



## JABBER CONFIGURATION FOR CISCO INSTANT CONNECT INTEGRATION

Revised November 8, 2016

*This document covers basic Jabber configuration on CUCM 10.5.1 version. Steps might vary slightly if using an older version of CUCM (for example, setting up mixed mode for CUCM). Please refer to troubleshooting notes at the end of this document for additional info.*

Prerequisite – **Jabber for Android CUCM Configuration Example**. Please follow the instructions on this <http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-85/113471-jabber-android-00.html>.

Note for Sonim phones, there are some updates to standard Android phones (Use secure device profile) that are listed at the bottom of this document.

After installing Cisco Jabber on each android phone, DNS has to be set on them manually for this to work

**Note:** This step (related to DNS) step may NOT be needed based on how the CUCM & DNS is configured at the customer site. At Cisco CIC QA lab, the DNS was manually configured and hence captured in this document.

### On Your Smartphone or Tablet

Android and iOS devices allow you to set a custom DNS server, but this will only apply to a single network. In other words, you can change the DNS server for your home network, but you'll have to change it again each time you connect to a new Wi-Fi network.

To do this on Android, open the Wi-Fi networks list and long-press the one you're connected to. Tap Modify network and check the Show advanced options box. Set IP settings to Static and you'll be able to change your DNS server — unfortunately, this also means you can't use DHCP on the network anymore.



TELUS2410

None

IP settings

Static

IP address

192.168.1.84

Gateway

192.168.1.254

Network prefix length

24

DNS 1

192.168.1.254

DNS 2

75.153.176.9

Cancel

Save

#### •A. On CUCM:•

1. Add Phones with customized template for Jabber (use dual mode Android option). Use Device security profile as secure profile for SONIM Phones and non secure for Samsung Phones. Add local domain and FQDN to CUCM under System > Enterprise Parameters > Clusterwide Domain Configuration•
2. Set the CUCM security mode to "mixed-mode". By running "utils ctl set-cluster mixed-mode" then reboot CUCM•
3. Activate CAPF and CTL Provider services•
4. Create a secure phone profile (authenticate is Encrypt, port 5061 for SIP), assign it to the BOT device.•
5. Set the CAPF parameter to "Install/upgrade" in the BOT device with a key size to 1024•
6. Create users with the phone numbers associated•Users:•User1 -> Directory number-1 User2 -> Directory number-2••

#### B. On Android device:•

1. Change Blizzard's(Wi-Fi) advanced settings from DHCP to Static , DNS server as 10.194.230.70 (lab DNS), secondary as 171.70.168.183 (corporate DNS)•
2. On Cisco Jabber app -> Advanced settings-> Change connect option to Manually-> 10.194.151.95 (This would be the CUPS server IP address)•Login to Jabber using user1 @domain name followed by Password. Same for user2. Example : (johndoe@.com/Jabberi\$gr8)•

*Note 1: For Sonim phones, ensure CAPF in CUCM for Install/Upgrade to send new certificates and make sure user accepts those certificates. Samsung Phones register fine with one time certificate•*

*Note 2: If CUPS is in domain with DNS name, users could register Jabber phones fine with DHCP using Corporate DNS. In our case, that was not working.•If Jabber registration was successful, phones should display Jabber Phone #s along with IM option and make successful Jabber calls••*

#### C. On IPICS server:•

1. Configure user's phone numbers in IPICS server->user->communication->business numbers and save•

2. In Quick launch application tab, make sure Cisco Jabber is configured (Cisco Jabber and package name com.cisco.im)•

3. In SONIM yellow key setting, configure long press to launch Cisco Jabber• •

D. On CIC APP• In Settings-> enable Cross launch applications (applicable only to SONIM with yellow button). Android Devices with no yellow button display this option as greyed .• •

If everything is configured correctly, business number should be displayed in CIC's contact details to make Jabber call and CIC users registered to Jabber should be able to tap on that number to make successful Jabber call. Ending the Jabber call, should have option to stay in Jabber or return back to CIC

## Troubleshooting Tips

Please note the for Sonim phones, ensure CAPF in CUCM for Install/Upgrade to send new certificates and make sure user accepts those certificates unlike Samsung Phones which registers with one time certificate.

Also the device security profile should be set for Secure Profile for Sonim phones. (snap shot below)

The screenshot shows the 'Phone Security Profile Configuration' page in CUCM. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the 'Status' section shows 'Status: Ready'. The 'Phone Security Profile Information' section contains the following fields: Product Type (Cisco Dual Mode for Android), Device Protocol (SIP), Name\* (Cisco Dual Mode for Android - Standard SIP Secure F), Description (Cisco Dual Mode for Android - Standard SIP Secure F), Nonce Validity Time\* (600), Device Security Mode (Encrypted), and Transport Type\* (TLS). There are also two checkboxes: 'Enable Digest Authentication' and 'Exclude Digest Credentials in Configuration File'. The 'Phone Security Profile CAPF Information' section contains Authentication Mode\* (By Null String) and Key Size (Bits)\* (1024). A note states: 'Note: These fields are related to the CAPF Information settings on the Phone Configuration page.' The 'Parameters used in Phone' section contains SIP Phone Port\* (5061).

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**

Status: Ready

**Phone Security Profile Information**

**Product Type:** Cisco Dual Mode for Android  
**Device Protocol:** SIP  
**Name\*** Cisco Dual Mode for Android - Standard SIP Secure F  
**Description** Cisco Dual Mode for Android - Standard SIP Secure F  
**Nonce Validity Time\*** 600  
**Device Security Mode** Encrypted  
**Transport Type\*** TLS

Enable Digest Authentication  
 Exclude Digest Credentials in Configuration File

**Phone Security Profile CAPF Information**

**Authentication Mode\*** By Null String  
**Key Size (Bits)\*** 1024

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

**SIP Phone Port\*** 5061

Due to an Android kernel issue, Cisco Jabber cannot register to the Cisco Unified Communications Manager on some Android devices. To resolve this problem, try the following:

- Upgrade the Android kernel to 3.10 or later version.
- Set the Cisco Unified Communications Manager to use mixed mode security, enable secure SIP call signaling, and use port 5061. See the Cisco Unified Communications Manager Security Guide for your release for instructions on configuring mixed mode with the Cisco CTL Client. You can locate the security guides in the Cisco Unified Communications Manager [Maintain and Operate Guides](#). This solution applies to the following supported devices:
  - HTC One M8 (Android OS 4.4.2 or later)
  - HTC One M7 (Android OS 4.4.2 or later)
  - .....
  - Huawei Ascend Mate 7 (Android OS 4.4 or later)
  - **Sonim XP7 (Android OS 4.4.4)**
  - Xiaomi 4 (Android OS 4.4 or later)

Step1: Configure CUCM as Mixed mode, creates a CTL file using the Cisco CTL Client.  
Step1.1 CTL client can be downloaded from CUCM Application-Plugins

Once it's downloaded, double-click on the file to install it on a PC.

Step1.2 Run the CTL client.

During the process, a prompt will be displayed that states that one of the keys must be plugged into the computer. Once information has been copied to and from the key, a prompt will state that the first key must be removed and the other key must be plugged into the computer. If you have two USB ports on the computer DO NOT insert both keys at the same time. If, at any point, a password is requested for the key, then note that the default is "**Cisco123**" (case sensitive). Note: If at any time another individual set a different password for the keys, do not guess what that password may be. After 15 wrong attempts at guessing the password, the key locks and nothing will unlock it (this is part of the reason the keys come in pairs). If both keys get locked, another pair of keys must be obtained from Cisco.

Step1.3 Restart CUCM Server after installation.

Step1.4 After CUCM Server restart, Go To: CUCM => System => Enterprise Parameters => Security Parameters

If "Cluster Security Mode" is 1, then succeed for Step 1.

---

#### Security Parameters

[Cluster Security Mode](#) \*

Step2 - Upload the Jabber for Android Cop File "cmterm-android\_9.6.0v11.cop.sgn".

Go To: CUCM => Cisco Unified OS Administrator => Software Upgrades => Install/Upgrade to upload the Cop File.

Go To: CUCM => Cisco Unified OS Administrator => Show => Software to see the uploaded Cop File.

*Note: if the CUCM version is high or equal to 10.5.0, then Step2 is not required as the Cop File has already been included in CUCM.*

cmterm-android\_9.6.0v10.cop

cmterm-jabberipad-130917.cop

cmterm-android\_9.6.0v11.cop

cmterm-iphone-install-130917.cop

Step3, Configure android secure profile and Device Security Mode is "Encrypted" or "Authenticated" and Transport Type is "TLS".

Go To: CUCM => System => Security => Phone Security Profile

### Phone Security Profile Information

<b>Product Type:</b>	Cisco Dual Mode for Android
<b>Device Protocol:</b>	SIP
Name*	<input type="text" value="Cisco Dual Mode for Android encrypted null string"/>
Description	<input type="text" value="Cisco Dual Mode for Android encrypted null string"/>
Nonce Validity Time*	<input type="text" value="600"/>
Device Security Mode	<input type="text" value="Encrypted"/>
Transport Type*	<input type="text" value="TLS"/>
<input type="checkbox"/> Enable Digest Authentication	
<input type="checkbox"/> TFTP Encrypted Config	
<input type="checkbox"/> Exclude Digest Credentials in Configuration File	

### Phone Security Profile CAPF Information

Authentication Mode*	<input type="text" value="By Null String"/>
Key Size (Bits)*	<input type="text" value="2048"/>

Note: These fields are related to the CAPF Information settings on the Phone Configur

### Parameters used in Phone

SIP Phone Port*	<input type="text" value="5061"/>
-----------------	-----------------------------------

Step4 - Apply the secure profile "Cisco Dual Mode for Android encrypted null string" to the Android BOT account. And make sure Certificate Operation is "Install/Upgrade", then Jabber will download the Certificate while firstly login.

Go To: CUCM => Device => Phone => Choose BOT account

Device Security Profile*	<input type="text" value="Cisco Dual Mode for Android encrypted null string"/>
--------------------------	--

## Certification Authority Proxy Function (CAPF) Information

Certificate Operation *	<input type="text" value="Install/Upgrade"/>
Authentication Mode *	<input type="text" value="By Null String"/>
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Size (Bits) *	<input type="text" value="2048"/>
Operation Completes By	<input type="text" value="2016"/> <input type="text" value="11"/> <input type="text" value="7"/> <input type="text" value="12"/> (YYYY:MM:DD:HH)

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: [www.cisco.com/go/trademarks](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)

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.

© 2016 Cisco Systems, Inc. All rights reserved.