



PatientTouch[®] Communications Set-up Guide for Cisco Unified Call Manager (CUCM)

July 2020

Table of Contents

PatientTouch® Communications Set-up Guide for Cisco Unified Call Manager (CUCM)	. 1
Overview	2
Requirements	2
DNS Setup	3
CUCM Setup	3
Login to CUCM	4
Enable AXL on CUCM	6
Enter AXL Data in Enterprise Manager	11
CUCM Settings	13
Route Partition & Calling Search Space	13
Enterprise Manager Properties	16
Device Pool	18
SIP Security Profile	21
Enterprise Manager Settings	22
SIP Profile	24
SIP Domain	27
Call History	30
Hunt Groups	33
Create New Voice System in Enterprise Manager	40
Appendix	44
Authentication	44
Fully Qualified Domain Name	45
Licensing	47

©2020 PatientSafe Solutions, Inc. All rights reserved.

CUCM Setup Guide 4.8 UG-CUCM Rev A

July 2020

Reproduction in any manner whatsoever without the written permission of PatientSafe Solutions, Inc. is strictly prohibited. Changes in equipment, software, or procedures may occur periodically; information describing these changes will be included in future editions of this document.

Information in this document is subject to change without notice and does not represent a commitment on the part of PatientSafe Solutions to provide additional services or enhancements.

All patient names and medical histories depicted in these materials are fictitious. Any resemblance to an actual person or case is purely coincidental. All drugs, drug orders, and dosages depicted in screen shots, videos, diagrams, or other media are for illustrative purposes only. PatientSafe Solutions, Inc. makes no recommendation or representation about any treatment or dosage. These materials are subject to revision by PatientSafe Solutions, Inc. from time to time, at any time.

PatientTouch is a registered trademark of PatientSafe Solutions, Inc. Other product or company names are the trademarks and/or registered trademarks of their respective owners.

PatientSafe Solutions, Inc.

9330 Scranton Rd. Suite #325

San Diego, CA 92121

Phone: (858) 746-3100

Fax: (858) 746-3101

www.patientsafesolutions.com

PatientTouch® Communications Set-up Guide for Cisco Unified Call Manager (CUCM)

The purpose of this document is to provide the step-by-step instructions on how to configure Cisco Unified Call Manager (CUCM) for integration with PatientTouch Communications. The target audience for this document is CUCM administrators/technicians.

To setup the CUCM, you will need to follow all of the instructions listed below. Click a link to access a topic or use your mouse to scroll through the pages.

[Login to CUCM and Enable AXL](#)

[CUCM Settings](#)

[Device Pool](#)

[SIP Security Profile](#)

[SIP Profile](#)

[SIP Domain](#)

[Call History](#)

[Hunt Groups](#)

[Create New Voice Settings in Enterprise Manager](#)

[Appendix](#)

Overview

The PatientTouch App for iOS can register with Cisco Unified Call Manager (CUCM) for making voice calls. The PatientTouch app connects to CUCM using the SIP protocol. Users can be assigned extensions in the Enterprise Manager web app, via auto provisioning or via LDAP using Org Services integration.

Org Services uses AXL (Cisco's Administrative XML Rest Interface for CUCM) to provision devices and extensions for each user in CUCM.

PatientTouch communicates with Org Services, an internal PatientTouch service. Org Services then communicates with Active Directory (AD) and CUCM to manage user extensions.

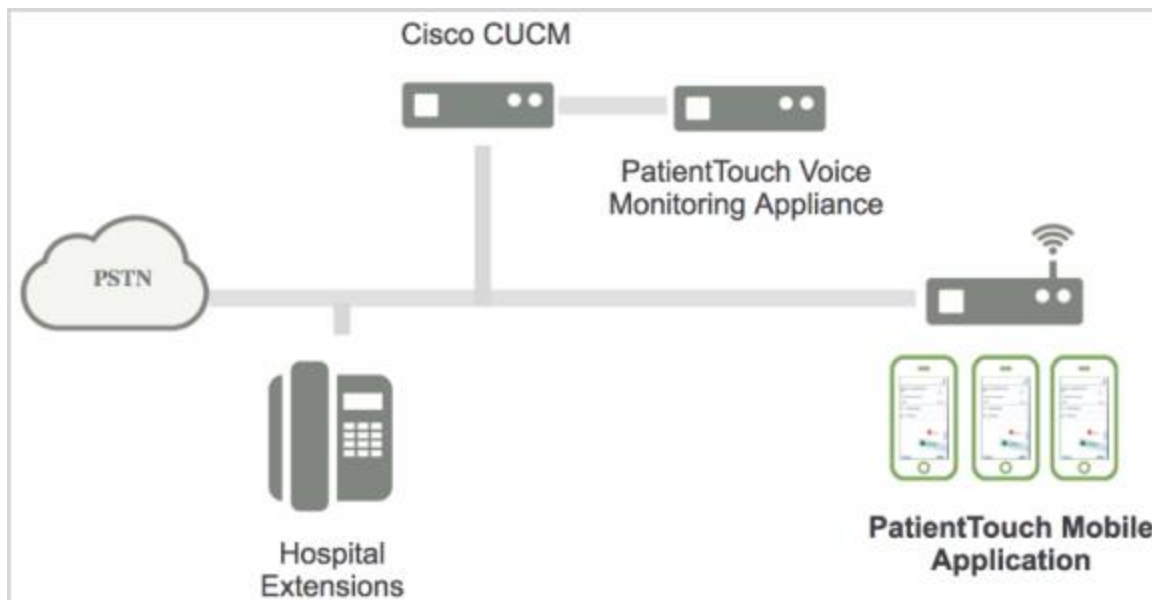
There are two ways that extensions can sync between PatientTouch and CUCM. This is dependent on whether or not the organization has enabled AD Sync.

If the organization has AD Sync enabled, extensions will sync periodically, as configured, and update the user profile in PatientTouch.

If the organization does not have AD sync enabled, when the user logs into a Patient Touch handheld with AD credentials, Org Services will query AD for user profile and extension information. Org Services will then send an AXL request to CUCM to provision a device and extension directory number (DN).

Similarly, when an extension is assigned via Enterprise Manager, Org Services will provision the device and extension information in CUCM on login.

This allows Patient Touch devices to connect automatically to CUCM as SIP devices.



Requirements

- Cisco Unified Call Manager 9.1 or greater.
- A Cisco license for each PatientTouch device that will connect to the network is required. PSS devices connect to CUCM as a "3rd Party Basic SIP" device. If your licenses are of the type "User Connect Licensing", each device will require one "Enhanced" license. If your licenses are of the type "Unified Workspace Licensing", you may utilize either a "Standard" or "Professional" license.

DNS Setup

The PatientTouch handheld app uses SRV records to locate CUCM subscribers to connect to. A domain is configured in the app and the app will query VOIP SRV records for this domain. Here is an example SRV setup for the 'test.pss.net' domain:

```
_pssvoip._udp.test.pss.net 0 0 5060 cucm.node1.pss.net  
_pssvoip._udp.test.pss.net 0 0 5060 cucm.node2.pss.net  
_pssvoip._udp.test.pss.net 0 0 5060 cucm.node3.pss.net
```

The PatientTouch app will round robin between the SRV records until a connection can be made. The CUCM subscribers can also be given a priority in the SRV. The PatientTouch app will try subscribers with a priority of '0' first, then '1', '2', etc. Load balancing can be achieved by adding multiple servers at the same priority.

CUCM Setup

The following CUCM configuration will be required (detailed in later sections):


- AXL Service Enabled (Cisco's Administrative XML REST interface for CUCM)
 - A valid AXL user account is required, to allow Org Services to provision PatientTouch devices.
- A new 'SIP Profile' for making changes specific to PatientTouch devices.
- A new 'Device Pool' for easy management and tracking of PatientTouch devices.
- (Optional) A new Calling Search space for managing how calls are routed from patient touch devices.
- A 'Route Partition' for sectioning off PatientTouch extensions. Only numbers and devices assigned to numbers in this partition will be modified by PatientTouch.
- A new SIP Security Profile for making SIP security changes specific to PatientTouch devices.
- Enable CDR reporting so PatientTouch devices can get call history, even for calls made while the device is offline.
 - Add PatientTouch server ips (VIP) as a CDR Billing Application Server

Login to CUCM

1. Click Cisco Unified Communications Manager.



2. Enter your Username and Password.
3. Click **Login**.



Cisco Unified CM Administration


For Cisco Unified Communications Solutions

Navigation **Cisco Unified CM Administration** Go

Cisco Unified CM Administration

Username

Password



Copyright © 1999 - 2015 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 encryption. Importers, exporters, 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 Communications Manager please visit our [Unified Communications System Documentation](#) web site.

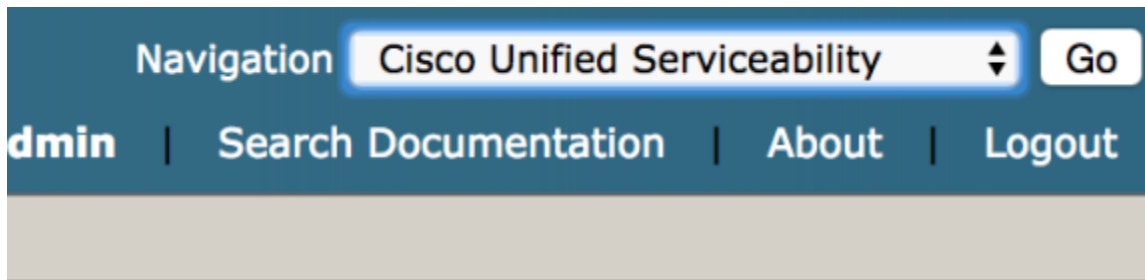
For Cisco Technical Support please visit our [Technical Support](#) web site.

Enable AXL on CUCM

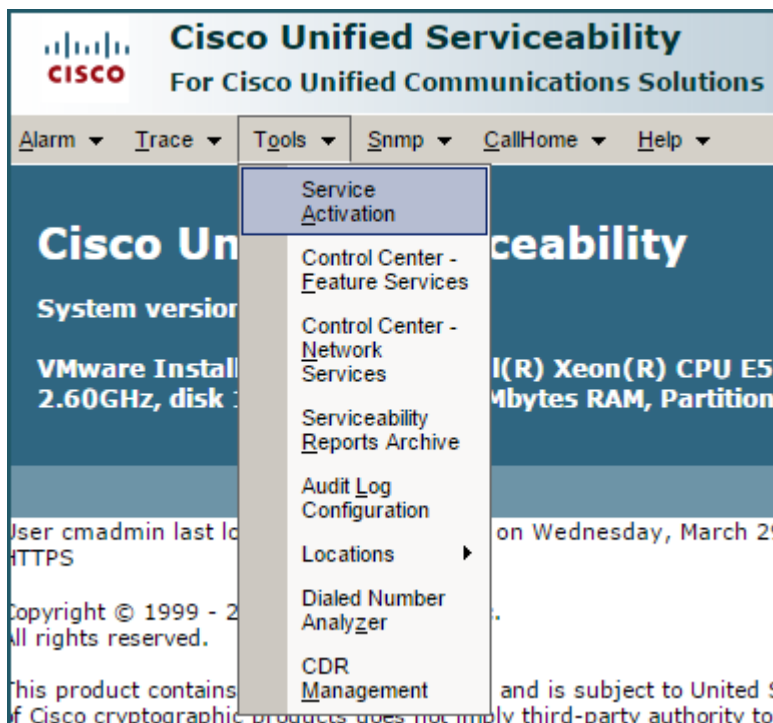
Org Services uses AXL to connect to CUCM and manage the per device SIP settings.

Enable AXL service in Service Availability:

1. In the Navigation drop down menu on the top right of the screen, select Cisco Unified Serviceability.
2. Click **Go**.



3. Select Tools>Service Activation to view the list of enabled services.



4. Select the Cisco AXL Web Service check box.
5. Click **Apply**.

Database and Admin Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco Bulk Provisioning Service	Deactivated
<input checked="" type="checkbox"/>	Cisco AXL Web Service	Activated
<input type="checkbox"/>	Cisco UXL Web Service	Deactivated
<input type="checkbox"/>	Cisco TAPS Service	Deactivated

Next you will need to add an Application User to allow PatientTouch CUCM-Sync to communicate (over AXL) to CUCM. This username and password will be entered in Enterprise Manager later.

- Go back to the Cisco Unified CM Administration using the drop down menu located on the top right of the screen.

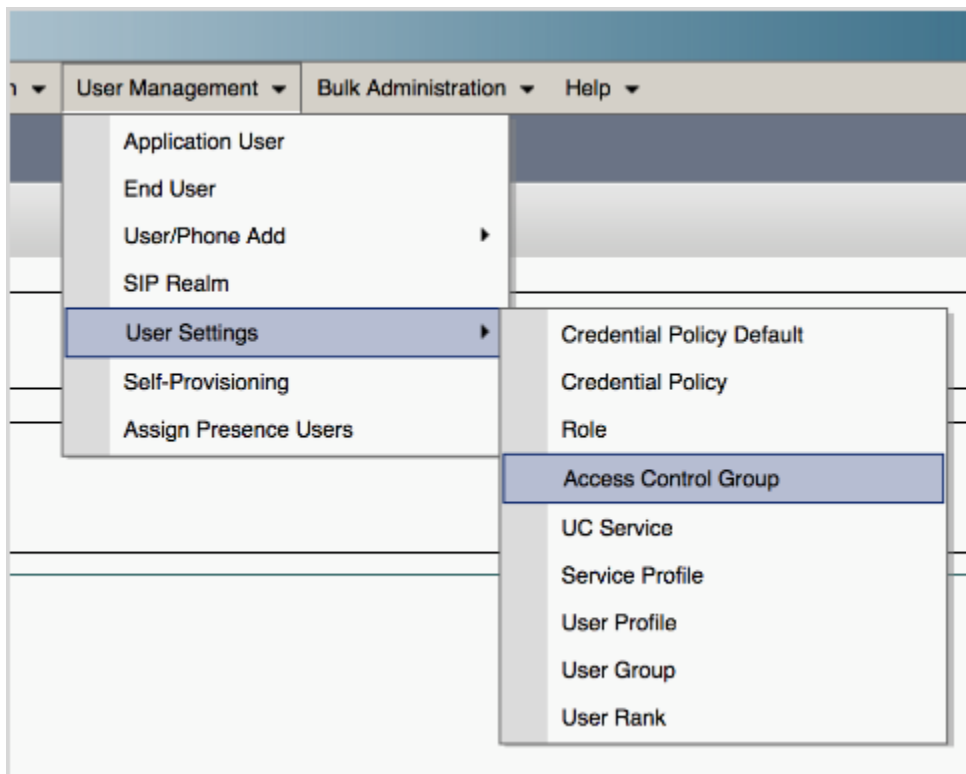
Make sure to click **Go**.

- Select User Management>Application User.

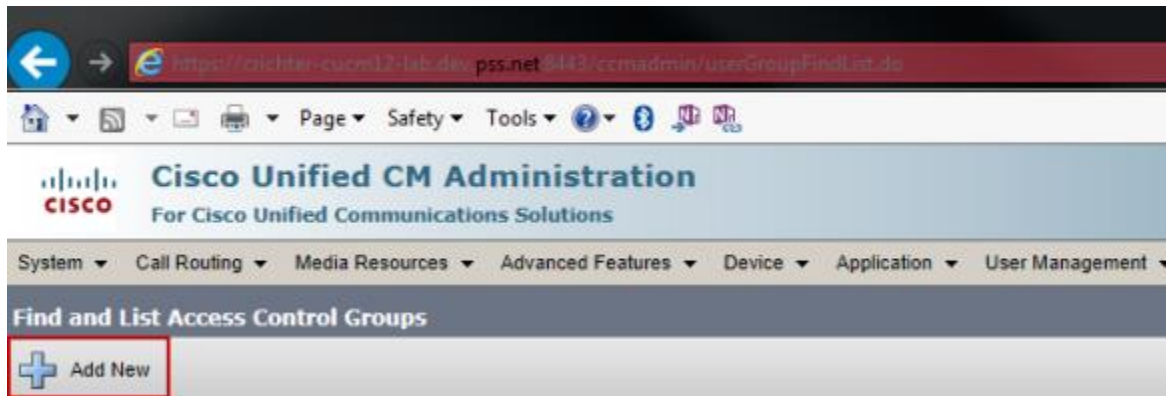


- Add the 'Standard AXL API Access' Role to the user. Roles are granted to CUCM Users by adding 'Access Control Groups'. See below for how to create a more restrictive Access Control Group.
- A more restrictive Access Control Group for PatientTouch can be created and added to the Application User. Create a new 'Access Control Group':

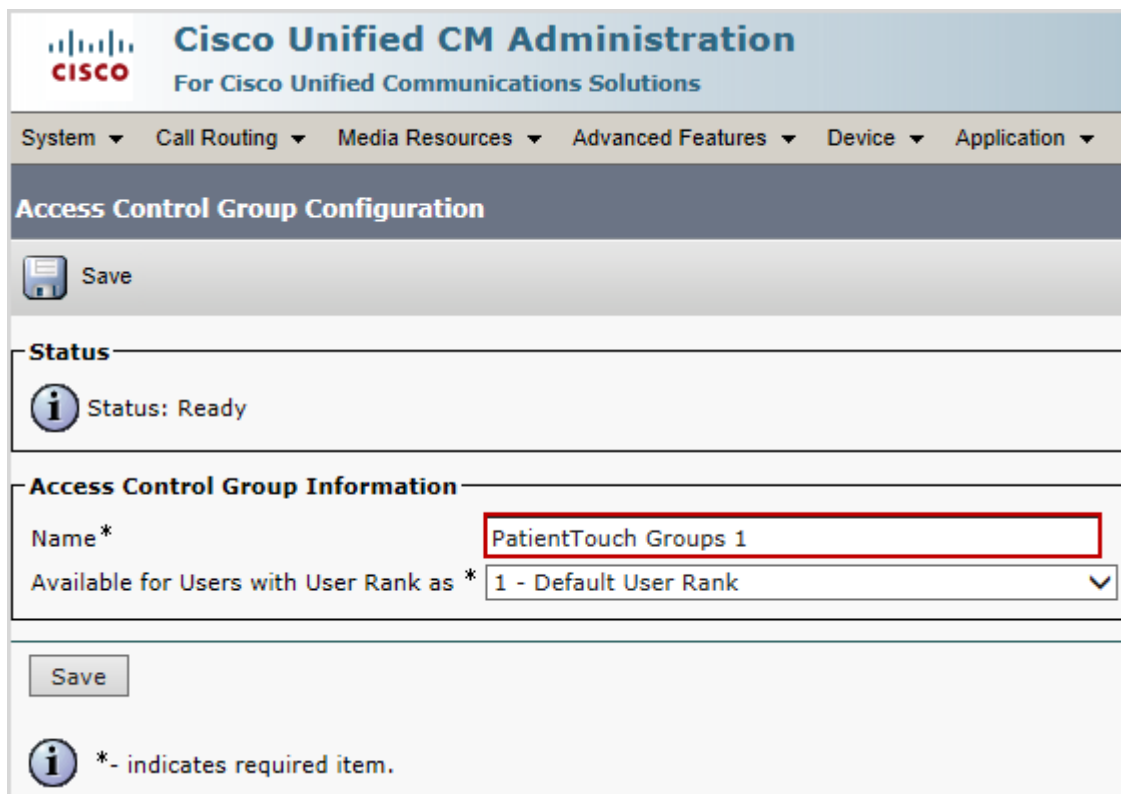
- Click **User Management>User Settings>Access Control Group**



- Click **Add New**



- Enter the Access Control Group Name
- Click **Save**


 This screenshot shows the "Access Control Group Configuration" page. At the top, there is a "Save" button. Below it, the "Status" section shows "Status: Ready" with an information icon. The "Access Control Group Information" section contains two fields: "Name*" with the value "PatientTouch Groups 1" (highlighted by a red box) and "Available for Users with User Rank as*" with a dropdown menu set to "1 - Default User Rank". At the bottom of this section, there is another "Save" button and a note: "*- indicates required item."

- Select Assign Role to Access Control Group from the drop down menu on the top right of the screen.
- Click **Go**

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Access Control Group Configuration Related Links: [Assign Role to Access Control Group](#)

Status
Add successful

Access Control Group Information
Name*
Available for Users with User Rank as*


User Rows per Page: 50

Find User where

No active query. Please enter your search criteria using the options above.


*. indicates required item


- Click Assign Role to Group


Cisco Unified CM Administration
 For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ Us

Access Control Group Configuration

 Save

Status
 Status: Ready

Access Control Group Information
 Name* PatientTouch Group 4

Role Assignment

Role <input style="width: 90%; height: 30px;" type="text"/>	<div style="border: 2px solid red; display: inline-block; padding: 2px 10px; margin-bottom: 5px;">Assign Role to Group</div> <div style="border: 1px solid #ccc; display: inline-block; padding: 2px 10px;">Delete Role Assignment</div>
---	---


- When you click Assign Role to Group, the window below should display. However, you may need to click **Find** in order to see the list of roles.

- Click the following roles and then click **Add Selected**

- Standard AXL API Access
- Standard Admin Rep Tool Admin
- Standard Audit Log Administration
- Standard CCM Admin Users
- Standard CCM Admin Administration









Find and List Roles

Select All Clear All **Add Selected** Close

Status
 50 records found

Role (1 - 50 of 50) Rows per Page 50

Find Role where Name begins with Find Clear Filter + -
 Select item or enter search text

<input type="checkbox"/>	Name ^	Application	Description	Copy
<input checked="" type="checkbox"/>	Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs	
<input type="checkbox"/>	Standard AXL API Users		All users with access to AXL APIs	
<input type="checkbox"/>	Standard AXL Read Only API Access	Cisco Call Manager AXL Database Read Only	Access the AXL Read Only APIs	
<input checked="" type="checkbox"/>	Standard Admin Rep Tool Admin		Administer CAR	
<input checked="" type="checkbox"/>	Standard Audit Log Administration	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	
<input checked="" type="checkbox"/>	Standard CCM Admin Users		All users with access to CCM web site	
<input type="checkbox"/>	Standard CCM End Users		Access to CCM User Option Pages	
<input type="checkbox"/>	Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	

Enter AXL Data in Enterprise Manager

Under Voice Systems, go to Properties and update the following properties:

1. Enter AXL Username and AXL Password for the user on the server you are setting up.
2. Enter AXL URL as the URL to the AXL API of the cluster: 'https://<cluster_hostname>:8443/axl/'. The host is normally just the 'SIP Server' one you entered above but can be any hostname that resolves to a server or multiple servers on the cluster.

Blue Hospital

User Admin

- Dashboard
- Assignment
- Configuration
- Settings**

Logout

Voice Systems

Affiliated Facilities

Facility ↑	DNS Mapping
No affiliated facilities	

Delete Edit Add

Properties

Name ↑	Value
AXL Password	
AXL URL	
AXL Username	
AXL Version	9.0
Call Forward CSS	
Calling Search Space	pss-css
Cluster Name	

Back Delete Fix Extensions Save

CUCM Settings

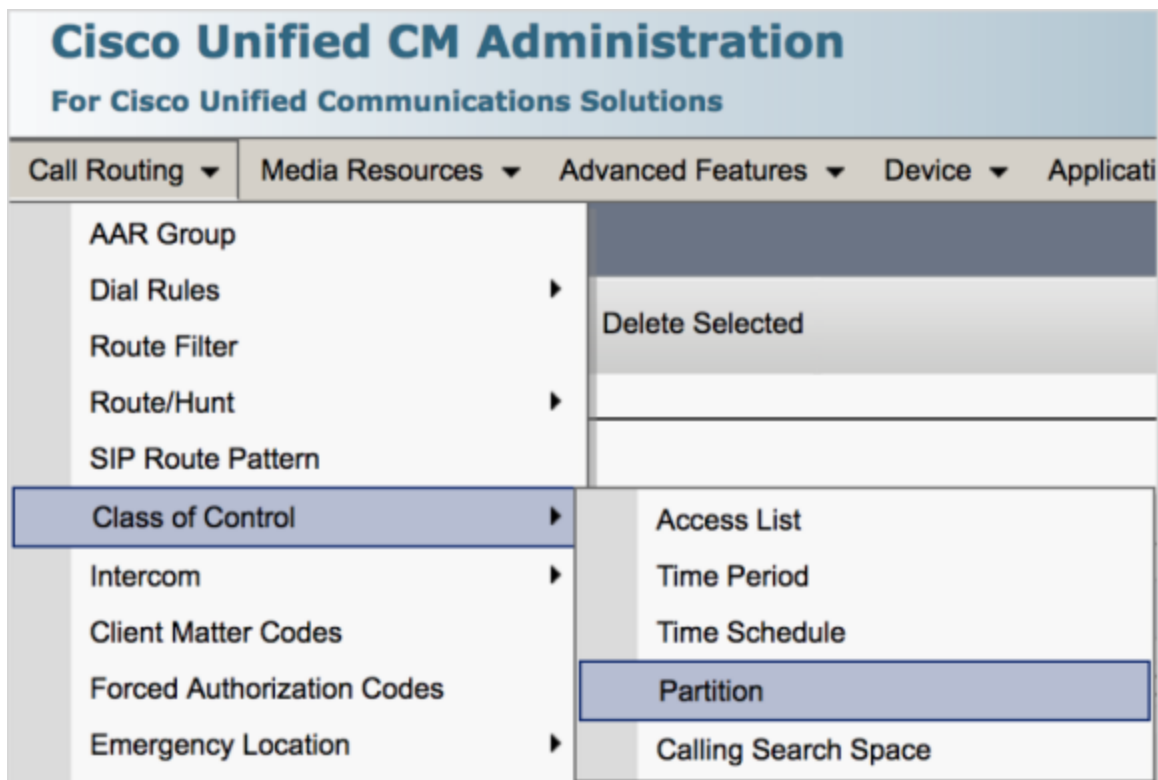
The following have to be configured on the CUCM server and the corresponding properties updated in Enterprise Manager> Voice Systems.

Route Partition & Calling Search Space

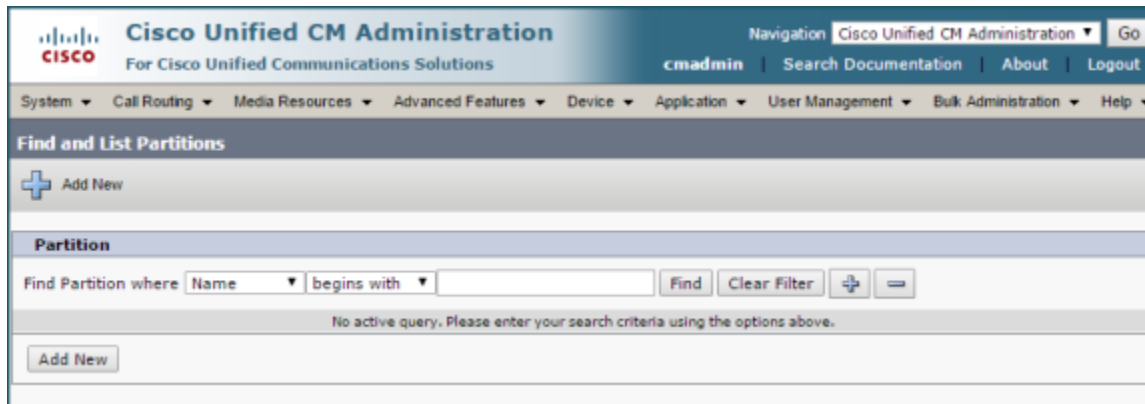
To enable custom call routing for PatientTouch devices, a new Route Partition and a new Calling Search Space specific to PSS devices are required. In addition to call routing, the Route Partition is also used to determine calls made by PatientTouch devices as part of the Call History feature.

Jot down the 'Route Partition' and 'Calling Search Space' names, these will need to be entered in Enterprise Manager under the Voice System Properties.

1. Select Call Routing>Class of Control>Partition.

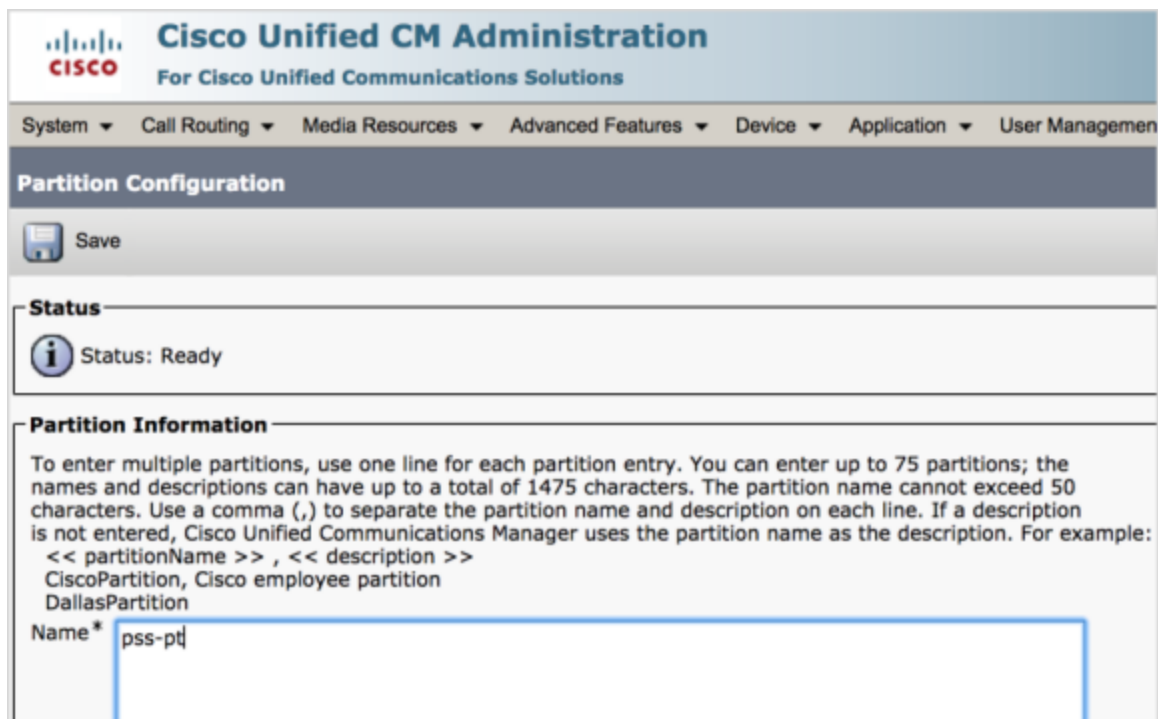


2. Click Add New.



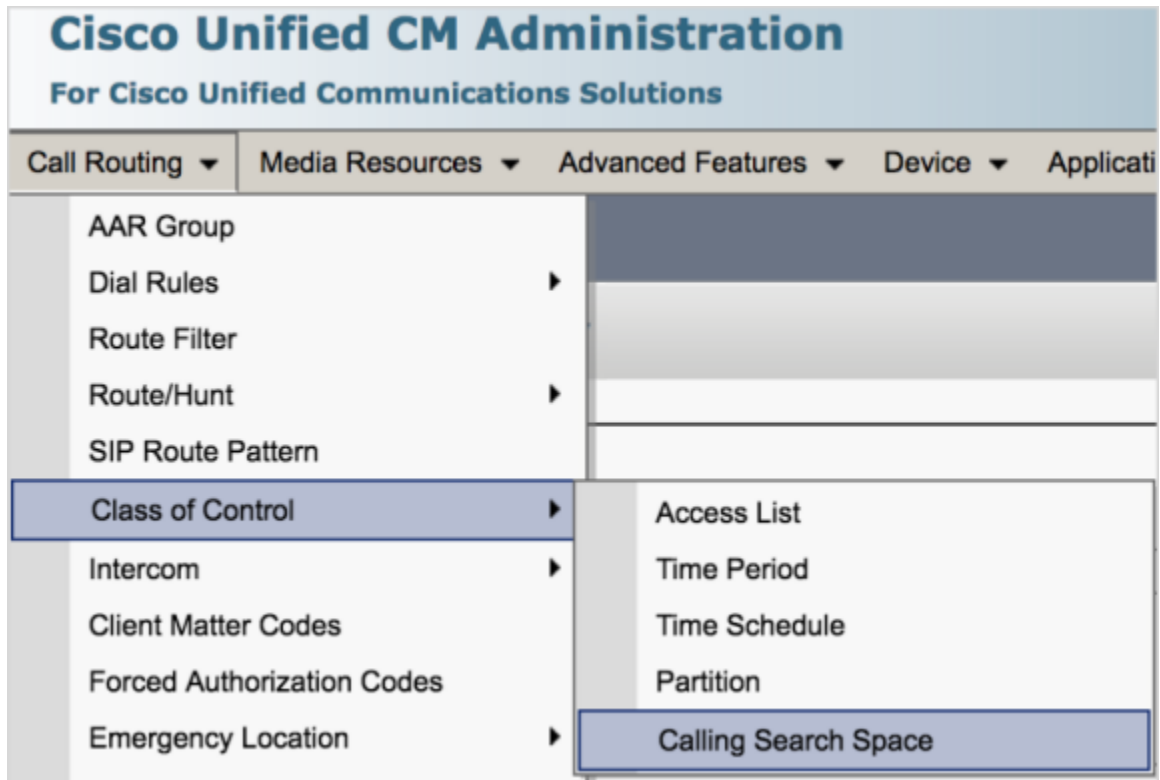
The screenshot shows the 'Find and List Partitions' page in Cisco Unified CM Administration. The page has a navigation bar with 'Cisco Unified CM Administration' and 'Go' buttons. Below the navigation bar, there are several menu items: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled 'Find and List Partitions' and includes an 'Add New' button. Below this, there is a search section with a 'Find Partition where' label, a dropdown menu for 'Name', a dropdown menu for 'begins with', a text input field, and buttons for 'Find', 'Clear Filter', and navigation arrows. A message below the search section reads: 'No active query. Please enter your search criteria using the options above.' At the bottom of the search section, there is another 'Add New' button.

3. Enter the Partition name.
4. Click **Save**.

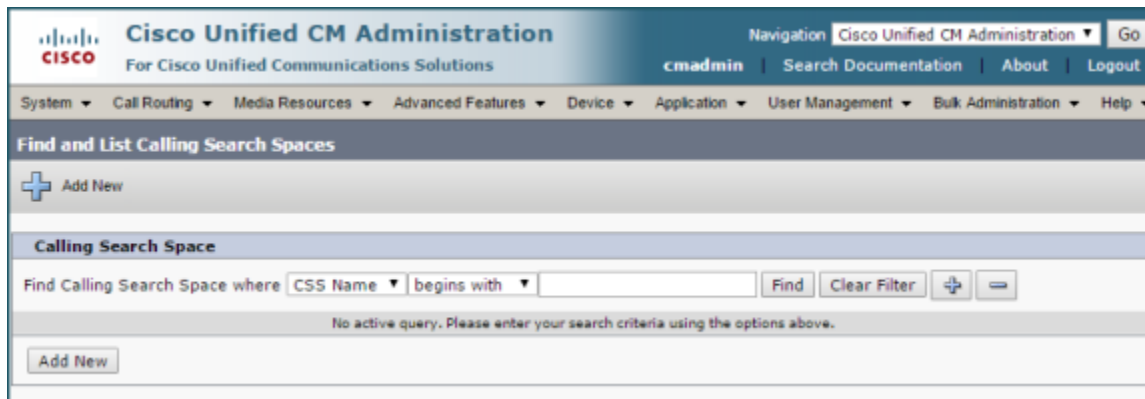


The screenshot shows the 'Partition Configuration' page in Cisco Unified CM Administration. The page has a navigation bar with 'Cisco Unified CM Administration' and 'Go' buttons. Below the navigation bar, there are several menu items: System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. The main content area is titled 'Partition Configuration' and includes a 'Save' button. Below this, there is a 'Status' section with an information icon and the text 'Status: Ready'. Below the status section, there is a 'Partition Information' section with a text area containing instructions: 'To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (,) to separate the partition name and description on each line. If a description is not entered, Cisco Unified Communications Manager uses the partition name as the description. For example: << partitionName >> , << description >> CiscoPartition, Cisco employee partition DallasPartition'. Below the instructions, there is a text input field labeled 'Name*' with the text 'pss-pt' entered.

5. Select Call Routing>Class of Control>Calling Search Space.







6. Click Add New.




7. Enter a Name.
8. Click Save.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manage

Calling Search Space Configuration

 Save
  Delete
  Copy
  Add New

Status

 Status: Ready

Calling Search Space Information

Name*

Description

Route Partitions for this Calling Search Space

Available Partitions**

- Directory URI
- Global Learned E164 Numbers
- Global Learned E164 Patterns
- Global Learned Enterprise Numbers
- Global Learned Enterprise Patterns

▼ ▲

Selected Partitions

▼ ▲

- Write down the 'Route Partition' and 'Calling Search Space' names as these will need to be entered in Enterprise Manager under the Voice System Properties.

Enterprise Manager Properties

Enter the Partition and Calling Search Space in Enterprise Manager under Voice Systems>Properties.

Properties	
Name	
Allow Create Users	false
AXL Password	*****
AXL URL	https://<your CUCM host>:8443/axl/
AXL Username	pssaxluser
AXL Version	9.0
Calling Search Space	pss-css
Device Pool	PSS Device Pool
Device Type	Third-party SIP Device (Basic)
Digest Password	*****
Digest Realm	ccmsipline
Route Partition	pss-pt
Sip Profile	PSS Sip Profile
Sip Security Profile	PSS Security Profile
User Prefix	

Device Pool

A separate Device Pool should be used for each CUCM Voice Setting in Enterprise Manager. The Device Pool is how Org Services knows where to find PatientTouch devices in CUCM. Take note of the name used for the Device Pool, this will be entered into Enterprise Manager later.

To allow multiple Voice Settings for the same CUCM cluster from a multi-facility installation of Org Services, each facility will have a single Voice Setting, that will have its own device pool and calling search space. A separate calling search space is necessary for each facility so that 0, 911, etc., can be routed. Separate Device Pools are needed to allow for different routing and Caller ID transforms mask (among other settings that may be optionally used).

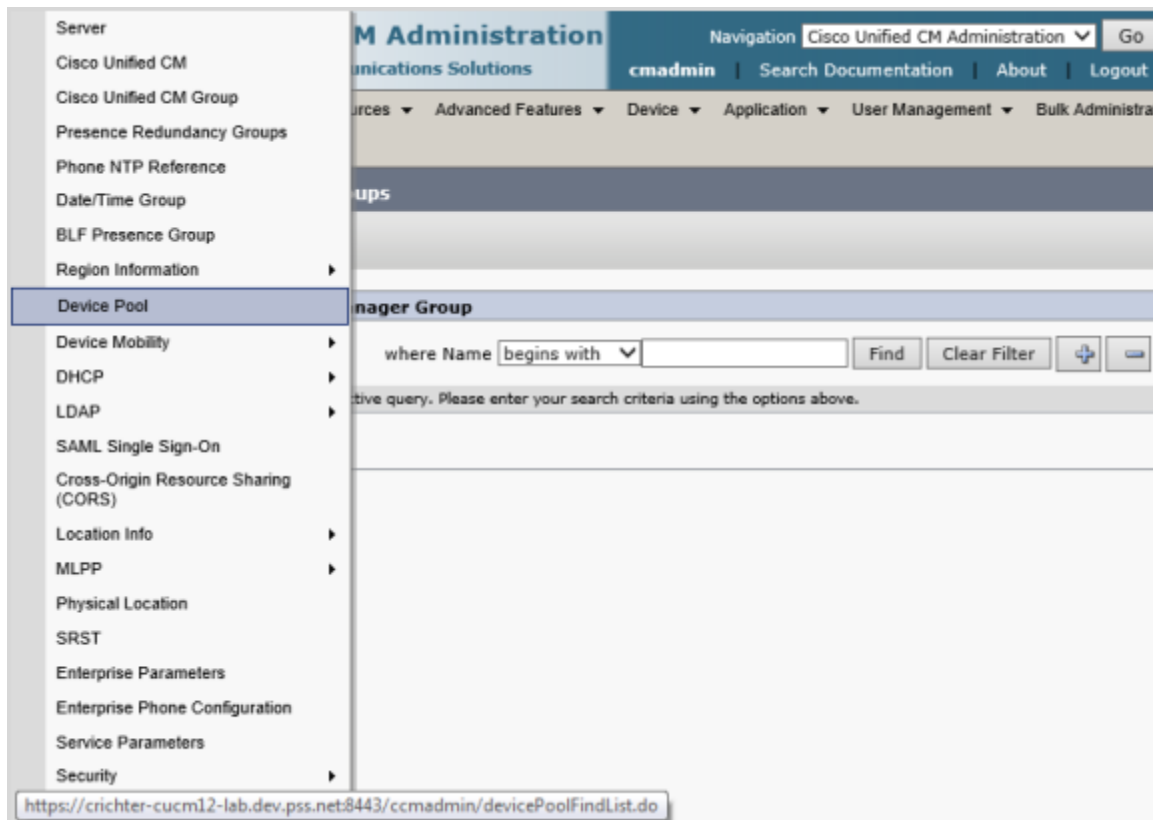
Device may be duplicated per facility OR move per facility in CUCM. This is determined by number of device pools listed per PBX.

- If single device pool entered, device will be duplicated across facilities.
- If multiple device pools, device will be moved between facilities.
- In both cases calling should work as expected.

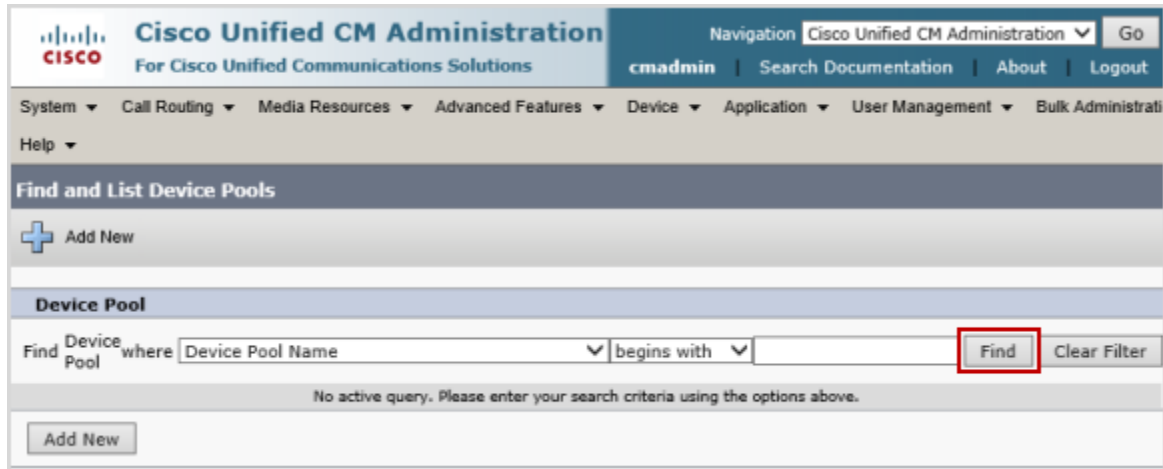
Only needed if you want to enable digest authentication. Add a new 'SIP Security Profile' and check 'Enable Digest Authentication'. Take note of the name you used for this SIP Security Profile, this will be configured in Enterprise Manager later.

The device type must match 'Third-Party SIP Device (Basic)'.

1. From the System menu, select Device Pool.



- Click **Find**.



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go

cmadmin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Find and List Device Pools

+ Add New

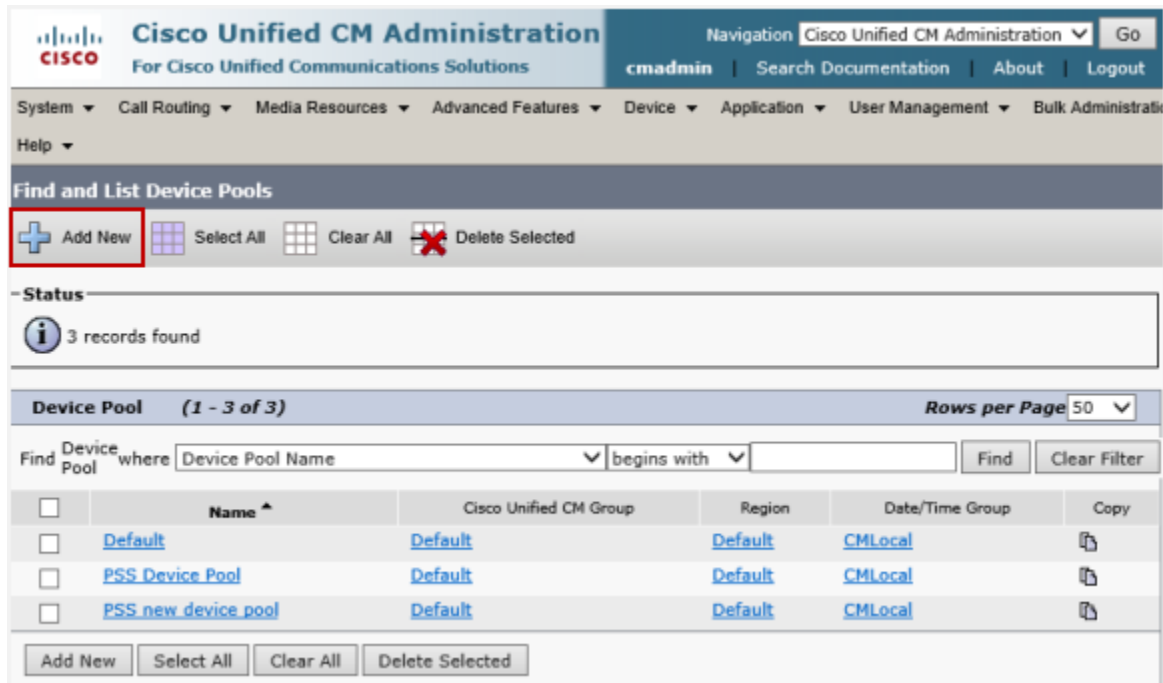
Device Pool

Find Device Pool where Device Pool Name begins with **Find** Clear Filter

No active query. Please enter your search criteria using the options above.

Add New

- Click **Add New**.



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go

cmadmin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Find and List Device Pools




+ Add New Select All Clear All Delete Selected

- Status

3 records found

Device Pool (1 - 3 of 3) Rows per Page 50

Find Device Pool where Device Pool Name begins with Find Clear Filter

<input type="checkbox"/>	Name ^	Cisco Unified CM Group	Region	Date/Time Group	Copy
<input type="checkbox"/>	Default	Default	Default	CMLocal	
<input type="checkbox"/>	PSS Device Pool	Default	Default	CMLocal	
<input type="checkbox"/>	PSS_new_device_pool	Default	Default	CMLocal	

Add New Select All Clear All Delete Selected

- Enter the following Device Pool Information:

- Device Pool Name
- Cisco Unified Communications Manager Group - Default
- Calling Search Space for Auto-registration - pss css
- Date/Time Group - CMLocal
- Region - Default

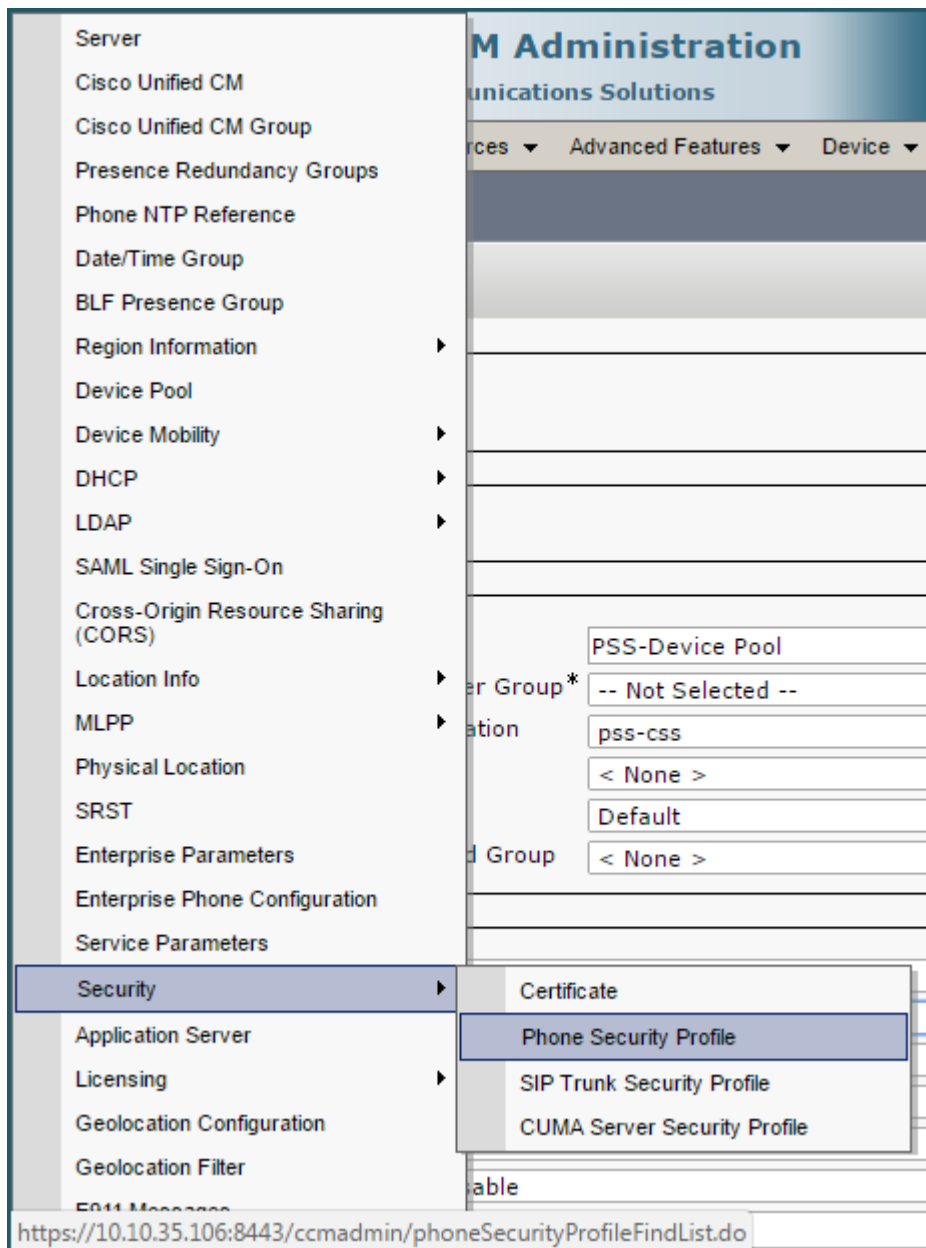
Device Pool Information	
Device Pool:	New
Device Pool Settings	
Device Pool Name*	<input type="text" value="PSS Device Pool"/>
Cisco Unified Communications Manager Group*	Default
Calling Search Space for Auto-registration	pss-css
Adjunct CSS	< None >
Reverted Call Focus Priority	Default
Intercompany Media Services Enrolled Group	< None >
Roaming Sensitive Settings	
Date/Time Group*	CMLocal
Region*	Default
Media Resource Group List	< None >
Location	< None >
Network Locale	< None >
SRST Reference*	Disable
Connection Monitor Duration***	<input type="text"/>
Single Button Barge*	Default
Join Across Lines*	Default
Physical Location	< None >
Device Mobility Group	< None >

SIP Security Profile

This is only needed if you want to enable digest authentication. Add a new SIP Security Profile and select 'Digest Authentication'. Take note of the name you used for this SIP Security Profile, this will be configured in Enterprise Manager later.

The device type must match the device type entered into Enterprise Manager. E.g. 'Third-Party SIP Device (Basic)'.

1. Click System>Security>Phone Security Profile.



2. Click **Add New**.
3. Enter the Phone Security Profile Type.
4. Click **Next**.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

cmadmin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Phone Security Profile Configuration Related Links: Back To Find/List Go

Next

Status
Status: Ready

Select the type of device profile you would like to create

Phone Security Profile Type* Third-party SIP Device (Advanced)

Next

5. Enter the following information:

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

Phone Security Profile Information

Product Type: Third-party SIP Device (Basic)
Device Protocol: SIP
Name* PSS Security Profile
Description Third-party SIP Device (Basic)
Nonce Validity Time* 600
Transport Type* UDP
 Enable Digest Authentication

Parameters used in Phone

SIP Phone Port* 5060

Save Delete Copy Reset Apply Config Add New

Enterprise Manager Settings

Enter the name of the new device security profile in Enterprise Manager under Settings>Voice Systems>Properties.

Properties	
Name ↑	Value
Digest Realm	ccmsipline
No Answer Timeout	15
Route Partition	pss-pt
Sip Port	5060
Sip Profile	PSS Sip Profile
Sip Security Profile	PSS Basic Security Profile
User Prefix	pss_blue_

SIP Profile

Create a new SIP Profile for PatientTouch devices, take note of the name used, this will be configured in Enterprise Manager later.

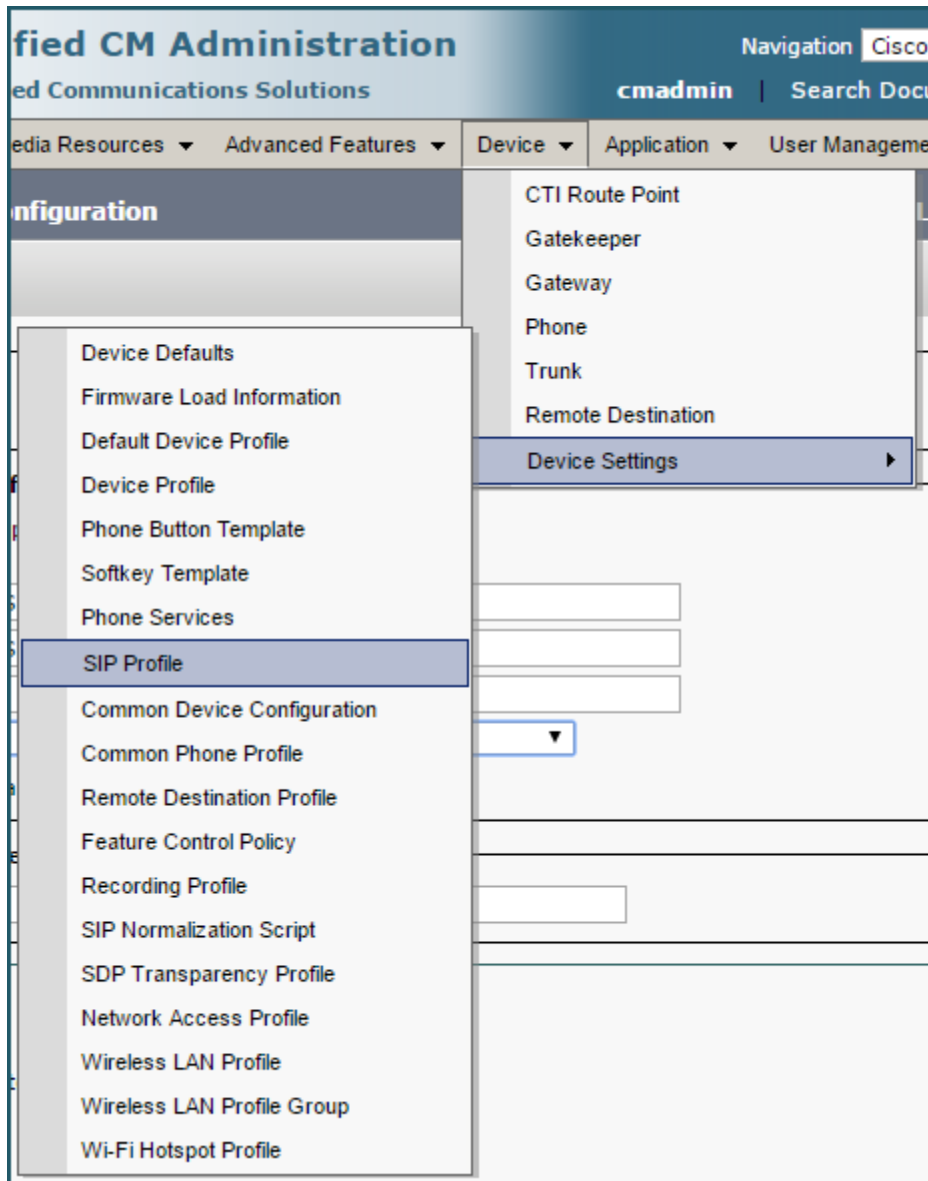
Call History has to be enabled on the CUCM server. Call history logs are uploaded by CUCM to the Org Services cluster over SFTP. Only logs for the route partition configured in 'Voice Systems' are considered.

Set the 'CDR File Time Interval' to '1' under 'System' -> 'Enterprise Parameters' (the call history records will be uploaded to Org Services every 1 minute).

- Directory should be '/callhistory/'
- User should be 'cucmsftp'
- Password is per install and provided by your PSS Support representative

Make sure 'Use Fully Qualified Domain Name in SIP requests' is enabled as well if you want to connect with a domain name instead of an IP (recommended):

1. Click Device>Device Settings>SIP Profile.



2. Click **Add New**.
3. Enter the following information:
 - Name
 - Description
 - Select the Redirect by Application check box
 - Select the Use Fully Qualified Domain Name in SIP Requests check box

Cisco Unified CM Administration

For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

[cadmin](#) | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ | Call Routing ▾ | Media Resources ▾ | Advanced Features ▾ | Device ▾ | Application ▾ | User Management ▾ | Bulk Administration ▾ | Help ▾

SIP Profile Configuration Related Links: [Back To Find/List](#) Go

Save

Status

Status: Ready

All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name*	<input type="text" value="PSS SIP Profile"/>
Description	<input type="text" value="PSS SIP Profile"/>
Default MTP Telephony Event Payload Type*	<input type="text" value="101"/>
Early Offer for G.Clear Calls*	<input type="text" value="Disabled"/>
User-Agent and Server header information*	<input type="text" value="Send Unified CM Version Information as User-Agen"/>
Version in User Agent and Server Header*	<input type="text" value="Major And Minor"/>
Dial String Interpretation*	<input type="text" value="Phone number consists of characters 0-9, *, #, anc"/>
Confidential Access Level Headers*	<input type="text" value="Disabled"/>

Redirect by Application

Disable Early Media on 180

Outgoing T.38 INVITE include audio mline

Use Fully Qualified Domain Name in SIP Requests

Assured Services SIP conformance

SDP Information

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	<input type="text" value="TIAS and AS"/>
SDP Transparency Profile	<input type="text" value="Pass all unknown SDP attributes"/>
Accept Audio Codec Preferences in Received Offer*	<input type="text" value="Default"/>

Require SDP Inactive Exchange for Mid-Call Media Change

Allow RR/RS bandwidth modifier (RFC 3556)

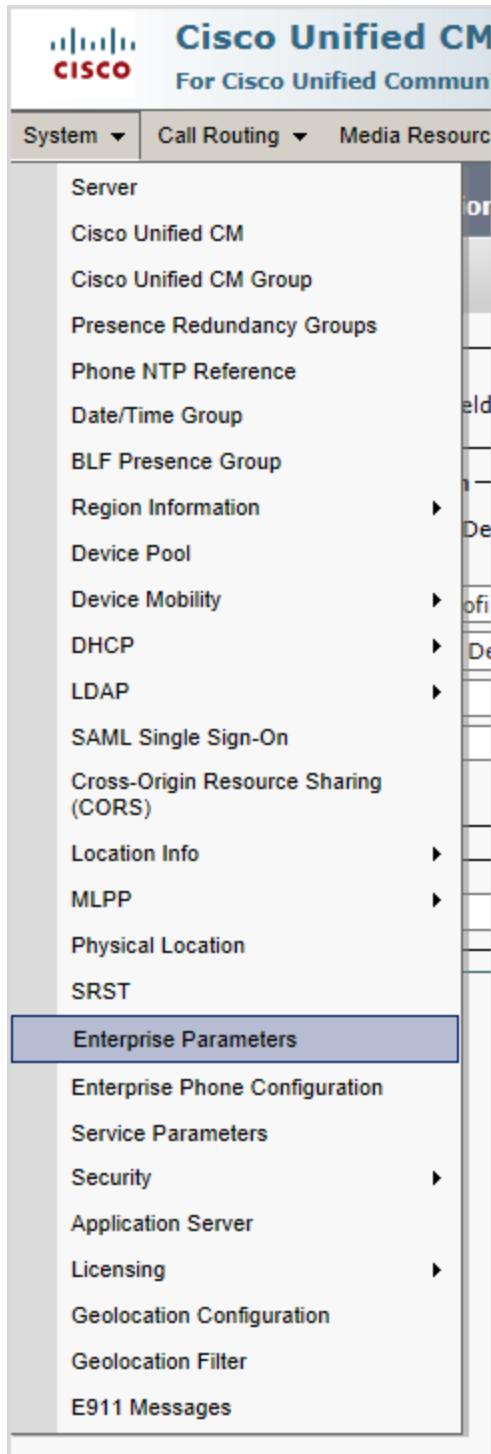
SIP Domain

The PatientTouch clients use the 'SIP Domain' when registering the SIP connection with CUCM, <extension>@<sipdomain>, e.g. 1000@cucm.mycompany.com.

This can be an IP or a fully qualified domain name (FQDN). The FQDN on the CUCM Publisher if set can be found below. Note this for later.

When connecting via a FQDN, make sure the SIP Security Profile (see previous section) has the setting 'Use Fully Qualified Domain Name in SIP requests' enabled.

1. Click **System>Enterprise Parameters**



2. Enter your CUCM server in the designated fields
3. Click **Save**

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Enterprise Parameters Configuration

Save Set to Default Reset Apply Config

Clusterwide Domain Configuration

[Organization Top Level Domain](#)

[Cluster Fully Qualified Domain Name](#)

Denial-of-Service Protection

[Denial-of-Service Protection](#) *

TLS Handshake Timer

[TLS Handshake Timer](#) *

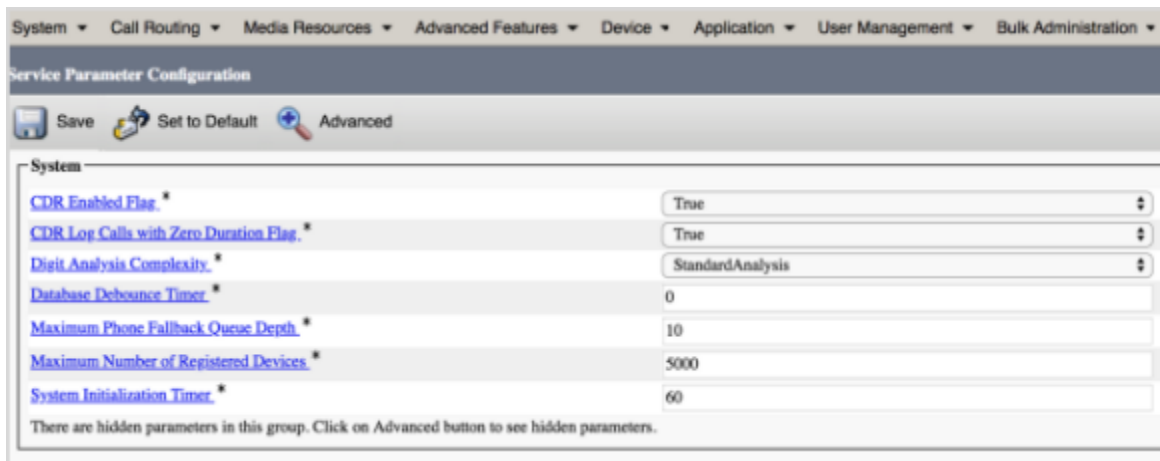
TLS Resumption Timer

[TLS Resumption Timer](#) *

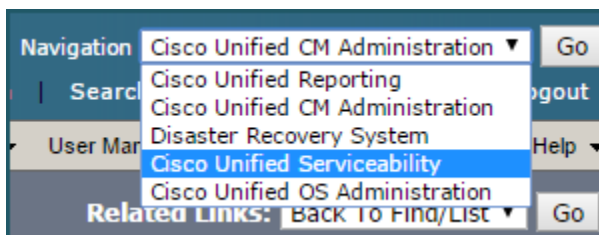
Call History

Call History has to be enabled on the CUCM server. Call history logs are uploaded by CUCM to the Org Services cluster over SFTP. Only logs for the route partition configured in Voice System are considered.

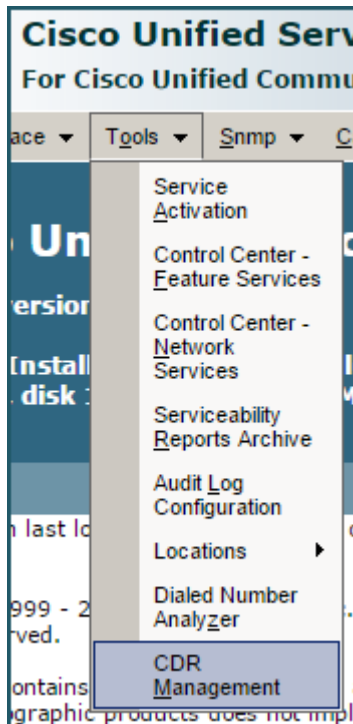
1. Set the 'CDR File Time Interval' to '1' under 'System' -> 'Enterprise Parameters' (the call history records will be uploaded to Org Services every 1 minute).
2. Go 'System' -> 'Service Parameters', then select the server and 'Cisco CallManager' this will bring up properties editor for call manager. Set the following:
 - 'CDR Enabled Flag' to 'true'
 - 'CDR Log Calls with Zero Duration Flag' to 'true'



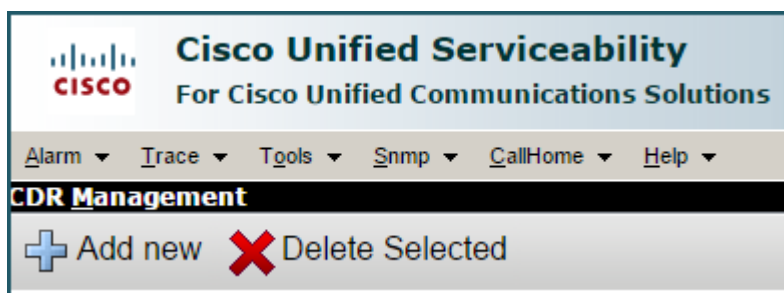
3. Then setup 'CDR Management': Select 'Cisco Unified Serviceability' and click 'Go'.



4. Click Tools>CDR Management.




5. Click **Add New** to add a new 'Billing Application Server'. This is just a server that accepts CDR CSV files, it's nothing to do with billing.



Fill out the Org Services server hostname (this can be any server in the org services cluster where cucm-sync is running. It can be a load balanced hostname/ip).

6. Enter the following information:
 - Host Name: enter your host name
 - User Name: should be 'cucmsftp'
 - Password: Password is per install and provided by your PSS Support representative
 - Directory Path: Should be '/callhistory/'





Cisco Unified Serviceability

For Cisco Unified Communications Solutions



Alarm ▾ Trace ▾ Tools ▾ Snmp ▾ CallHome ▾ Help ▾

CDR Management



Billing Application Server Parameters

Host Name / IP Address*	<input type="text" value="blue.qa.pss.net"/>
User Name*	<input type="text" value="cucmsftp"/>
Password*	<input type="password" value="....."/>
Protocol*	<input type="button" value="SFTP ▾"/>
Directory Path*	<input type="text" value="/callhistory/"/>
Resend on Failure	<input checked="" type="checkbox"/>

* - indicates required item.
Updation of IPAddress/Hostname and Directory Path is not allowed, CD

Hunt Groups

A hunt group is a method of distributing phone calls from a single extension or number to a group of users. In order to use Hunt Groups with PatientTouch they must first be configured in CUCM.

Terminology:

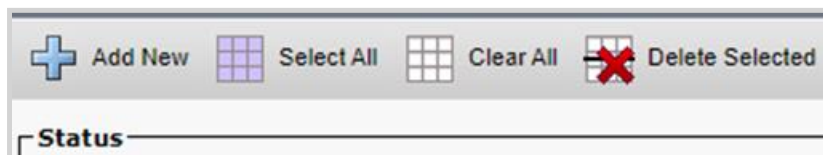
- **Line Group** - A line group allows you to designate the order in which directory numbers are chosen. PatientTouch Extensions are added and removed from this line group. In general, we anticipate sites configuring the Distribution Algorithm(Ring Order) to Broadcast, which will ring all numbers.
- **Hunt List** - A Hunt List lists a set of Line groups in a specific order.
- **Hunt Pilot** - A Hunt Pilot is the extension that routes calls to the Hunt List.

Create a new Line Group. PatientTouch extensions will be added/removed from this line group.

1. Click **Route/Hunt > Line Group**.



2. Click **Add New**.






3. Enter the following information:

- Line Group Name. Note this as it will need to be entered into Enterprise Manager.
- Ring No Answer (RNA) Timer. The recommended length is 15 seconds.
- Distribution Algorithm. The recommended option is Broadcast.
- Optionally, set responses for No Answer and Busy settings.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manage

Line Group Configuration

 Save
  Delete
  Add New

Line Group Information

Line Group Name*

RNA Reversion Timeout*

Distribution Algorithm*

Hunt Options

No Answer*




Automatically Logout Hunt Member on No Answer

Busy**

Not Available**

Optionally, a second line group may be set up as a fallback.

Line Group Configuration Related Links: [Back To](#)

 Save
  Delete
  Add New

Line Group Information

Line Group Name*

RNA Reversion Timeout*

Distribution Algorithm*

Hunt Options

No Answer*

Automatically Logout Hunt Member on No Answer

Busy**

Not Available**

Line Group Member Information

Find Directory Numbers to Add to Line Group

Partition

Directory Number Contains

Available DN/Route Partition

- 6101/ps-pt
- 88881/ps-pt
- 8888252*1#/ps-pt
- 9101/ps-mwtest1-pt
- Too many matches; use more specific search.

Current Line Group Members

Selected DN/Route Partition

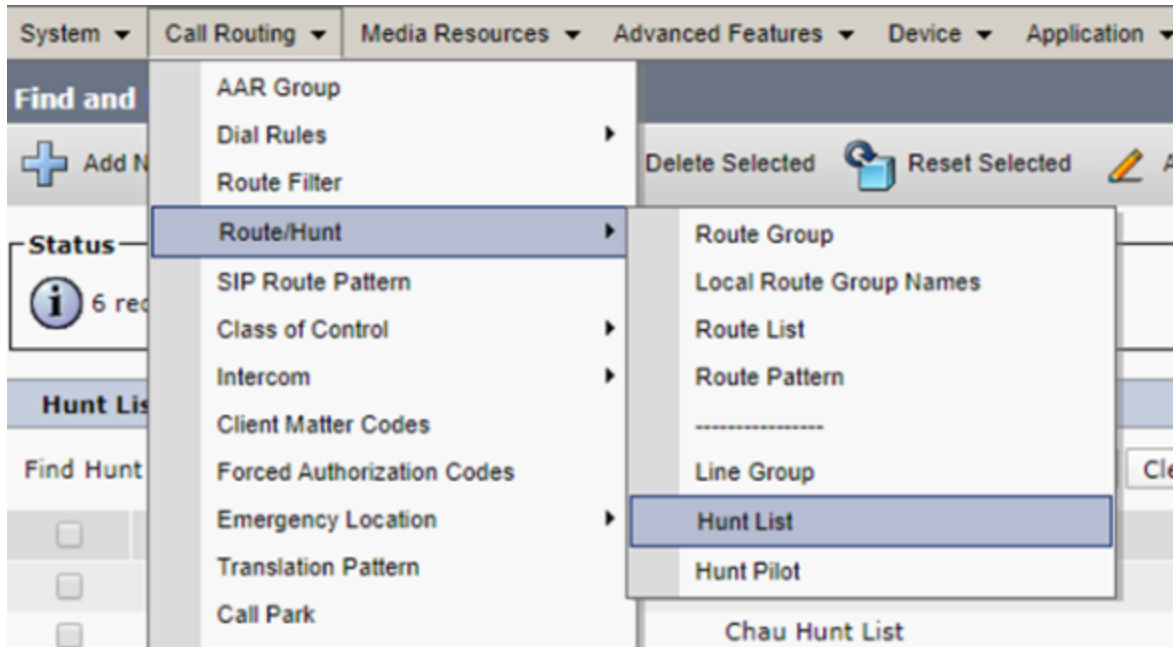
Removed DN/Route Partition

Directory Numbers

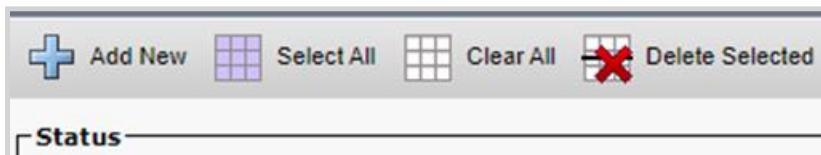
- 1006 in oss-white-pt

Create a Hunt List.

1. Click on **Route/Hunt > Hunt List**.



2. Click **Add New**.




3. Enter the following information:

- Name
- Description
- Check the box next to “Enable Hunt List”.
- Click “Add Line Group” and add the line group created in the first step.

Hunt List Configuration
Related

Save ✖ Delete 📄 Copy 🔄 Reset ✍ Apply Config ➕ Add New

- Status -

 Status: Ready

- Hunt List Information -

Device is trusted

Name*

Description

Cisco Unified Communications Manager Group*

Enable this Hunt List (change effective on Save; no reset required)

For Voice Mail Usage

- Hunt List Member Information -


Add Line Group


Selected Groups**

▼ ▲

Removed Groups***

- Hunt List Details -

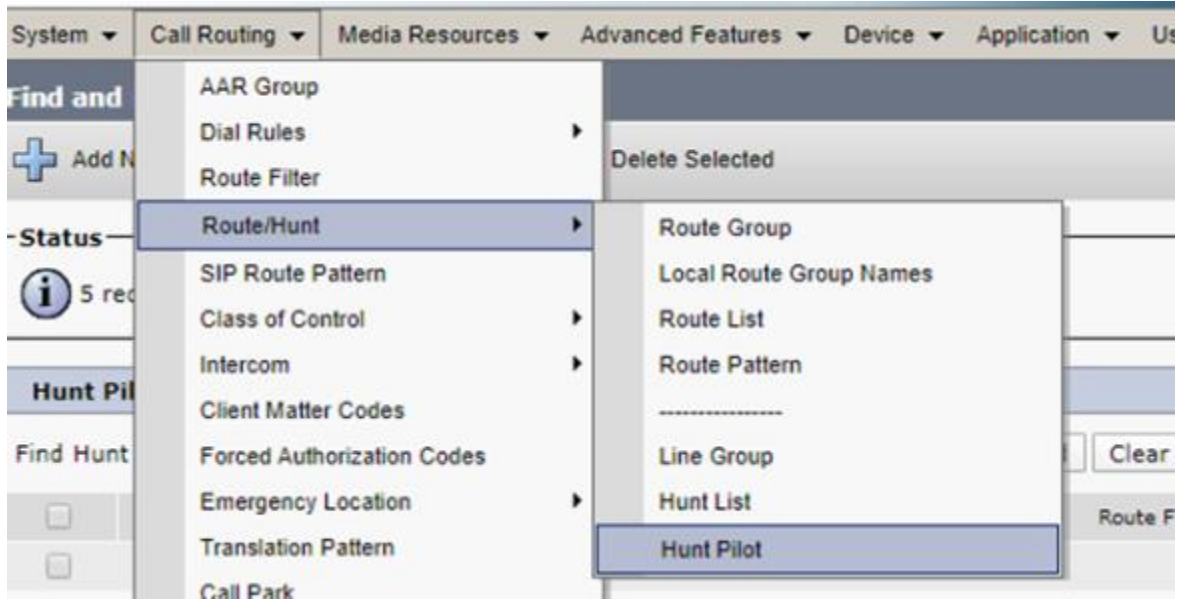
 [Line Group PSS 1](#)

 [7001 Fall Back Number](#)

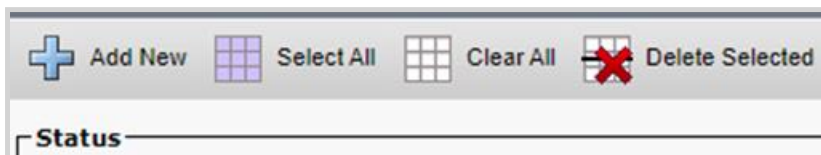
Save
Delete
Copy
Reset
Apply Config
Add New

Create Hunt pilot.






1. Click on **Route/Hunt > Hunt Pilot**.



2. Click **Add New**.



3. Enter the following information:
 - Hunt Pilot DN
 - Select the Route Partition
 - Description
 - Select the Hunt List created in the second step.
 - Alerting name
 - Optionally, set forward no answer and busy settings.

Hunt Pilot Configuration		Related Link
 Save  Delete  Copy  Add New		
Status		
 Status: Ready		
Pattern Definition		
Hunt Pilot*	<input type="text" value="7001"/>	
Route Partition	<input type="text" value="pss-white-pt"/>	
Description	<input type="text" value="Hunt Group PSS 1"/>	
Numbering Plan	<input type="text" value=" < None >"/>	
Route Filter	<input type="text" value=" < None >"/>	
MLPP Precedence*	<input type="text" value=" Default"/>	
Hunt List*	<input type="text" value=" Hunt List PSS 1"/>	(Edit)
Call Pickup Group	<input type="text" value=" < None >"/>	
Alerting Name	<input type="text" value=" Hunt Group PSS 1"/>	
ASCII Alerting Name	<input type="text" value=" Hunt Group PSS 1"/>	
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern <input type="text" value=" No Error"/>	
<input type="checkbox"/> Provide Outside Dial Tone		
<input type="checkbox"/> Urgent Priority		
Hunt Call Treatment Settings		
Forward Hunt No Answer		
<input checked="" type="radio"/> Do Not Forward Unanswered Calls <input type="radio"/> Use Forward Settings of Line Group Member <input type="radio"/> Forward Unanswered Calls to		
Destination	<input type="text"/>	
Calling Search Space	<input type="text" value=" < None >"/>	
Maximum Hunt Timer	<input type="text"/>	
Forward Hunt Busy		
<input checked="" type="radio"/> Do Not Forward Busy Calls <input type="radio"/> Use Forward Settings of Line Group Member <input type="radio"/> Forward Busy Calls to		
Destination	<input type="text"/>	
Calling Search Space	<input type="text" value=" < None >"/>	

When setting up the Hunt Group in Enterprise Manager, enter the Line Group Name from CUCM. Please see step by step instructions in the Enterprise Manager User Guide.

Voice

Facility:	PatientSafe Temecula	Name:	3RDFLOOR: Consulting Endocrinologist
Voice System:	pss-cucm-12-5-cluster	Extension (Display Only):	6010
		Fallback # (Display Only):	6000
		Hunt Group:	<input checked="" type="checkbox"/>
		External Number:	
		Line Group Name:	<input type="text"/> ⓘ

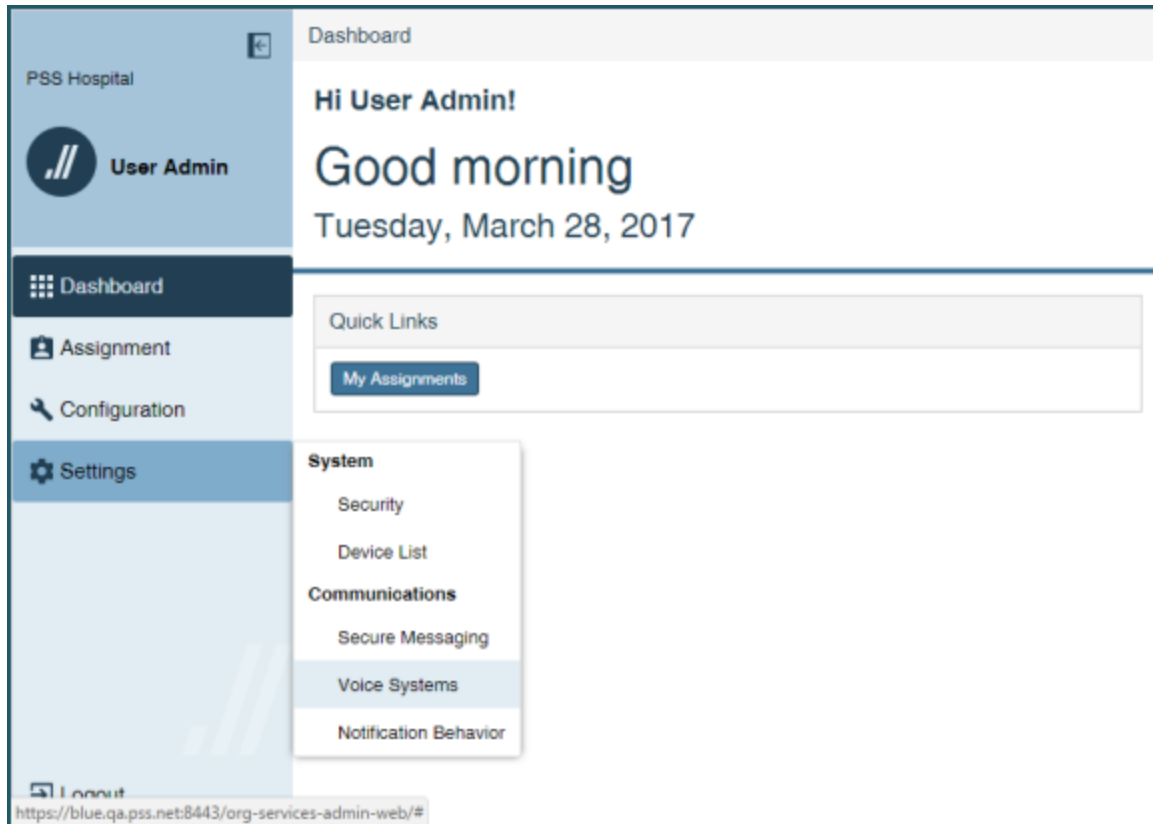
Cancel Done

Create New Voice System in Enterprise Manager

A 'Voice System' in Enterprise Manager allows directory numbers (extensions) to be provisioned on a Call Manager/PBX.

There may be an existing 'PatientTouch Voice Appliance' example Voice System added, remove this if connecting only to CUCM.

1. Select Settings>Voice Systems.



2. Click **Create New**. Enter a Name.
3. Select 'Cisco CUCM' as the type
4. Make sure 'Enable Extension Configuration' is selected (it is selected by default).

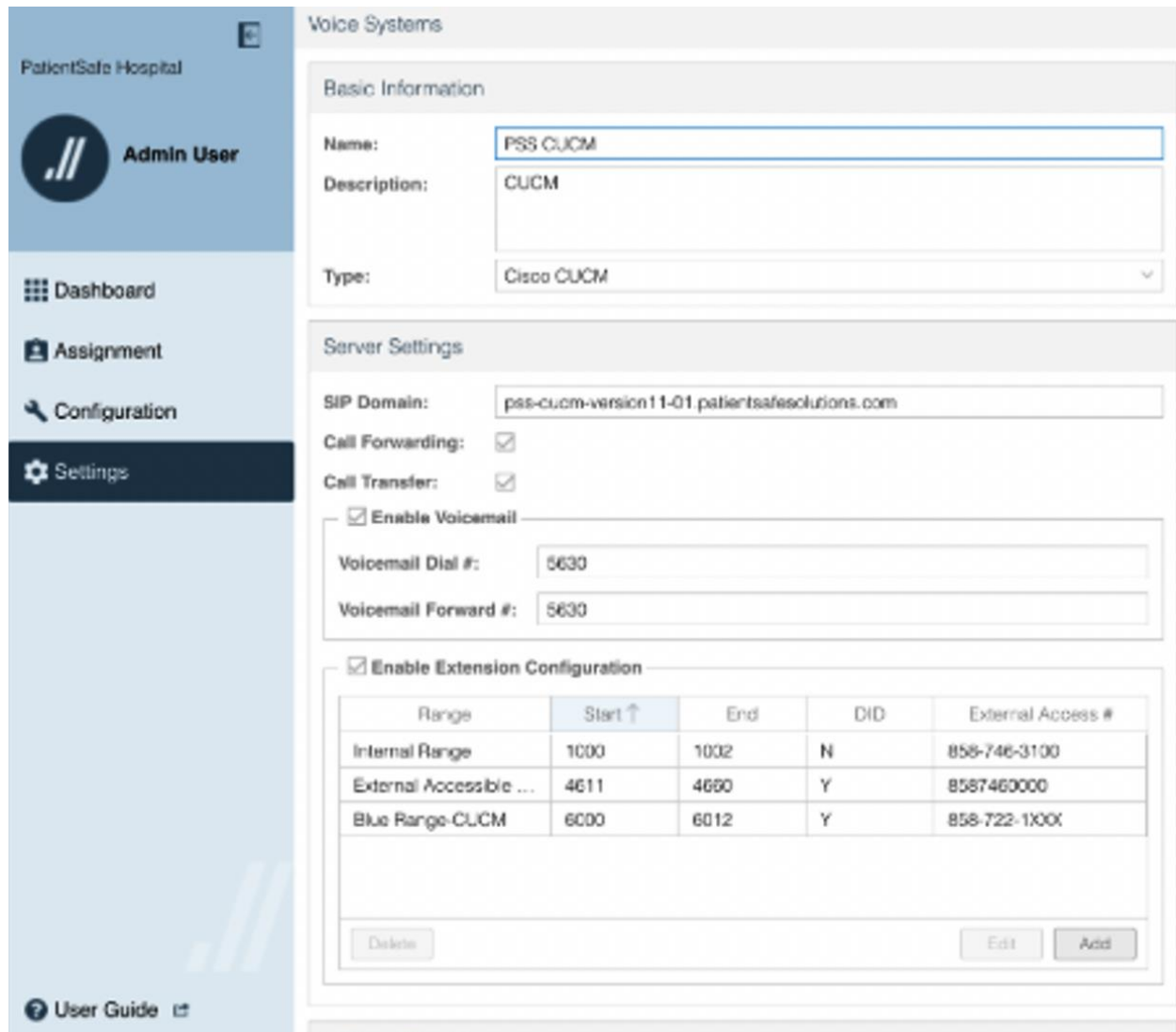
When Enable Extension Configuration is enabled, users, devices and lines in CUCM will be managed by Enterprise Manager. When disabled Enterprise Mgr will only read these from CUCM. However, in both cases the forwarding number on the line will be updated every time a user logs in or changes it from the client.

5. Add the CUCM SIP domain under SIP Domain. This can be an IP but a fully qualified domain name (FQDN) is preferred. PatientTouch devices register over SIP to CUCM using this 'SIP Domain'

VOIP settings in Org Services

The handheld then requests VOIP settings from Org Services, to allow the handheld to login over SIP. Settings include:

- SIP domain & Extension (SIP URL)
- CUCM subscribers to connect to
- Digest Username & Password (Encrypted)



Basic Information

Name: PSS CUCM

Description: CUCM

Type: Cisco CUCM

Server Settings

SIP Domain: pss-cucm-version11-01.patientsafesolutions.com

Call Forwarding:

Call Transfer:

Enable Voicemail

Voicemail Dial #: 5630

Voicemail Forward #: 5630

Enable Extension Configuration

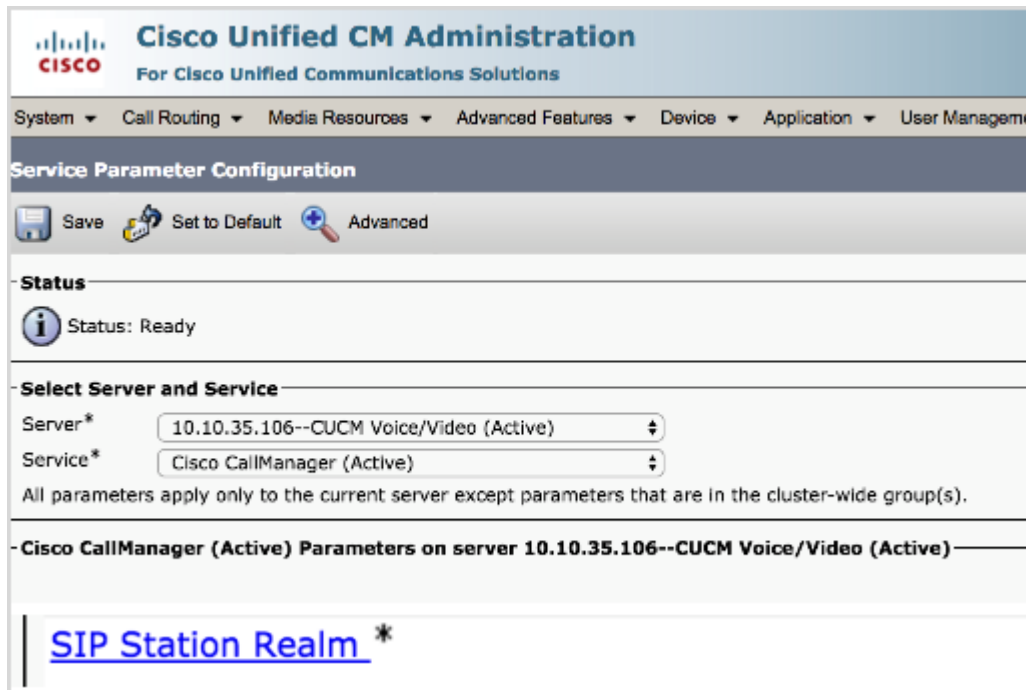
Range	Start ↑	End	DID	External Access #
Internal Range	1000	1002	N	858-746-3100
External Accessible ...	4611	4690	Y	8587460000
Blue Range-CUCM	6000	6012	Y	858-722-1000

Delete Edit Add

The PatientTouch clients use the 'SIP Domain' when registering the SIP connection with CUCM, <extension>@<sipdomain>, e.g. 1000@cucm.mycompany.com.

Affiliate with facilities you want the voice server to be available for. For each facility enter in the host name of the CUCM server to connect to. This can be different per facility. Multiple CUCM servers can be specified by comma separating them in this field.

The 'Digest Password' property in Enterprise Manager allows you to set the digest password configured on CUCM. This password will be set by Org Services as the digest password for any users that have a PatientTouch extension. The PatientTouch client will authenticate with this password. The password is not sent directly to clients instead a hash of the username and Digest Realm is used. The default digest realm used in CUCM is 'ccmsipline'. If this is changed to something else in CUCM you will need to change the 'Digest Realm' property in Enterprise Manager.



The screenshot shows the Cisco Unified CM Administration interface. The breadcrumb navigation is: System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management. The page title is "Service Parameter Configuration". There are three buttons: Save, Set to Default, and Advanced. The "Status" section shows "Status: Ready". The "Select Server and Service" section has two dropdown menus: "Server*" set to "10.10.35.106--CUCM Voice/Video (Active)" and "Service*" set to "Cisco CallManager (Active)". Below this is the text: "All parameters apply only to the current server except parameters that are in the cluster-wide group(s)". The "Cisco CallManager (Active) Parameters on server 10.10.35.106--CUCM Voice/Video (Active)" section is expanded to show the "SIP Station Realm" property, which is currently blank and marked with an asterisk.

Enter the following properties:

- Set 'AXL Password' to the password for the AXL user you created.
- Set 'AXL URL' as the URL to the AXL API of CUCM host(s), example 'https://<cucm_host>:8443/axl/'.
- Set 'AXL Username' to the username for the AXL user you created.
- Set 'Calling Search Space' to the name of the PSS specific 'Calling Search Space' you added.
- Set 'Device Pool' to the name of the PSS specific 'Device Pool' you added.
- Set 'Device Type' to blank, by default 'Third-party SIP Device (Basic)' is used as the device type.
- Set 'Route Partition' to the name of the PSS specific 'Route Partition' you added.
- Set 'SIP Profile' to the name of the PSS specific 'SIP Profile' you added.
- Set 'SIP Security Profile' to the name of the PSS specific 'SIP Security Profile' you added.
- Set 'User Prefix' to blank - this is only used in test environments.

Other properties:

- Make sure 'Allow Create Users' is set to 'false' (it is by default) if users will be already created in CUCM via Active Directory (AD). If your CUCM install is NOT Active Directory integrated with 'CUCM Dir Sync', set this to 'true' so that Org Services will create the users as needed in CUCM.
- Set 'Digest Password' to a custom password - This will be used by the PatientTouch client devices to connect to CUCM.

- Make sure the 'Digest Realm' matches the setting 'SIP Station Realm' in CUCM - See the 'Authentication' section below.
- Make sure the 'CUPI' settings are blank (they are by default) - these are only used in test environments.

Properties	
Name	
Allow Create Users	false
AXL Password	*****
AXL URL	https://<your CUCM host>:8443/axl/
AXL Username	pssaxluser
AXL Version	9.0
Calling Search Space	pss-css
Device Pool	PSS Device Pool
Device Type	Third-party SIP Device (Basic)
Digest Password	*****
Digest Realm	ccmsipline
Route Partition	pss-pt
Sip Profile	PSS Sip Profile
Sip Security Profile	PSS Security Profile
User Prefix	

PatientTouch Client SIP Setup

SIP REGISTER to sip:1000@pss-cucm-version11-01.patientsafesolutions.com

Will register every 20 seconds (this is configured in CUCM and communicated to the client over the SIP protocol directly).

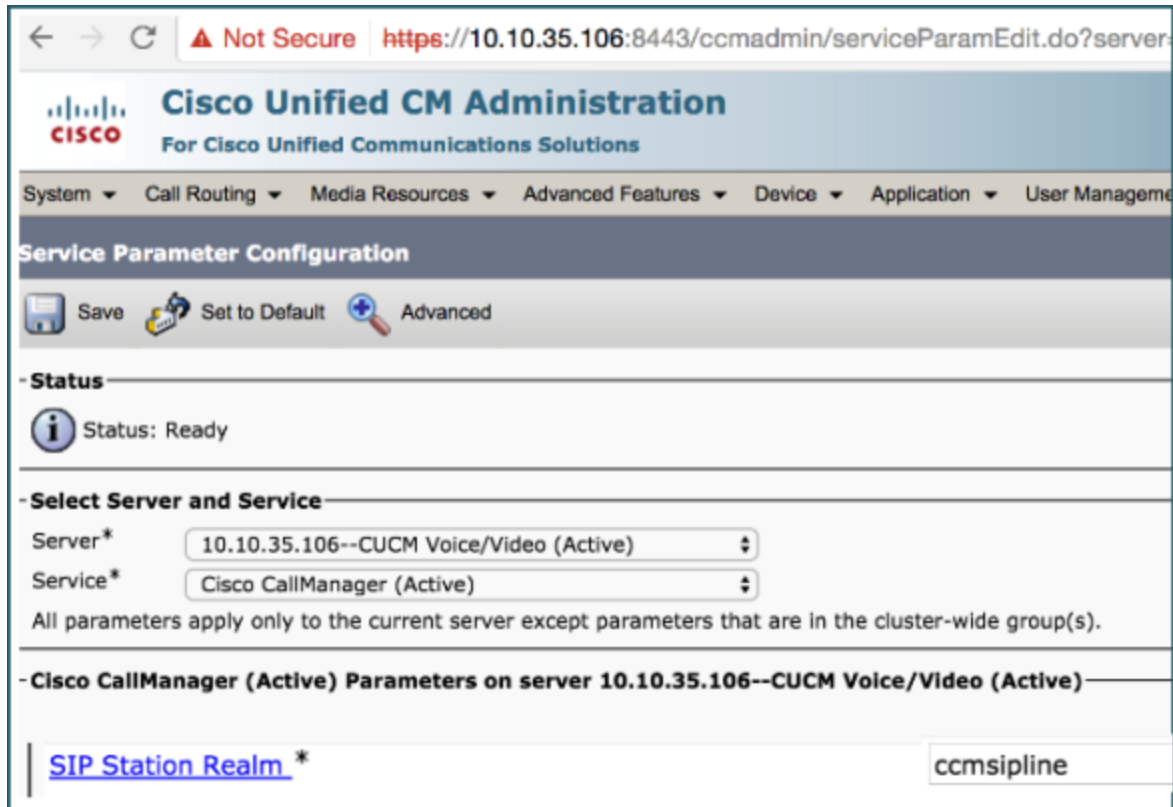
The registration is done to the 'SIP Domain' configured under Server Settings.

NOTE : Prior to 4.5 (4.4.1 and before) the client apps would register using the subscriber hostname as the domain.

Appendix

Authentication

The 'Digest Password' property in Enterprise Manager allows you to set the digest password configured on CUCM. This password will be set by Org Services as the digest password for any users that have a PatientTouch extension. The PatientTouch client will authenticate with this password. The password is not sent directly to clients. Instead a hash of the username and Digest Realm is used. The default digest realm used in CUCM is 'ccmsipline'. If this is changed to something else in CUCM you will need to change the 'Digest Realm' property in Enterprise Manager.



We use digest authentication when registering with SIP. The credentials (username/password) are passed to the client from Org Services when the client requests /pt/voip/settings

CUCM itself has some limitations on digest passwords:

Each user in CUCM can only have 1 digest password, no matter how many devices they log into.

The digest password cannot be sync'ed to CUCM over AD, it has to be set manually or over AXL (we set it over AXL).

In our setup, one password is shared across all PSS users (This can be changed per Voice System in Enterprise Manager -> Voice Systems). The customer can set a password of their choosing for all PSS users, and we will set this password via AXL on extension / user setup.

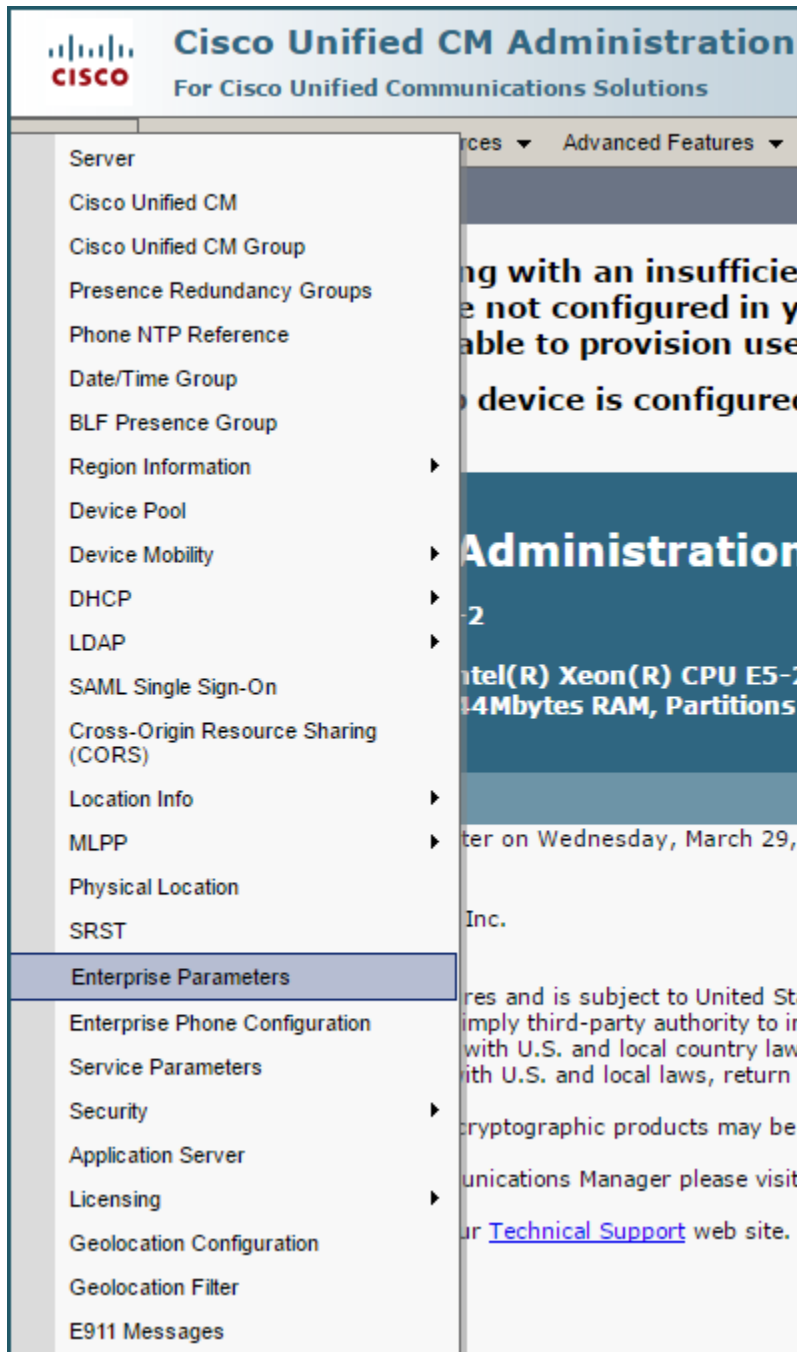
The password is not passed to the client in plaintext, instead a hash (per user) is sent to the client. So having this hash you can only log in as that user. This prevents one leaked password allowing for login to any extension. The 1 password is not sent in the /pt/voip/settings response.

The reason for one password across all PSS users is because the digest password can be used outside of PatientTouch. Non PSS devices can require digest passwords, and these require the digest password to be entered on admin setup of the device. If we were to generate our own password per user, we would have to give the customer a way to lookup this password in Enterprise Manager. We could also have a way to set it per user in Enterprise Manager. This would be error prone from an admin perspective and should not be the default; it's not common to use digest auth. These changes could be a future enhancement if needed, but right now the customer can set 1 password of their choosing for all users.

Fully Qualified Domain Name

To connect with the fully qualified domain name for 'SIP Domain' you will need to make sure CUCM is configured correctly.

1. Under Cisco Unified CM Administration, select System>Enterprise Parameters.









Clusterwide Domain Configuration	
Organization Top Level Domain	pssvoip.brown.pss.srv
Cluster Fully Qualified Domain Name	pssvoip.brown.pss.srv



- Under the SIP Security Profile (see section above), make sure 'Use Fully Qualified Domain Name in SIP requests' is enabled:

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help

SIP Profile Configuration

 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

Status

 Status: Ready
 All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name* PSS SIP Profile
 Description PSS SIP Profile
 Default MTP Telephony Event Payload Type* 101
 Early Offer for G.Clear Calls* Disabled ▾
 User-Agent and Server header Information* Send Unified CM Version Information as User-Agent ▾
 Version in User Agent and Server Header* Major And Minor ▾
 Dial String Interpretation* Phone number consists of characters 0-9, *, #, and ▾
 Confidential Access Level Headers* Disabled ▾

Redirect by Application
 Disable Early Media on 180
 Outgoing T.38 INVITE include audio mline
 Use Fully Qualified Domain Name in SIP Requests
 Assured Services SIP conformance

SDP Information

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites* TIAS and AS ▾
 SDP Transparency Profile Pass all unknown SDP attributes ▾
 Accept Audio Codec Preferences in Received Offer* Default ▾
 Require SDP Inactive Exchange for Mid-Call Media Change
 Allow RR/RS bandwidth modifier (RFC 3556)

Licensing

The number of Cisco licenses required by your organization will depend on the number of devices your organization will connect to the network.

Each physical device that connects direct to CUCM (rather than a SIP Trunk alternative) requires a CUCM “Enhanced” license. In these cases, PatientTouch device connects direct to CUCM as a 3rd Party Basic SIP device. If your licenses are of the type "User Connect Licensing", each device will utilize one "Enhanced" license. For example, if your organization has 1500 nurses and 600 shared devices connect direct to CUCM , then 600 licenses are required.

Care Role Forwarding extension numbers do not require any additional licenses.

For Cisco Unified Workspace Licensing (UWL) this equates to a Standard UWL or Professional UWL license. You may utilize either a "Standard" or "Professional" license.

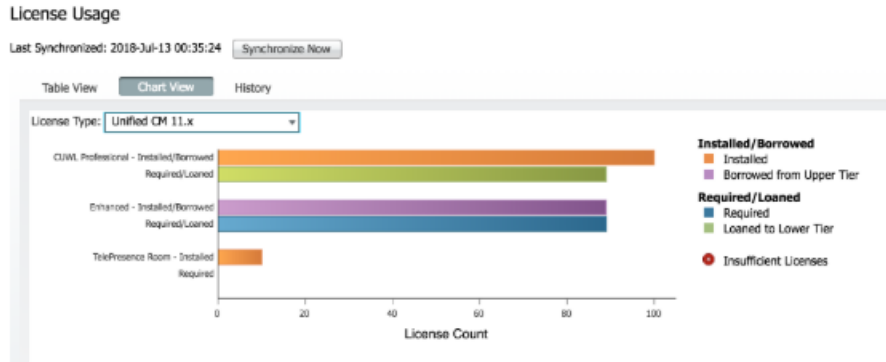
We’ve highlighted a few examples in the figure below:

License Type	Supported Devices
Essential UCL	<ul style="list-style-type: none"> • Cisco Unified SIP Phone 3905 • Cisco Unified IP Phone 6901 • Analog devices
Basic UCL	<ul style="list-style-type: none"> • Cisco Unified IP Phone 6911 and 6921 models • Any Essential device
Enhanced UCL or Enhanced Plus UCL or UWL Standard or UWL Professional	<ul style="list-style-type: none"> • Cisco Unified IP Phone 6941, 6945, and 6961 models • Cisco Unified IP Phone 7900 Series (7900G, 7911G, 7912G, 7931G, 794xG, 796xG, and 7975G models) • Cisco Unified IP Phone 8900 Series (8941, 8945, and 8961 models) • Cisco Unified IP Phone 9900 Series (9951 and 9971 models) with or without camera • Cisco Unified Wireless IP Phones Series (792xG and 7925G-EX models) • Cisco Unified IP Conference Stations (7936G and 7937G stations) • Cisco Unified Softphones (Cisco Unified Personal Communicator, Cisco UC Integration for Lync, Cisco UC Integration for Connect, and Cisco IP Communicator) • Jabber clients (Jabber for Mac, Jabber for Windows, Jabber for iPhone, Jabber for Android, Jabber for iPad and Jabber SDK) • Cisco Virtual Experience Clients (VXC) with voice and video firmware • Cisco TelePresence System E20 • TelePresence System EX Series (EX60 and EX90) • Third-party SIP devices • Any Basic or Essential device
Cisco TelePresence Room	<ul style="list-style-type: none"> • Cisco TelePresence Systems 500, 1000, 1100, 1300, 3000, 3200, TX9000, TX9200 • Cisco TelePresence System Profile 42-inch 6000 MXP, 52-inch MXP, 52-inch Dual MXP, 65-inch, and 65-inch Dual • Cisco TelePresence System Codecs C90, C60, and C40; Cisco TelePresence System Quick Set C20 • Cisco TelePresence MX Series (MX300 and MX200)

For example, a health system with 100 CUWL Professional licenses, where 89 of the devices are used by the Enhanced license requirement of the 3rd Party Basic SIP devices we have setup will appear as follows in the CUCM License Usage display:

License Usage

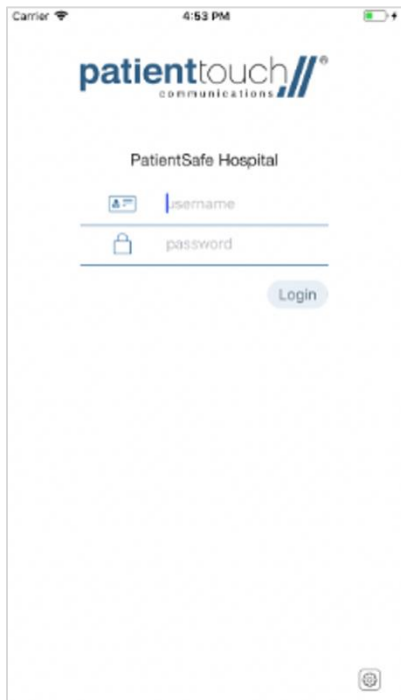
Type	Required
User (11.x) - Emergency Responder	0
CUWL Professional (11.x) - Unified CM	0
Enhanced (11.x) - Unified CM	89
TelePresence Room (11.x) - Unified CM	0
CUWL Professional Messaging (11.x) - Unity Conne...	0
Basic Messaging (11.x) - Unity Connection	8



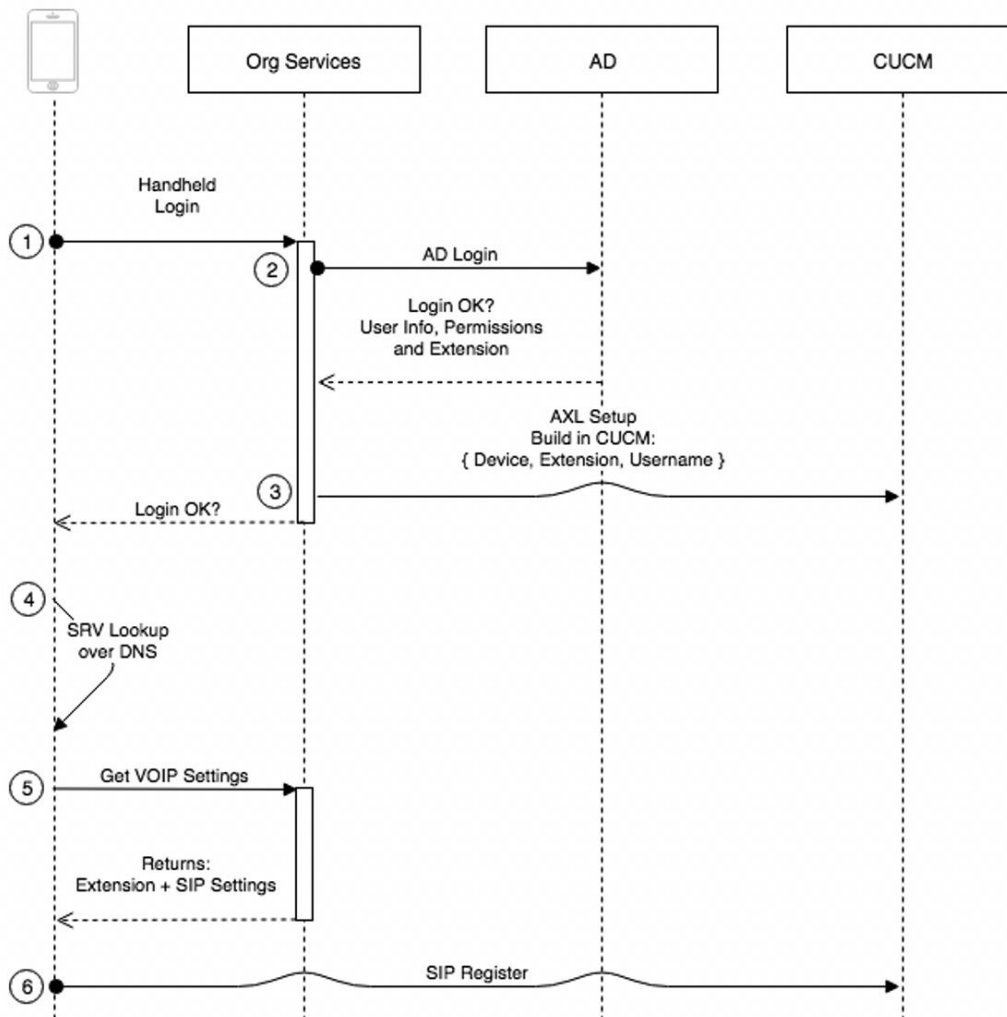
For more information on Cisco licensing, you may visit Cisco's licensing site.

PatientTouch Login

User logs in from handheld with their AD login name and password.



Handheld to CUCM Login Process



Org Services AD Login

Org Services contacts AD and retrieves user profile and extension based on predefined mapping (customer IT department works with PSS support to come up with this mapping).

Org Services AXL connection to CUCM

The Device & Extension is created in CUCM. The device can be found by going to 'Device' → 'List' and searching by 'Description' 'contains' and the username of the user who just logged in. (All PatientTouch devices can be viewed by searching for 'PatientTouch' in the 'Description').

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
cadmin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Find and List Phones Related Links: [Actively Logged In Device Report](#) | Go

Status
1 records found

Phone (1 - 1 of 1) Rows per Page: 50

Find Phone where: Description contains jcar

<input type="checkbox"/>	Device Name(Line)	Description	Device Pool	Device Protocol	Status	IPv4 Address	Copy	Super Copy
<input type="checkbox"/>	SEP0A0A09E90B	PatientTouch - jcar	Default	SIP	None	None	<input type="button" value="Copy"/>	<input type="button" value="Super Copy"/>

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
cadmin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Phone Configuration Related Links: [Back To Find List](#) | Go

Status
Status: Ready

Association

Modify Button Icons

1	SEP Line [1] - 9559.0.000.01	Unassigned Associated Items
2	SEP Line [7] - Add Line DN	

Phone Type

Product Type: **Third-party SIP Device (Basic)**
Device Protocol: SIP

Real-time Device Status

Registrations: Unknown
IPv4 Address: None

Device Information

- Device is Active
- Device is not trusted
- MAC Address*: AD0A09E90B
- Description: PatientTouch - jcar
- Device Pool*: Default [View Details](#)
- Common Device Configuration: < None > [View Details](#)
- Phone Button Template*: Third-party SIP Device (Basic)
- Common Phone Profile*: Standard Common Phone Profile [View Details](#)
- Calling Search Space: ps-co
- AAR Calling Search Space: < None >
- Media Resource Group List: < None >
- Location*: Hub_None
- AAR Group: < None >
- Device Mobility Mode*: Default [View Current Device Mobility Settings](#)
- Owner: User Anonymous (Public/Shared Space)
- Owner User ID*: jcar

SRV lookup

The handheld performs a SRV lookup - much like the following DIG to find the CUCM subscribers to connect to for it's current location.

```
[root@blue ~]# dig SRV _pssvoip._udp.blue.qa.pss.net

; <>> DiG <>> SRV _pssvoip._udp.blue.qa.pss.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56837
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;_pssvoip._udp.blue.qa.pss.net. IN      SRV

;; ANSWER SECTION:
_pssvoip._udp.blue.qa.pss.net. 600    IN      SRV     2 0 5060 pss-cucm-sub02-version11-01.patientsafesolutions.com.
_pssvoip._udp.blue.qa.pss.net. 600    IN      SRV     1 0 5060 pss-cucm-sub01-version11-01.patientsafesolutions.com.

;; AUTHORITY SECTION:
blue.qa.pss.net.                360    IN      NS      ns2.pss.dev.
blue.qa.pss.net.                360    IN      NS      ns1.pss.dev.

;; ADDITIONAL SECTION:
blue.qa.pss.net.                360    IN      A       172.17.10.16
ns1.pss.dev.                    38400  IN      A       192.168.10.120
ns2.pss.dev.                    38400  IN      A       192.168.10.121

;; Query time: 1 msec
;; SERVER: 192.168.10.120#53(192.168.10.120)
;; WHEN: Fri Jul 13 16:57:48 2018
;; MSG SIZE rcvd: 406
```

Call History

Call History has to be enabled on the CUCM server. Call history logs are uploaded to the org services cluster using sftp. The 'cucm-sync' tomcat app monitors '/pss/cucm-call-logs' for new CDR CSV files and uploads them to the org services database.

The 'CDR File Time Interval' under 'System' -> 'Enterprise Parameters' to be '1' (for 1 minute, this will cause the call history to be uploaded every 1 minute).

Directory is '/callhistory/'

User is 'cucmsftp'

The iOS handheld maintains its own call history, so sometimes you can see duplicates or the call history appears to work but once you log out and log back in again the call history is gone. In this case the call history is not setup in CUCM - follow the steps in the CUCM Setup Guide.

Offline Mode

When Org Services goes offline, SIP calls (and registrations) can still be made. The client has to store the username / password combination along with any other SIP settings while Org Services is down to be able to continue to register and reregister with SIP (Wi-Fi can be lost while Org Services is down, and the client will still reconnect to SIP once WiFi becomes available again).

The password / password hash is persistent. It will remain the same for a user across Org Services logins (at least as long as the user has the same extension configured). Enable Extension Configuration

When this is enabled, users, devices and lines in CUCM will be managed by Enterprise Mgr. When disabled Enterprise Mgr will only read these from CUCM. However, in both cases the forwarding number on the line will be updated every time a user logs in or changes it from the client.

Logs

Logs are under:

/pss/org-services/logs/cucm-sync.log

Call transfer rules

Calling a PatientTouch extension from another PatientTouch extension:

Case	Call Forward	No Call Forward
Offline / Not Registered	Call forwarded immediately	Call immediately disconnected, no ringing
Busy / Call Rejected By User	Call forwarded after user rejects	Rings until call is rejected then disconnects
No Answer	Call forwarded after 15 seconds by default (we set this number)	Rings until hangup
No line for dialed number	N/A	Call immediately disconnected, no ringing

Calling a PatientTouch extension from another Skinny and/or Desk Phone:

Case	Call Forward	No Call Forward
Offline / Not Registered	Call forwarded immediately	Fast Busy Tone
Busy / Call Rejected By User	Call forwarded after user rejects	Rings until call is rejected then busy tone

Case	Call Forward	No Call Forward
No Answer	Call forwarded after customer configured number of seconds	Rings until hangup
No line for dialed number	N/A	Fast Busy Tone

In addition call forwarding chains, so the above rules extend when forwarded to another PatientTouch extension.

There are no voice prompts by CUCM when a call is forwarded, it is forwarded immediately by CUCM and next number starts ringing once the forwarding is invoked.

Hang ups occur immediately when a SIP call can't be made.

Calling a Care Role Call Forwarding Extension: The call is always immediately forwarded.

Calling Offline Users

If a patient touch user is offline (or any line is not registered on CUCM) and that user is called from a PatientTouch client, the call will immediately fail and the client will display 'unable to complete call' message.

FAQ

Q: What the difference when someone logs in the first time vs 2nd time?

A: It's the same process, but the extension (and possibly device) will already exist in CUCM, so we won't need to modify those in CUCM for the user to login. This goes for the first time too, if someone manually setup the { extension, device, user } we won't attempt to recreate. When a user logs into a different device, they have to be associated with the new device, in that case the device will be added or reused in CUCM if it already exists.

Q: Does Org Services and CUCM have a nailed up connection or is it transactional when someone logs in ?

A: Conceptually we have a separate process that handles updates to the PBX that runs in the background. It calls CUCM on login, but also anytime the voice settings for a user are changed (e.g. forwarding number is changed / enabled, or extension is manually unassigned). It's separate HTTP AXL calls each time something changes.

Q: What does CUCM integration with AD add to the flow ?

A: There'll be a prior setup when the user is added to AD, and then either manually synced to CUCM by an admin logging into to CUCM and doing it as part of the user on-boarding process or more likely, just waiting for CUCM – AD 'DirSync' to be called which will typically be setup to sync once a day (or however it is configured, highest frequency is every 6 hours).

Q: Does PatientTouch CUCM integration require its own partition?

A: Adding a separate partition is highly recommended as it limits automated PatientTouch extension changes to single namespace. Having all extensions in the same namespace, gives PatientTouch the ability to clobber any extension, a mistake in configuring the extension ranges could cause an existing hospital extension to be removed.

Partition changes to an existing Calling Search Space does not require resetting any devices attached to the CUCM cluster. In addition, and perhaps more importantly, we do not have any current deployments configured to have all extensions in one partition.