

Configure Self-Provisioning Feature on CUCM (IVR Based)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[What is Self-Provisioning?](#)

[Configure](#)

[Services Associated with Self-Provisioning](#)

[End-user experience on the Phone](#)

[Troubleshoot](#)

[Logs to be Collected](#)

[Known defects](#)

[Related Information](#)

Introduction

This Document describes how to configure Self-Provisioning Feature on CUCM (IVR Based).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communication Manager.
- Voice over Internet Protocol (VoIP)
- Phone Registration Process.

Components Used

The information in this document is based on Cisco Unified Communications Manager 10.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

What is Self-Provisioning?

Self-Provisioning is a feature introduced in the 10.x release of Cisco's Unified Communications Manager (CUCM). It provides a **plug and play** type of functionality that simplifies the phone

deployment process. Using **auto-registration**, some template and profile configurations, along with an IVR service, CUCM administrators have the ability to deploy phones with minimal upfront configuration.

Self-Provisioning (IVR Based) similar in function to the old Tool for Auto-Registered Phones (TAPS) method. The key difference with Self-Provisioning is that the **IVR service runs on CUCM** so you don't need UCCX as you do with TAPS.

Configure

1. Create a **Universal Device template** (UDT).

Step 1. Navigate to **User management > User Phone add > Universal Device Template** and Add New Template.

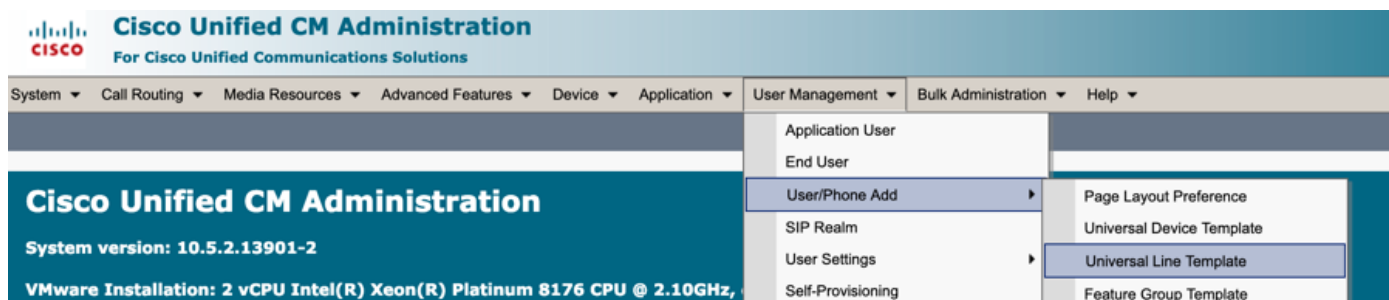
The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The 'User Management' menu is expanded, showing options like Application User, End User, UserPhone Add, SIP Realm, User Settings, Self-Provisioning, and Assign Presence Users. The 'UserPhone Add' option is further expanded to show Page Layout Preference, Universal Device Template, Universal Line Template, Feature Group Template, and Quick User/Phone Add. The 'Universal Device Template' option is highlighted. Below this, the 'Find and List Universal Device Templates' section is visible, with the 'Add New' button highlighted in a red box.

Step 2. Apply the Configuration that you expect the phones to take after auto registration to the new UDT.

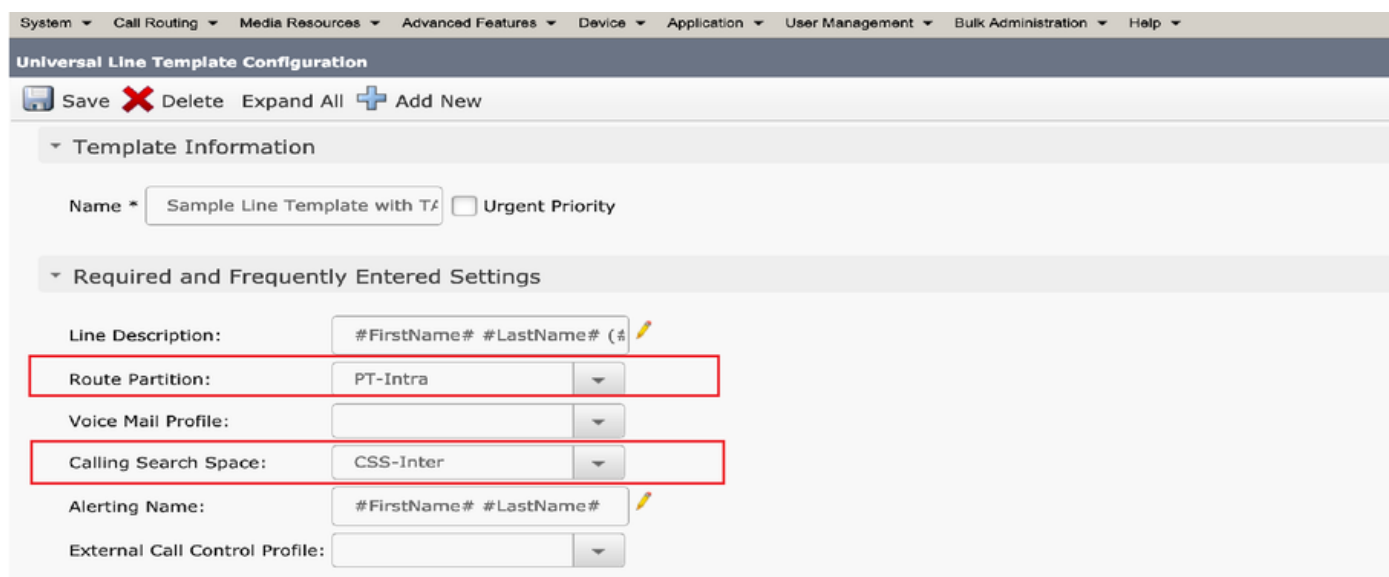
The screenshot shows the 'Universal Device Template Configuration' page. The top navigation bar is the same as in the previous screenshot. Below the navigation bar, there are buttons for Save, Delete, Expand All, and Add New. The 'Template Information' section shows the 'Name' field set to 'Auto-registration Template'. The 'Required and Frequently Entered Settings' section is highlighted with a red box and contains the following fields: Device Description (set to '#FirstName# #LastName# (#Pro)'), Device Pool (set to 'Default'), Device Security Profile (set to 'Universal Device Template - Moc'), SIP Profile (set to 'Standard SIP Profile'), and Phone Button Template (set to 'Universal Device Template Butto').

2. Create **Universal Line Template** (ULT).

Step 1. Navigate to **User Management > User/Phone Add > User Line Template**, as shown in the image.

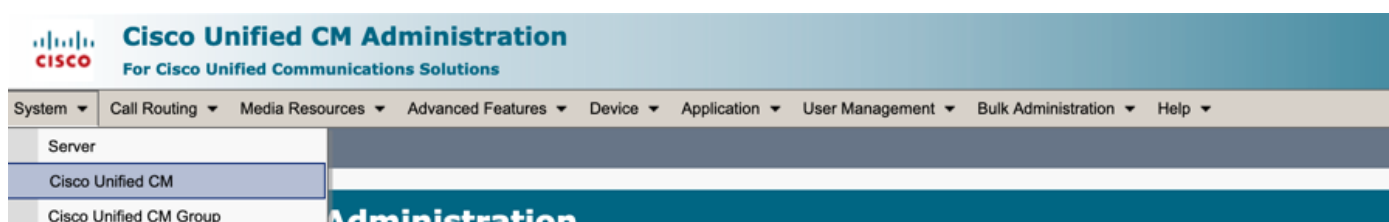


Step 2. Add the Route partition and CSS that is expected on the Phone after Auto Registration.



Note: These Universal Device Template and Universal Line Template should be linked with Auto registration so that the Phones Can take the Configuration when Auto-Registered.

3. Add the Templates to the CUCM node for **Auto-registration** Configuration and navigate to **System > Cisco Unified CM**, as shown in the image.



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

Cisco Unified CM Configuration

Save Reset Apply Config

Status

Status: Ready

Cisco Unified Communications Manager Information

Cisco Unified Communications Manager: CM_UCM-PUB10 (used by 74 devices)

Server Information

CTI ID: 1

Cisco Unified Communications Manager Server*: 10.106.114.151

Cisco Unified Communications Manager Name*: CM_UCM-PUB10

Description: 10.106.114.151

Location Bandwidth Manager Group: < None >

Auto-registration Information

Universal Device Template*: Auto-registration Template

Universal Line Template*: Sample Line Template with TAG usage examples

Starting Directory Number*: 1000

4. Add a New **User Profile** for Self-Provisioning.

Step 1. Navigate to **User Management > User Settings > User Profile**, as shown in the image.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

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

Cisco Unified CM Administration

System version: 10.5.2.13901-2

VMware Installation: 2 vCPU Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz, **WARNING: DNS unreachable**

Last Successful Backup: 514 day(s) ago

User administrator last logged in to this cluster on Friday, February 15, 2019 8:57:30 PM CST, to node 10.106.114.151, from 10.142.18...

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. 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. In certain countries, users are prohibited from using or distributing this product unless they are permitted to do so under a license issued by the applicable regulatory authority. For more information, contact your local sales representative. This document does not imply third-party authority, and is not intended to be used in any way that would violate applicable laws, return this product to the manufacturer.

- Application User
- End User
- User/Phone Add
- SIP Realm
- User Settings**
 - Credential Policy Default
 - Credential Policy
 - Role
 - Access Control Group
 - Application User CAPF Profile
 - End User CAPF Profile
 - UC Service
 - Service Profile
 - User Profile**
- Self-Provisioning
- Assign Presence Users

Step 2. Add the User Device Template, User Line Template and Check the **Allow End User to Provision their Own Phone** CheckBox.

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

User Profile Configuration

Save **X** Delete **+** Add New

Status
i Status: Ready

User Profile
 Name*
 Description
 Make this the default User Profile for the system

Universal Device Template

| | | |
|------------------------------------|---|------------------------------|
| Desk Phones | <input type="text" value="Auto-registration Template"/> | View Details |
| Mobile and Desktop Devices | <input type="text" value="Auto-registration Template"/> | View Details |
| Remote Destination/Device Profiles | <input type="text" value="Auto-registration Template"/> | View Details |

Universal Line Template

Universal Line Template [View Details](#)

Self-Provisioning

Allow End User to Provision their own phones
 Limit Provisioning once End User has this many phones

Note: These Setting Are Applied When the Users try to Self-Provision the Devices with Their own Extensions.

Note: You Can Also set a Maximum Limit to Users for Number of Devices After Which the Self Provisioning would not work for Users.
 E.g.: if User has 9 devices assigned already since the Maximum limit in Above screenshot is set to 10, User can self-provision only one Device.

Note: If the “Allow End User to Provision their Own Phone” Check-box is left unchecked. Self-Provisioning would not work for Users.

5. Create **Feature Template Group** and assign the **User Profile**. Now navigate to **User Management > User/Phone Add > Feature Group Template** and click **Add New**.

Cisco Unified CM Administration
 For Cisco Unified Communications Solutions



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

Cisco Unified CM Administration
 System version: 10.5.2.13901-2
 VMware Installation: 2 vCPU Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz
 WARNING: DNS unreachable
 Last Successful Backup: 514 day(s) ago

- Application User
- End User
- User/Phone Add**
 - Page Layout Preference
 - Universal Device Template
 - Universal Line Template
 - Feature Group Template**
 - Quick User/Phone Add
- SIP Realm
- User Settings
 - Self-Provisioning
 - Assign Presence Users

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

Feature Group Template Configuration

Save  Delete  Add New

Feature Group Template

Name *

Description

Features

Home Cluster

Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service)

Include meeting information in Presence(Requires Exchange Presence Gateway to be configured on)

Services Profile [View Details](#)

User Profile [View Details](#)

Allow Control of Device from CTI

Enable Extension Mobility Cross Cluster

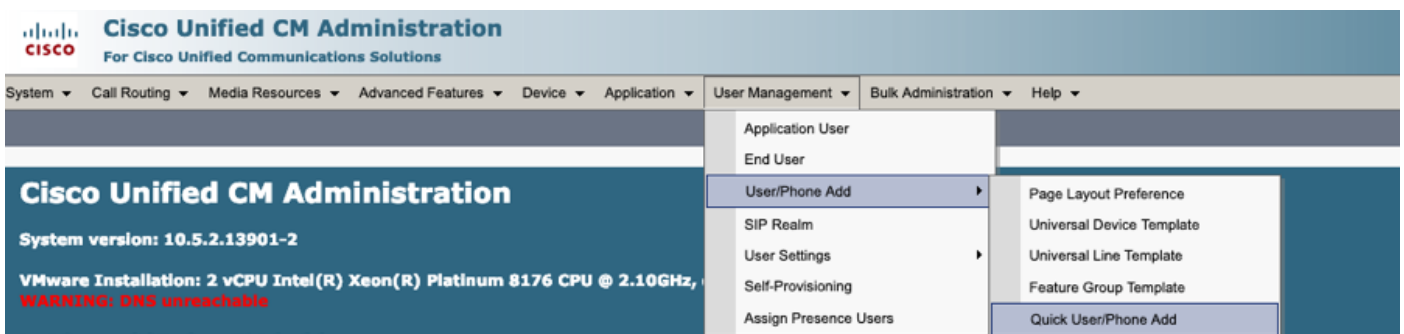
Enable Mobility

Enable Mobile Voice Access

Maximum Wait Time for Desk Pickup *

6. Create a user from **Quick user/phone add** page and Add the **Feature Group Template**.

Step 1. Navigate to **User management > User Phone Add > Quick User/Phone Add**.



Step 2. Add the **Standard CCM End Users** under Access Control Group membership.

Quick User/Phone Add

 Save



User Information

First Name
Middle Name
Last Name *
User ID *
Feature Group Template [View Details](#)

Access Control Group Membership

User is a member of: 

Access Control Group Membership

User is a member of:  

Step 3. Add an extension in the extension field to the User, click on + Icon under Action to enable the Field.

Access Control Group Membership

User is a member of:  

Credentials

Use default credential
Password
Confirm Password
PIN
Confirm PIN

Extensions

| Order | Extension | Line Primary URI/Partition | Action |
|-------|---|---|---|
| | <input type="text"/> New... | <input type="text"/> / <input type="text"/> |  |



Step 4. If a New Extension is to be created click on **New** and Add a New DN, as shown in the image option 1. If the Extension already Exists on CUCM and is to be assigned to User, choose

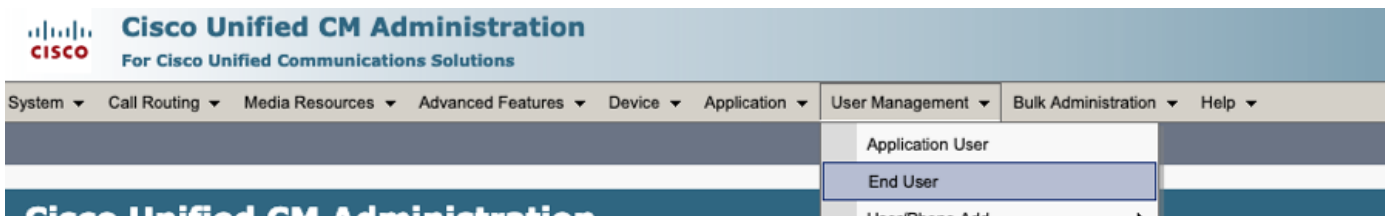
that from Dropdown menu shown in option 2 of the image here.

The screenshot shows the 'Access Control Group Membership' section with a dropdown menu set to 'Standard CCM End Users'. Below is the 'Credentials' section with a checked 'Use default credential' option and input fields for Password, Confirm Password, PIN, and Confirm PIN. The 'Extensions' section contains a table with columns: Order, Extension, Line Primary URI/Partition, and Action. The 'Extension' column has a dropdown menu (labeled with a red '2') and a 'New...' button (labeled with a red '1').

| Order | Extension | Line Primary URI/Partition | Action |
|-------|-------------------------------------|---|----------------------------------|
| | <input type="text" value="New..."/> | <input type="text"/> / <input type="text"/> | <input type="button" value="-"/> |

Note: Once the User is Created, it Takes Primary Line as Self-Service User ID by default.

7. Verify the End User has received the **primary Extension, Self-service User ID, User Profile and Standard CCM End User Role**. Now navigate to **User Management > End User** and Access the newly Created User, as shown in the image.



End User Configuration


 Save  Delete  Add New

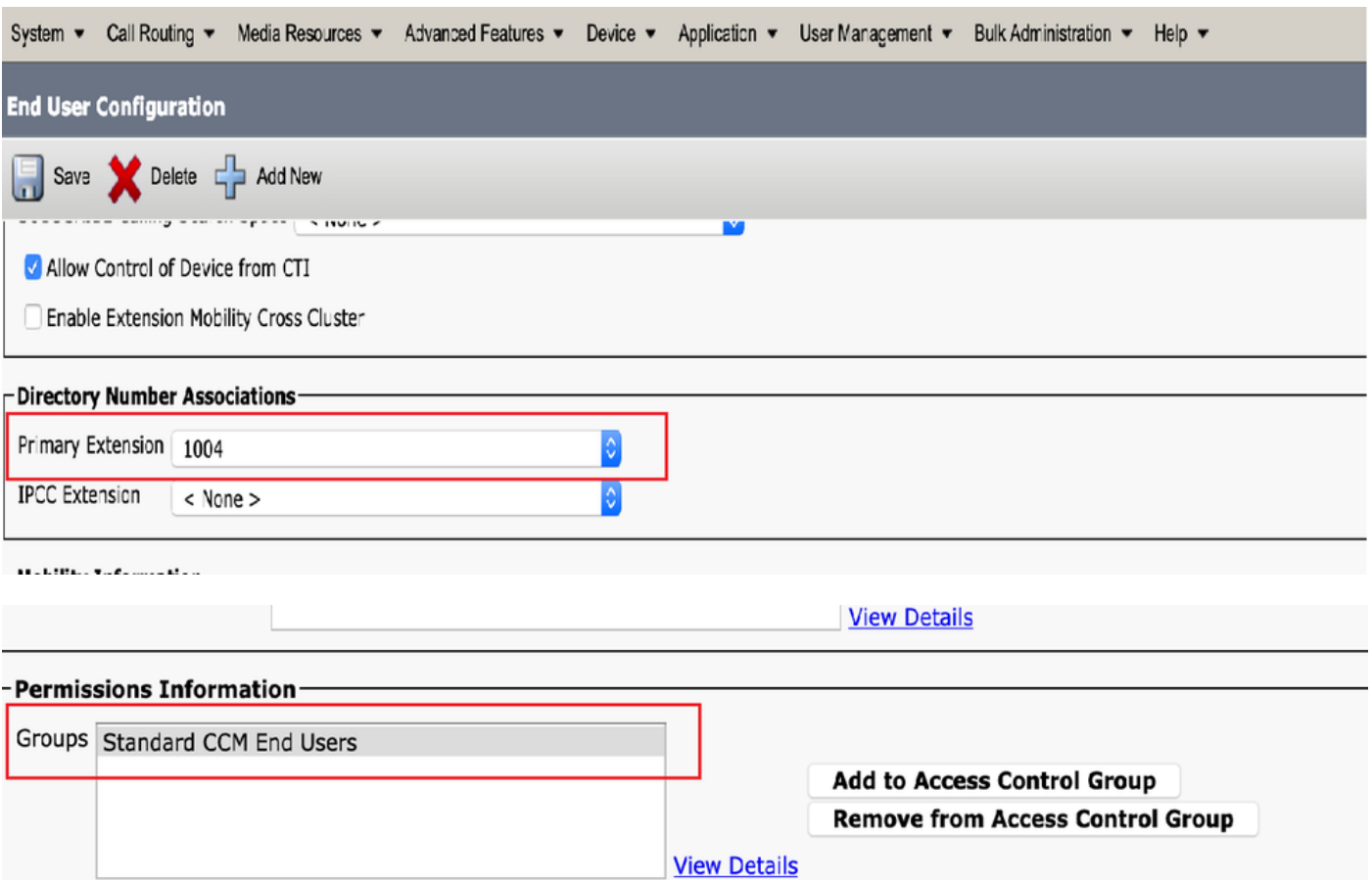
- User Information

| | | |
|----------------------|--------------------------------------|---------------------------------|
| User Status | Enabled Local User | |
| User ID* | <input type="text" value="aksethi"/> | |
| Password | <input type="password"/> | Edit Credential |
| Confirm Password | <input type="password"/> | |
| Self-Service User ID | <input type="text" value="1004"/> | |
| PIN | <input type="password"/> | Edit Credential |
| Confirm PIN | <input type="password"/> | |
| Last name* | <input type="text" value="sethi"/> | |
| Middle name | <input type="text"/> | |
| First name | <input type="text" value="akash"/> | |
| Title | <input type="text"/> | |

End User Configuration

 Save  Delete  Add New

| | | |
|--|---|--|
| User Locale | <input type="text" value="< None >"/> |  |
| Associated PC | <input type="text"/> | |
| Digest Credentials | <input type="password"/> | |
| Confirm Digest Credentials | <input type="password"/> | |
| User Profile | <input type="text" value="selfprc"/> |  View Details |
| Name Dialing | <input type="text" value="sethiakash"/> | |
| Number of Digits needed for the Unique AA Name 2 | <input type="text"/> | |



8. In order to create a **CTI Route point**, navigate to **Device > CTI Route Point**, and click on **Add New**, as shown in the image.



Step 1. Add the Name and Device Pool entries and click on **Save**, as shown in the image.

CTI Route Point Configuration



Save

Status

Status: Ready

Device Information

Device is trusted

Device Name*

Description

Device Pool* [View Details](#)

Common Device Configuration [View Details](#)

Calling Search Space

Location*

User Locale

Media Resource Group List

Network Hold MOH Audio Source

User Hold MOH Audio Source

Use Trusted Relay Point*

Calling Party Transformation CSS

Geolocation

Use Device Pool Calling Party Transformation CSS

Save

Step 2. Add a Directory Number to the CTI Route Point,

Device Information

Registration: Unknown

IPv4 Address: None

Device is trusted

Device Name*

Description

Device Pool* [View Details](#)

Common Device Configuration [View Details](#)

Calling Search Space

Location*

User Locale

Media Resource Group List

Network Hold MOH Audio Source

User Hold MOH Audio Source

Use Trusted Relay Point*

Calling Party Transformation CSS

Geolocation

Use Device Pool Calling Party Transformation CSS

Association

Line [1] - Add a new DN

CTI Route Point Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

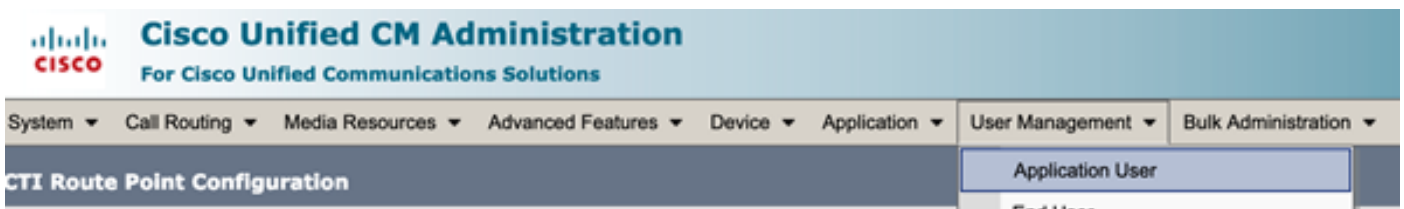
Device Information

Registration: Unknown
IPv4 Address: None
 Device is trusted
Device Name* Self_Pro
Description Self_Pro
Device Pool* Default [View Details](#)
Common Device Configuration < None > [View Details](#)
Calling Search Space < None >
Location* Hub_None
User Locale < None >
Media Resource Group List < None >
Network Hold MOH Audio Source < None >
User Hold MOH Audio Source < None >
Use Trusted Relay Point* Default
Calling Party Transformation CSS < None >
Geolocation < None >
 Use Device Pool Calling Party Transformation CSS

Association

7715 Line [1] - 1111111 (no partition)
7715

9. In order to add a New **Application User**, navigate to **User Management > Application User**, and click on **Add New**.



Step 1. Add the Created **CTI Route Point**, under **Controlled Devices**

Application User Configuration

Save Delete Copy Add New

Status

Status: Ready

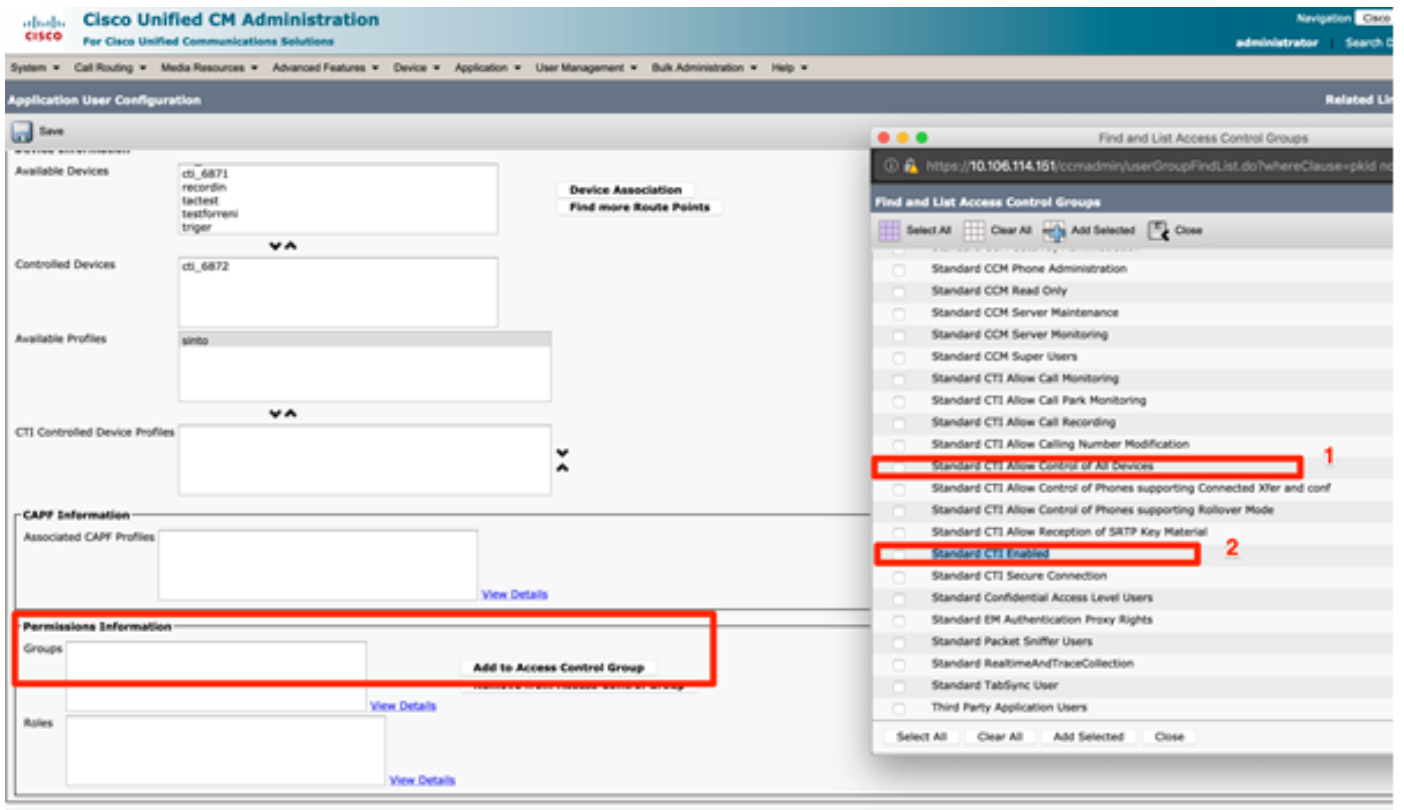
Application User Information

| | | |
|----------------------------|---------------------------------|---------------------------------|
| User ID * | selfpro | Edit Credential |
| Password | | |
| Confirm Password | | |
| Digest Credentials | | |
| Confirm Digest Credentials | | |
| BLF Presence Group * | Standard Presence group | |
| <input type="checkbox"/> | Accept Presence Subscription | |
| <input type="checkbox"/> | Accept Out-of dialog REFER | |
| <input type="checkbox"/> | Accept Unsolicited Notification | |
| <input type="checkbox"/> | Accept Replaces Header | |

Device Information

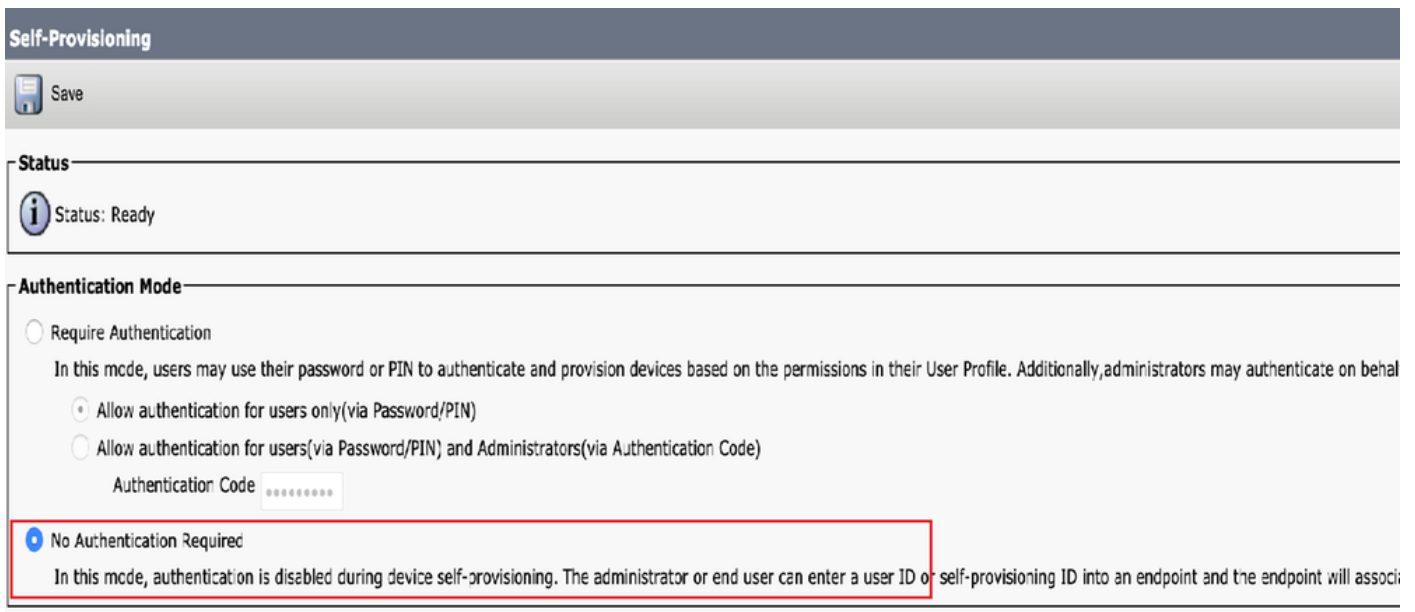
| | | |
|--------------------|--|--|
| Available Devices | Sample Device Template with TAG usage examples Self:procti TEST UPCNTPC VTNMLL | Device Association Find more Route Points |
| Controlled Devices | Self_Pro | |

Step 2. Add the **Standard CTI Enabled** and **Standard CTI Allow Control of All Devices** under Permission Information Section.



10. Self-Provisioning Service Can be Set up at the System Level to Use Secure mode and a Password can be set. This feature is set to **Non-Authentication Required** Mode by default, which Does not Require any PIN to Use Self Provisioning.

Step 1. Navigate to **User Management > Self-Provisioning**.




Step 2. Add the **CTI Route Point** and **Application User** to **Self-Provisioning**.

Self-Provisioning

 Save

- Status

 Status: Ready

- Authentication Mode

Require Authentication

In this mode, users may use their password or PIN to authenticate and provision device

Allow authentication for users only(via Password/PIN)

Allow authentication for users(via Password/PIN) and Administrators(via Authentication Code)

No Authentication Required

In this mode, authentication is disabled during device self-provisioning. The administrat

- IVR Settings

Language Preference

Available Language

简体中文, 普通话, 简体字, 中华人民共和国

Selected La

English, Ur

CTI Route Point

Self_Pro



Dial 1111111 from

Application User

selfpro



Note: Every time a Configuration change is made on IVR Settings, a Restart of Self Provisioning IVR Setting is required to trigger the change.

Services Associated with Self-Provisioning

Cisco Call Manager

This Service is associated with the Phone registration and Must be enabled on the Node to which registration is attempted.

Self Provisioning IVR

This Service can be found under **CM services** on **Feature Services** Page In **Cisco Unified Serviceability**.

Note: You can configure self-provisioning even if the service is deactivated, but the administrator cannot assign IP phones to users using the IVR service. By default, this service is deactivated.

Note: Self-provisioning IVR service runs only on Publisher.

End-user experience on the Phone

- End User Dials the CTI Route Point and is Prompted to enter the Self-Service ID.
- The user is asked to Confirm the Self-Service ID and enter the PIN.
- Once the PIN is verified the Device goes for a reboot to get the new Extension.

Troubleshoot

Error: Alert “device Cannot be provisioned” is received.

Cause: Device is Already Provisioned, cannot be re-provisioned.

Logs to be Collected

In order to further troubleshoot, Collect the “Self-Provisioning IVR service” Log from RTMT.

File names are of format PnP#####.log. (# represents a number.)

The Traces are Set to Info Level by Default.

The maximum file size is 1 MB by default. The maximum number of stored files defaults to 10.

Note: When you change either the Maximum No. of Files or the Maximum File Size settings in the Trace Configuration window, the system deletes all service log files except for the current file, that is, if the service runs.

If the service has not been activated, the system deletes the files immediately after you activate the service.

Known defects

[CSCun16461](#)

Related Information

- [Technical Support & Documentation - Cisco Systems](#)