



REVIEW DRAFT - CISCO CONFIDENTIAL



Cisco Jabber Guest 10.6 Administration Guide

First Published: January 27, 2015

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

Get Started 1

Sign In to Cisco Jabber Guest Administration 1

Sign In to Cisco Jabber Guest Server CLI 2

Set Links for Mobile Users 2

CHAPTER 2

Manage Users 3

About Users 3

Create User 4

Update User 4

Set User Password 5

Unlock User Account 5

Delete User 6

CHAPTER 3

Manage Call Links 7

About Call Links 7

Best Practices for Creating Links 8

Maximum Number of Call Links 8

Create Link 8

Request Path Cannot Be Changed After Link is Created 9

Set Default Display Name for Links 9

Set Default Caller ID for Links 10

Set Your Links to Automatically Delete 10

Set Up Ad Hoc Links for Video Conference Bridges 10

CHAPTER 4

Perform Routine Maintenance 13

Change Password Policies 13

Download Logs 14

Monitor Product Use 14

REVIEW DRAFT - CISCO CONFIDENTIAL

- [View Plug-in Download Count 14](#)
- [View Current Call Session Count 14](#)
- [View Call Session Usage Log 15](#)

CHAPTER 5**Backup and Restore System 17**

- [Disaster Backup and Recovery 17](#)
 - [Save the MAC Address of Each Virtual Machine 17](#)
 - [Export a Virtual Machine to an OVA 18](#)
 - [Restore a Backed Up OVA After a Disaster 19](#)
 - [Update the MAC Address of Each Virtual Machine 19](#)
- [Short-Term Backup and Recovery 20](#)
 - [Back Up Data Short-Term 20](#)
 - [Restore Data from an Earlier Time 21](#)

CHAPTER 6**Troubleshoot 23**

- [Locate chip.log File 23](#)
- [Locate chip.dmp File 23](#)
- [Reset Admin Password for Cisco Jabber Guest Administration 24](#)
- [Reset Root Password for Cisco Jabber Guest Server 24](#)

CHAPTER 7**Reference 27**

- [Call Link Format 27](#)
- [Mapping Between Link Fields and SIP Headers 28](#)



Get Started

- [Sign In to Cisco Jabber Guest Administration, page 1](#)
- [Sign In to Cisco Jabber Guest Server CLI, page 2](#)
- [Set Links for Mobile Users, page 2](#)

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
- 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.

REVIEW DRAFT - CISCO CONFIDENTIAL

The first time that you sign in you must change your password.

Step 4 Enter a new password.

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.

Set Links for Mobile Users

Use the settings on the **Mobile** page for iOS support.

Procedure

Step 1 From Cisco Jabber Guest Administration, choose **Settings > Mobile**.

Step 2 For **iOS App Store link**, enter the URL to the application in the iOS App Store.

Step 3 For **iOS URL scheme**, enter the URL scheme for the iOS application.

Step 4 For **Redirect URL for iOS**, enter the URL that you want the server to redirect iOS users to when they click a call link. The server can redirect users to another domain.

Step 5 Click **Update**.



Manage Users

- [About Users, page 3](#)
- [Create User, page 4](#)
- [Update User, page 4](#)
- [Set User Password, page 5](#)
- [Unlock User Account, page 5](#)
- [Delete User, page 6](#)

About Users

Think of users as accounts that you can use as organizational units for links. There is no association between a user and a link at which they can be reached.

All users are administrators.

REVIEW DRAFT - CISCO CONFIDENTIAL

Create User

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Users**.
 - Step 2** Click **New**.
 - Step 3** For **Alias**, enter the appropriate user name. User aliases must be unique across all users.
 - Step 4** For **First name**, enter the given name of the user.
 - Step 5** For **Last name**, enter the surname of the user.
 - Step 6** For **Display name**, enter the publicly displayed name of the user.
 - Step 7** For **Password**, enter a default password for the user.
 - Step 8** For **Confirm password**, confirm the password.
 - Step 9** Click **Create**.
-

Update User

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Users**.
 - Step 2** Click the user name of the user that you want to update.
 - Step 3** For a new user, enter the information in the appropriate fields, and then click **Update**.
 - Step 4** For an existing user, update the appropriate fields, and then click **Update**.
 - Step 5** To remove the user from the database, click **Delete**.
-

REVIEW DRAFT - CISCO CONFIDENTIAL

Set User Password

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Users**.
 - Step 2** Click the user name of the user for whom you want to set a password.
 - Step 3** Click **Password**.
 - Step 4** Check **Must change**.
 - Step 5** Enter a default password for the user.
 - Step 6** Confirm the password.
 - Step 7** Click **Update**.
-

Unlock User Account

Complete this task to unlock a locked account, or provide users with a temporary password.

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Users**.
 - Step 2** Click the user name of the user whose password you want to unlock.
 - Step 3** Click **Password**.
 - Step 4** Click **Unlock**.
 - Step 5** If the user has forgotten his or her password, do the following:
 - a) Check **Must change**.
 - b) Enter a temporary password for the user.
 - c) Confirm the password.
 - d) Click **Update**.
 - e) Provide the user with the temporary password.
-

REVIEW DRAFT - CISCO CONFIDENTIAL

Delete User

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Users**.
- Step 2** Click the user name of the user to delete. You can search for a specific user.
- Step 3** At the bottom of the **Details** page, click **Delete**.
-



Manage Call Links

- [About Call Links, page 7](#)
- [Best Practices for Creating Links, page 8](#)
- [Maximum Number of Call Links, page 8](#)
- [Create Link, page 8](#)
- [Request Path Cannot Be Changed After Link is Created, page 9](#)
- [Set Default Display Name for Links, page 9](#)
- [Set Default Caller ID for Links, page 10](#)
- [Set Your Links to Automatically Delete, page 10](#)
- [Set Up Ad Hoc Links for Video Conference Bridges, page 10](#)

About Call Links

Call links are classified either as in database or ad hoc. When a call link is clicked, the Cisco Jabber Guest web client opens and checks if the link exists in the database. If the link exists in the database, the following operational parameters for the call are taken from the database:

- Destination endpoint
- Caller ID
- Called ID
- Time

If the link is not listed in the database, the server checks the **Allow ad hoc links** setting (in Cisco Jabber Guest Administration > **Settings** > **Links**). If ad hoc links are enabled, the server sends the call to Cisco Expressway or Cisco Unified Communications Manager using the string to the right of `/call/` as the route string. If **Allow ad hoc links** is disabled, the call is not routed unless the link exists in the database.

Calls can be made to any Cisco Unified Communications Manager endpoint by dialing the directory number (DN). Calls also can be placed using a URI if URI dialing has been enabled.

REVIEW DRAFT - CISCO CONFIDENTIAL

Best Practices for Creating Links

Allow Time for Links to Replicate

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. This applies whether you create the link by using Cisco Jabber Guest Administration or the link API. In both cases, the link information replicates automatically to all other servers in the cluster. The amount of time required for replication varies depending on factors such as the network connection speed between the servers. Complete replication can occur within a second or may take several seconds.

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. If a Cisco Jabber Guest user attempts to use a link that has not yet been replicated to the Cisco Jabber Guest server that handles the request, the attempt will fail.

Maximum Number of Call Links

There is no hard limit on the number of links that you can create on a Cisco Jabber Guest single server or cluster. We have tested with upwards of 25,000 links.

Create Link

Want to specify a time and date in which a link is active? For example, if your company is hiring, you can create a link that a candidate uses to call for an interview. You can specify that the link is active between 2:00 p.m. and 4:00 p.m. on the day of the interview.

Procedure

Step 1 From Cisco Jabber Guest Administration, click **Links**.

Step 2 Click **New**.

Step 3 Set the request path, which is the part of the link after `/call`. The request path must be unique:

- If you want the domain name or DN to appear, click the **Destination** drop-down arrow, and choose **Destination**.
- If you want a custom string to appear, click the **Destination** drop-down arrow, choose **Custom string**, and enter the string in the **Request path** field.
- If you want a random string to appear, click the **Destination** drop-down arrow, and choose **Random string**.

For more information, see [Call Link Format](#), on page 27.

Step 4 For **Destination**, do one of the following:

- Enter the DN or URI and domain name of the person who you want to call. For example, `1000@cisco.com` or `johndoe@cisco.com`.

REVIEW DRAFT - CISCO CONFIDENTIAL

- Enter the DN of the person who you want to call. For example, *1000*. The Cisco Jabber Guest server will populate the domain name by using the value in the **SIP domain** field (in **Settings > Call Control and Media**).

Important The destination must resolve to a DN or URI that is routable from Cisco Expressway-C and Cisco Unified Communications Manager.

- Step 5** For **Display name**, enter the name to display on the client when a call is placed using this link. For example, if the link calls a help desk, enter Customer Support.
You can set a default display name for all links.
- Step 6** For **Caller name**, enter the name to display on the destination endpoint in the enterprise. For example, if the link calls a physician's hotline, enter MD Hotline caller. If you do not enter a value, the caller name is *Jabber Guest*.
- Step 7** For **Caller SIP alias**, enter the caller ID that you want to display on the destination endpoint in the enterprise. If you do not enter a value, the caller ID is the value in the **Default caller SIP alias** field.
The caller ID can only contain the following characters: A–Z, a–z, 0–9, hyphen (-), underscore (_), period (.), and plus sign (+).
- Step 8** If the link calls a video conference bridge that requires a unique caller name, check **Append unique identifier to SIP alias**. A unique number is appended to the SIP alias. Each time the link is clicked, the number increments.
- Step 9** For **State**, choose when the link is active.
- Step 10** Click **Create**.

What to Do Next

If you chose start and end dates for any of the links that you created, you can [Set Your Links to Automatically Delete, on page 10](#)

Related Topics

[Set Default Display Name for Links, on page 9](#)

[Mapping Between Link Fields and SIP Headers, on page 28](#)

Request Path Cannot Be Changed After Link is Created

You cannot change the request path of a link after the link is created. For example, if the request path of a link reflects the link destination and the link destination changes, you must create a new link. You cannot update the request path to reflect the updated destination.

Set Default Display Name for Links

Complete this task to set a default display name for all links, including ad hoc links.

REVIEW DRAFT - CISCO CONFIDENTIAL**Procedure**

-
- Step 1** From Cisco Jabber Guest Administration, choose **Settings > Links**.
- Step 2** For **Default display name**, enter the name to display on the client when calls are placed. If a **Display name** is set for an individual link, that name overrides the **Default display name**.
- Step 3** Click **Update**.
-

Set Default Caller ID for Links

Complete this task to set a default caller ID for all links, including ad hoc links.

Procedure

-
- Step 1** From Cisco Jabber Guest Administration, choose **Settings > Links**.
- Step 2** For **Default caller SIP alias**, enter the caller ID that you want to display on the destination endpoint. If a **Caller SIP alias** is set for an individual link, that value overrides the **Default caller SIP alias**.
The caller ID can only contain the following characters: A–Z, a–z, 0–9, hyphen (-), underscore (_), period (.), and plus sign (+).
- Step 3** Click **Update**.
-

Set Your Links to Automatically Delete

If you chose start and end dates for any of the links that you created, you can choose to automatically delete these links after the end date passes.

Procedure

-
- Step 1** From Cisco Jabber Guest Administration, choose **Settings > Links**.
- Step 2** For **Expired links deleted after *n* days**, choose how many days after the end date passes that you want to delete the links.
If you do not enter a value or if you enter a value of 0, expired links are kept in the database indefinitely.
-

Set Up Ad Hoc Links for Video Conference Bridges

A unique caller name is required to allow Cisco Jabber Guest callers into some video conference bridges. Complete this task to append a unique identifier to ad hoc links.

REVIEW DRAFT - CISCO CONFIDENTIAL**Procedure**

- Step 1** From Cisco Jabber Guest Administration, choose **Settings > Links**.
- Step 2** Check **Append unique identifier to SIP alias for ad-hoc links**.
A unique number is appended to the SIP alias. Each time the link is clicked, the number increments.
- Step 3** Click **Update**.
-

REVIEW DRAFT - CISCO CONFIDENTIAL



CHAPTER

4

Perform Routine Maintenance

- [Change Password Policies, page 13](#)
- [Download Logs, page 14](#)
- [Monitor Product Use, page 14](#)

Change Password Policies

Procedure

- Step 1** From Cisco Jabber Guest Administration, choose **Services > Passwords**.
- Step 2** Check **Complexity check** if you want passwords to meet the following requirements:
- Passwords must be eight or more characters in length.
 - Passwords must include three of the following characters:
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one number
 - At least one symbol
- Step 3** For **History size**, enter the number of passwords that are remembered.
For example, if you enter 3, the user's previous three passwords are remembered. If a user tries to change the password and reuses one of the previous three passwords, the user is prompted to specify a different password.
- Step 4** For **Maximum failed sign ins**, enter the number of sign in attempts allowed before the user account is locked.
- Step 5** Click **Update**.
-

Related Topics

[Unlock User Account, on page 5](#)

REVIEW DRAFT - CISCO CONFIDENTIAL

Download Logs

Complete this task to download log files as a zip archive for troubleshooting or maintenance.

Procedure

Step 1 From Cisco Jabber Guest Administration, click **Logs**.

Step 2 Do one of the following:

- To download all of the log files on the system, click **Download All**. A zip file named `diagnosticFiles_YYYY-mm-dd_hh-mm-ss.zip` downloads.
 - To download a specific log:
 - 1 Click the log file.
 - 2 Click **Download Current Log**.
-

Monitor Product Use

You can monitor product use in several ways.

View Plug-in Download Count

Complete this task to view the number of unique (per device) browser plug-ins that have been downloaded since Cisco Jabber Guest was installed.

Procedure

Step 1 From Cisco Jabber Guest Administration, click **Reports**.

Step 2 Click **Session Activity**.

The count does not update in real time. You must refresh the page to view a real-time count.

View Current Call Session Count

Complete this task to view the number of current active call sessions. This number includes all users who have clicked a link but have not yet clicked **Call**.

REVIEW DRAFT - CISCO CONFIDENTIAL

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Reports**.
- Step 2** Click **Session Activity**.
The count does not update in real time. You must refresh the page to view a real-time count.
-

View Call Session Usage Log

Complete this task to help you determine the capacity that is required for your deployment. Usage logs show the number of call sessions that were active each minute in a day.

Procedure

- Step 1** From Cisco Jabber Guest Administration, click **Logs**.
- Step 2** Do one of the following:
- To view all of the daily usage logs on the system:
 - 1 Click **Download**. A zip file named `diagnosticFiles_YYYY-mm-dd_hh-mm-ss.zip` downloads.
 - 2 Open the zip file. Each daily usage log file is named `usage.log-YYYYmmdd`.
 - To view the usage log for today:
 - 1 Click **Jabber Guest Usage CSV**.
 - 2 Click **Download**. A file named `usage.log` downloads.
- Step 3** Open the usage log with an application that can open CSV-format files, such as Microsoft Excel or Notepad ++.
- The data appears in the format: *mm/dd/yyyy hh:mm:ss, number of active call sessions*.
-

REVIEW DRAFT - CISCO CONFIDENTIAL



Backup and Restore System

- [Disaster Backup and Recovery, page 17](#)
- [Short-Term Backup and Recovery, page 20](#)

Disaster Backup and Recovery

To minimize the effects of a disaster, you must create a disaster recovery plan to minimize downtime and data loss. You can achieve this by using a VMware-supported disaster backup and recovery solution or you can export the OVA files as described in this section.

The following provides an overview of the steps required to back up and recover one, two, or all three servers in your cluster by exporting the OVA files:

- 1 Record the media access control (MAC) address of each virtual machine in the cluster. Make sure that you save the addresses in both an on-site and off-site location.
- 2 Back up each virtual machine in the cluster by exporting its OVA. Make sure that you store the exported OVAs in an off-site location.
- 3 If a disaster occurs, restore one, two, or all three virtual machines that you have lost by deploying the exported OVAs.
- 4 Before you turn on each restored virtual machine, update its MAC address.

Save the MAC Address of Each Virtual Machine

As part of your disaster backup and recovery plan, make sure that you record the MAC address of each virtual machine in the cluster. When you restore a backed up OVA, you must update the MAC address before you turn on the machine.

REVIEW DRAFT - CISCO CONFIDENTIAL**Procedure**

- Step 1** Open vSphere Client.
 - Step 2** Right-click the virtual machine and click **Edit Settings**.
 - Step 3** On the **Hardware** tab, select **Network adapter 1** or the equivalent.
 - Step 4** Record the value that is in the **MAC Address** field.
 - Step 5** Save the address in both an on-site and off-site location.
 - Step 6** Click **Cancel**.
 - Step 7** Repeat Steps 2 through 6 for each virtual machine in the cluster.
-

Export a Virtual Machine to an OVA

Make sure that you are prepared to recover from a disaster. On a regular basis, back up each virtual machine in the cluster by exporting its OVA.

Procedure

- Step 1** Open vSphere Client.
 - Step 2** Turn off the virtual machine:
 - a) In the virtual machines and templates inventory tree, right-click the virtual machine.
 - b) Choose **Power > Power Off**.
 - Step 3** Make sure that the virtual machine is selected and choose **File > Export > Export OVF Template**.
 - Step 4** Enter a meaningful name for the file.
 - Step 5** Choose a directory in which to save the file.
 - Step 6** From the **Format** drop-down list, select **Single file (OVA)**.
 - Step 7** Enter a meaningful description for the file.
Add a date, version, and reason for export to help you determine which file to restore later.
 - Step 8** Click **OK**.
 - Step 9** Repeat Steps 2 through 8 for each virtual machine in the cluster.
 - Step 10** Store the OVAs in an off-site location.
-

REVIEW DRAFT - CISCO CONFIDENTIAL

Restore a Backed Up OVA After a Disaster

Procedure

-
- Step 1** In vSphere Client, verify that the virtual machine involved in the disaster does not appear in the virtual machines and templates inventory tree.
- Step 2** If the virtual machine appears in the virtual machines and templates inventory tree, turn off and delete this virtual machine:
- a) Right-click the virtual machine.
 - b) Choose **Power > Power Off**.
 - c) Right-click the virtual machine and click **Delete from Disk**.
- Step 3** In the virtual machines and templates inventory tree, select the location where you want to deploy the backed up OVA.
- Step 4** Choose **File > Deploy OVF Template**.
- Step 5** In the **Source** screen, browse to the location of the OVA, and then click **Next**.
- Step 6** Verify the details in the **OVF Template Details** screen, and then click **Next**.
- Step 7** In the **Name and Location** screen, enter a name for the template, select its location, and then click **Next**.
- Step 8** In the **Host / Cluster** screen, select where you want to run the template, and then click **Next**.
- Step 9** In the **Storage** screen, select where you want to store the virtual machine files, and then click **Next**.
- Step 10** In the **Disk Format** screen, select the format in which you want to store the virtual disks, and then click **Next**.
- Step 11** In the **Networking Mapping** screen, select the appropriate Destination Networks for OVA deployment, and then click **Next**.
- Step 12** In the **Properties** screen, enter the properties that are appropriate for your network, and then click **Next**.
- Step 13** On the **Ready to Complete** screen, make sure that **Power on after deployment** check box is unchecked.
- Important** Before you turn on the virtual machine, you must update its MAC address.
- Step 14** Click **Finish**.
- Step 15** Repeat Steps 1 through 14 for each virtual machine in the cluster that you need to restore.
-

Related Topics

[Update the MAC Address of Each Virtual Machine, on page 19](#)

Update the MAC Address of Each Virtual Machine

After you restore a backed up OVA, you must update the MAC address before you turn on the virtual machine.

REVIEW DRAFT - CISCO CONFIDENTIAL**Procedure**

-
- Step 1** Open vSphere Client.
- Step 2** Right-click the restored virtual machine and click **Edit Settings**.
- Step 3** On the **Hardware** tab, select **Network adapter 1** or the equivalent.
- Step 4** Under the **MAC Address** field, select **Manual**.
- Step 5** In the **MAC Address** field, enter the MAC address of the virtual machine that you recorded as part of your disaster backup and recovery plan.
- Step 6** Click **OK**.
- Step 7** Restart the virtual machine:
- In the virtual machines and templates inventory tree, right-click the virtual machine.
 - Choose **Power** > **Restart Guest**.
- Step 8** Repeat Steps 2 through 7 for each virtual machine in the cluster that you need to restore.
- Step 9** If you restored only one or two servers in the cluster, you must restart Tomcat on the server that was always up and running:
- ```
service tomcat-as-standalone.sh restart
```
- Step 10** If you restored all three servers in the cluster, after each of the restored virtual machines have been restarted, restart all three virtual machines in the cluster.
- 

## Short-Term Backup and Recovery

### Back Up Data Short-Term

We recommend that you regularly back up your data by taking snapshots. These short-term backups allow you to recover data from an earlier time.

A backup captures the entire state of the virtual machine at the time you create the backup. You can back up a virtual machine when the machine is powered on, powered off, or suspended.




---

**Important** Make sure that you back up your server cluster before you upgrade.

---

**Procedure**

- 
- Step 1** Open vSphere Client.
- Step 2** In the virtual machines and templates inventory tree, right-click the virtual machine, and then choose **Snapshot** > **Take Snapshot**.
- Step 3** Type a meaningful name for the snapshot.
- Step 4** Type a meaningful description for the snapshot.



**REVIEW DRAFT - CISCO CONFIDENTIAL**

**Important** Adding a date and time or a description can help you determine which snapshot to restore.

- Step 5** Select whether the snapshot includes the virtual machine's memory. If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot:

**Table 1: Virtual Machine State**

| Virtual Machine State When Parent Snapshot Is Taken | Virtual Machine State After Restoration                                            |
|-----------------------------------------------------|------------------------------------------------------------------------------------|
| Powered on (includes memory)                        | Reverts to the parent snapshot, and the virtual machine is powered on and running. |
| Powered on (does not include memory)                | Reverts to the parent snapshot and the virtual machine is powered off.             |
| Powered off (does not include memory)               | Reverts to the parent snapshot and the virtual machine is powered off.             |

- Step 6** Click **OK**.  
It will take a few minutes to take the snapshot. When the snapshot has been created, in the **Recent Tasks** list, the **Create virtual machine snapshot** task status shows **Completed**.
- Step 7** Repeat Steps 2 through 6 to back up the other virtual machines in the cluster.

## Restore Data from an Earlier Time

You can restore snapshots in the following ways:

- **Revert to Current Snapshot**—Restores the most recent snapshot, the parent snapshot.
- **Go to**—Lets you restore any snapshot in the snapshot tree and makes that snapshot the parent snapshot of the current state of the virtual machine.

Restoring snapshots has the following effects:

- The current disk and memory states are discarded, and the virtual machine reverts to the disk and memory states of the snapshot that you restore. Any users or links that are not captured in the snapshot are discarded.
- Existing snapshots are not removed. You can restore those snapshots at any time.
- If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot.



**Important** Mixed version clusters are not supported outside of an upgrade or revert maintenance window.

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

---

- Step 1** Open vSphere Client.
- Step 2** Make sure that you have backed up each virtual machine in the cluster.
- Step 3** Shut down each virtual machine in the cluster:
- In the virtual machines and templates inventory tree, select the virtual machine.
  - On the **Getting Started** tab, click **Shut down the virtual machine**.
- Step 4** In the virtual machines and templates inventory tree, right-click the virtual machine, and then point to **Snapshot**.
- Step 5** Restore the snapshot:
- If you want to revert to the most recent snapshot, click **Revert to Current Snapshot**.
  - If you want to restore to another snapshot in the snapshots tree:
    - Click **Manage Snapshots**.
    - From the list of snapshots, click the snapshot that you want to restore.
    - Click **Go to** to restore the virtual machine to the snapshot.
    - Click **Yes** in the confirmation dialog box.
- When the snapshot is restored, in the **Recent Tasks** list, the status of the **Revert** task shows **Completed**.
- Step 6** Repeat Steps 4 and 5 to restore the other virtual machines in the cluster.
- Step 7** Verify that the cluster restored correctly by signing in to Cisco Jabber Guest Administration as an administrator. The Cisco Jabber Guest version number to which you restored appears at the bottom of the screen.
- Step 8** Check to make sure that all users and links look as you expect.
-



## CHAPTER

# 6

## Troubleshoot

---

- [Locate chip.log File, page 23](#)
- [Locate chip.dmp File, page 23](#)
- [Reset Admin Password for Cisco Jabber Guest Administration, page 24](#)
- [Reset Root Password for Cisco Jabber Guest Server, page 24](#)

## 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.

---

## 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.

**REVIEW DRAFT - CISCO CONFIDENTIAL****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 [PCSPP,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.

---



# Reference

- [Call Link Format](#), page 27
- [Mapping Between Link Fields and SIP Headers](#), page 28

## Call Link Format

Call links are constructed in the following format:

```
https://example-jabberguest/call/directory number (DN) or UserID@example.com
```

The following table provides some examples of how links are constructed.

Table 2: Example Call Link URLs

| URL                                                      | Notes                                                          |
|----------------------------------------------------------|----------------------------------------------------------------|
| http://example-jabberguest.com/call/janedoe@example.com  | URI links work only for endpoints with URI dialing enabled.    |
| http://example-jabberguest.com/call/5309@example.com     | 4-digit DNs work only for endpoints homed on the same cluster. |
| http://example-jabberguest.com/call/17011701@example.com | 8-digit DNs work for all endpoints on the same domain.         |



**Note**

The domain is optional. If the domain is supplied, it must match the enterprise domain configured in Cisco Unified Communications Manager. If a domain is not supplied on an ad hoc link, the SIP domain (in **Settings > Call Control and Media**) for this server is used.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

# Mapping Between Link Fields and SIP Headers

| Link Field                                                                                                                                                               | SIP Header                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Destination</b>                                                                                                                                                       | Request-URI in the INVITE                                                                                                                                                                                                                                 |
| <b>Caller SIP Alias</b><br><b>Note</b> If you do not enter a value in the <b>Caller SIP alias</b> field, the value in the <b>Default caller SIP alias</b> field is used. | User portion of the <i>From:</i> and <i>Remote Party ID:</i> (RPID) headers<br>Example: <ul style="list-style-type: none"> <li>• From: &lt;sip:alice@cisco.com&gt;</li> <li>• Remote-Party-ID: &lt;sip:alice@cisco.com&gt;</li> </ul>                     |
| <b>Caller name</b><br><b>Note</b> If you do not enter a value in the <b>Caller name</b> field, the caller name is <i>Jabber Guest</i> .                                  | Display name of the <i>From:</i> and <i>Remote Party ID:</i> (RPID) headers<br>Example: <ul style="list-style-type: none"> <li>• From: "Alice" &lt;sip:alice@cisco.com&gt;</li> <li>• Remote-Party-ID: "Alice" &lt;sip:alice@cisco.com&gt;</li> </ul>     |
| <b>Append unique identifier to SIP alias</b>                                                                                                                             | Adds a unique identifier to the <i>From:</i> and <i>Remote Party ID:</i> (RPID) headers<br>Example: <ul style="list-style-type: none"> <li>• From: &lt;sip:alice-123@cisco.com&gt;</li> <li>• Remote-Party-ID: &lt;sip:alice-123@cisco.com&gt;</li> </ul> |