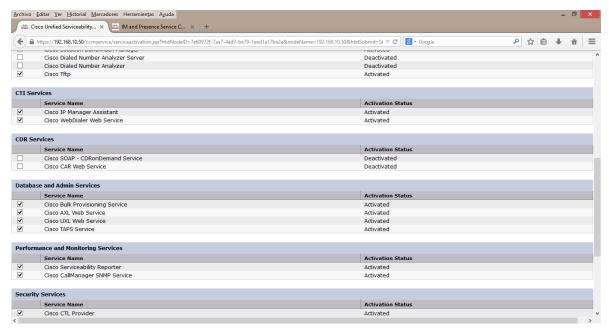
## Configuring Cisco Unified IM & Presence Server 9x

# **Configure CUCM for CUPS Functionality**

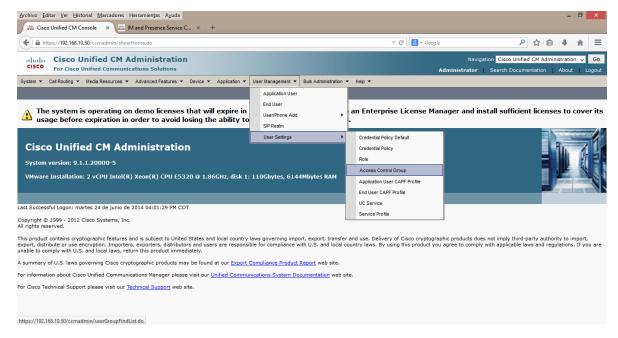
#### **Activate Services**

On the CUCM server, activate the CTI Manager Services and verify that the AXL Web Service is active

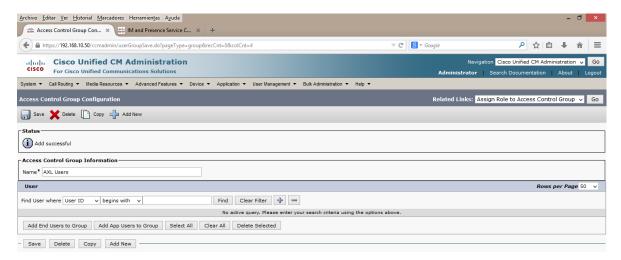


## Add an AXL Group and User

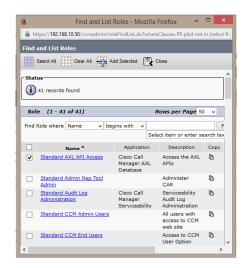
To create a new user group, on the Cisco Unified CM Administration page, navigate to User Managment>User Settings>AccessControlGroup



- 1. Click the Add New button to create a group.
- 2. Enter AXL Users for the Name field, and click the Save button.
- 3. From the Related Links drop-down list, select Assign Role to Access Control Group and click Go.
- **4.** In the Role Assignment area, click the **Assign Role to Group** button to open the Find and List Roles window. Click the **Find** button in the roles if none show.

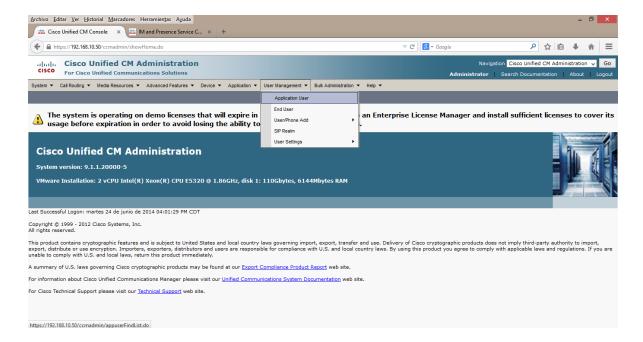


- 5. Select the check box in front of the Standard AXL API Access name
- 6. Click the Add Selected button.
- 7. The User Group Configuration window shows the Standard AXL API Access role. Click Save.

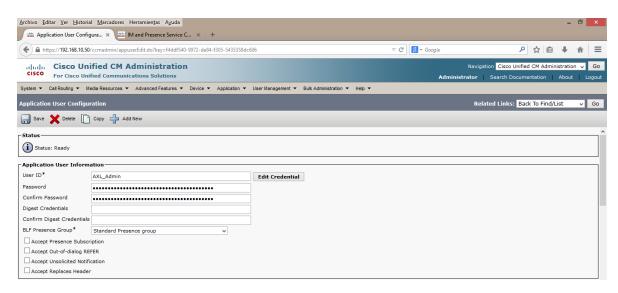


### Create the New AXL User

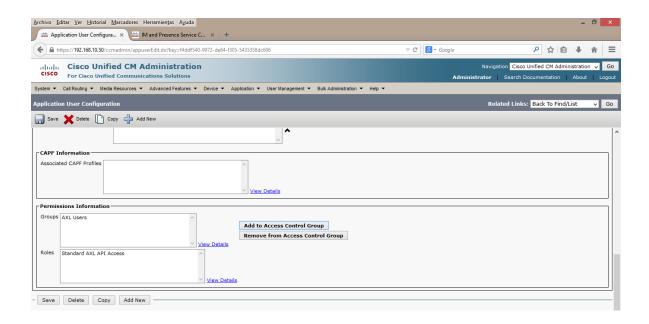
On the Cisco Unified CM Administration page, navigate to User Management > Application User.



- 1. Click the **Add New** button and the Application User Configuration window opens.
- 2. For the User ID, enter AXL\_Admin (note the underscore in the name).
- 3. Enter cisco for both the Password and Confirm Password fields.
- **4.** Scroll down to the Permissions Information section and click the **Add to Access Control Group** button to open the Find and List User Groups window.



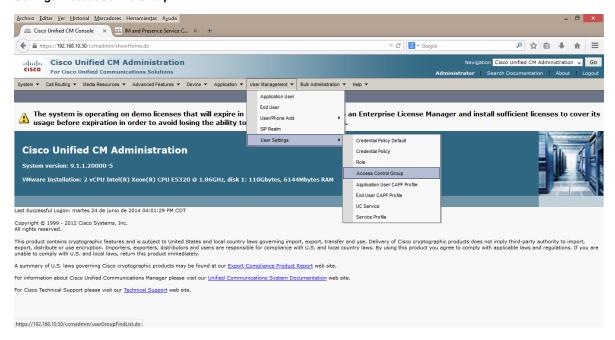
- 5. Select the AXL Users check box to choose that group. Click the Add Selected button to save the group.
- **6.** The Groups box now shows the AXL Users group. (Notice that the Roles box is still empty at this point.) Click the **Save** button. Now that the user is saved, the Roles box will show the assigned role.



## Add a CTI-Enabled Group

To enable desk phone control and other aspects of Presence functionality, computer telephony integration (CTI) control must be enabled between CUPS and CUCM.

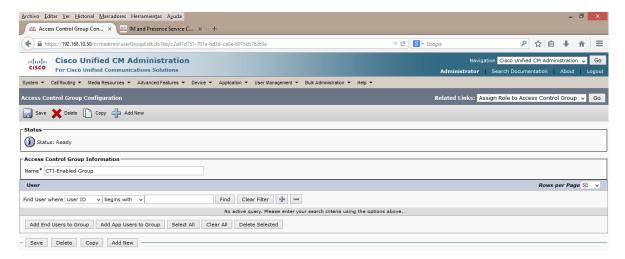
To create a new user group, on the Cisco Unified CM Administration page, navigate to User Managment>User Settings>AccessControlGroup



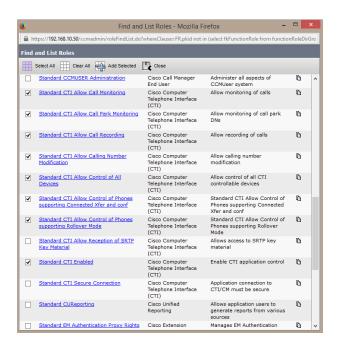
- 2. Enter CTI-Enabled-Group in the Name field, and then click Save.
- 3. On the User Group Configuration page, select Assign Role to Access Control Group from the Related Links drop-down list at

the upper right.

- 4. Click Go.
- 5. Click Assign Role to Group, and then click Find in the pop-up window that appears.

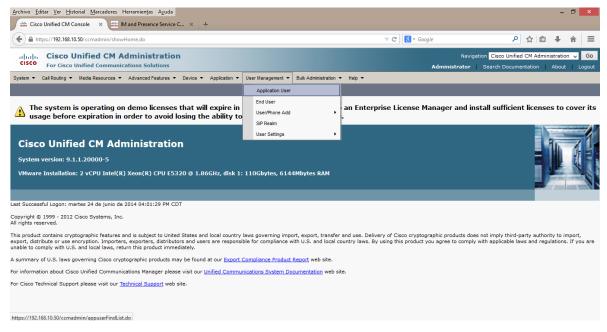


- 6. Select all CTI-related roles except Standard CTI Allow Reception of SRTP Key Material and Standard CTI Secure Connection.
- 7. Click the Add Selected button. Click Save.

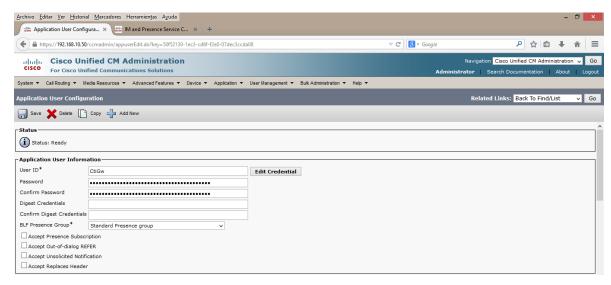


#### Add a CTI User

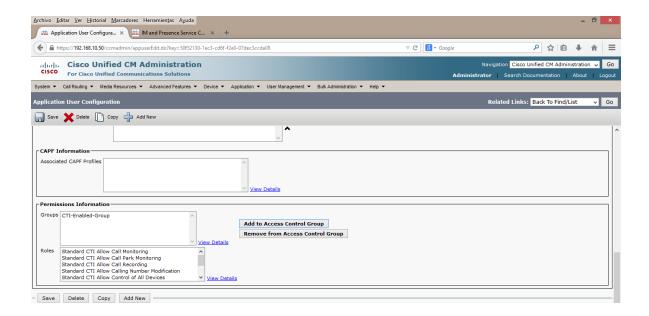
- 1. Navigate to User Management > Application User.
- 2. Click Add New.



- 3. Enter CtiGw (case sensitive) in the User ID field.
- **4.** Enter **cisco** in the Password and Confirm Password fields. In a production environment, always use a strong password. In the lab, an easy password is fine.
- **5.** Scroll down to the Permissions Information section and click the **Add to Access Control Group** button to open the Find and List User Groups window.

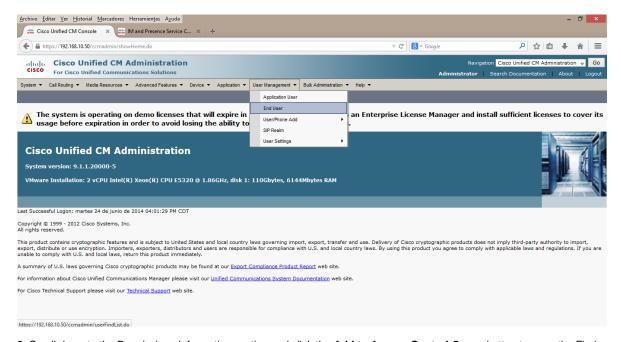


- 5. Select the CTI-Enabled-Group check box to choose that group. Click the Add Selected button to save the group.
- **6.** The Groups box now shows the **CTI-Enabled-Group** group. (Notice that the Roles box is still empty at this point.) Click the **Save** button. Now that the user is saved, the Roles box will show the assigned role.

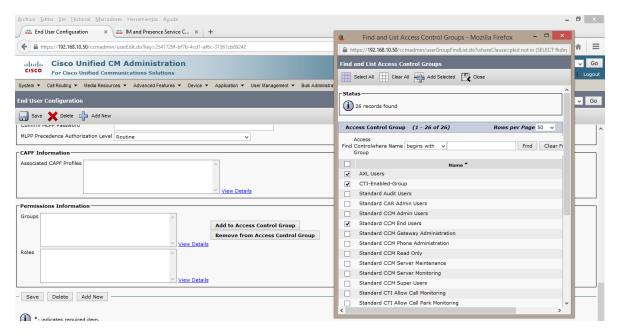


## Add a Access Control Groups to End User

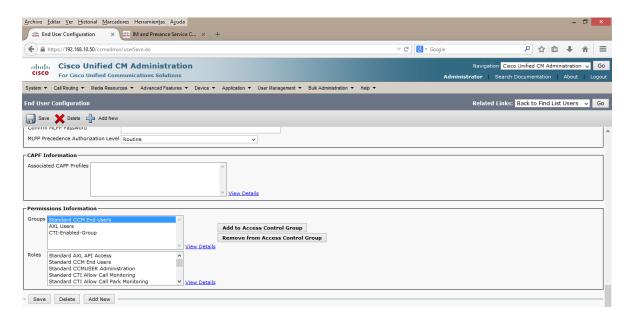
- 1. Navigate to User Management > End User.
- 2. Select the user to asign the groups (LDAP Synchronized User or Local User)



- 3. Scroll down to the Permissions Information section and click the Add to Access Control Group button to open the Find and List User Groups window.
- 4. Select the CTI-Enabled-Group, AXL Users and Standard CCM End Users check box. Click Add Selected.

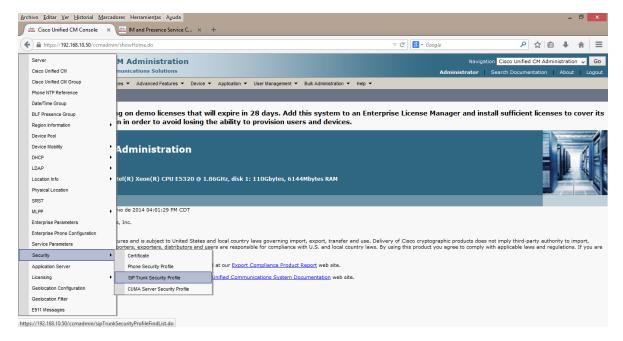


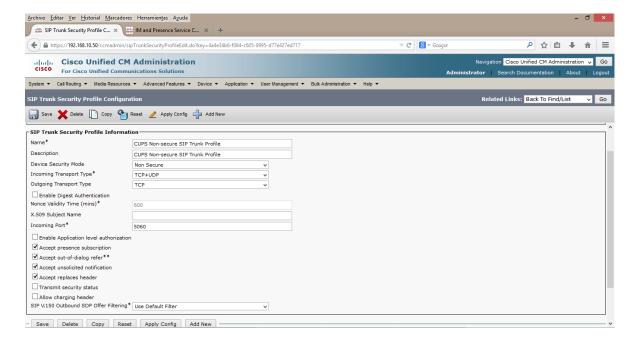
5. Click the **Save** button. Now that the user is saved, the Roles box will show the assigned role.



## Add a SIP Trunk Security Profile

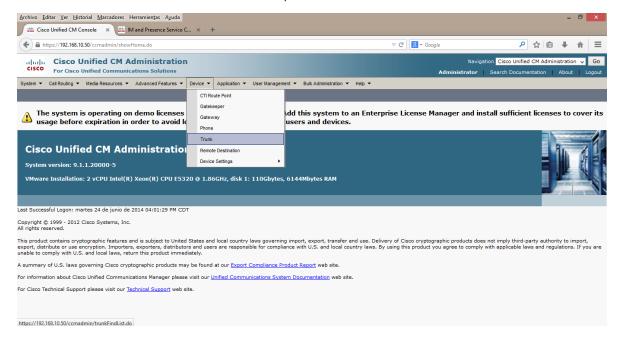
- 1. Navigate to System > Security > SIP Trunk Security Profile
- 2. Click Add New.
- 3. Enter CUPS Non-secure SIP Trunk Profile in both the Name and Description fields.
- 4. Verify that the following parameters are selected:
- Device Security Mode field: Non Secure
- Incoming Transport Type field: TCP+UDP
- Outgoing Transport Type field: TCP
- 5. Select the following check boxes:
- Accept presence subscription
- Accept out-of-dialog refer
- Accept unsolicited notification
- Accept replaces header
- 6. Click Save

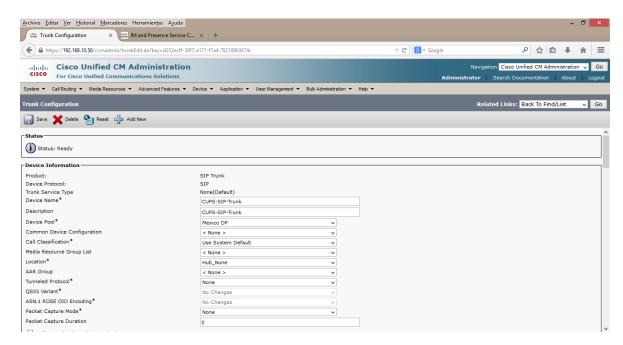


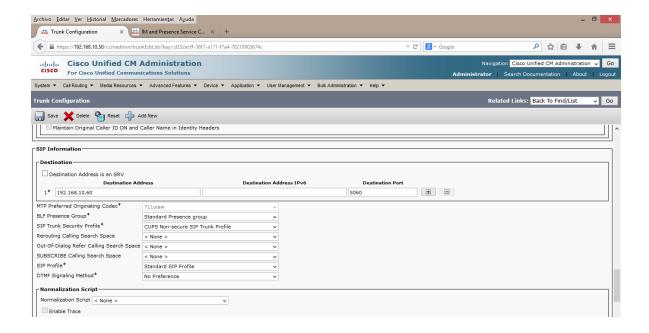


#### **Add SIP Publish Trunk**

- 1. Navigate to Device > Trunk.
- 2. Click Add New to bring up the Trunk Configuration screen.
- 3. As this will be a SIP trunk, select SIP Trunk from the Trunk Type drop-down list. The Device Protocol field will autopopulate with SIP.
- 4. Leave the Trunk Service Type field at its default setting.
- 5. Click Next.
- 6. Enter CUPS-SIP-Trunk in the Device Name and Description fields.
- 7. Select Device Pool drop-down list.
- **8.** Scroll all the way to the bottom of the screen to the SIP Information section. The Destination Address field must be configured to point to the Presence Server's IP address (192.168.10.60).
- 9. Select CUPS Non-secure SIP Trunk Profile from the SIP Trunk Security Profile drop-down list to tie the two together.
- 10. Select Standard SIP Profile from the SIP Profile drop-down list.. Click Save.



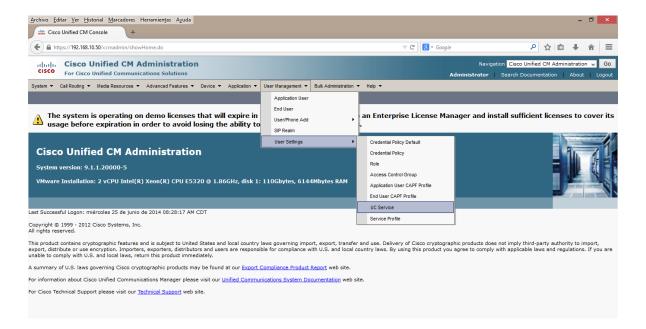




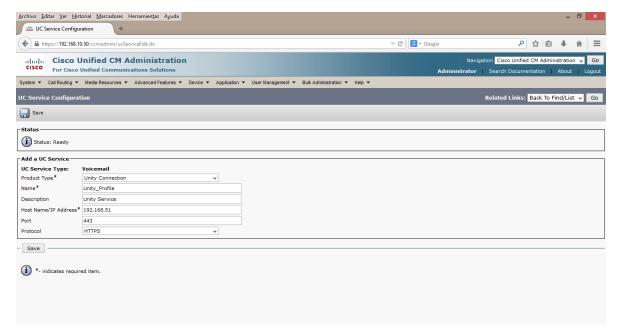
## **Configure Jabber Profile**

### Voice Mail Service.

- 1. Navigate to User Management > User Settings > UC Service.
- 2. Click Add New
- 3. Select Voice Mail.

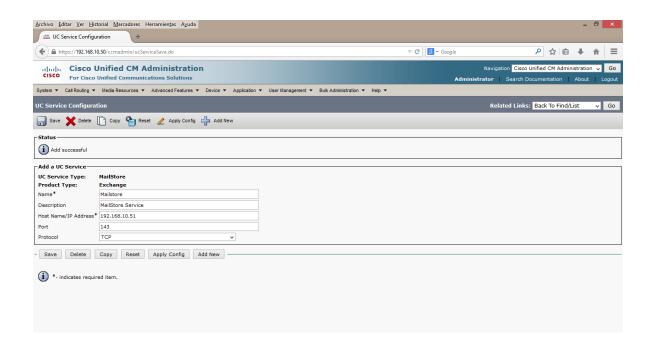


- 4. Select Unity Connection on drop-down
- 5. Enter Name and Description.
- 6. Enter the IP address of Cisco Unity Connection.
- 7. Click Save.



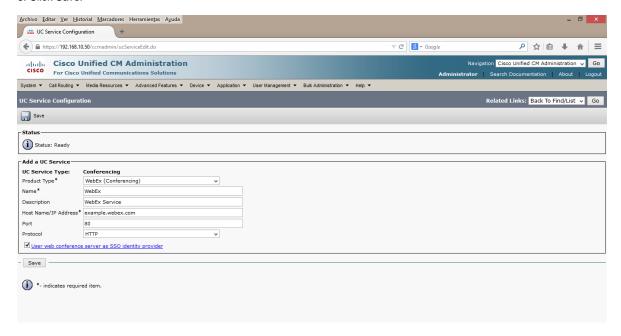
### MailStore Service.

- 1. Navigate to User Management > User Settings > UC Service.
- 2. Click Add New
- 3. Select MailStore.
- 4. Enter Name and Description.
- 5. Enter the IP address of Cisco Unity Connection.
- 6. Click Save.



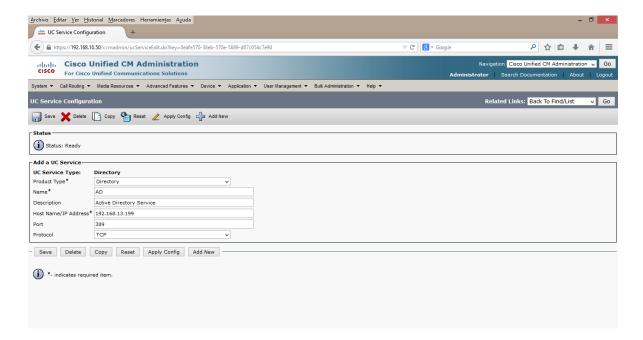
### Web Ex Conferencing Service

- 1. Navigate to User Management > User Settings > UC Service.
- 2. Click Add New
- 3. Select Conferencing.
- 4. Enter Name and Description.
- 5. Enter the hostname of your Webex Page.
- 6. Click Save.



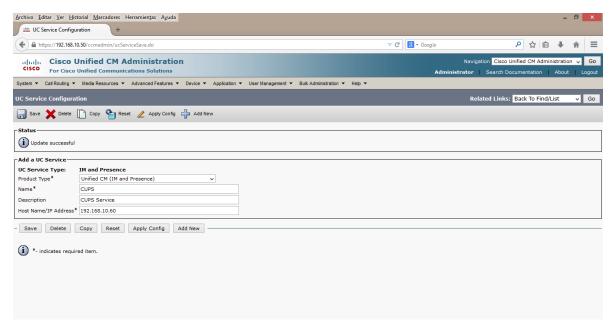
# **Directory Service**

- 1. Navigate to User Management > User Settings > UC Service.
- 2. Click Add New
- 3. Select Directory.
- 4. Enter Name and Description.
- 5. Enter the IP add of your Active Directory Server.
- 6. Click Save.



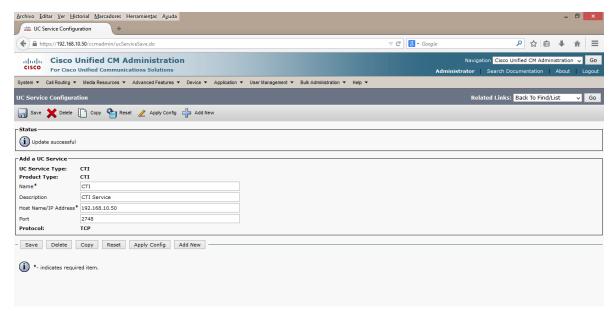
#### **IM and Presence Service**

- 1. Navigate to User Management > User Settings > UC Service.
- 2. Click Add New
- 3. Select IM and Presence.
- 4. Enter Name and Description.
- 5. Enter the IP add of Presence Server.
- 6. Click Save.



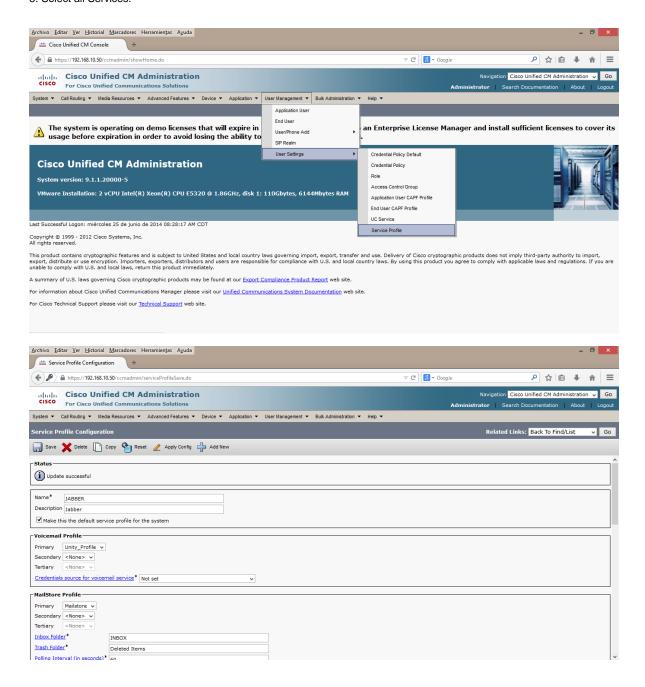
## CTI Service.

- 1. Navigate to User Management > User Settings > UC Service.
- 2. Click Add New
- 3. Select CTI.
- 4. Enter Name and Description.
- 5. Enter the IP add of CUCM.
- 6. Click Save.



#### **Service Profile**

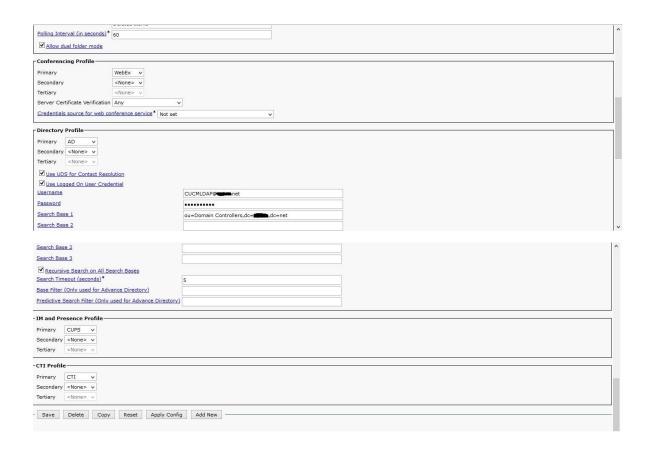
- 1. Navigate to User Management > User Settings > Service Profile.
- 2. Click Add New
- 3. Enter Name and Description.
- 4. Select the check box, Make this the default profile
- 5. Select all Services.



### On Directory Profile.

Username = is the Username of Active Diretory to synchronize users to CUCM. Password = Is the password of username.

SearchBase1 = Is the Organizative Unit where is the users.



# Assign the Jabber profile to End User.

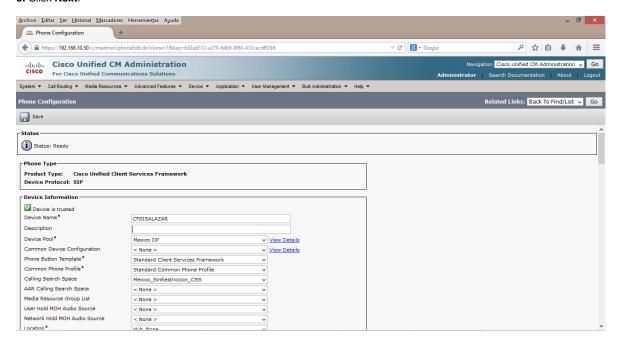
- 1. Navigate to User Management > End User.
- 2. Select the user to asign the profile.
- 3. On Service Settings, select the checkbox, Home Cluster.
- 4. Select the checkbox Enable User for Unified CM IM and Presence, for synchronize End User with Presence Server.
- 5. Drop down, select the **UC Service Profile**, previously created.
- 6. Click Save.



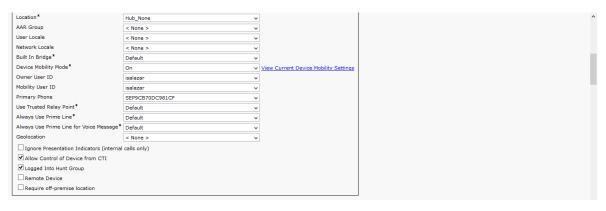
## **Create CSF Device in CUCM (Windows)**

CUCM provides call control for the soft phone features in Jabber. To do that Jabber must be defined in CUCM as a phone

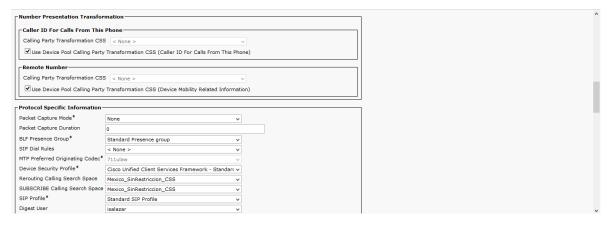
- 1. Navigate to **Device** > **Phone** > **Add New**.
- 2. In the Phone Type drop-down list, scroll down and select Cisco Unified Client Service Framework.
- 3. Click Next.



- 5. Enter the device name CFS<username>.
- 6. Configure the following parameters to match the user's desk phone configuration:
- Device Pool
- Phone Button Template: Standard Client Services Framework
- · Calling Search Space

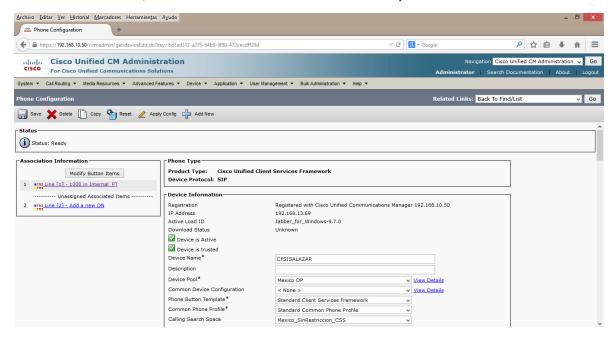


- Owner User ID: <username of the phone>
- Primary Phone: <MAC address of the desk phone>
- 7. Scroll down to the Protocol Specific Information section.
- 8. Select Cisco Unified Client Services Framework Standard SIP Non-Secure from the Device Security Profile drop-down list.
- 9. Select from the SUBSCRIBE Calling Search Space drop-down list.
- 10. Select Standard SIP Profile from the SIP Profile drop-down list.
- 11. Select the <username for the phone> from the Digest User drop-down list.



### 12. Click Save.

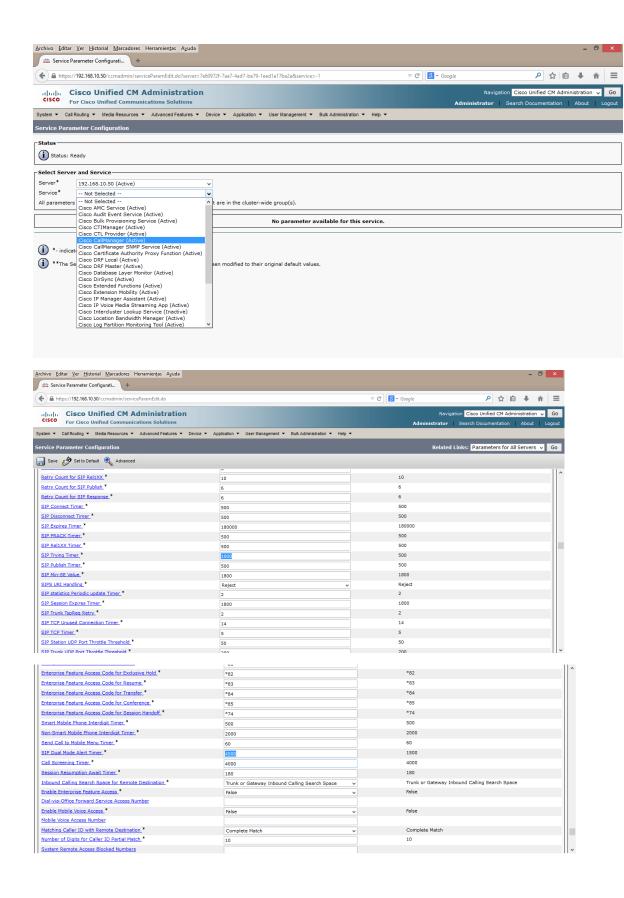
On Association Information, must be associate with a number extension and finally with the End User.



Configure Values For Jabber Android.

## **Modify SIP Timers**

- 1. Go to System > Service Parameters.
- 2. Choose the server.
- 3. Select the Cisco CallManager (Active) service.
- 4. Scroll to the Clusterwide Parameters (System Mobility) section.
- 5. Increase the SIP Dual Mode Alert Timer to 4500 milliseconds.
- 6. Scroll to the Clusterwide Parameters (Device SIP) section.
- 7.. Click Save.

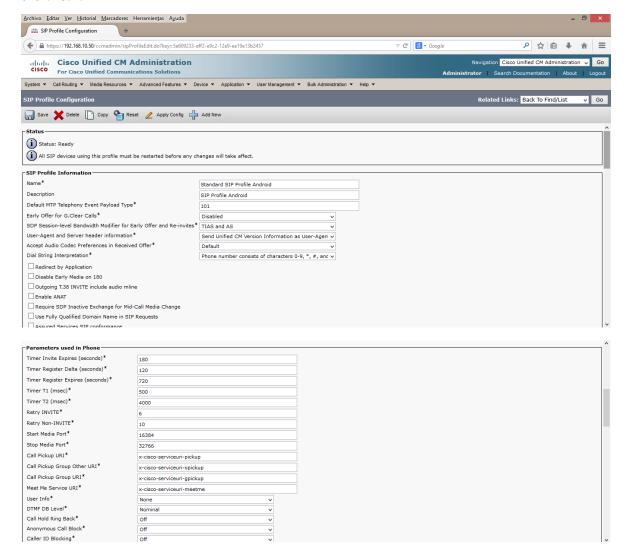


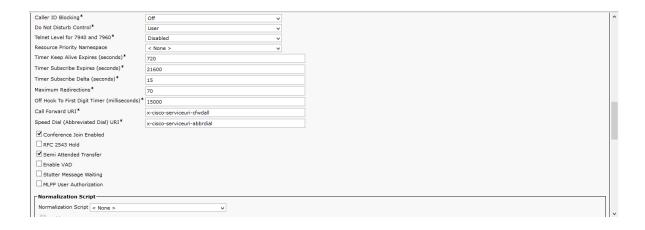
#### Create dedicated SIP Profile

- 1. In CUCM, go to **Device > Device Settings > SIP Profile**.
- 2. Copy Standard SIP profile.
- 3.Enter the Name and Description.
- 4. Change this values

Timer Register Delta to 120
Timer Register Expires to 720
Timer Keep Alive Expires to 720
Timer Subscribe Expires to 21600
Timer Subscribe Delta to 15

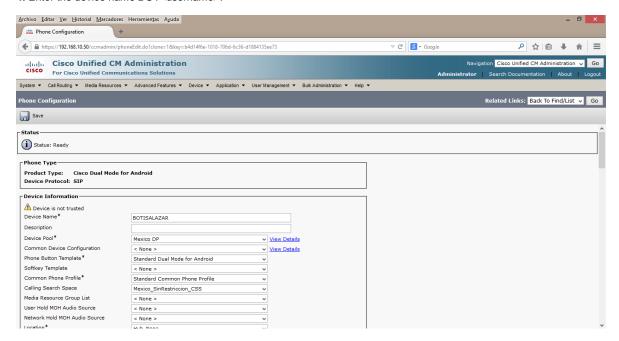
#### 5. Click Save



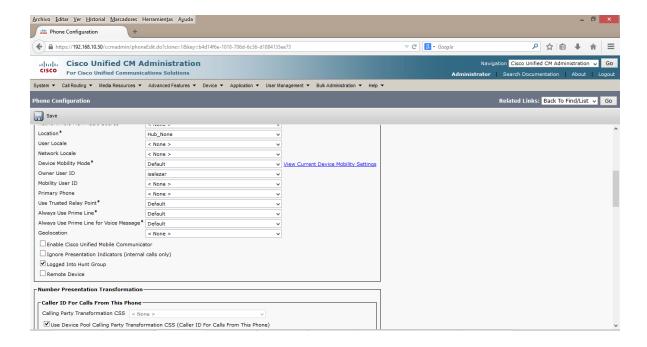


## Create BOT Device in CUCM (Android)

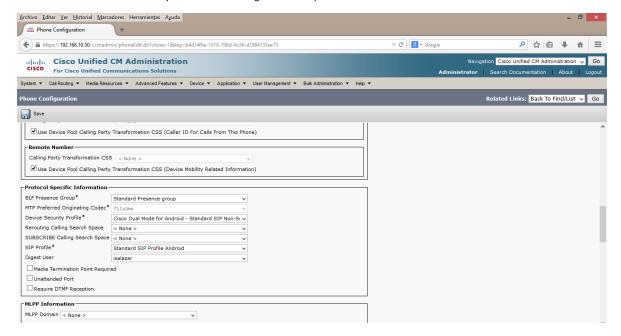
- 1. Go to Device > Phone.
- 2. Click Add New.
- 3. From the Phone Type drop-down list, choose Cisco Dual Mode for Android
- 4. Enter the device name BOT<username>.



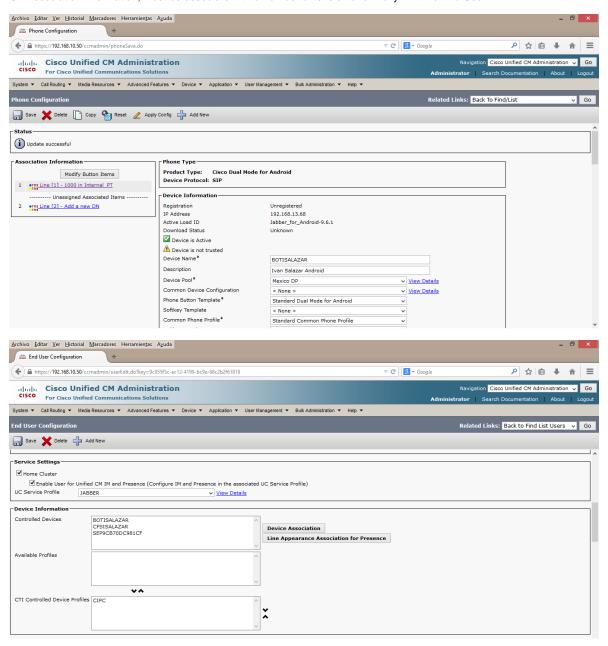
- 5. Configure the following parameters to match the user's desk phone configuration:
- Device Pool
- Phone Button Template: Standard Dual Mode for Android
- Calling Search Space
- Owner User ID: <username of the phone>



- 6. Scroll down to the Protocol Specific Information section.
- 7. Select Cisco Dual Mode for Android Standard SIP Non-Secure Profile from the Device Security Profile drop-down list
- 8. Select Standard SIP Profile Android from the SIP Profile drop-down list.
- **9.** Select the *<username* for the phone> from the Digest User drop-down list.



On Association Information, must be associate with a number extension and finally with the End User.



## **Configure CUPS Connectivity to CUCM**

## **Access the CUPS Web Administration Page**

- 1. Open a browser and enter the URL of the Presence Server. It will be in the format of https://<cups-ip-address>/cupadmin
- 2. Log in using the application administration username and password, This username and password were created during the installation of the CUPS operating system.
- 3. Provide the host name and IP address of the CUCM Publisher.
- 4. Click Next. The next screen allows the entry of the AXL.



- 5. Enter the username (AXL\_Admin) and password (cisco) of the AXL user created.
- 6. Click Next.

Assuming successful validation of the AXL user information, the wizard progresses to the Security Password Configuration entry. This security password must match that which was configured on the CUCM Publisher upon its initial installation. The security password is necessary to provide synchronization access to the Publisher for outside applications, even its own cluster subscribers.

- 7. Enter the security password in each field, and then click Next.
- 8. Finally, you arrive at the wizard's confirmation screen. It will present the information you've entered for validation.
- a. If all is well, click Confirm.
- b. If not, click Back and alter any necessary entries.
- 9. Upon confirmation, the post install wizard is complete. Click the Home button to access the CUPS administration page.

### **Activate Services**

By default, all services are deactivated on the Presence Server.

- 1. From the CUPS Administration page, click the Navigation drop-down list in the upper-right corner of the screen and select Cisco Unified IM and Presence Serviceability.
- 2. Click Go.
- 3. Navigate to **Tools** > **Service Activation** to see the status of all services. Note the Activation Status column. All services should show as Deactivated.
- 4. The most efficient way to get all services going is to select the Check All Service check box near the top of the screen.
- 5. Click Save.



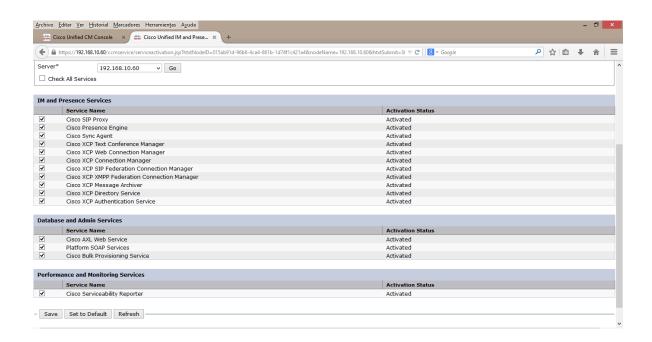
Copyright © 1999 - 2012 Cisco Systems, Inc. All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encrypton. Importers, exporter, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified CM IM and Presence please visit our <u>IM and Presence Documentation</u> web site.

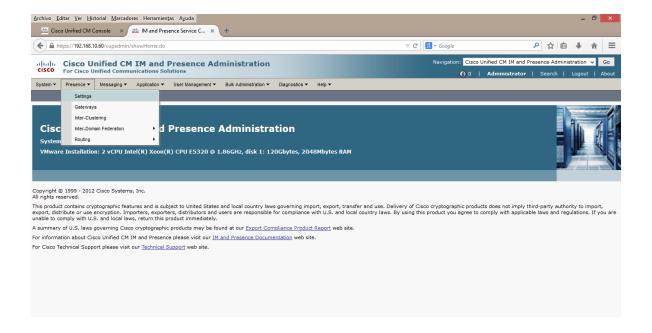
For Cisco Technical Support please visit our Technical Support web site.

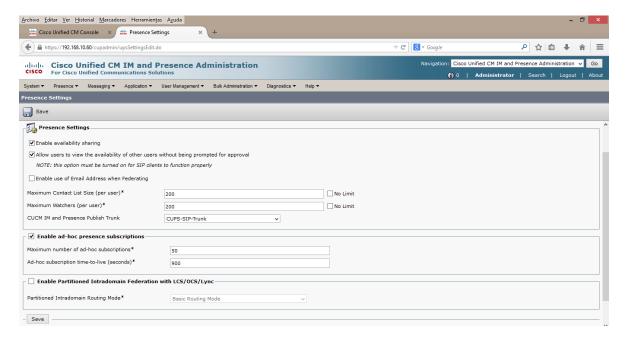


## Add a Presence Gateway

Return to the Cisco Unified CM IM and Presence Administration page

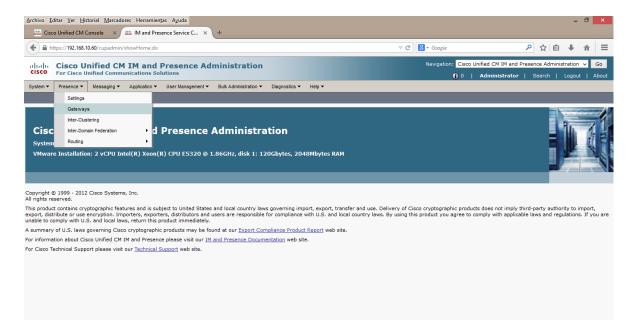
- 1. Navigate to Presence > Settings
- 2. Verify that CUPS-SIP-Trunk (created in CUCM) is selected in the CUCM SIP Publish Trunk drop-down list.
- 3. Leave the other parameters on this screen at their default settings.
- 4. Click Save.



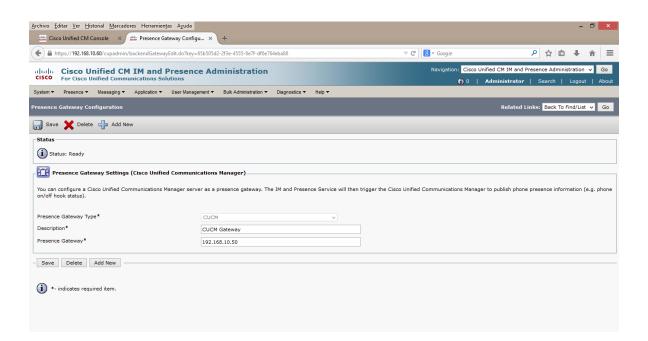


### Add CUCM as a Presence Gateway

- 1. Navigate to Presence > Gateways.
- 2. Click Add New.

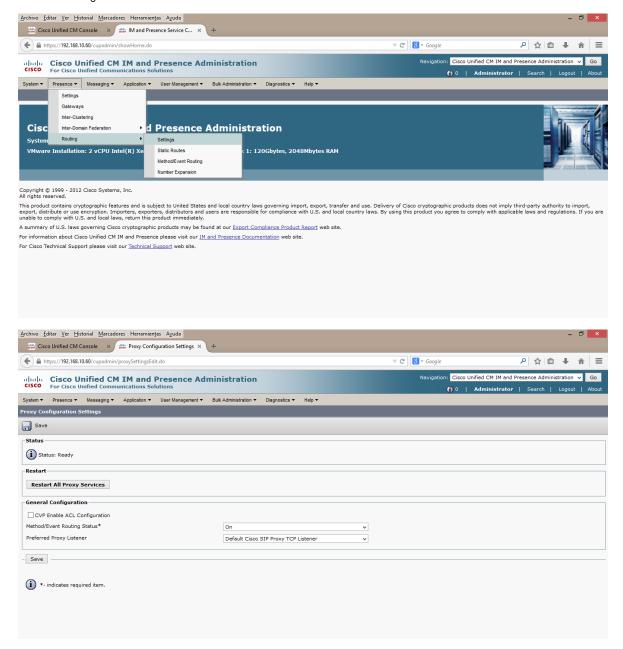


- 3. Leave the Presence Gateway Type field default to CUCM.
- 4. Enter a description.
- 5. Enter the Publisher's CUCM IP address
- 6. Click Save.

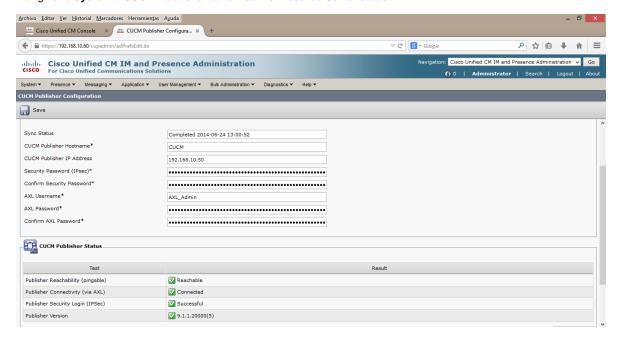


## **Add Proxy Configuration**

- 1. Navigate to Presence > Routing > Settings
- 2. On General Information section, drop-down list, and select ON
- 3. Select drop-down list, Default Cisco SIP Proxy TCP Listener
- 4. Click save.
- 5. Click on Restart All Proxy Services
- 6. Click Save again.



Navigate to **System > CUCM Publisher** to verified the Presence Server status.

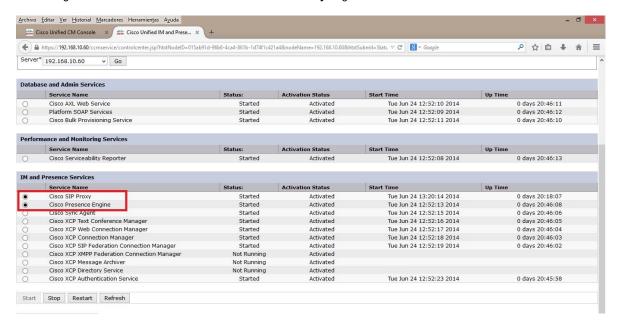


## **Cluster Topology**

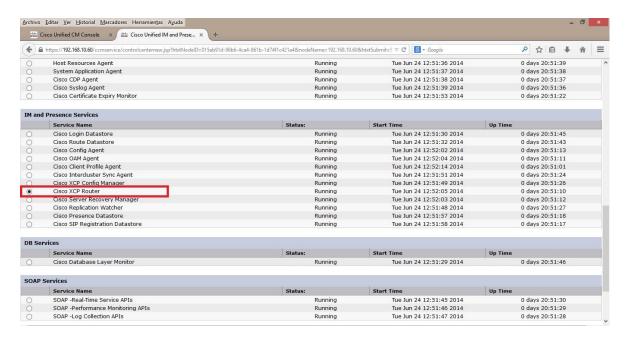
### **Change Domain Name**

- 1. Navigate to System > Cluster Topology.
- 2. Click on Settings.

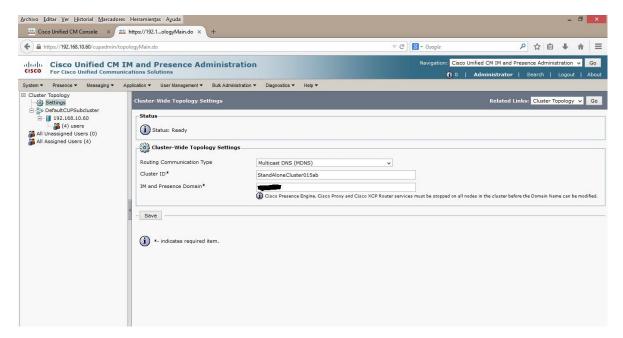
First must be stopped some services, Cisco UP Presence Engine, Cisco UP Proxy and Cisco UP XCP Router services. Let's Navigate to Cisco Unified IM and Presence Serviceability Page. Tools > Service Activation



#### Cisco UP XCP Router is located under Tools > Control Center -Network Services

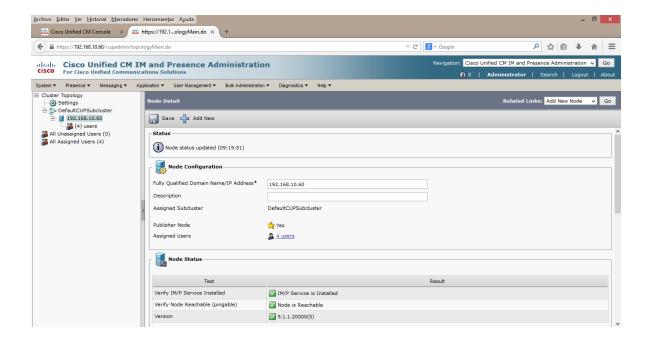


- 2. Change IM and Presence Domain.
- 3. Click Save.
- 4. Restart the Services.

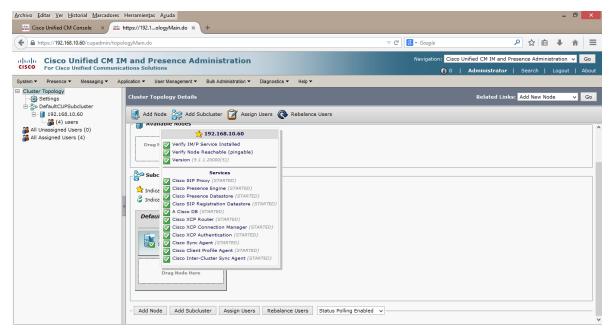


## Change Hostname to IP address

- 1. Navigate to System > Cluster Topology.
- 2. Click on Hostname Presence Server,
- 3. Change the Hostname to IP address of Presence Server
- 4. Click save.

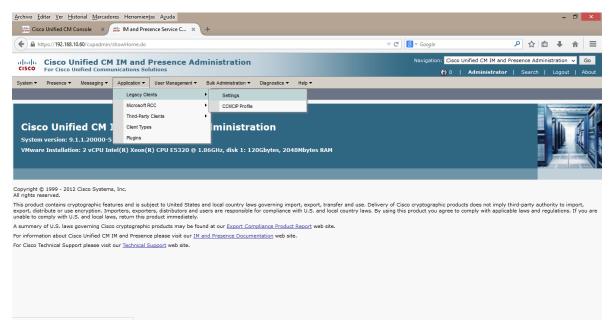


On Cluster Topology details check all services must be active and green.

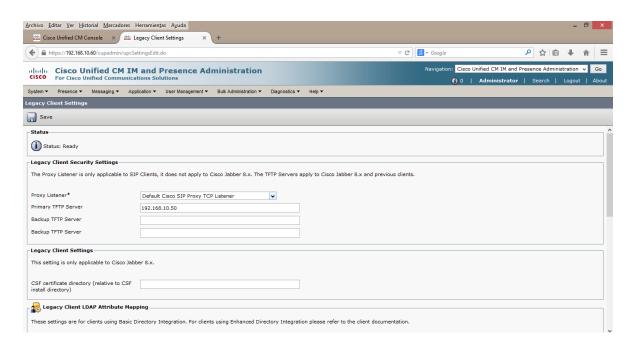


### **Configure Presence Jabber Settings**

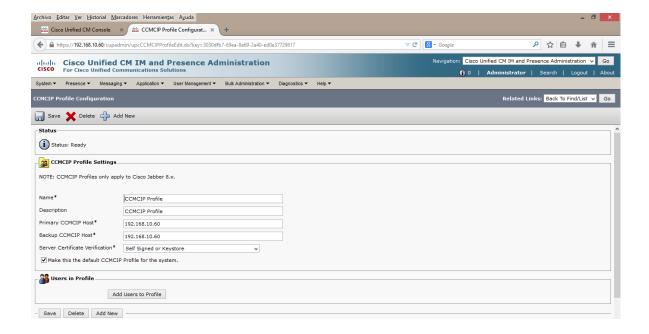
- 1. Navigate to Application > Legacy clients > Settings.
- 2. On Proxy Listener , Select Default Cisco SIP Proxy TCP Listener



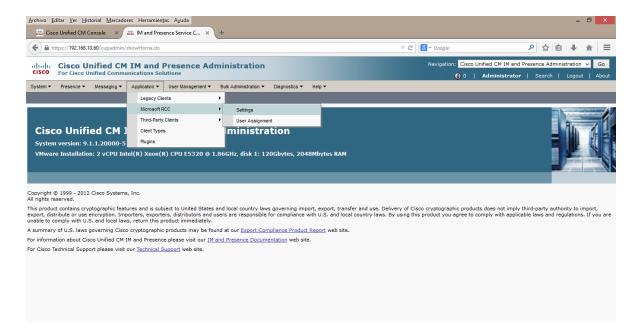
- 3. Primary TFTP Server is the IP of CUCM .
- 4. Click save.

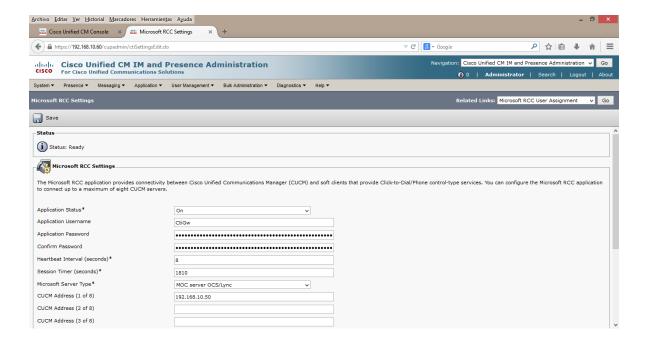


- 1. Navigate to Application > Legacy clients > CCMCIP Profile.
- 2. Click Add New.
- 3. Enter a name Profile for the Name field. And Description.
- 4. On Primary CCMCIP and Backup Host, enter the IP address of Presence Server.
- 5. Select the check box, Make this the default CCMCIP Profile for the system.
- 6. Click Save.

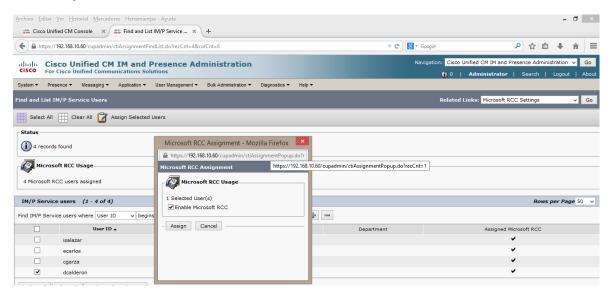


- 1. Navigate to Application > Microsoft RCC> Settings.
- 2. Select ON,
- 3. Enter CtiGw on Application Username,
- 4. Enter the password (cisco, previously configured on CUCM)
- 5. On CUCM Address field, enter the IP of CUCM.
- 6. Click Save.





- 1. Navigate to Application > Microsoft RCC> User Assignment.
- 2. click **Find** in the pop-up window that appears.
- 3. Select the users to control CTI phone.
- 6. Click Assign.



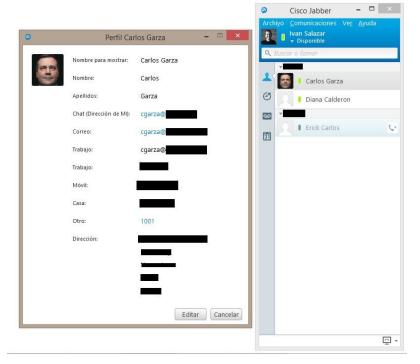
## **Configure Jabber Windows**

Install Jabber version 9.7, CiscoJabber-Install-ffr.9-7-0

- 1. Enter username and Click Continue.
- 2. Click, Configure Login
- 3. Select Cisco IM&Presence, click on Server Address, enter Presence Server IP address and Save
- 4. Enter your password and click Login







The UC Services previously configured, automatically allow synchronized all services, LDAP for contact search, CUCM for calls, Instant Messages, Voice Mail, CTI Control, WebEx profile, Mail Store. All user information is synchronized with the Active Directory like Address, Phone, E-mail, and Profile Picture.

http://www.cisco.com/c/en/us/td/docs/voice\_ip\_comm/jabber/Windows/9\_7/JABW\_BK\_C4C679C9\_00\_cisco-jabber-for-windows-97/JABW\_BK\_C4C679C9\_00\_cisco-jabber-for-windows-97\_chapter\_0111.html

#### Add User Profile Picture.

To upload a picture can use this software, AD Photo Edit Free Edition,

Scanned all Domain of your Active Directory, find the users and change the Photo Attribute: thumbnailPhoto . can upload , resizing and export pictures.

## **Configure Jabber Android**

#### Create xml file.

This file is for Non-Windows platforms, like Android and IPhone. Synchronized the values of the Active Directory, Address, Phone, E-mail, and Profile Picture.

Open a new Notepad and paste this configuration, and save as: jabber-config.xml

## **Example:**

<?xml version="1.0" encoding="UTF-8"?> <config version="1.0"> <!-- LDAP Directory configuration for non-Windows platform clients --> <Directory> <DirectoryServerType>BDI</DirectoryServerType> <BDIPhotoURISubstitutionEnabled>True</BDIPhotoURISubstitutionEnabled> <BDIPhotoURISubstitutionToken>sAMAccountName</BDIPhotoURISubstitutionToken> <BDIPhotoURIWithToken>http://192.168.10.109/sAMAccountName.jpg</BDIPhotoURIWithToken> <BDIOtherPhone>ipPhone</BDIOtherPhone> <BDIEmailAddress>mail</BDIEmailAddress> <BDIPresenceDomain>My Domain</BDIPresenceDomain> <BDILDAPServerType>AD</BDILDAPServerType> <BDIPrimaryServerName>192.168.10.109</BDIPrimaryServerName> <BDIServerPort1>389</BDIServerPort1> <BDISearchBase1>ou=Domain Controllers,dc=example,dc=net</BDISearchBase1> <BDIConnectionUserDN>CUCMLDAP@example.net</BDIConnectionUserDN> <BDIConnectionPassword>password</BDIConnectionPassword> <OtherPhone>ipPhone</OtherPhone> </Directory> </config>

192.168.10.109 = IP of my Active Directory

ou=Domain Controllers,dc=example,dc=net = OU where are the end users

**CUCMLDAP@example.net** = User of Active Directory to synchronizer users

http://192.168.10.109/sAMAccountName.jpg = is the addess of contact photos, must be create a web server and storage the profile pictures, with the Active Directory name, for example =cgarza.jpg, ensure that you can view the picture in a web browser.

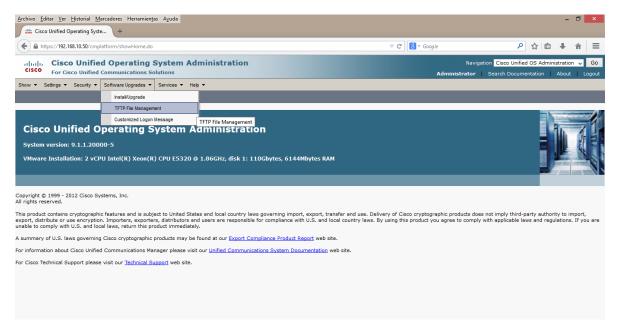


http://www.cisco.com/c/en/us/td/docs/voice\_ip\_comm/jabber/Android/9\_6/JABA\_BK\_J0A7146D\_00\_jabber-android-install-config-9-6/JABA\_BK\_J0A7146D\_00\_jabber-android-install-config-9-6\_chapter\_0110.html#CJAB\_RF\_C3A1DB71\_00\_

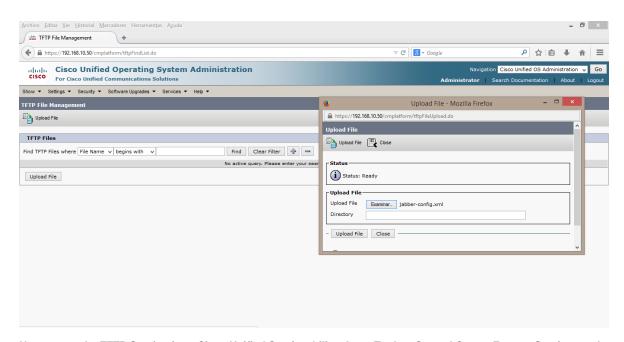
## Upload jabber-config.xml File.

For upload the file

- 1. Go to Cisco Unified OS Administration
- 2. Software Upgrades > TFTP File Management



- 3. Select Upload File button.
- 4. Search for the jabber-config.xml file.
- 5. Directory leave by default.
- 6. Click Upload File.



Now restart the TFTP Service from Cisco Unified Serviceability. Go to Tools > Control Center-Feature Services and restart TFTP.

Install Jabber version 9.6.1 .apk download from Google PlayStore.

- 1. Enter username and Click Continue.
- 2. Click, Configure Login
- 3. Select CUCM IM and Presence.
- 4. Enter your username and password, Presence Server IP address, and click Login.

