. | <p>This message indicates that the web client could not allocate the TURN relay on the TURN server. This could occur for one of the following reasons:</p> <ul style="list-style-type: none"> <li>• UDP port 3478 is blocked. You must allow this port inbound from the public Internet to the Cisco Expressway-E.</li> <li>• The DNS record for the TURN server is not resolvable (must be a DNS A-record).</li> <li>• The <b>Expressway-E TURN Server (IP Address or DNS Name)</b> field and <b>Turn Port</b> fields are not configured correctly in Cisco Jabber Guest Administration (<b>Settings &gt; Call Control and Media</b>).</li> <li>• The <b>Domain</b> name (<b>Settings &gt; Call Control and Media</b>, under <b>Cisco Expressway-C</b>) is not a configured domain name on Cisco Expressway-C or is not configured for Cisco Jabber Guest services.</li> </ul> |

**Related Topics**

[Set Up TURN Server Information, on page 40](#)

[Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment, on page 31](#)

[Configure TURN Credential Provisioning, on page 39](#)



## CHAPTER

# 8

## Documentation Reference

---

- [Cisco Unified Communications Manager](#), page 65
- [Cisco TelePresence Video Communication Server](#), page 65

### Cisco Unified Communications Manager

- Documentation Home  
[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)
- *Documentation Guide for Cisco Unified Communications Manager, Release 8.6(2a)*  
[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/docguide/8\\_6\\_2/dg862a.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/8_6_2/dg862a.html)
- *Documentation Guide for Cisco Unified Communications Manager, Release 9.1(1)*  
[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/docguide/9\\_1\\_1/CUCM\\_BK\\_CBABE0BB\\_00\\_cucm-documentation-guide-91.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/docguide/9_1_1/CUCM_BK_CBABE0BB_00_cucm-documentation-guide-91.html)
- *Documentation Guide for Cisco Unified Communications Manager, Release 10.5(1)*  
[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/docguide/10\\_5\\_1/CUCM\\_BK\\_C2CFB1F8\\_00\\_cucm-documentation-guide-1051.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/10_5_1/CUCM_BK_C2CFB1F8_00_cucm-documentation-guide-1051.html)

### Cisco TelePresence Video Communication Server

- Documentation Home  
[http://www.cisco.com/en/US/products/ps11337/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11337/tsd_products_support_series_home.html)
- *Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide*  
<http://www.cisco.com/c/en/us/support/unified-communications/expressway/model.html>
- *Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide*

***REVIEW DRAFT - CISCO CONFIDENTIAL***

[http://www.cisco.com/c/en/us/support/unified-communications/  
telepresence-video-communication-server-expressway/model.html](http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-expressway/model.html)