



# Setup Guide for Cisco Jabber for Android

## Modification History

Revision	Date	Originator	Comments
1	March 20, 2012	Sheila Sadorra	Initial draft
2	March 20, 2012	Sheila Sadorra	CUC admin install
3	May 15, 2012	Sheila Sadorra	Updates to admin dual timers
4	June 14, 2012	Sheila Sadorra	Update to add supported phone list
5			

**TABLE of CONTENTS**

1.	<b>Getting Started:</b>	<b>3</b>
2.	<b>ReCOMMENDED Setup:</b>	<b>3</b>
3.	<b>Sample Diagram</b>	<b>4</b>
4.	<b>Adding new device to CUCM</b>	<b>5</b>
5.	<b>Directory Search Configuration</b>	<b>6</b>
6.	<b>Handoff to Cellular/Desktop &amp; Call control - SNR</b>	<b>7</b>
7.	<b>VPN / Secure Connect</b>	<b>8</b>
8.	<b>Visual Voicemail Configuration (rEQUIRES jABBER 9.0)</b>	<b>9</b>
9.	<b>SIP Digest Configuration (rEQUIRES jABBER 9.0)</b>	<b>9</b>
10.	<b>Update or Add New End User</b>	<b>10</b>
11.	<b>Phone Security Profile (no SIP Digest Authentication)</b>	<b>12</b>
12.	<b>Phone Security Profile with SIP Digest Auth enabled</b>	<b>12</b>
13.	<b>Device SIP Profile</b>	<b>13</b>
14.	<b>Device Softkey Template</b>	<b>14</b>
15.	<b>Dialing Rules</b>	<b>15</b>
16.	<b>User/LDAP Directory Server Integration to CUCM</b>	<b>16</b>
17.	<b>COP File</b>	<b>17</b>
18.	<b>Unity Connection Integration to CUCM and Viceversa VIA SIP Trunk</b>	<b>18</b>
19.	<b>Install and Configure Unity Connection Server for Voicemail</b>	<b>20</b>
20.	<b>Install and Configure Call Manager</b>	<b>20</b>
21.	<b>Install and Configure ASA Server</b>	<b>20</b>
22.	<b>SAMPLEUSER End User Configuration look alike – for reference</b>	<b>21</b>
23.	<b>BOTSAMPLE Device – look alike for reference</b>	<b>22</b>
24.	<b>BOTSAMPLE Device Phone Number (aka DN number) for reference</b>	<b>24</b>

Notes: Screen shots are captured from a CUCM ver9.x and CUC ver 9.x

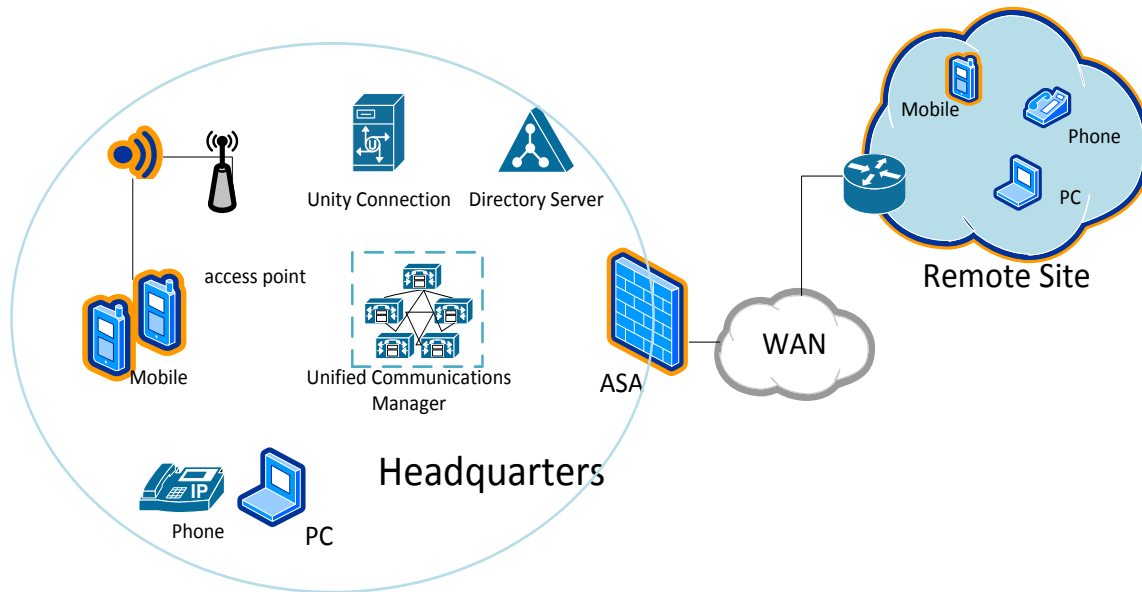
## 1. GETTING STARTED:

Recommend to Read User Guide, Release Notes, Admin Guide

## 2. RECOMMENDED SETUP:

Server/Platform	Version supported	Quantity	Notes
Unity Connection	8.5, 8.6., 9.0	1	Must
Call Manager	8.0, 8.5, 8.6, 9.0	1	Must
Headset	See supported device section below	1	Headset testing
Phone device (Android)	2.3, 4.0	2 or more	Android Phone under test
IPPhone	Models (any)  (ie 7975, 7965)	2	for multi-user testing and handoff to deskphone
LDAP	MS AD or  Open LDAP	1	Directory Search
ASA	Model number version 4.3	1	For secure connect testing
Mobile Data network			For handoff to mobile, 3g ssa testing

### 3. SAMPLE DIAGRAM

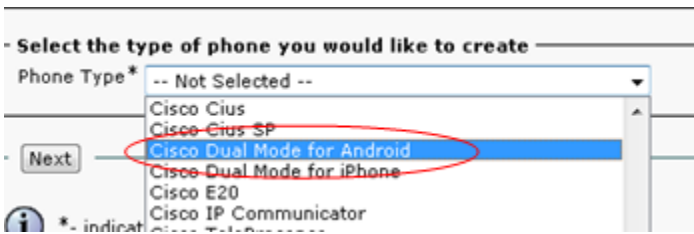


## 4. ADDING NEW DEVICE TO CUCM

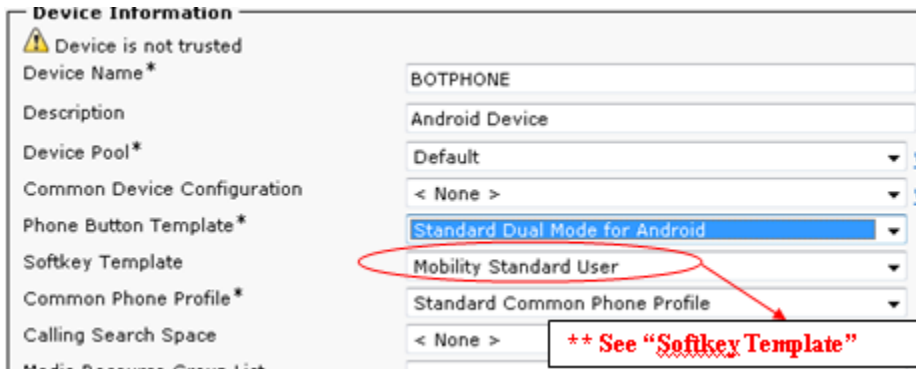
1. Log into call manager as administrator
2. Go to Device > phone
3. Click Add New



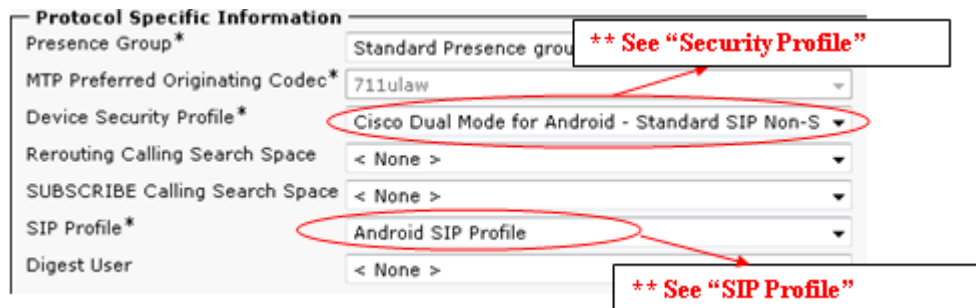
4. Select Phone Type. The phone type should be Cisco Dual Mode for Android. Hit Next.



5. Fill in device information
  - a. Fill in Device Name. Select a name that starts with "BOT" (e.g. BOTXXXX, BOTPHONE) – ALL CAPS
6. Device Pool should be DEFAULT.
7. Phone button template should be Cisco Dual Mode for Android



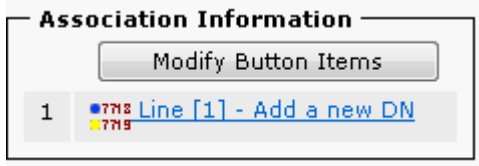
8. Under Protocol Specific Information, select "Cisco Dual Mode for Android - Standard SIP Non-secure profile" for Device Security Profile
9. SIP Profile should be Standard SIP Profile



10. Click Save and Apply Config



11. On the left side of the screen, click on Add a new DN



12. Fill in your directory number configuration

a. Put in your 5 digit extension for the Directory Number and hit Tab for auto-complete. Your new device should be now listed under Associated Devices.

Directory Number Information	
Directory Number*	44444
Route Partition	< None >

13. Click Save

You should now be able to register with the Call Manager by specifying BOTPHONE as your “Device ID” during provisioning of Cisco Jabber for Android on your mobile device.

## 5. DIRECTORY SEARCH CONFIGURATION

1. On CUCM: BOTPHONE Device Configuration to enable directory search feature

- a. LDAP username: [domain\user](#)
- b. LDAP password: password
- c. LDAP Server: server ip or hostname
- d. LDAP search base: cn=users,dc=cisco,dc=com
- e. LDAP Field Mapping: department=development;userid=uid
- f. LDAP Photo location: <http://companyname/path/%%uid%%.jpg>

Note; the photo location is a web server that has all the user’s pictures in it.

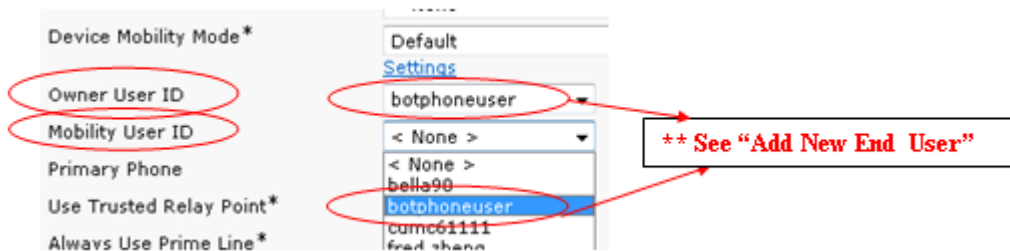
Enable LDAP User Authentication	Enabled
LDAP Username	userhere
LDAP Password	passwordhere
LDAP Server	serverhere
Enable LDAP SSL	Disabled
LDAP Search Base	cn=users,dc=mobility,dc=csst,dc=com
LDAP Field Mappings	
LDAP Photo Location	http://serverhere/ldapphoto/%%uid%%.jpg

**To validate your setup:** From Cisco Jabber application, click on the directory search tab from the main screen and search for a user within your ldap directory.

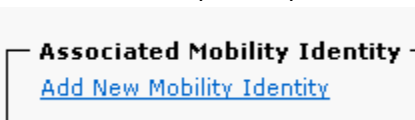
## 6. HANDOFF TO CELLULAR/DESKTOP & CALL CONTROL - SNR

### 1. Device -> Phone Device, Search for BOTPHONE

- a. Associate Owner User ID to your botphoneuser
- b. Associate Mobility User ID to your botphoneuser



- c. Click Save <<<< **MUST save before continuing** to next step.
- d. Add a new Mobility Identity



- e. On the Mobility Identity Configuration page, apply the appropriate values for the following fields
- f. Name = any name
- g. Destination Number = mobile number
- h. Answer Too Soon Time = set to 3000
- i. Answer Too Late Timer = set to 20000
- j. Delay Before Ringing Timer = set to 0
- k. Enable Mobile Connect = checked

Mobility Identity Information	
Name	BOTHandoffSNR
Destination Number*	4081234567
Single Number Reach Voicemail Policy*	Use System Default
Answer Too Soon Timer*	3000
Answer Too Late Timer*	20000
Delay Before Ringing Timer*	0
Mobility Profile	< None >
Dual Mode Phone	BOTPHONE
<input checked="" type="checkbox"/> Mobile Phone	
<input checked="" type="checkbox"/> Enable Mobile Connect	

I. Click Save

**To Validate your setup:** Place a point to point voip call with an end point. From the incall progress screen, select more -> handoff to cellular. The you should get an incoming cellular call. Accept this call and your call should resume automatically.

## 7. VPN / SECURE CONNECT

**Device -> Phone Device, Search for BOTPHONE**

a. Under the Specific device configuration, enter the following

Enable Secure Connect	Enabled
Secure Connect Gateway Address	ASAserverhere.company.com
Secure Connect Certificate Enrollment Group	scep
Secure Connect Authentication Group	certauth
Secure Connect Username	usernamehere

b. Click on save and apply config

**To Validate your setup:** During provisioning, you should be prompt to accept the secure connect certification, enter a password to ASA user.



## 8. VISUAL VOICEMAIL CONFIGURATION (REQUIRES JABBER 9.0)

### 1. Device -> Phone Device, Search for BOTPHONE

- a. Under the Specific device configuration, enter the following
- b. Voicemail username – this is the userid of the voicemail user  
Voicemail server – ip address or FQDN of the Unity Connection server  
Message store username and server – (optional) used only if you use an external exchange server to serve as your mailstore.

Voicemail Username	botphoneuser
Voicemail Server	vmfqdn.company.com
Voicemail Message Store Username	
Voicemail Message Store	

c. Save and Apply Config

### 2. Device -> Phone Device -> Click on the Line Number (DN)

- a. Under the Specific device configuration
- b. Set Directory Number Setting -> Voice Mail Profile = Default

— **Directory Number Settings**

Voice Mail Profile	Default
--------------------	---------

Assuming Default is where the voicemail profile has voicemail server configured/enabled.

**To validate your setup:** From Cisco Jabber application, click on the voicemail tab from the main screen and you should see a list of voicemail currently in your inbox.

## 9. SIP DIGEST CONFIGURATION (REQUIRES JABBER 9.0)

### 1. User Management -> End User Configuration

- a. Enter **botphoneuser** user and enter a value for the following fields
- b. Associated PC Digest Credentials and Confirm Digest Credentials

Associated PC	
Digest Credentials	.....
Confirm Digest Credentials	.....

c. Save

### 2. Device -> Phone Device, Search for BOTPHONE

- a. Under Protocol Specific Information, select the following

- b. Device Security Profile: select the customized security profile for sip digest authentication enabled  
Digest User: select the user associated with this BOTPHONE device

Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Dual Mode for Android - Digest Authenticatio
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Android SIP Profile
Digest User	botphoneuser

- c. Under the Specific device configuration, Enable this field: Enable DIP Digest Authentication.

Enable SIP Digest Authentication: Enabled

- d. Save and Apply Config

**To Validate your setup:** During provisioning, you should be prompted to enter a password to botphoneuser user. Enter the value you configured for Digest Credential field. Click Verify on the wizard screen.

## 10. UPDATE OR ADD NEW END USER

**From CUCM-> User Management -> End User -> select the end user you wish to associate with your BOTPHONE account or Add a new end user**

- a. Fill in the fields and save it

<b>- User Information</b>		Directory URI	
User Status	Active Local User	Telephone Number	44444
User ID*	botphoneuser	Mail ID	botphoneuser
Password	*****	Manager User ID	
Confirm Password	*****	Department	
PIN	*****	User Locale	English, United States
Confirm PIN	*****	Associated PC	
Last name*	Documentation	Digest Credentials	
Middle name	Test	Confirm Digest Credentials	
First name	Testing		
<b>- Mobility Information</b>			
<input checked="" type="checkbox"/> Enable Mobility			
Primary User Device	< No		

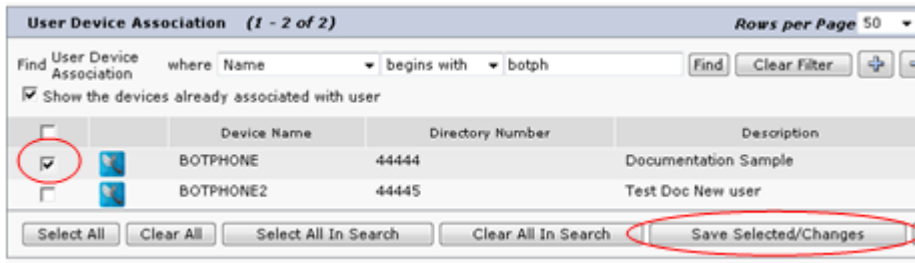
- b. Save

**Continue to edit the user to associate the device and assign appropriate groups**

c. Associate the BOTPHONE device to this user by clicking on the Device Association button,



d. select BOTPHONE from the list. Save selected item.



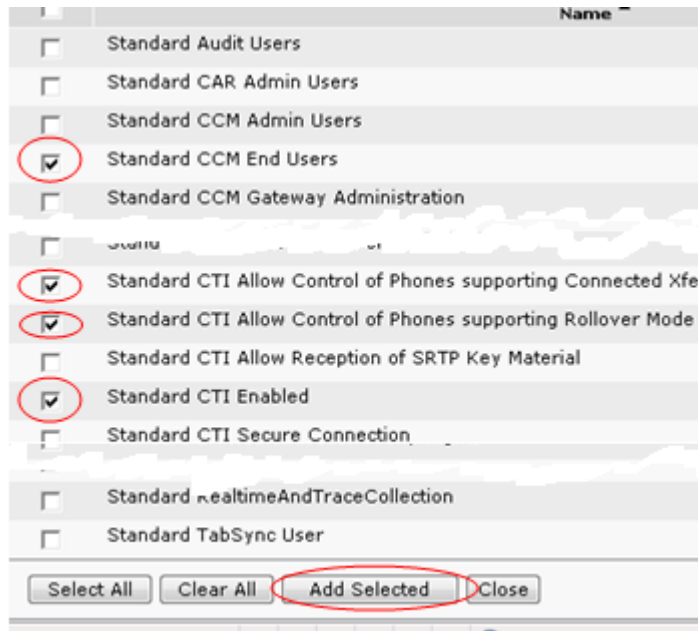
e. Click on Go button to go back to the user configuration

f. Click on "Save" button then proceed to the next step

g. Assign appropriate groups.



h. Select the following groups



i. Click on "Save" button then proceed to the next step

j. You should see the "Roles" are now pre-filled

Permissions Information	
Groups	<ul style="list-style-type: none"><li>Standard CTI Enabled</li><li>Standard CCM End Users</li><li>Standard CTI Allow Control of Phone</li><li>Standard CTI Allow Control of Phone</li></ul>
Roles	<ul style="list-style-type: none"><li>Standard CCM End Users</li><li>Standard CCMUSER Administration</li><li>Standard CTI Allow Control of Phone</li><li>Standard CTI Allow Control of Phone</li><li>Standard CTI Enabled</li></ul>

k. Save all settings

## 11. PHONE SECURITY PROFILE (NO SIP DIGEST AUTHENTICATION)

Note: Skip this section if using CUCM 8.6 or above.

### 1. From CUCM: Define a new phone security profile

System -> Security -> Phone Security Profile

a. Click on Add New

Phone Security Profile Information	
Product Type:	Cisco Dual Mode for Android
Device Protocol:	SIP
Name*	Cisco Dual Mode for Android - Standard SIP Non-Secur
Description	Cisco Dual Mode for Android - Standard SIP Non-Secur
Nonce Validity Time*	600
Transport Type*	TCP+UDP
<input type="checkbox"/>	Enable Digest Authentication
<input type="checkbox"/>	Exclude Digest Credentials in Configuration File

Parameters used in Phone	
SIP Phone Port*	5060

## 12. PHONE SECURITY PROFILE WITH SIP DIGEST AUTH ENABLED

### 1. From CUCM: Define a new phone security profile with SIP Digest Authentication enabled

System -> Security -> Phone Security Profile

a. Click on Add New

Phone Security Profile Information	
Product Type:	Cisco Dual Mode for Android
Device Protocol:	SIP
Name*	Cisco Dual Mode for Android - Digest Authentication Proc
Description	Cisco Dual Mode for Android - Digest Authentication Proc
Nonce Validity Time*	600
Transport Type*	TCP+UDP
<input checked="" type="checkbox"/> Enable Digest Authentication	
<input checked="" type="checkbox"/> Exclude Digest Credentials in Configuration File	

Parameters used in Phone	
SIP Phone Port*	5060

b. Save

### 13. DEVICE SIP PROFILE

1. From CUCM: Define SIP Profile to be used by the Android devices

Device -> Device Settings -> SIP Profile

a. Search for "Default SIP Profile" and make a copy

b. Modify the following fields

SIP Profile Information	
Name*	Android SIP Profile
Description	Android Default SIP Profile
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled

Parameters used in Phone	
Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	120
Timer Register Expires (seconds)*	720
Timer Keep Alive Expires (seconds)*	720
Timer Subscribe Expires (seconds)*	720
Timer Subscribe Delta (seconds)*	15

c. Click Save

## 14. DEVICE SOFTKEY TEMPLATE

### 1. From CUCM: Define a new Softkey Template for Android devices to use Device -> Device Settings -> Softkey Template

a. Search for the "Standard User" template and make a copy

<a href="#">Standard Shared Mode Manager</a>	Standard template for shared mode manager phones	
<a href="#">Standard User</a>	Standard Softkey Template for CallManager only	

b. Enter a new name called Mobility Standard User

c. Save

**Softkey Template Information**

Name\* Mobility Standard User

Description Standard Softkey Template for CallManager only

Applications\* Cisco CallManager

Default Softkey Template

d.

e. Click on the "GO" button to Configure Softkey Layout. This is located on the top right corner of this page.



f. For Call State = On Hook, Add Mobility (Mobility) softkey

g. For Call State = Connected, Add Mobility (Mobility) softkey

**Softkey Layout Configuration**

Softkey Template: Mobility Standard User

Select a call state to configure On Hook

Unselected Softkeys

- Call Back (CallBack)
- Conference List (ConfList)
- Direct Transfer (DirTrfr)
- Group Pick Up (GPickUp)
- HLog (HLog)
- Join (Join)
- Meet Me (MeetMe)

Selected Softkeys (ordered by position)\*\*

- Redial (Redial)
- \*\*NewCall (NewCall)
- Mobility (Mobility)
- Immediate Divert (iDivert)
- Toggle Do Not Disturb (DND)
- Forward All (CfwdAll)

**Softkey Layout Configuration**

Softkey Template: Mobility Standard User

Select a call state to configure Connected

Unselected Softkeys

- HLog (HLog)
- Immediate Divert (iDivert)
- Quality Report Tool (QRT)
- Record (Record)
- Remove Last Conference Party (RmLstC)
- Toggle Do Not Disturb (DND)
- Toggle Malicious Call Trace (MCID)
- Undefined (Undefined)

Selected Softkeys (ordered by position)

- Hold (Hold)
- End Call (EndCall)
- Transfer (Trnsfer)
- Park (Park)
- Mobility (Mobility)
- Conference (Confm)
- Conference List (ConfList)
- Select (Select)

h. Click on Save and Apply Config buttons

## 15. DIALING RULES

### 1. From CUCM: Configure Dialing Rules

Call Routing -> Dial Rules -> Application Dial Rules

Application Dial Rule (1 - 6 of 6)						Rows per Page 50
Find Application Dial Rule where Name begins with						
<input type="checkbox"/>	Name ^	Description	Number Begins With	Number of Digits	Total Digits to be Removed	Prefix With Pattern
<input type="checkbox"/>	<a href="#">International 12 rule1</a>	International + 12 1 9011	+	12	1	9011
<input type="checkbox"/>	<a href="#">International 13</a>	International + 13 1 9011	+	13	1	9011
<input type="checkbox"/>	<a href="#">International 14</a>	International + 14 1 9011	+	14	1	9011
<input type="checkbox"/>	<a href="#">Local</a>	Local Call - 7 0 9		7	0	9
<input type="checkbox"/>	<a href="#">Long Distance 11</a>	Long distance 1 11 0 9	1	11	0	9
<input type="checkbox"/>	<a href="#">Long distance 10</a>	Long distance - 10 0 91		10	0	91

### 2. From CUCM: Configure Voice/PSTN Gateway

Device -> Gateway

#### Device Information

Product	H.323 Gateway
Device Protocol	H.225
Registration	Unknown
IP Address	voice/pstn gateway here
Device is not trusted	
Device Name*	voice/pstn gateway here
Description	
<input checked="" type="checkbox"/> PSTN Access	

### 3. From CUCM: Configure Route Pattern

Call Routing -> Route/Hunt -> Route Pattern

Below are sample route patterns

011! - this is to route all numbers that starts with 011 to the voice/pstn gateway for international calls

9.@ - this is to route all calls starting with a 9 to the voice/pstn gateway for domestic calls.

<input type="checkbox"/>	<a href="#">011!</a>	any num starts with 011 goes to voice gateway
<input type="checkbox"/>	<a href="#">9.@</a>	Anything starts with 9 goes to voice gateway

Depending on how you configured the application dial rules, and what set of digits are accepted by the voice/pstn gateway will determine how you will configure the Route Pattern.

## 16. USER/LDAP DIRECTORY SERVER INTEGRATION TO CUCM

### 1. From CUCM: Enable LDAP System

#### System -> LDAP -> LDAP System

- a. Select the LDAP type that you wish to integrate with and the User ID mappings
- b. See sample below: Open LDAP (left) or MS AD (right)

**LDAP System Information**

Enable Synchronizing from LDAP Server

LDAP Server Type:

LDAP Attribute for User ID:

**LDAP System Information**

Enable Synchronizing from LDAP Server

LDAP Server Type:

LDAP Attribute for User ID:

### 2. From CUCM: Define Directory Server

#### System -> LDAP -> LDAP Directory

- a. Fill in the directory information

**LDAP Directory Information**

LDAP Configuration Name\*:

LDAP Manager Distinguished Name\*:

LDAP Password\*:

Confirm Password\*:

LDAP User Search Base\*:

LDAP Custom Filter:

**LDAP Server Information**

Host Name or IP Address for Server*	LDAP Port*	Use SSL
<input type="text" value="LDAP Server here"/>	<input type="text" value="389"/>	<input type="checkbox"/>



## 17. COP FILE

1. The COP File can either be burned on a CD/DVD or stored on an SFTP location.
2. Use the CallManager platform UI to download and install the COP file.
3. Log onto the CM portal under Cisco Unified OS Administration (select using the drop-down menu on the top right corner)
4. Go to Software Upgrades -> Install Upgrade
5. Follow the steps to install the COP file. Provide either an SFTP server information or CD/DVD location to download the file and run the install.
6. For example if it's source is a remote file location your settings might look like this:

Source: Remote Filesystem  
Directory: /path\_here  
Server: ftp\_server\_ip  
User Name: < username>  
Password: < password>  
Transfer Protocol: SFTP or FTP

7. Make sure to Reboot servers after installation is complete.
8. (Restart under Settings->Version in OS Admin page)

Cisco Jabber for Android (8.6.3.1434) – downloadable from Market	COP file version 17
Cisco Jabber for Android (9.0.1.x) – upcoming release	COP file version 23

## 18. UNITY CONNECTION INTEGRATION TO CUCM AND VICEVERSA VIA SIP TRUNK

1. **Assumption: Both CUC and CUCM are installed and online and working**
2. **From CUC: Integrate with CUCM**  
**CUC -> Telephony Integration -> Phone System**
  - a. Define CUC -> Telephony Integration -> Phone System  
Enter a phone system name and accept all default and check "send message count"
  - b. Define CUC -> Telephony Integration -> Port Group  
Select appropriate Phone System in the dropdown box  
Create From "Port Group Type = select SIP  
Display Name = enter any name  
Enter CUCM fqdn or ip address in IPv4 Address or Host Name field.  
Leave everything else default.
  - c. Define CUC -> Telephony Integration -> Port  
Enter # of ports = 5 (at least 5). Select appropriate Phone System, Port Group and Server and click save.
3. **From CUCM: Integrate with Unity Connection**
  1. **CUCM -> Define dial-in number to call the voice mail system**
    - a. Define Pilot number (CUCM -> Advance Features -> Voicemail -> Voicemail Pilot)  
Enter a pilot number (the number to call the voicemail system)  
Check the box "make this the default Voicemail Pilot for the system"
    - b. Define Voicemail profile (CUCM -> Advance Features -> Voicemail -> Voicemail Profile)  
Enter a name that is easy to remember  
Select the pilot number you defined in previous step  
Check the box "make this the default Voicemail Profile for the system"
  2. **CUCM -> Define a new SIP trunk for voicemail to use**
    - c. Define SIP Profile (Device -> Device Settings -> SIP Profile)  
Enter a name such as "Conection SIP Profile" and accept all default.
    - d. Define SIP Trunk Security profile (System -> Security -> Security Profile)

**- SIP Trunk Security Profile Information**

Name *	Connection SIP Trunk Sec
Description	Connection SIP Trunk Sec
Device Security Mode	Non Secure
Incoming Transport Type *	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins) *	600
X.509 Subject Name	
Incoming Port *	5060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	

e. Define Trunk of type SIP

**- Outbound Calls**

Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS	
Calling Party Selection *	Originator
Calling Line ID Presentation *	Default
Calling Name Presentation *	Default
Calling and Connected Party Info Format *	Deliver DN
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Outbound	
Redirecting Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Redirecting Party Transformation C	

**- SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Des
1 *	CUC_company.com		5060

MTP Preferred Originating Codec \* 711ulaw

Presence Group \* Standard Presence group

SIP Trunk Security Profile \* Connection SIP Trunk Security Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile \* Connection SIP Profile

DTMF Signaling Method \* No Preference

f. Define SIP Profile (Device -> Device Settings -> SIP Profile)

Enter a name such as "Conection SIP Profile" and accept all default.

## 19. INSTALL AND CONFIGURE UNITY CONNECTION SERVER FOR VOICEMAIL

1. **Acquire iso image to use for installing unity connection**
2. **Acquire hardware for installing Unity Connection Server.**
3. **Run through the wizard**
4. **The following are input data you must have handy during installation wizard**
  - a. Hostname, IPAddress, DNS, Default Gateway, NTP server
  - b. Security Password
  - c. Web Administrator ID and Password
  - d. OS Administrator ID and Password
5. **The following are input data you must have handy during installation wizard**
6. **Apply appropriate license (using demo license is ok until it expires)**
7. **Configure integration with CUCM**
8. **Add users or import from CUCM or import from LDAP**

## 20. INSTALL AND CONFIGURE CALL MANAGER

1. **Acquire iso image to use for installing Call Manager**
2. **Acquire hardware for installing Call Manager Server.**
3. **Run through the wizard**
4. **The following are input data you must have handy during installation wizard**
  - a. Hostname, IPAddress, DNS, Default Gateway, NTP server
  - b. Security Password
  - c. Web Administrator ID and Password
  - d. OS Administrator ID and Password
5. **The following are input data you must have handy during installation wizard**
6. **Apply appropriate license (using demo license is ok until it expires)**
7. **Configure integration with CUC**
8. **Add users or integrate with LDAP for LDAP sync**

## 21. INSTALL AND CONFIGURE ASA SERVER

1. **Acquire iso image to use for installing ASA**
2. **Acquire hardware for installing ASA.**
3. **NEED more detailed instructions here.**

## 22. SAMPLEUSER END USER CONFIGURATION LOOK ALIKE – FOR REFERENCE

LDAP Sync Status	Active
User ID*	sheilavvm1
Password	.....
Confirm Password	.....
PIN	.....
Confirm PIN	.....
Last name*	SadorraVVM1
Middle name	
First name	SheilaVVM1
Telephone Number	4123
Mail ID	sheilavvm1@INTEROP.CSST.COM
Manager User ID	
Department	
User Locale	English, United States
Associated PC	
Digest Credentials	.....
Confirm Digest Credentials	.....

### - Device Information

Controlled Devices	BOTSHEILA CSFSHEILAVVM1 SEP001D450C39FC
--------------------	---

### - Directory Number Associations

Primary Extension	4123 in Internal_CSST_pt
-------------------	--------------------------

### - Mobility Information


<input checked="" type="checkbox"/> Enable Mobility	
Primary User Device	< None >

### - Permissions Information

Groups	Standard CCM End Users Standard CTI Allow Control of Phones supporting C Standard CTI Allow Control of Phones supporting R Standard CTI Enabled
--------	--

**23. BOTSAMPLE DEVICE – LOOK ALIKE FOR REFERENCE**

**— Device Information**

Registration Registered with Cisco Unified Communications Manager  
 IP Address 10.33.119.45  
 Active Load ID loada  
 Download Status Unknown  
 Device is Active  
 Device is not trusted  
 Device Name\* BOTSHEILA  
 Description sheila\_44123  
 Device Pool\* Default  
 Common Device Configuration < None >  
 Phone Button Template\* Standard Dual Mode for Android  
 Softkey Template Mobility Standard User  
 Common Phone Profile\* Standard Common Phone Profile  
 Call Transfer Settings [Mobility Settings](#)  
 Owner User ID sheila90  
 Mobility User ID sheila90  
 Primary Phone cipcshela

**— Protocol Specific Information**

Presence Group\* Standard Presence group  
 MTP Preferred Originating Codec\* 711ulaw  
 Device Security Profile\* Cisco Dual Mode for Android - Digest Authenticatio  
 Rerouting Calling Search Space < None >  
 SUBSCRIBE Calling Search Space < None >  
 SIP Profile\* Android SIP Profile  
 Digest User sheila90

**Associated Mobility Identity**

Name	
<a href="#">NexusG2</a>	<a href="#">914088072094</a>

**Associated Remote Destinations**



[Add a New Remote Destination](#)

### Product Specific Configuration Layout


Cisco Usage and Error Tracking	Disabled
Enable SIP Digest Authentication	Enabled
SIP Digest Username	sheila90
Directory Lookup Rules URL	
Application Dial Rules URL	
Transfer to Mobile Network	Use Mobility Softkey (user receives call)
Voicemail Username	sheila90
Voicemail Server	10.10.10.1
Voicemail Message Store Username	
Voicemail Message Store	
Enable LDAP User Authentication	Enabled
LDAP Username	userhere
LDAP Password	passhere
LDAP Server	ldapservers
Enable LDAP SSL	Enabled
LDAP Search Base	cn=Users,DC=company,DC=com
LDAP Field Mappings	department=ciscoI;userid=uid
LDAP Photo Location	http://www.company.com/dirphoto/%%uid%%.jpg
Emergency Numbers	911,123
Domain Name	company.com
Preset Wi-fi Networks	corpwifi1/corpwifi2
Enable Secure Connect	Enabled
Secure Connect Gateway Address	asaserver.company.com
Secure Connect Certificate Enrollment Group	scep
Secure Connect Authentication Group	certauth
Secure Connect Username	sheila0-
Enable Device Security Policies	Enabled
Reserved	

### Association Information

[Modify Button Items](#)

1	  <a href="#">Line [1] - 44123 (no partition)</a>
---	---

**24. BOTSAMPLE DEVICE PHONE NUMBER (AKA DN NUMBER) FOR REFERENCE**

**Status**  
 Status: Ready

**Directory Number Information**

Directory Number\* 44123

Route Partition < None >

Description Sheila's Phone

Alerting Name sheila90

ASCII Alerting Name sheila90

Allow Control of Device from CTI

Associated Devices BOTSHEILA  
cipcsheila  
SEP001D450C39FC

**Directory Number Settings**

Voice Mail Profile Default

**Call Forward and Call Pickup Settings**

	Voice Mail
Calling Search Space Activation Policy	
Forward All <input type="checkbox"/> or	
Secondary Calling Search Space for Forward All	
Forward Busy Internal <input checked="" type="checkbox"/> or	
Forward Busy External <input checked="" type="checkbox"/> or	
Forward No Answer Internal <input checked="" type="checkbox"/> or	
Forward No Answer External <input type="checkbox"/> or	
Forward No Coverage Internal <input checked="" type="checkbox"/> or	
Forward No Coverage External <input type="checkbox"/> or	
Forward on CTI Failure <input type="checkbox"/> or	
Forward Unregistered Internal <input type="checkbox"/> or	
Forward Unregistered External <input type="checkbox"/> or	
No Answer Ring Duration (seconds) 12	
Call Pickup Group < None >	



**25. SUPPORTED DEVICES PER RELEASE**

<b>Product Version</b>	<b>Model</b>	<b>OS Version</b>	<b>Manufacturer</b>
8.6.1, 8.6.4	Samsung Galaxy S1	2.2.1	Samsung
8.6.1, 8.6.4	Samsung Galaxy Tab	2.2.1	Samsung
8.6.4, 9.0.1	Samsung Galaxy S2	2.3.6	Samsung
8.6.4, 9.0.1	Samsung Galaxy S1	2.3.3	Samsung
8.6.4, 9.0.1	Samsung Galaxy Tab	2.3	Samsung
9.0.1	Nexus Galaxy	4.0.1, 4.0.2	HTC
9.0.1	Samsung Ace	2.3	Samsung
TBD	Samsung Galaxy S2	4.0	Samsung