Skype for Business 2019 using SIP trunk (TLS) to Cisco Unified Communications Manager Release 12.5.1

Table of Contents

Introduction

This document describes the steps and configurations necessary for Cisco Unified Communications Manager (Cisco UCM) release 12.5.1 to interoperate with the Skype for Business 2019 on TLS using the following configuration:

The following items were tested:

- Basic call between the two systems and verification of voice path, using both SIP and Legacy phones on the Cisco side, and SIP client on the Skype for Business side (Refer to limitation section for more info)
- CLIP/CLIR/CNIP/CNIR features: Calling party Name and Number delivery (allowed and restricted) (Refer to limitation section for more info)
- COLP/CONP/COLR/CONR features: Connected Name and Number delivery (allowed and restricted) (Refer to limitation section for more info)
- Call Transfer: Attended and Early attended (Refer to limitation section for more info)
- Alerting Name Identification (Refer to limitation section for more info)
- Call forwarding: Call Forward Unconditional(CFU), Call Forward Busy (CFB), and Call Forward No Answer (CFNA)
- Hold and Resume with Music on Hold
- Three-way conferencing (Refer to limitation section for more info)
- Voice messaging and MWI activation-deactivation (Refer to limitation section for more info)
- Extend and Connect (Refer to limitation section for more info)
- Call Park (Refer to limitation section for more info)

Listed below are the highlights of the integration issues:

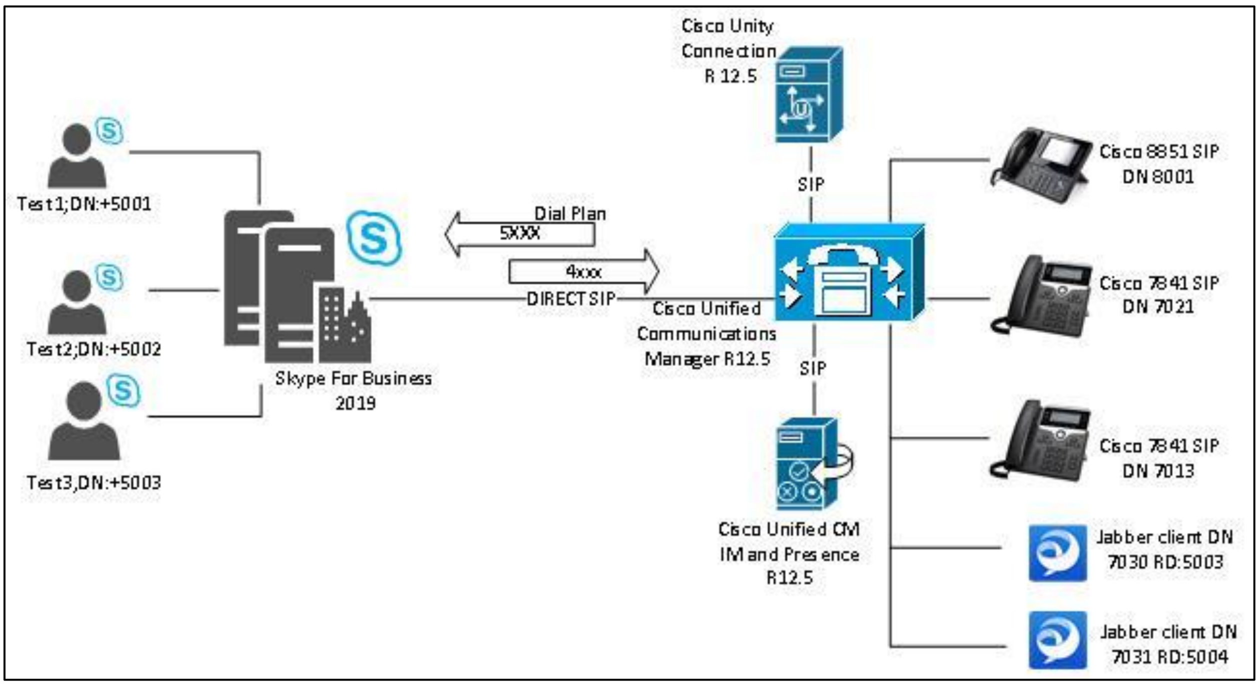
- Basic calls work from Cisco UCM to Skype for Business and vice versa. Only Cisco SIP phones were used on Cisco UCM side as SCCP phones do not support 80-bit crypto attribute required by Skype for Business
- Skype for Business drops the call on HOLD after 30 seconds where the call hold inititated from Skype for Business client.
- Basic calls work from Cisco UCM to Skype for Business and vice versa using G711 ulaw and alaw
- Caller name and number is not updated correctly for basic calls, attended and early-attended transfer scenarios
- Video calls between the Cisco UCM and Skype for Business users were not tested
- REFER support should be disabled in Skype for Business for the Call Park scenarios
- Skype for business does not consider privacy:id sent in 18x and 2xx message from Cisco UCM

- A call placed on hold by the Skype client is dropped after 30 seconds when Skype for Business Server 2019 version 7.0.2046.123 is used. The issue is resolved with the newer release of Skype for Business 2019 version 7.0.2046.151 and above.

Below are the key results:

- Basic call, Call Transfer, Call Forwarding, Conference Call, and Hold and Resume tested successfully with a few caveats and limitations.
- Centralized voicemail, using Unity Connection server integrated with Cisco UCM via SIP is used for testing. This voicemail solution can provide centralized voicemail services, supporting both Skype for Business users and Cisco end users.

Network Topology



Limitations

These are the known limitations, caveats, or integration issues:

- Skype for Business does not support G729 codec. Trunk tested with only G711 ulaw and alaw.
- Disable Media Bypass on Skype for Business. If enabled, the Hold INVITE sent by Cisco UCM (without SDP) being rejected with 488 on Skype for Business.
- Skype for Business and Cisco UCM does not support overlap dialing modes on their SIP endpoints

- Skype for Business does not consider Privacy: ID parameter sent by Cisco UCM during 180 Ringing or 200 OK when Connected Name/ID is resticted on Cisco UCM. Subsequently, Skype for Business does not support updating the Connected Party’s display as Private.
- Skype for Business does not update the CLID in transfer/conference scenarios. After transfer/conference is completed, Cisco UCM sends mid call INVITE and UPDATE messages that contain PAI and RPI. Skype for Business does not update this information on thier client display.
- Skype for Business sends incorrect number in history-info during forward scenarios. As a work around Skype for Business, users DN are configured with a prefix "+".
- Cisco UCM Remote Destination is configured with a prefix “+” and a Route Pattern to route a DN with a preix ‘+’ is added. (Refer Cisco UCM configuration section - Cisco Unified Communications Manager Route Pattern to invoke Jabber client with Remote Destination configured as Skype for Business Extension).
- Skype for Business does not support MWI notification from Cisco Unity Connection. It responds with a “405 Method Not Allowed” for a NOTIFY Message received from the Cisco UCM that has MWI information.
- In Multiple Call Forwarding scenario between Skype for Business Users and Cisco UCM Users, wherein both originator and terminator being Skype for Business Users, originator does not display the Caller ID of terminator.
- When Cisco UCM User completes the conference, the audio is on RTP. Pad-lock symbol on the Cisco phone disappears.
- When Skype for Business user makes a caller ID, restricted call to Cisco Phone A, caller ID is displayed as Private. However, when Cisco Phone A transfers the call to Cisco Phone B, the caller ID displayed on Cisco Phone B is Skype for Business user’s caller ID instead of displaying as Private.

System Components

Hardware Requirements

The following hardware are used:

- Cisco UCS-C240-M3S VMWare Host
- Cisco 8851 and 7841 IP phones

Software Requirements

The following software are used:

- Cisco UCSC-C240-M3S VMware vSphere Image Profile: ESXi-5.5.0-1331820-standard
- Cisco Unified Communications Manager release 12.5.1.11900-146
- Cisco Unified Communications Manager IM & Presense Service release 12.5.1.11900-117
- Cisco Unity Connection release 12.5.1.11900-57
- Cisco Jabber 12.6.1.34405 Build 284405
- Skype for Business Server 2019 version 7.0.2046.0
- Skype for Business Client version 16.0.11328.20390

Features

This section lists supported and unsupported features. No deviation from the configuration presented in this document will be supported by Cisco. Please see the Limitations section for more information.

Features Supported

- CLIP—calling line (number) identification presentation
- CLIR—calling line (number) identification restriction
- CNIP—calling Name identification presentation
- CNIR—calling Name identification restriction
- Attended call transfer
- Early attended call transfer
- CFU—call forwarding unconditional
- CFB—call forwarding busy
- CFNA—call forwarding no answer
- COLP—connected line (number) identification presentation
- COLR—connected line (number) identification restriction
- CONP—connected Name identification presentation
- CONR—connected Name identification restriction
- Hold and resume
- Conference call
- MWI—Message Waiting Indicator (only for Cisco Endpoints)

- Audio Codec Preference List
- Call Park/Pickup(see limitation section)
- Extend and Connect
- Shared Line on Cisco Endpoints

Features Not Supported or Not Tested

- G729 voice codec
- Call completion (callback, automatic callback)
- Shared Line on Skype for Business
- Message Waiting Indicator on Skype for Business Endpoints
- Blind transfer
- Video calls
- Scenarios that required third PBX.
- Scenarios involving Non-SIP interfaces
- Scenarios involving Cisco UCM SCCP Phones
- Scenarios involving Non-SIP interfaces
- Connected party restriction sends and receives on Skype for Business Server is not supported

Configuration

The goal of this guide is to provide an overview of the integration between Cisco Unified Communication Manager and Skype for Business. The deployment will interconnect the UC systems using SIP. No PSTN connectivity has been tested with this integration. The following sections provide the required configurations for a successful integration.

Global Trunk Configuration Highlights:

Setting	Value
Skype for Business Media Bypass	DISABLED
Skype for Business Encryption Support	OPTIONAL
Skype for Business REFER Support	DISABLED
Cisco UCM SIP Trunk MTP	DISABLED
Cisco UCM PRACK	ENABLED
Cisco UCM Early Offer	ENABLED
Transport type Cisco UCM to Skype for Business	TLS
Cisco UCM SRTP allowed	Enabled

Configuring Sequence and Tasks:

Configuring the Skype for Business:

- Add Cisco UCM to Skype for Business Topology
- Trunk Configuration
- Route Configuration
- Voice Policy and PSTN Usage Configuration
- Dial Plan Configuration
- Call Park range Configuration
- Media Bypass Configuration
- User Configuration
- Client Configuration

Configuring the Cisco Unified Communications Manager:

- SIP trunk security profile
- SIP profile
- Media resource group and media resource group list
- Assign media resource group list (MRGL) in the default device pool
- Region configuration
- Normalization script

- SIP trunk to Skype for Business
- SIP Trunk to Cisco Unity Connection
- Assign User in Cisco Unity Connection
- SIP phones device configuration
- Route Group, Route List and SIP Route Pattern
- Voice Mail
- Route pattern to Skype for Business, Unity Connection and Skype for Business call Park Range
- Extend and Connect Feature and User configuration

Configuring the Cisco Unity Connection:

- Cisco Unity Connection Telephony Integration
- Cisco Unity Connection User Configuration

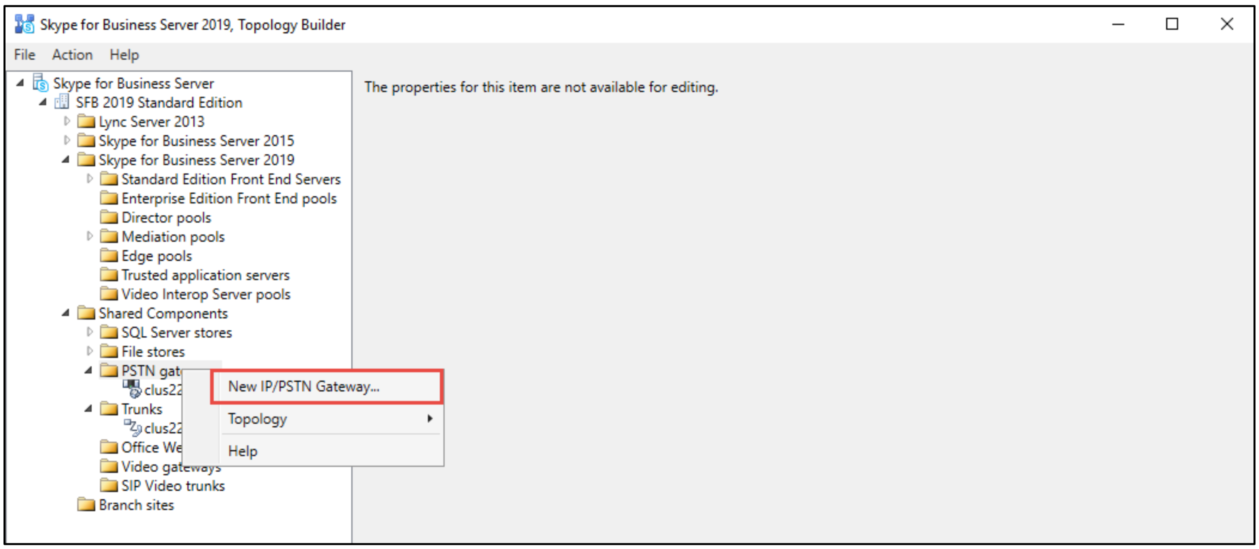
Configuring the Skype for Business

Add Cisco UCM to Skype for Business Topology

Run the Skype for Business 2019 Topology Builder as a user in the CSAdministrator group.

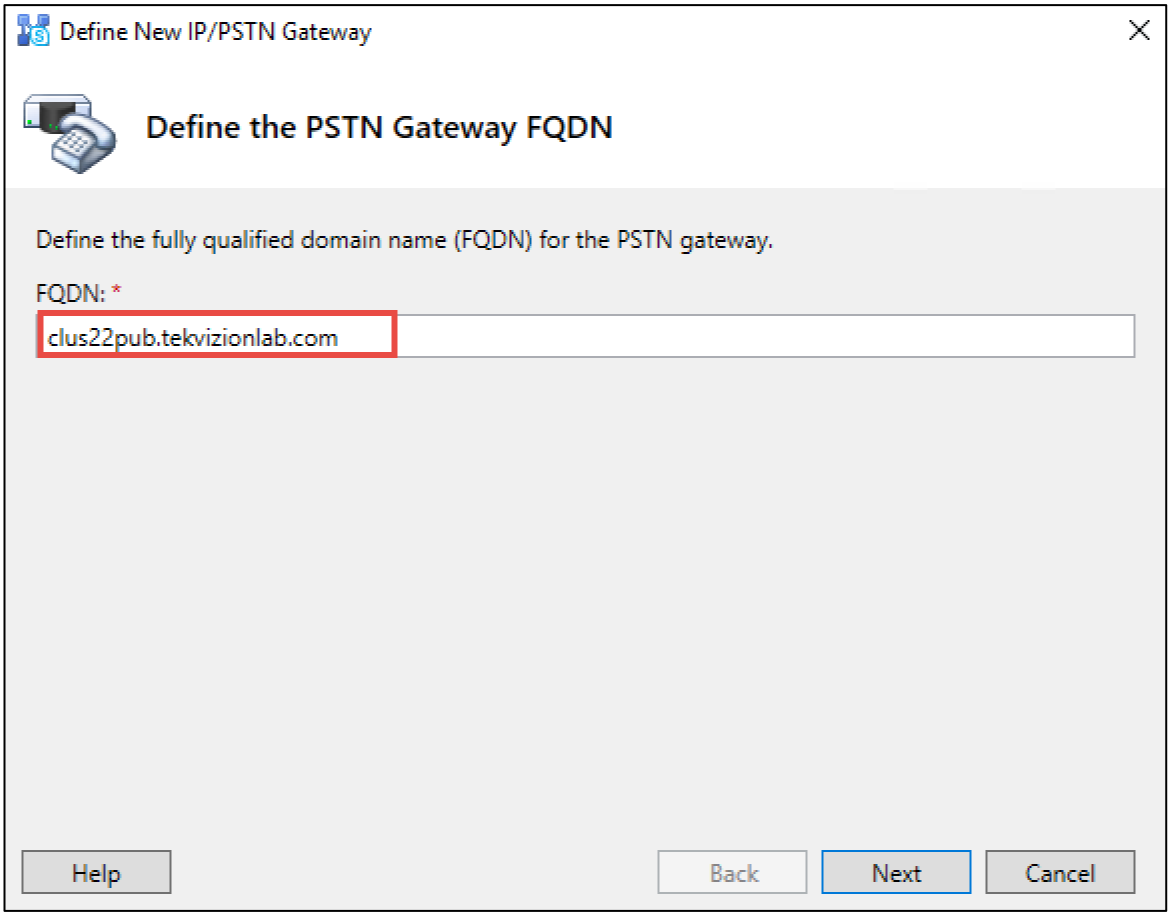
Navigation: Skype for Business Server→CleanDefaultTopology→Shared Components→PSTN gateways

Right click and select "New IP/PSTN Gateway"

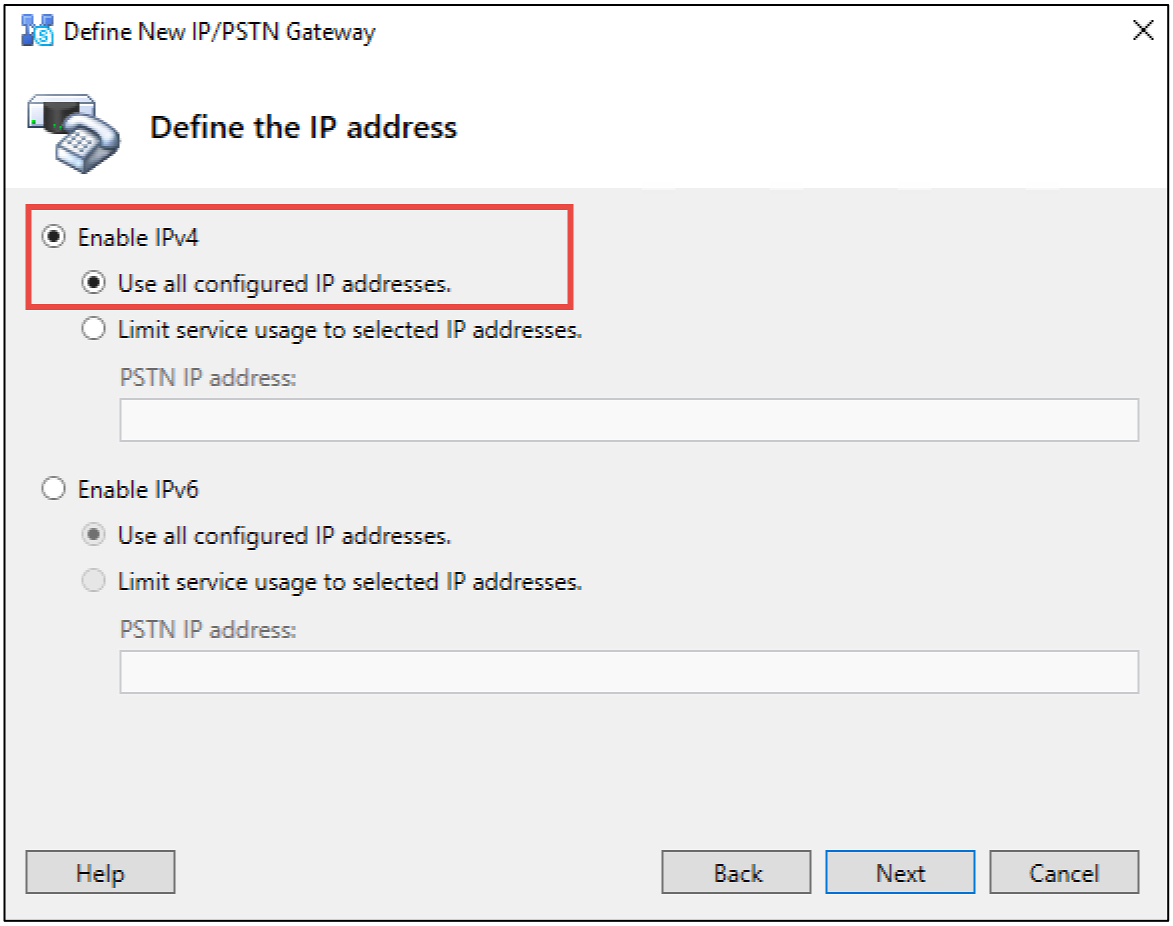


Set FQDN = <FQDN of the Cisco UCM>– clus22pub.tekvizionlabs.com is used in this test.
Click Next.

Skype for Business – Add PSTN Gateway (Continued)

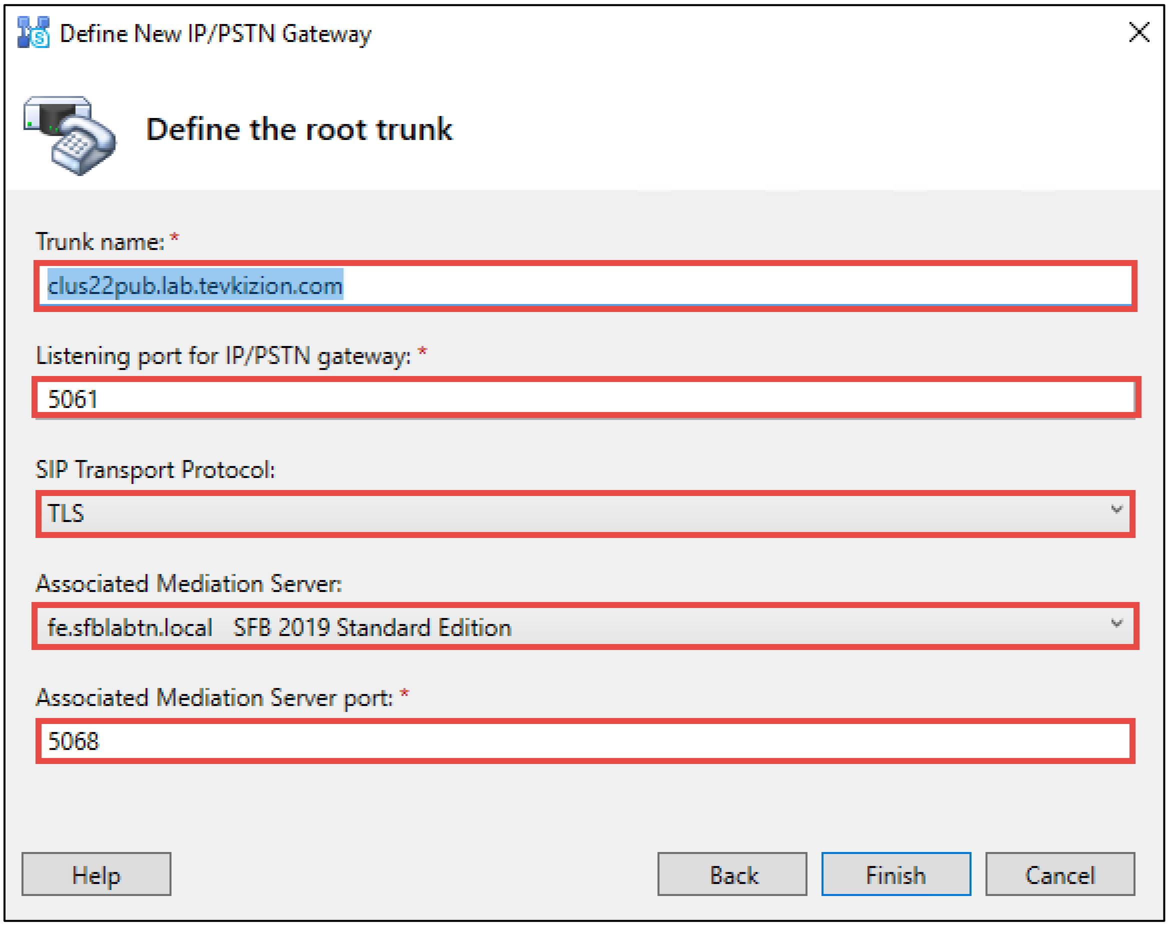


Check the Enable IPv4 and Use all configured IP addresses radio button
Click Next.



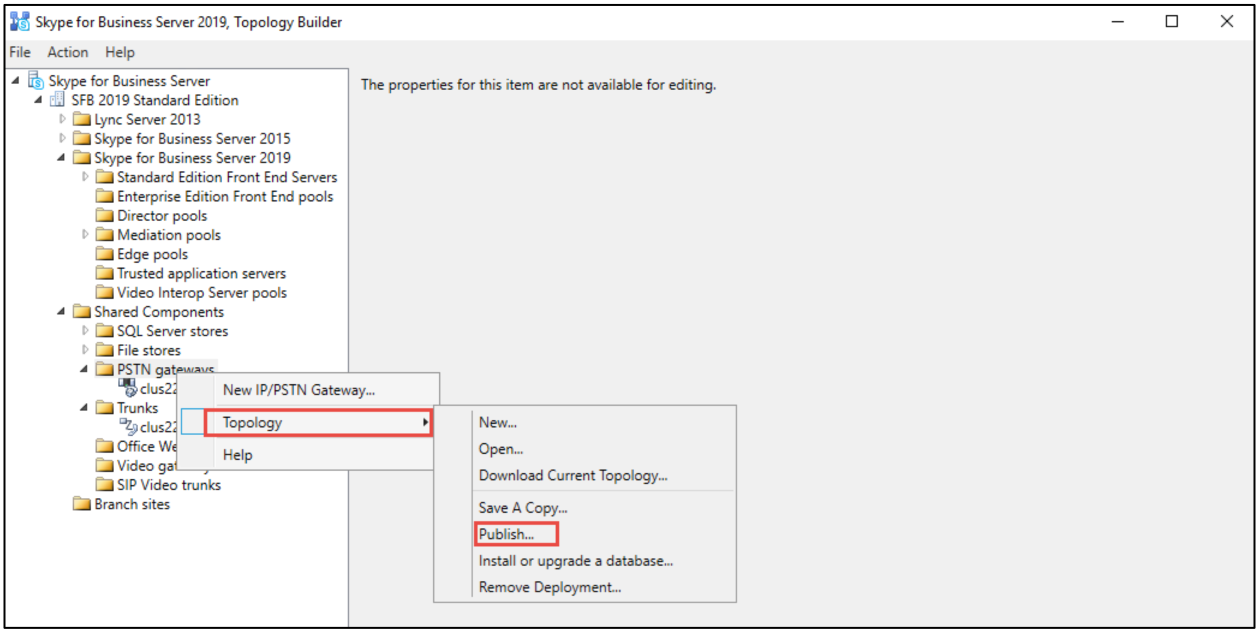
Set **Trunk Name** = FQDN of the Cisco UCM – **clus22pub.tekvizionlabs.com** is used for this test
Set **Listening port for IP/PSTN gateway =** The **Listening port** should match the **Incoming Port** setting in the CISCO UCM's **SIP Trunk Security Profile – 5061** is used for this test
Set **SIP Transport Protocol** = TLS
Set **Associate Mediation Server**: Assign this PSTN gateway to the Front End co-located mediation server – **fe.sfblabtn.local** is used for this test.
Click Finish.

Skype for Business – Add PSTN Gateway (Continued)



Publish the topology so these new configurations take effect.

Skype for Business – Add PSTN Gateway (Continued)

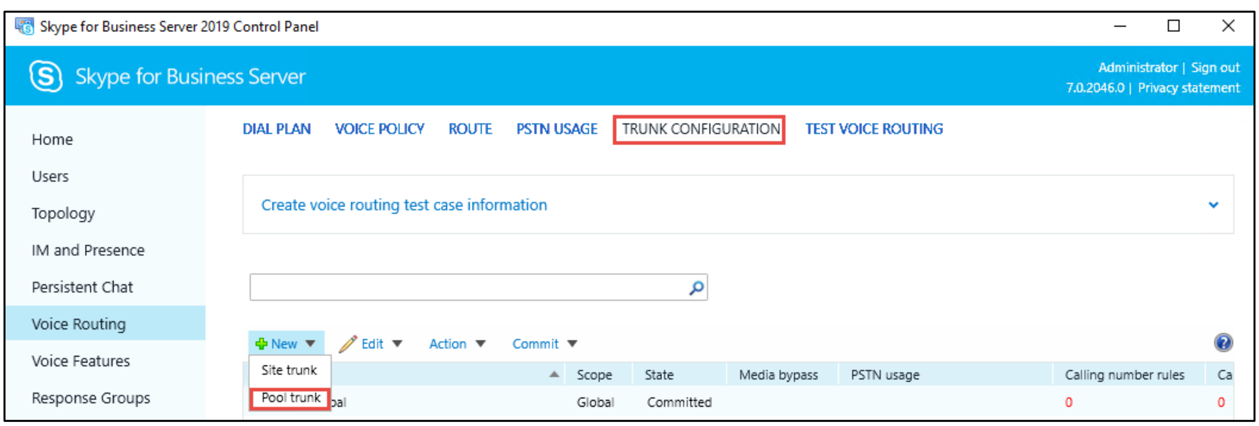


Trunk Configuration

Open the Skype for Business 2019 Control Panel.

Navigation: Voice Routing -> Trunk Configuration

Select New →Pool Trunk



Set **Service** = Trunk to Cisco UCM that was created earlier as a PSTN gateway in the topology builder – clus22pub.tekvizionlabs.com is used for the test.

Set **Maximum early dialogs supported** = **23**

Set **Encryption support level = Optional**

Set **Refer Support = None**

Uncheck **Enable media bypass**

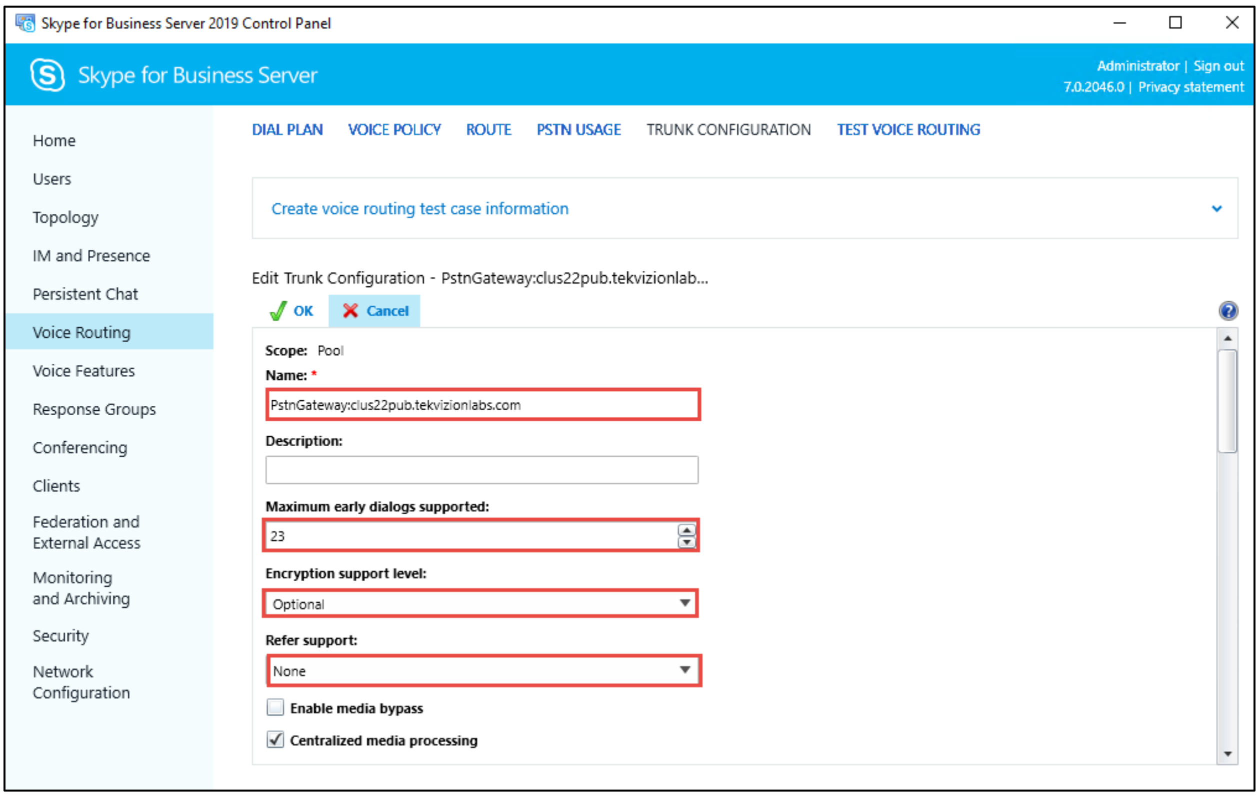
Check **Centralized media processing**

Uncheck **Enable RTP latching**

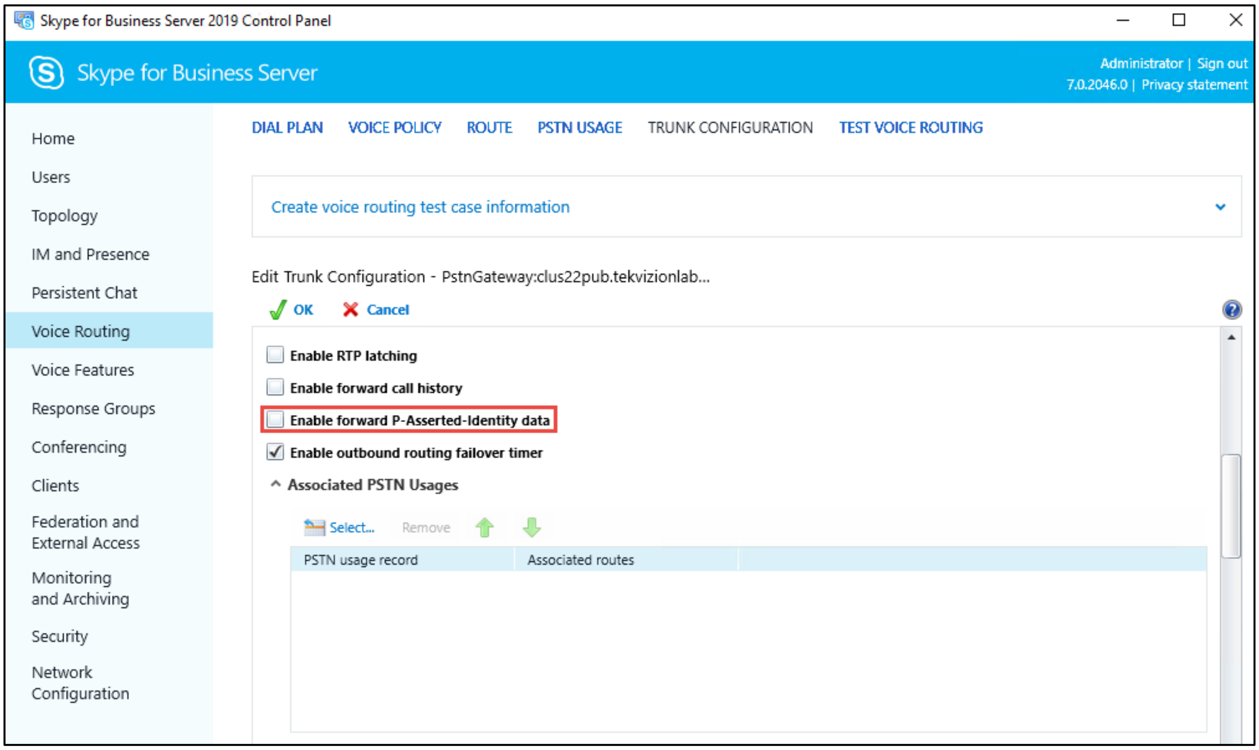
Check **Enable forward call history**

Uncheck **Enable forward P-Asserted-Identity data*** [Note: this is checked when test scenarios that involve restrict ID need to be executed]

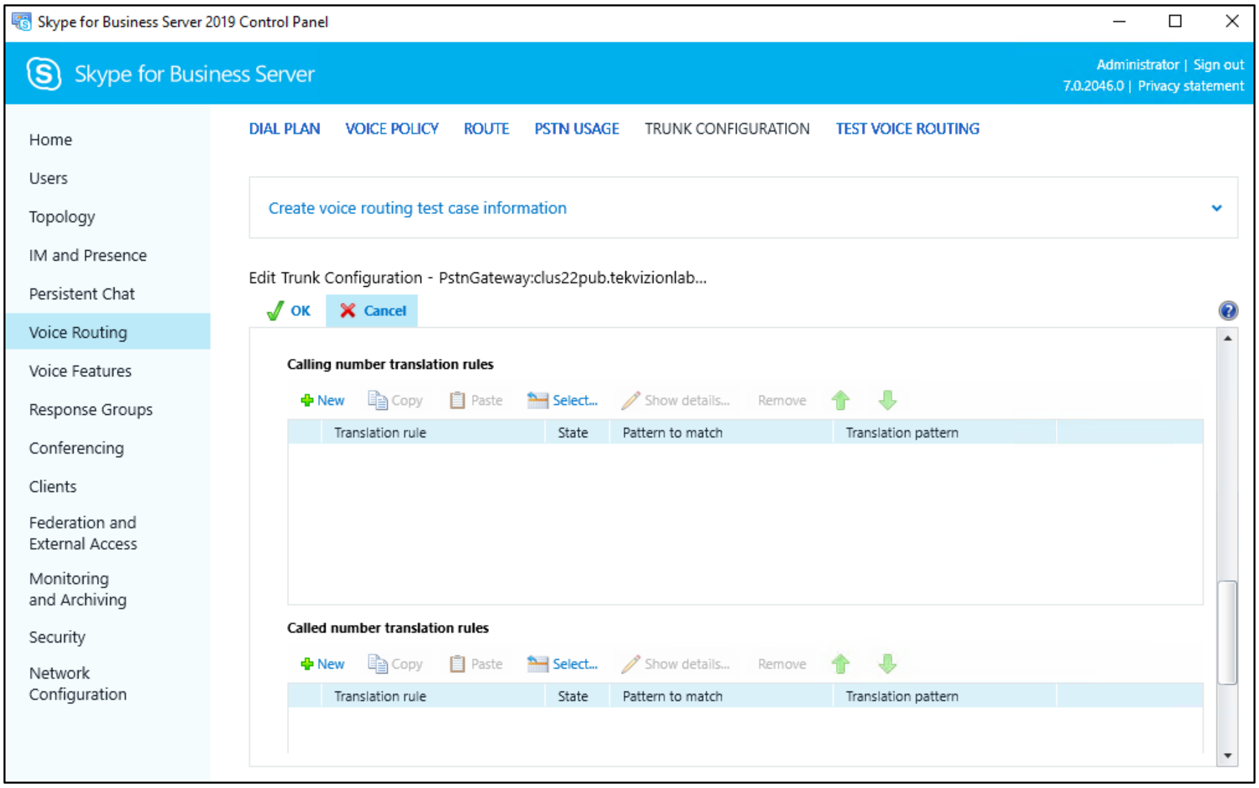
Uncheck **Enable outbound routing failover timer**



Skype for Business –Trunk Configuration (Continued)



Skype for Business –Trunk Configuration (Continued)



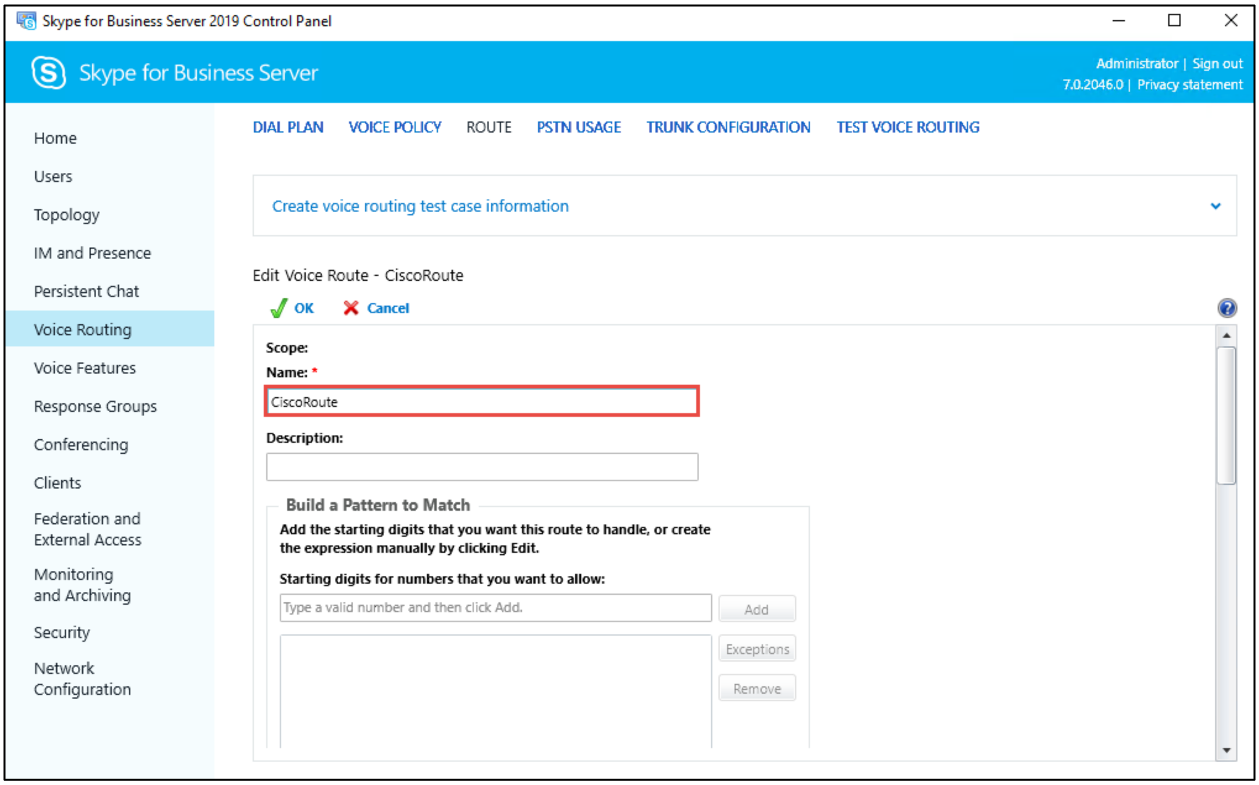
Route Configuration

Navigation: Voice Routing -> Route

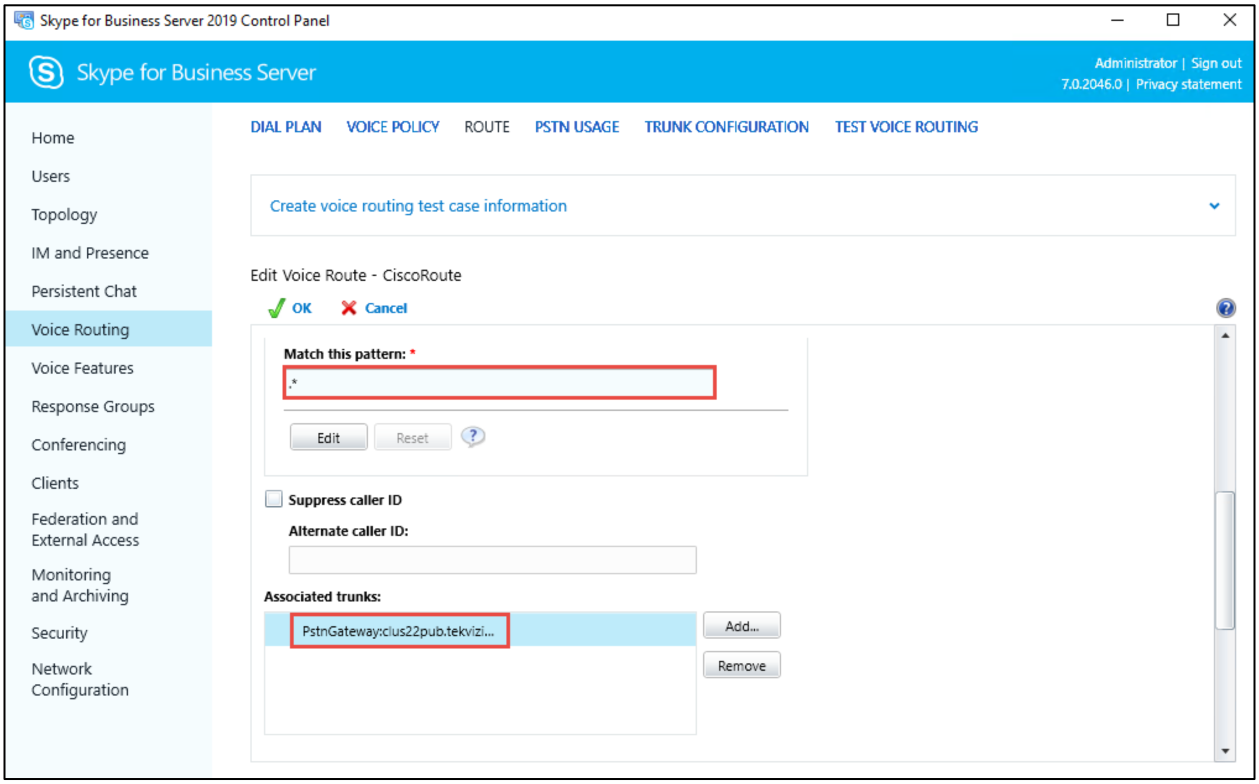
Click New

Set Name = enter a name to identify this Route. CiscoRoute is used for this test.

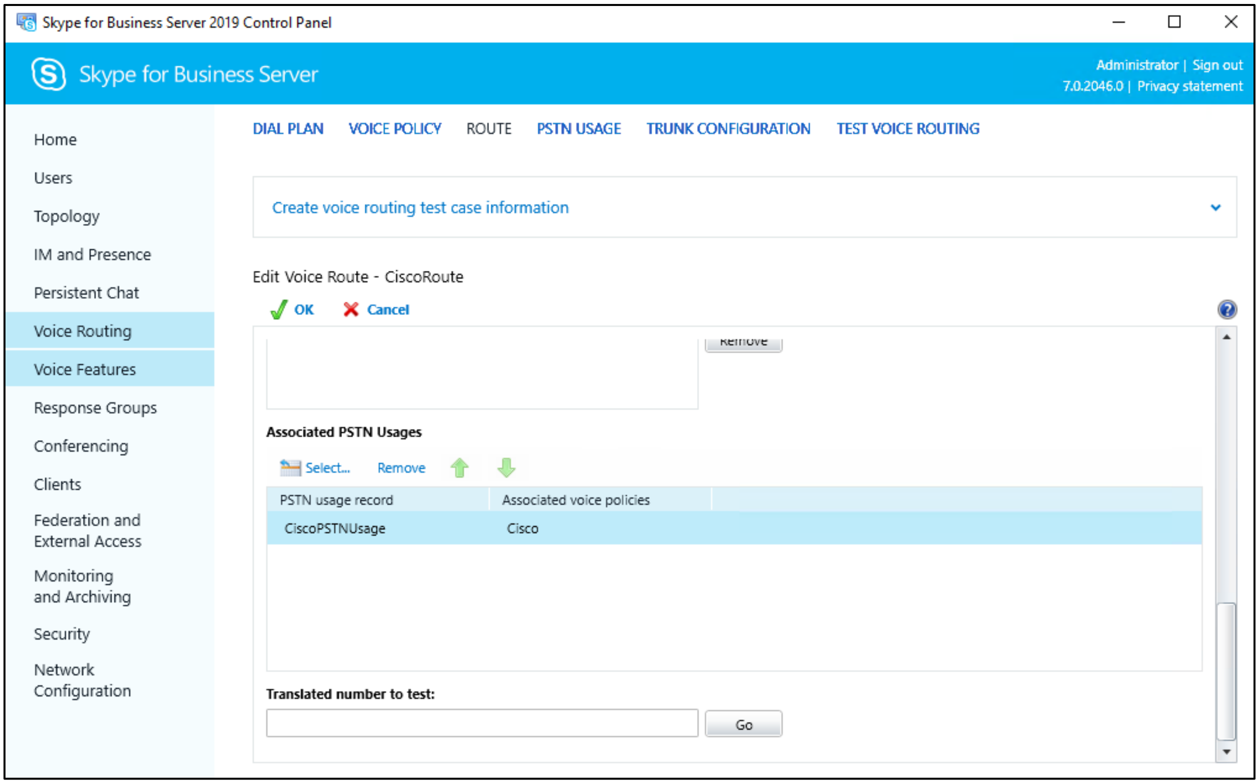
Add associated trunks = select the trunk configured earlier – PstnGateway: clus22pub.tekvizionlabs.com



Skype for Business –Route Configuration (Continued)



Skype for Business –Route Configuration (Continued)



Voice Policy and PSTN Usage Configuration

Navigation: Voice Routing -> Voice Policy

Click New

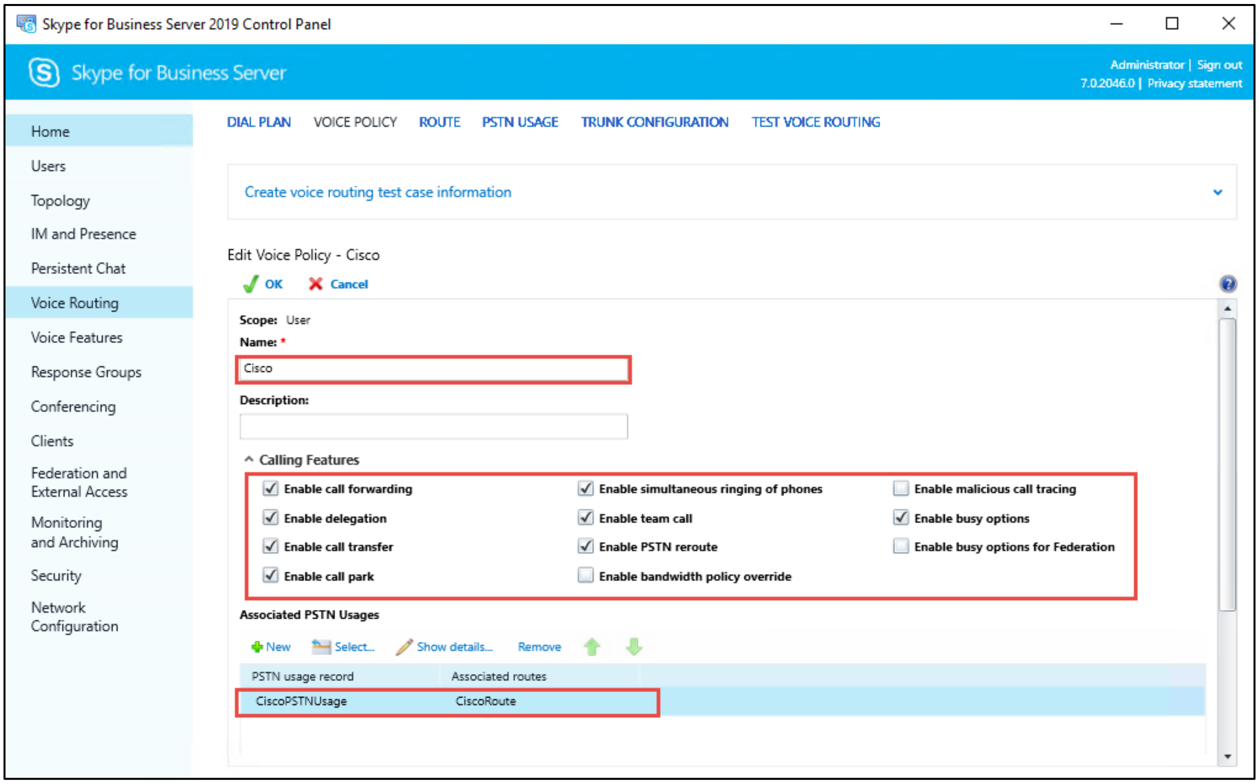
Set Name = enter a name to identify this voice policy – Cisco is used in this test.

Set Calling Features:

- Check Enable call forwarding
- Check Enable delegation
- Check Enable call transfer
- Check Enable call park
- Check Enable simultaneous ringing of phones
- Check Enable team call
- Check Enable PSTN reroute
- Uncheck Enable bandwidth policy override
- Uncheck Enable malicious call tracing
- Enable Busy options
- Uncheck Enable busy options for Federation

Set Associated PSTN usages:

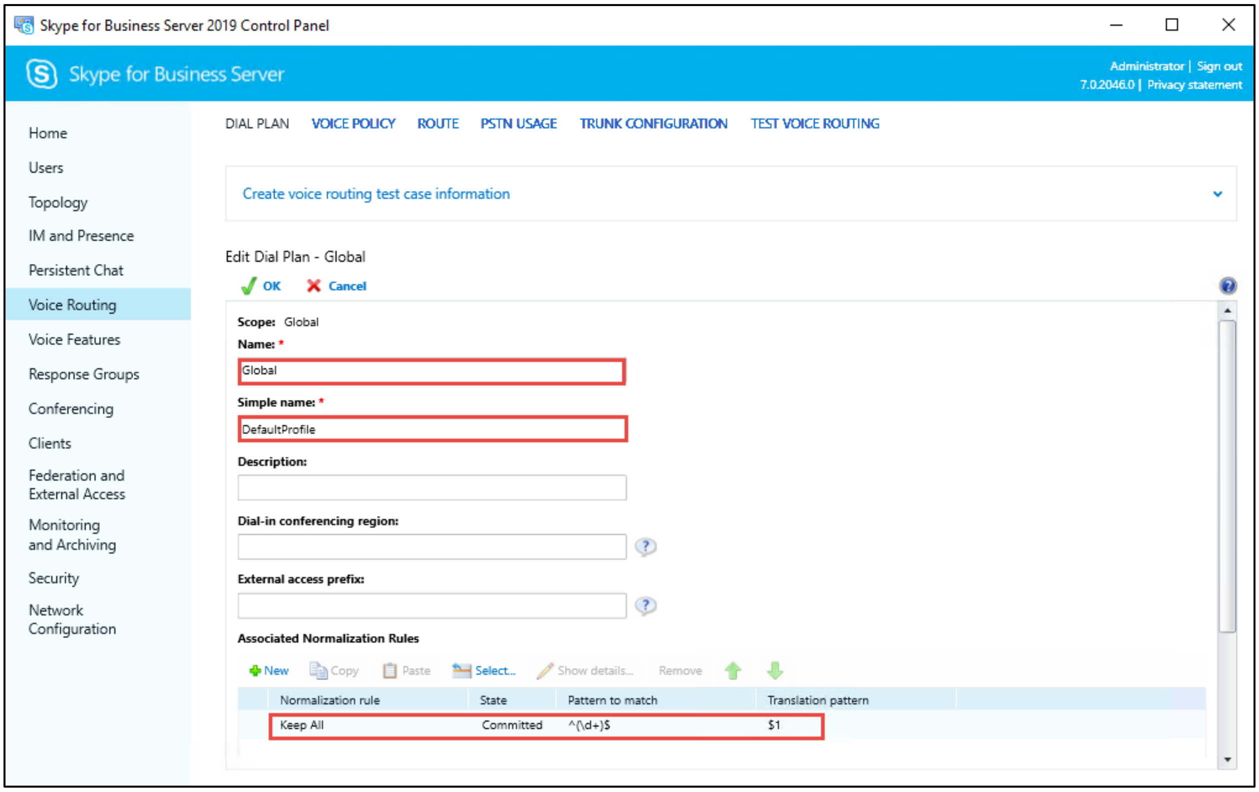
- Click New
- Set Name: enter a name to identify the PSTN Usage record – CiscoPSTNUsage is used in the test.
- Set Associated Routes = select the route created earlier= CiscoRoute


Skype for Business Server 2019 Control Panel
Skype for Business Server
Administrator | Sign out
7.0.2046.0 | Privacy statement
Home
Users
Topology
IM and Presence
Persistent Chat
Voice Routing
Voice Features
Response Groups
Conferencing
Clients
Federation and External Access
Monitoring and Archiving
Security
Network Configuration
DIAL PLAN
VOICE POLICY
ROUTE
PSTN USAGE
TRUNK CONFIGURATION
TEST VOICE ROUTING
Create voice routing test case information
Edit Voice Policy - Cisco
OK
Cancel
Scope: User
Name: *
Cisco
Description:
Calling Features
Enable call forwarding
Enable simultaneous ringing of phones
Enable malicious call tracing
Enable delegation
Enable team call
Enable busy options
Enable call transfer
Enable PSTN reroute
Enable busy options for Federation
Enable call park
Enable bandwidth policy override
Associated PSTN Usages
New
Select...
Show details...
Remove
PSTN usage record
Associated routes
CiscoPSTNUsage
CiscoRoute

Dial Plan Configuration

Navigation: Voice Routing-> Dial Plan

Default Dial plan used for this topology



Call Park Range Configuration

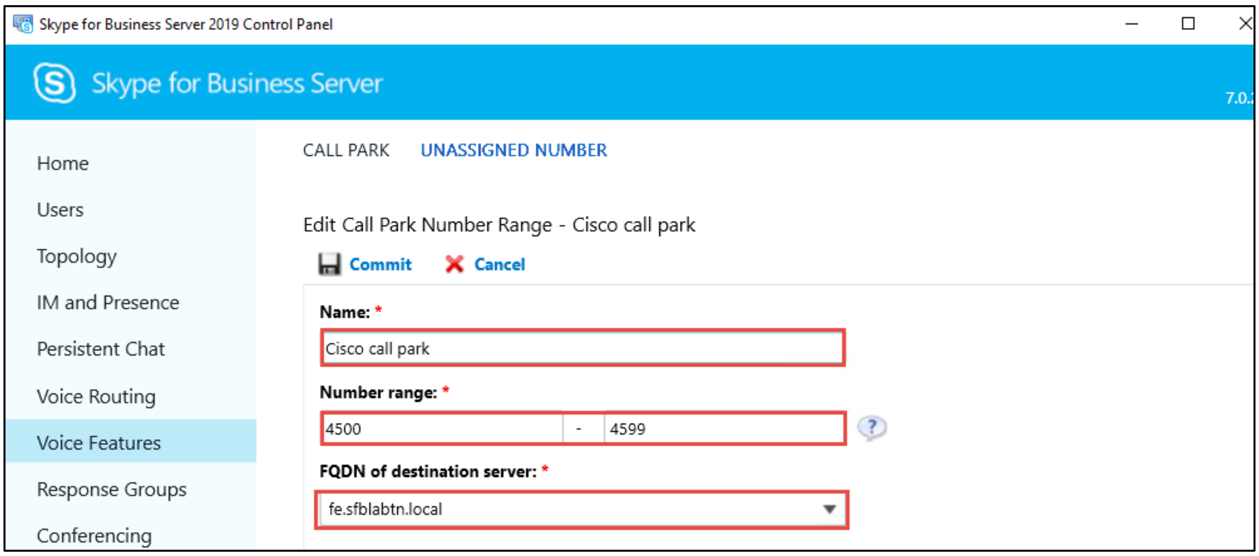
Navigation: Voice Features -> Call Park

Click New.

Set **Name** = enter text to identify the call Park Range – Orbit range is used in the test.

Set **Number Range** = 4500 to 4599 is used in the test.

Set **FQDN of destination server**= select the desired server – fe.sfblabtn.local is used in the test



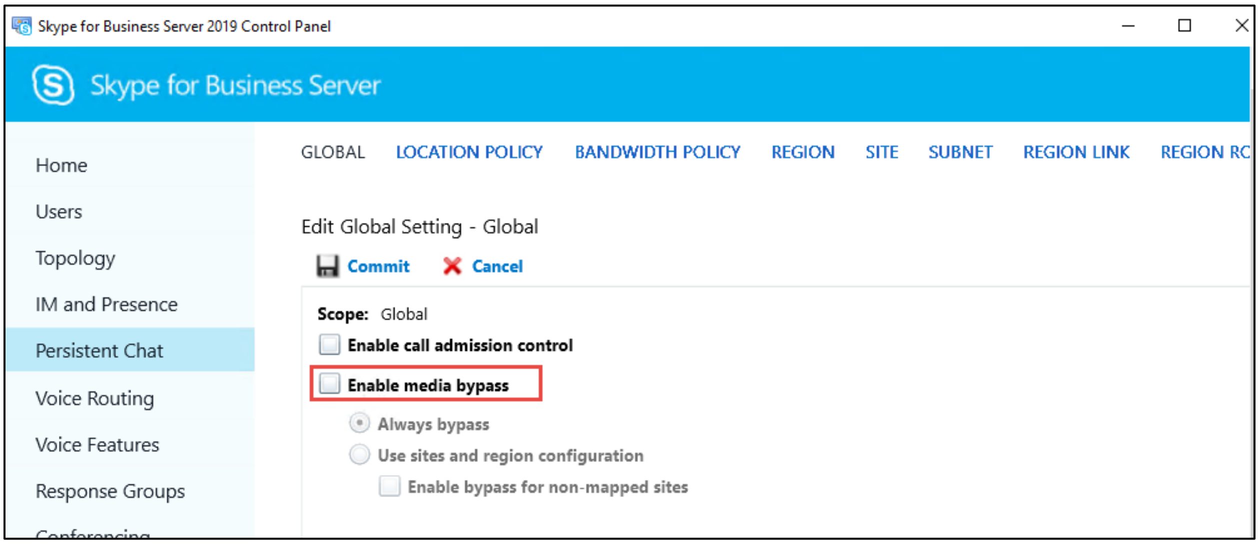
Global Media Bypass Configuration

Navigation: Network Configuration -> Global

Edit Global Setting –

- Uncheck Enable media bypass

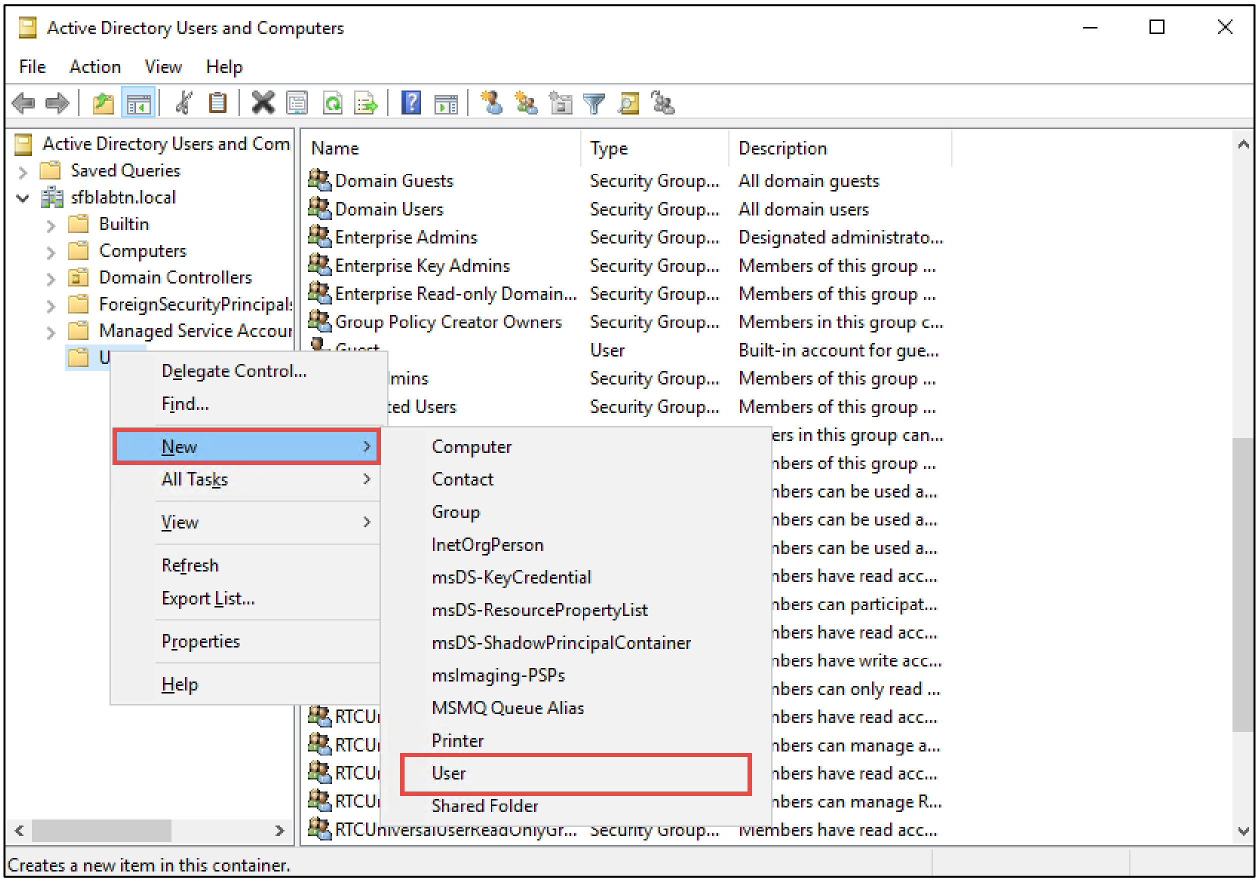
Commit the configuration.



User Configuration

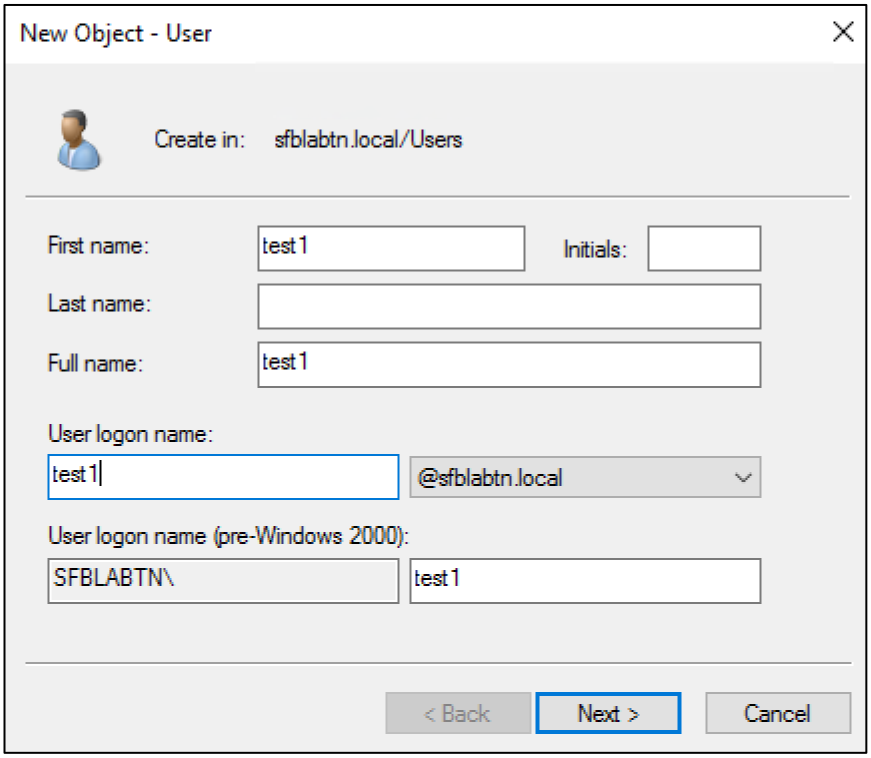
Login to the Skype for Business Active Directory

Navigation: Active Directory Users and Computers →Users
Add a New User

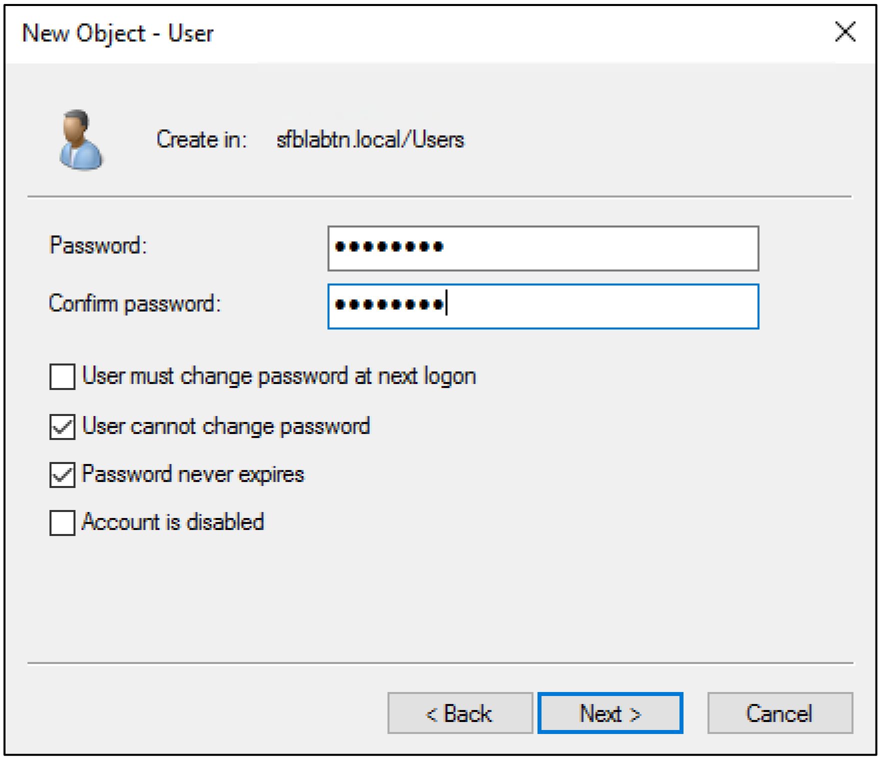


Skype for Business – New User configuration (continued)

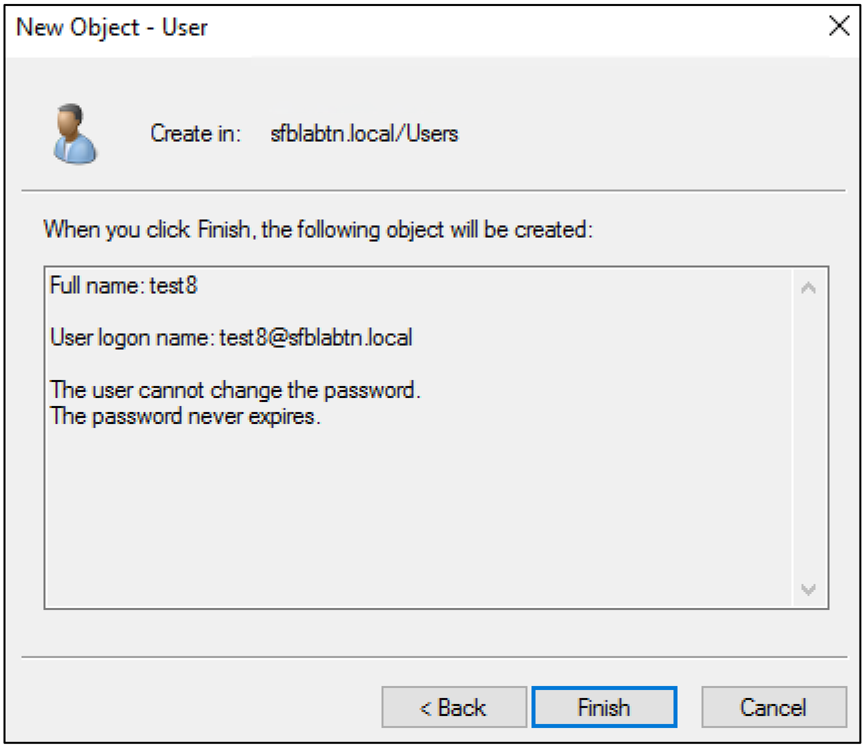
Follow the screenshots below to add a new user:



Skype for Business – New User configuration (continued)



Skype for Business – New User configuration (continued)

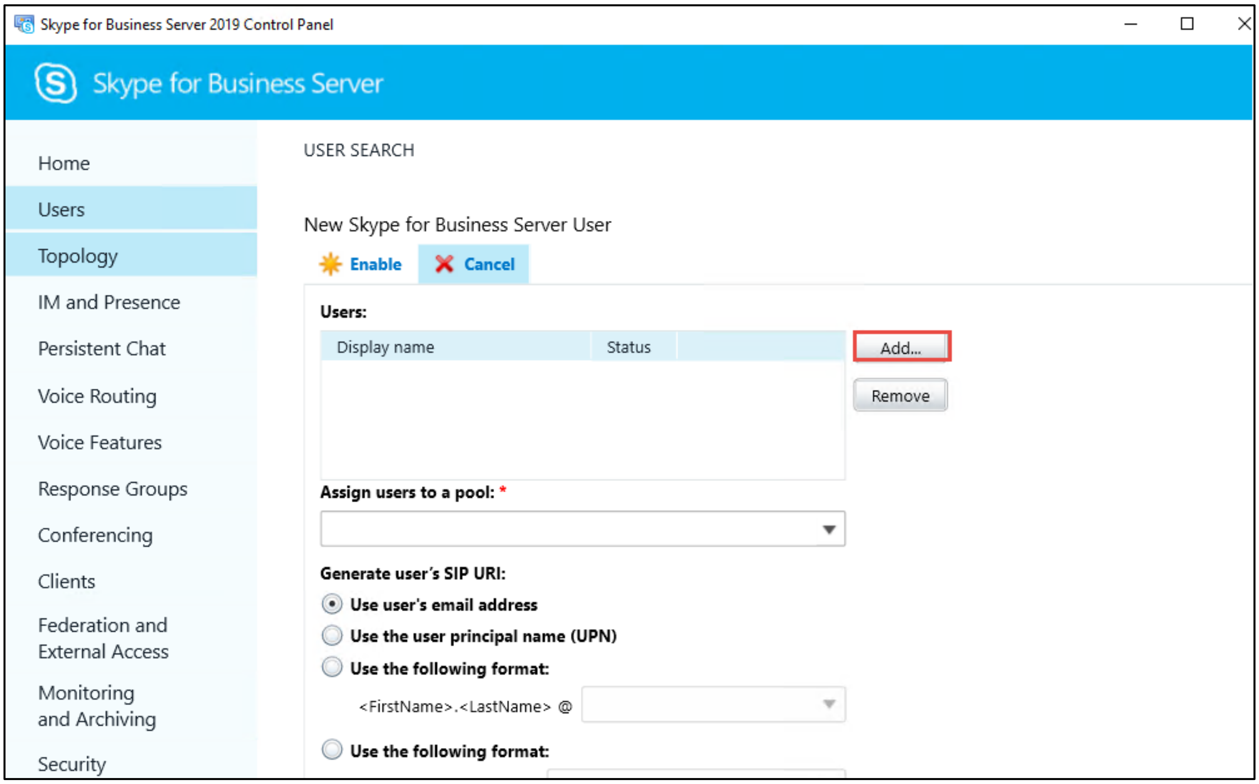


Once the user is created, login to the Skype for Business 2019 Control Panel

Navigation: Users→ Enable users

Click on the Add button and find the new user created earlier.

Skype for Business – New User configuration (continued)



Set Assign users to a **pool**= **fe.sfblabtn.local** from drop down menu

Set Generate user's **SIP URI**: Specify a SIP URI: sip:test1@sfbsp.local .This is used in this test

Set **Telephony**=**Enterprise Voice**

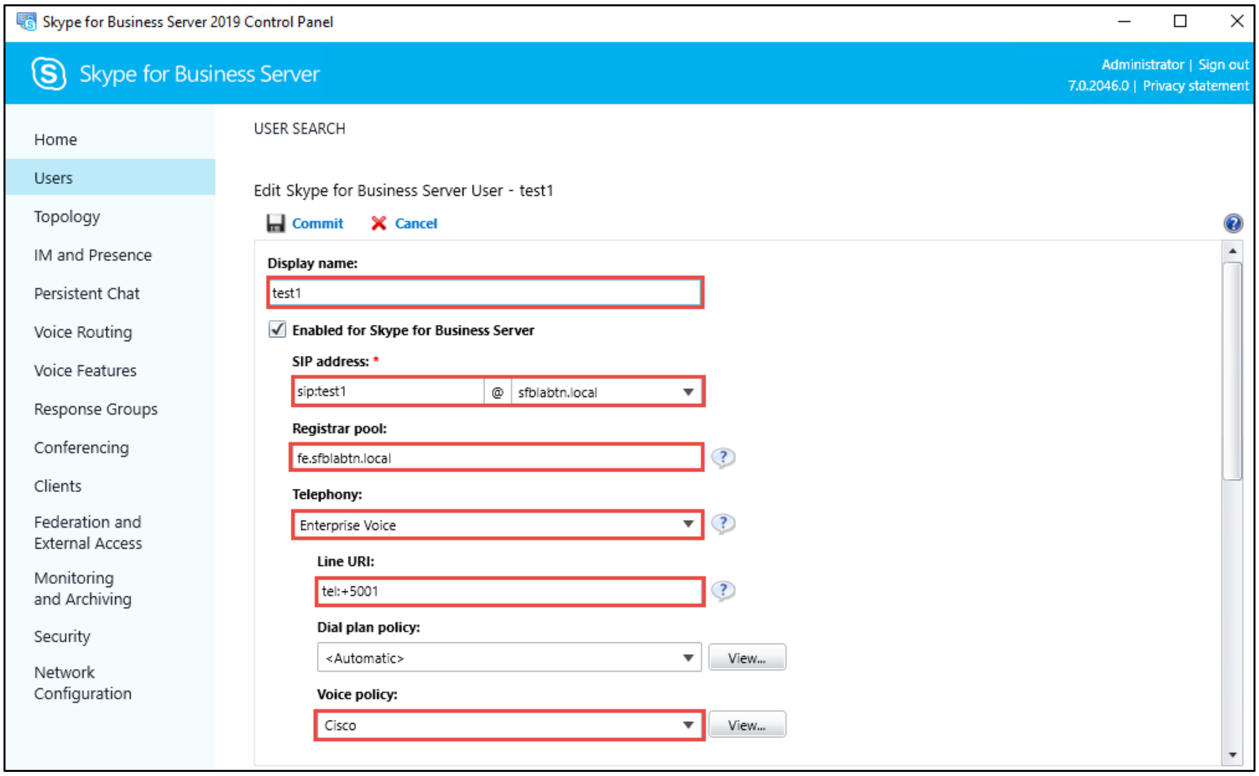
Set Line **URI**: = **tel: +5001** is used for the test. This is the DN for the user.

Set Dial **plan policy** = **Automatic** (as configured earlier)

Set **Voice policy**= **Cisco** (as configured earlier)

Click Enable.

Skype for Business – New User configuration (continued)

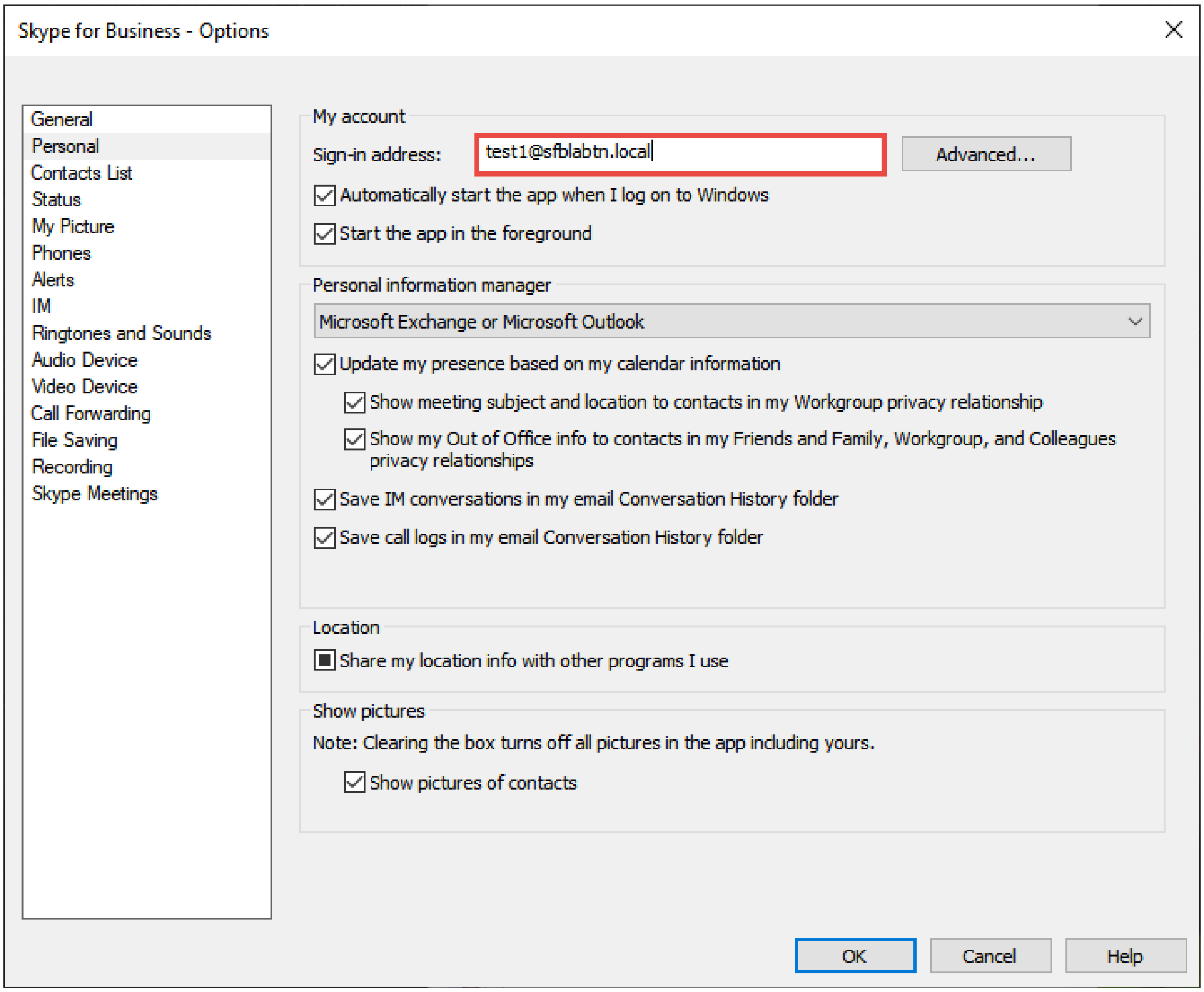


Client Configuration

Download the latest version of the Skype for Business client and launch the same.

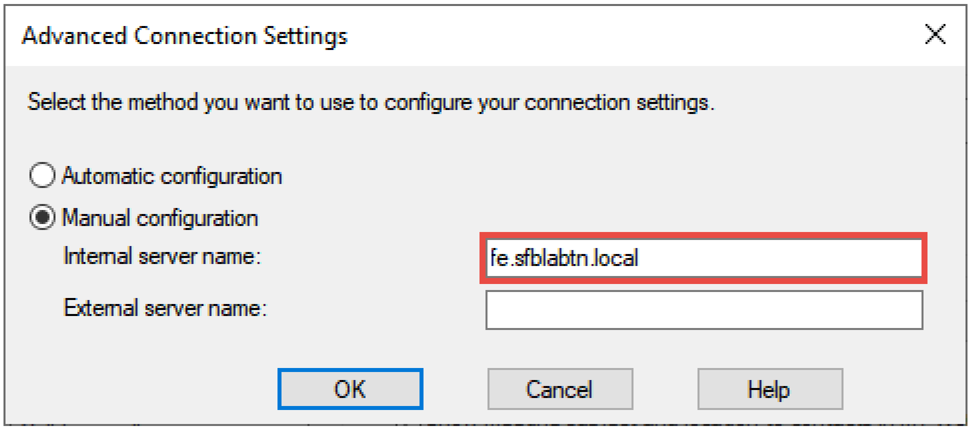
Navigation: Settings→Tools→Options→Personal→MyAccount

Set Sign-in-address= enter the sip uri of the user configured in username@domain format. test1@sfblabtn.local is used for example.



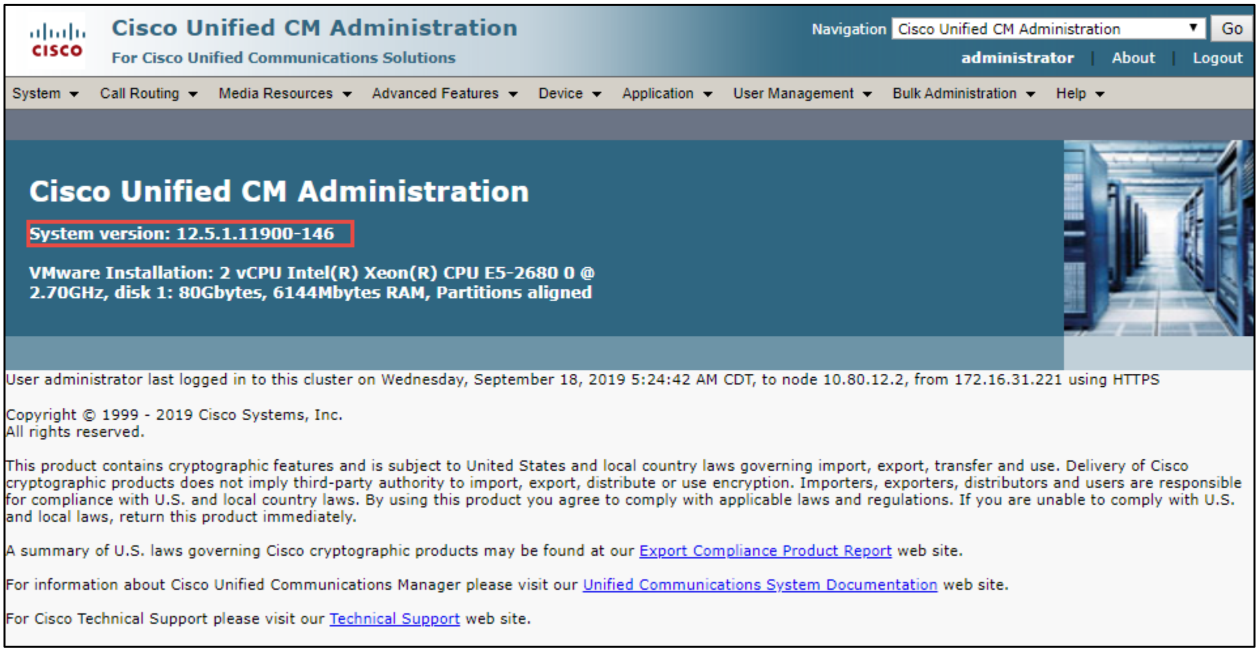
Click Advanced. Select Manual Configuration.

Set Internal Server Name= Enter the FQDN of the domain (fe.sfblabtn.local is used for example)


Advanced Connection Settings
Select the method you want to use to configure your connection settings.
Automatic configuration
Manual configuration
Internal server name:
fe.sfblabtn.local
External server name:
OK
Cancel
Help

Configuring the Cisco Unified Communications Manager

Cisco Unified Communications Manager Software Version



SIP Trunk Security Profile for Trunk to Skype for Business

Navigation: System→ Security → SIP trunk security profile

Set **Name*= SFB_SECURITY_PROFILE**. This is used for the test.

Set Device Security mode = Encrypted

Set **Incoming Transport Type = TLS**

Set **Outgoing Transport Type = TLS**

Set **X.509 Subject Name = fe.sfblabtn.local**

Set **Incoming Port = 5061**

Check **Accept Presence Subscription**

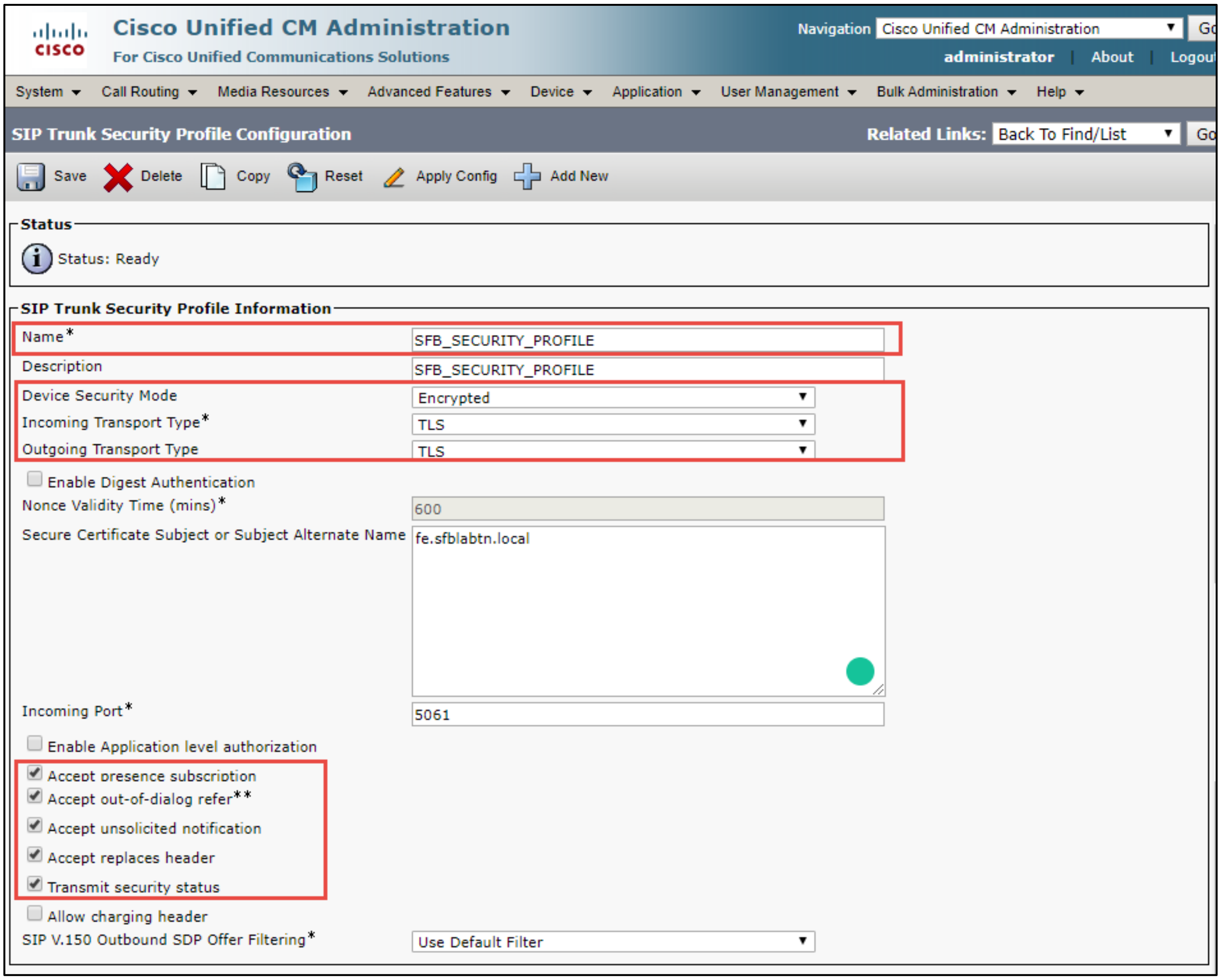
Check **Accept out of dialog refer**

Check **Accept unsolicited notification**

Check **Accept Replaces header**

Check **Transmit security status**

All other values are default.



SIP Trunk Security Profile for Trunk to Unity Connection

Navigation: System→ Security → SIP trunk security profile

Set **Name***= **TLS_CUC**. This is used for the test.

Set Device **Security mode** = **Encrypted**

Set **Incoming Transport Type = TLS**

Set **Outgoing Transport Type = TLS**

Set X**.509 Subject Name = clus22cuc.tekvizionlabs.com**

Set **Incoming Port = 5061**

check **Accept Presence Subscription**

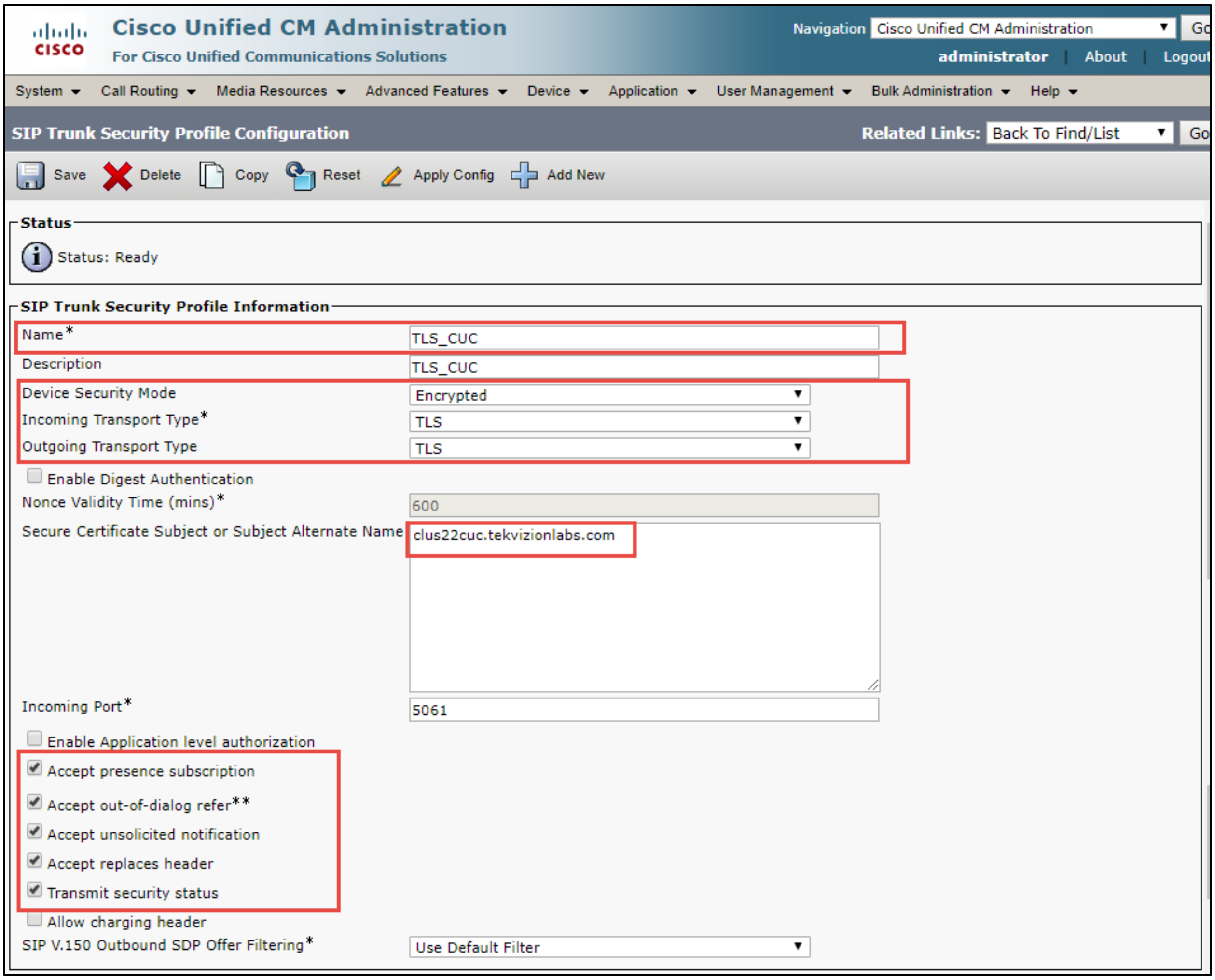
Check **Accept out-of-dialog refer****

Check **Accept unsolicited notification**

Check **Accept Replaces header**

Check **Transmit security status**

All other values are default.



SIP Profile

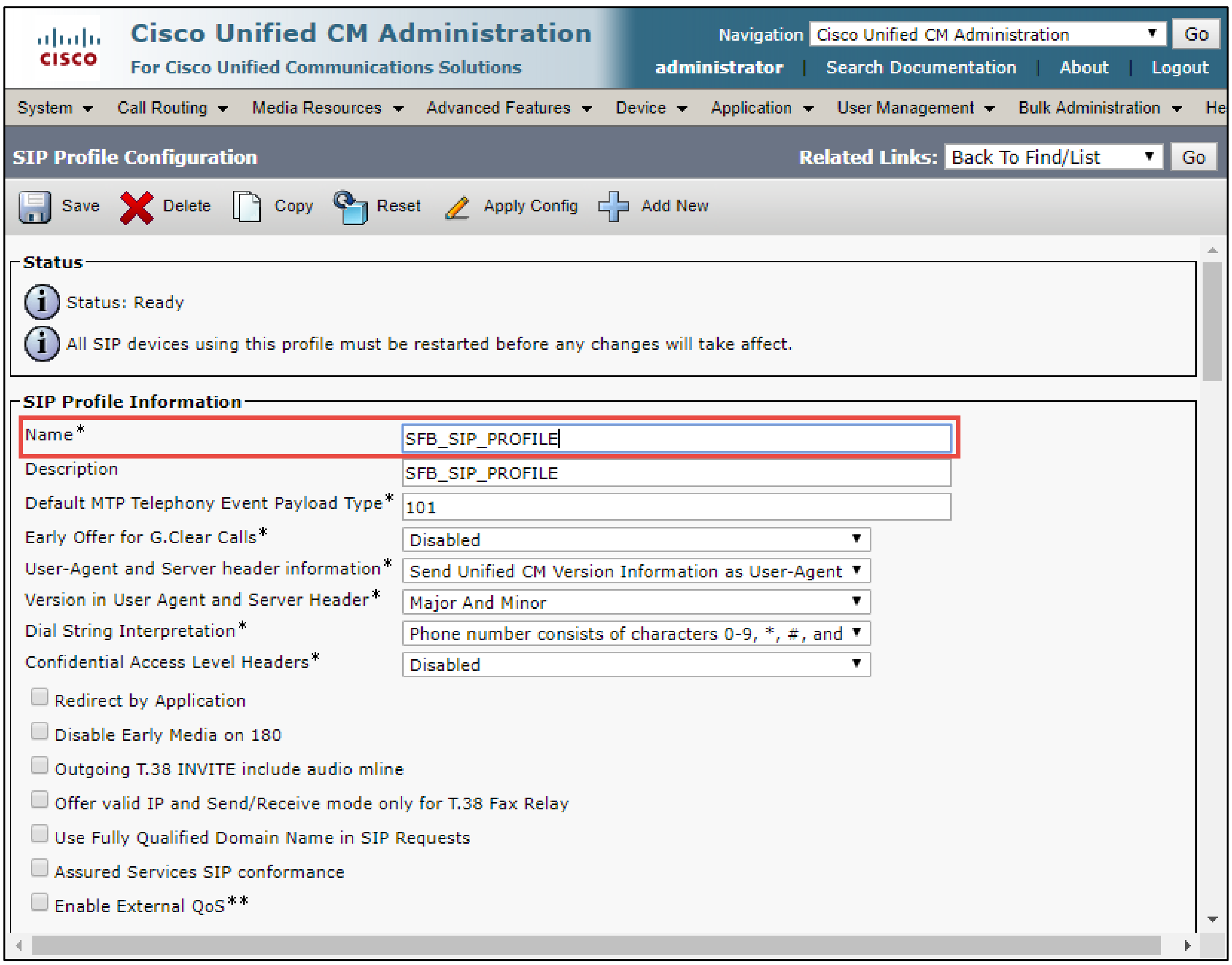
Navigation: Device → Device Settings → SIP Profile
Set **Name*= SFB_SIP_PROFILE** - Standard SIP Profile. This is used for this test.

Set **SIP Rel1XX Options = Send PRACK for all 1xx messages**

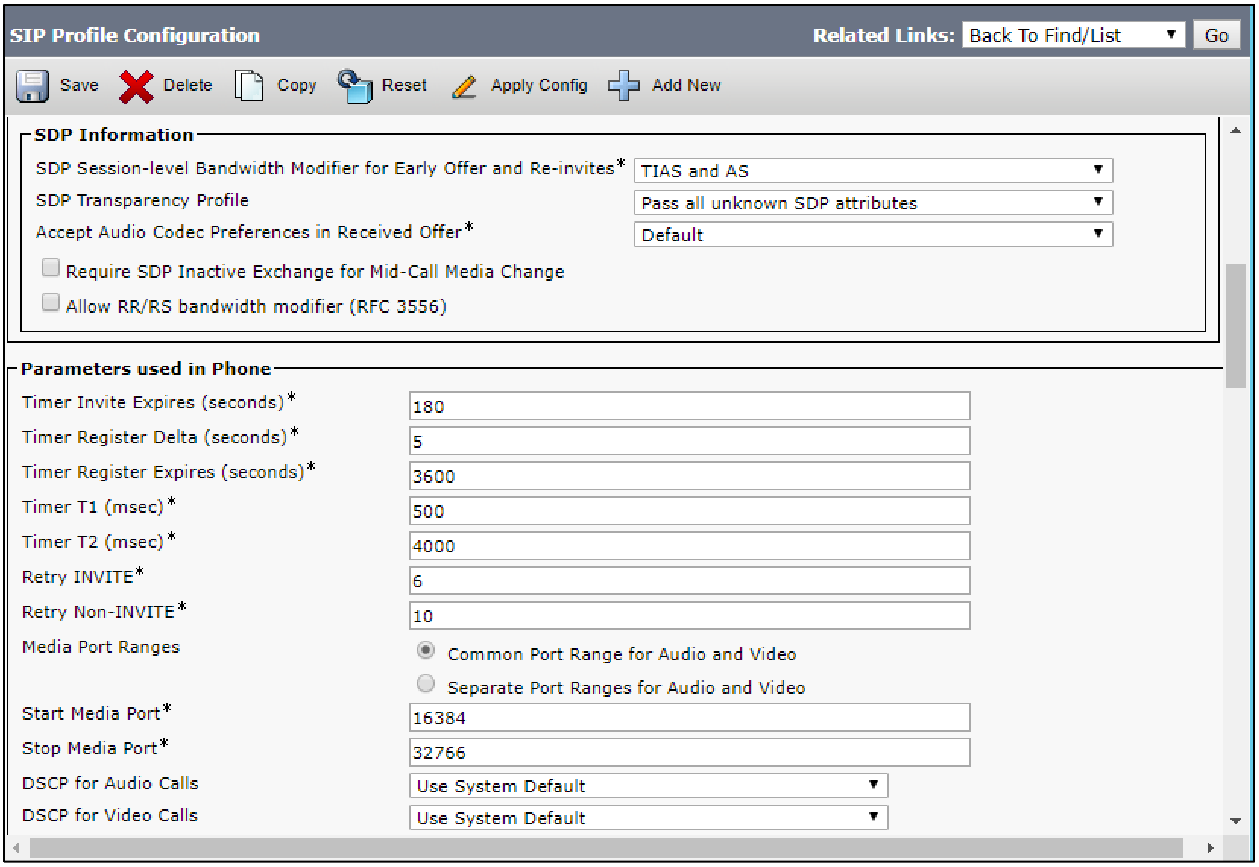
Set **Early Offer support for voice and video calls = Best Effort (no MTP inserted)**

Check Enable OPTIONS Ping to monitor Destination status for Trunks with Service Type "None (Default)"

All other values are default.



Cisco Unified Communications Manager SIP Profile (Continued)



SIP Profile Configuration | Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Apply Config | Add New

SDP Information

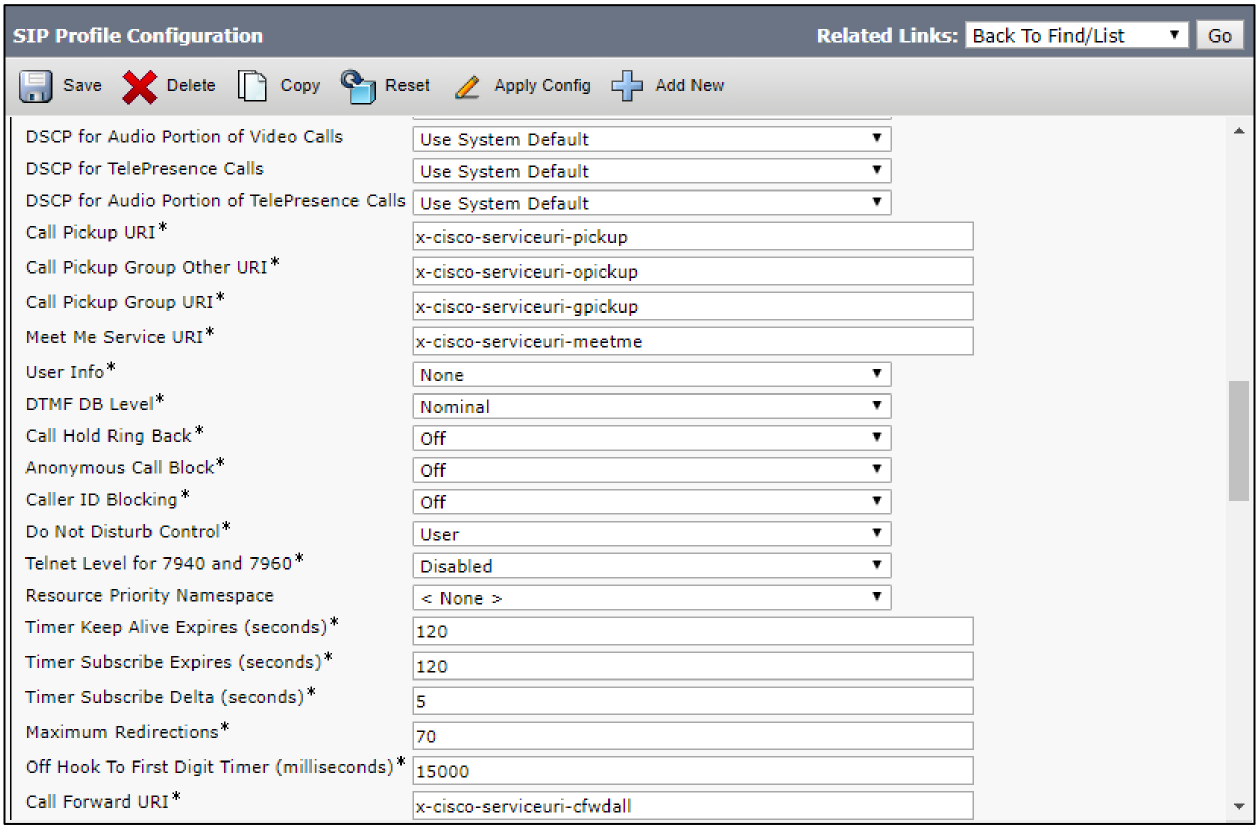
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
SDP Transparency Profile	Pass all unknown SDP attributes
Accept Audio Codec Preferences in Received Offer*	Default

- [ ] Require SDP Inactive Exchange for Mid-Call Media Change
- [ ] Allow RR/RS bandwidth modifier (RFC 3556)

Parameters used in Phone

Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	5
Timer Register Expires (seconds)*	3600
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Media Port Ranges	(•) Common Port Range for Audio and Video ( ) Separate Port Ranges for Audio and Video
Start Media Port*	16384
Stop Media Port*	32766
DSCP for Audio Calls	Use System Default
DSCP for Video Calls	Use System Default

Cisco Unified Communications Manager SIP Profile (Continued)

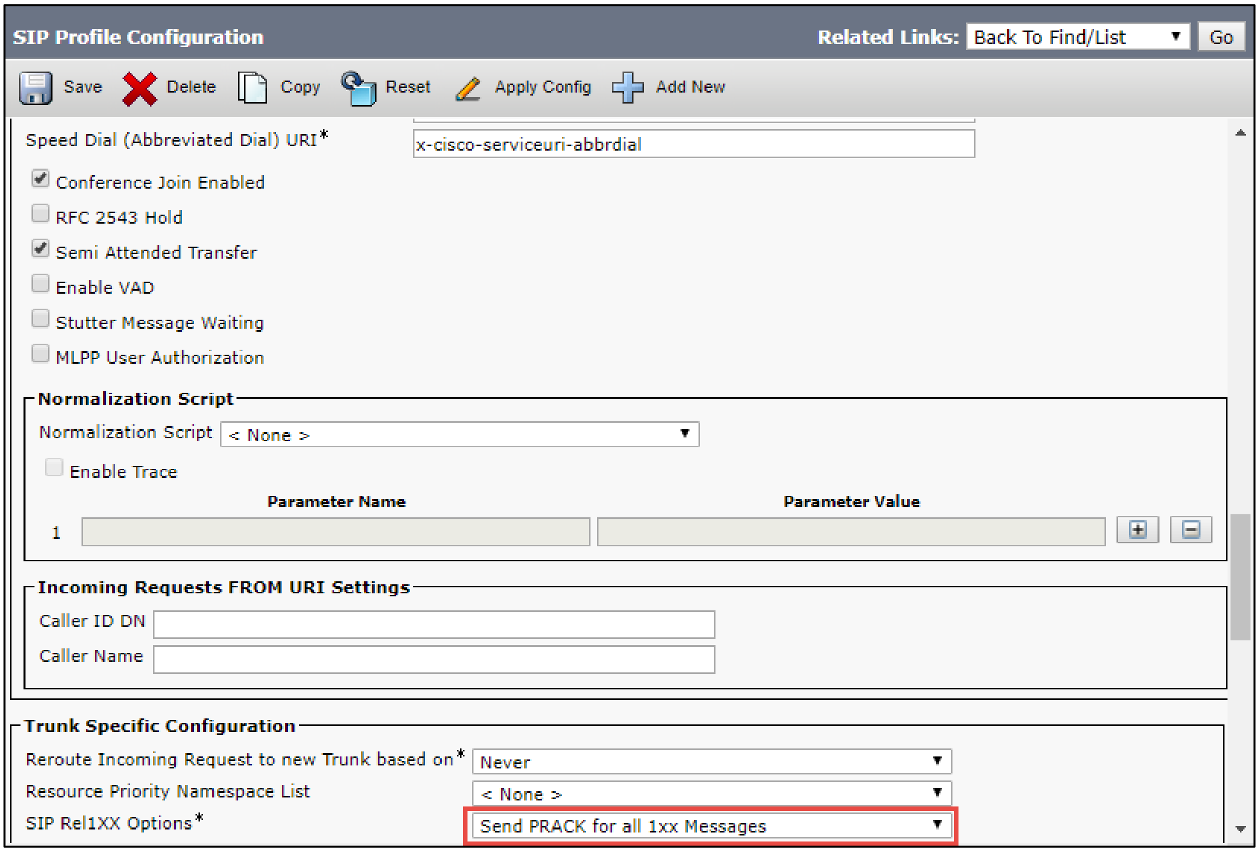


SIP Profile Configuration — Related Links: Back To Find/List | Go

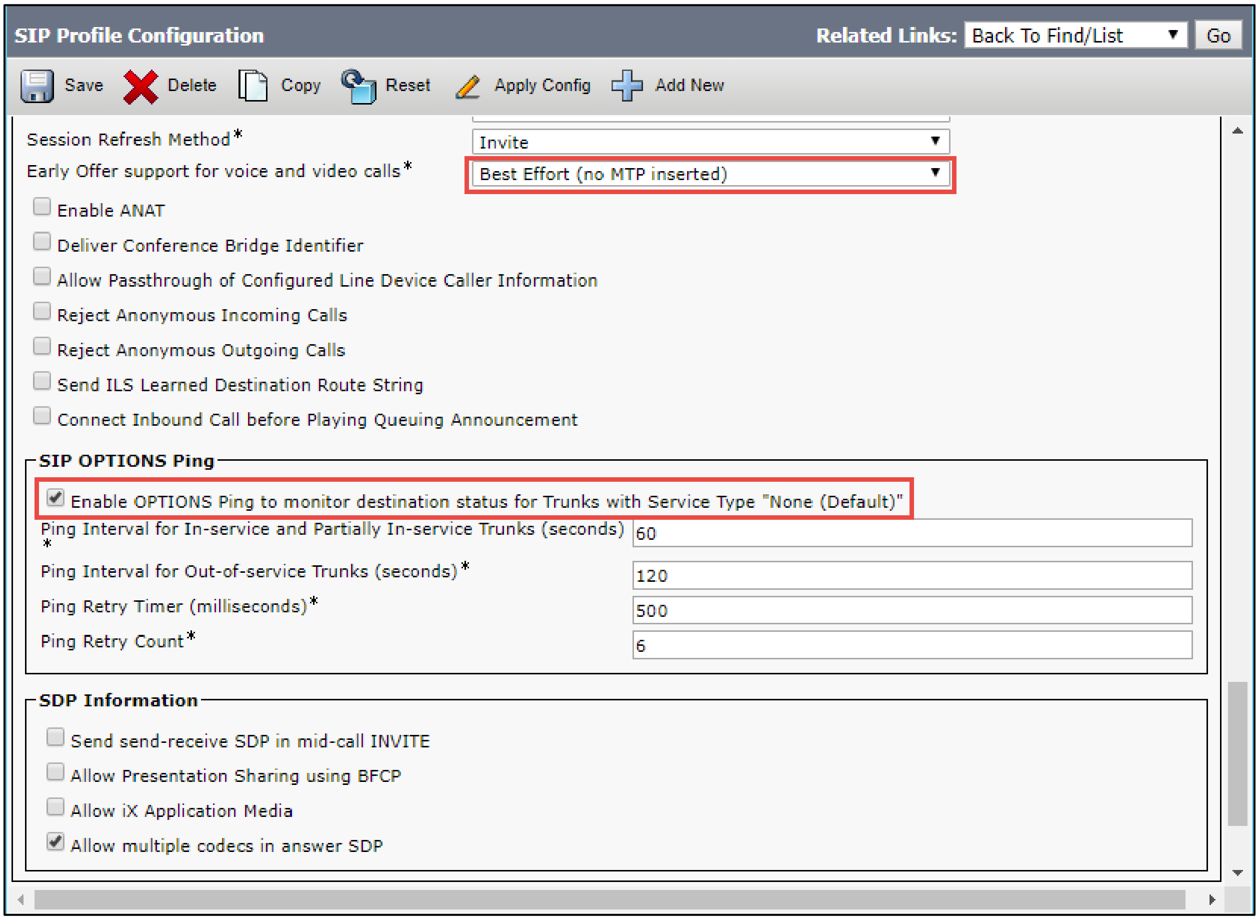
Save | Delete | Copy | Reset | Apply Config | Add New

DSCP for Audio Portion of Video Calls	Use System Default
DSCP for TelePresence Calls	Use System Default
DSCP for Audio Portion of TelePresence Calls	Use System Default
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Resource Priority Namespace	< None >
Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward URI*	x-cisco-serviceuri-cfwdall

Cisco Unified Communications Manager SIP Profile (Continued)



Cisco Unified Communications Manager SIP Profile (Continued)



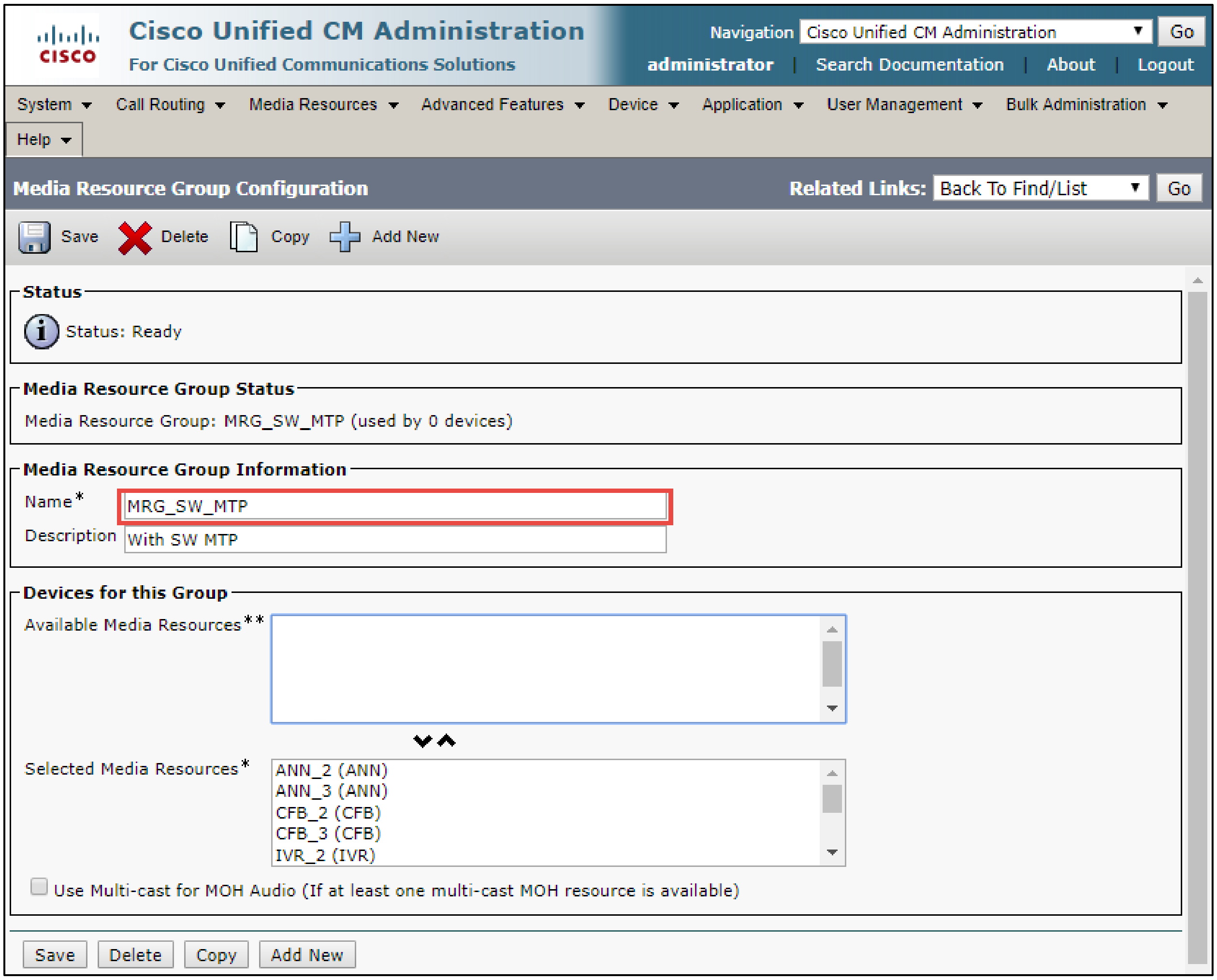
Media Resource Group

Navigation Path: Media Resources→ Media Resource Group; Add New
Media Resource Group MRG

Set **Name*= MRG_SW_MTP**, This is used for this test.

Set all resources in the Selected Media Resources* Box.

All other values are default.



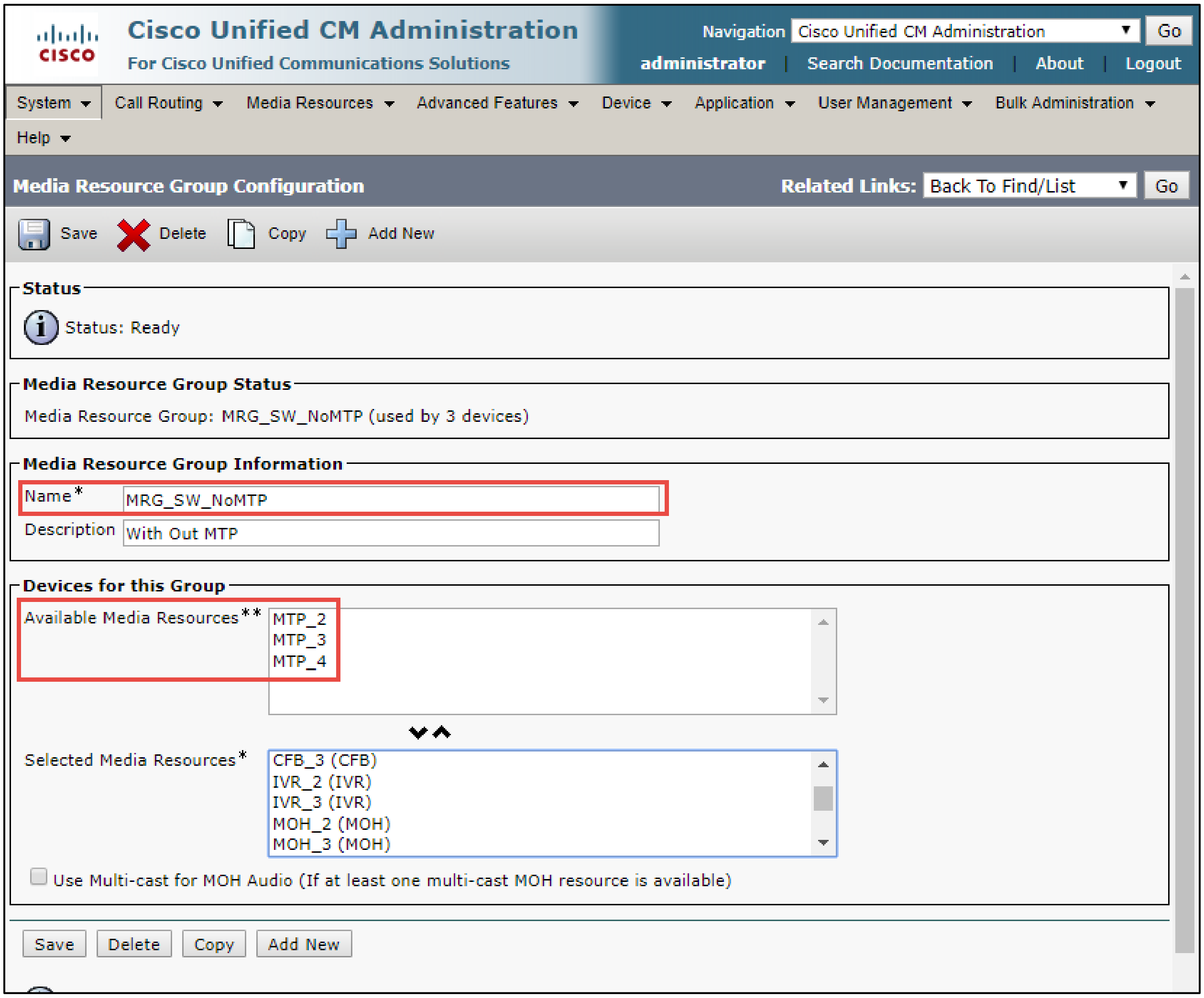
Resource Group for MRG_SW_NoMTP

Set **Name*= MRG_SW_NoMTP**. This is used for the test.

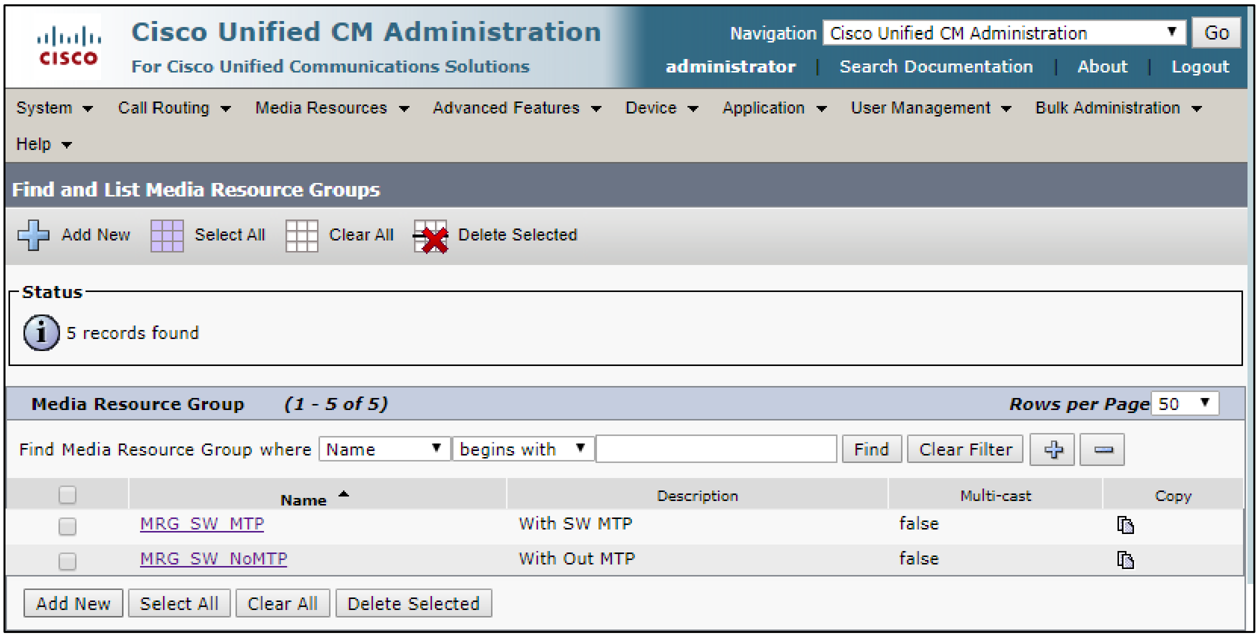
Set **Available Media Resources = MTP_2, MTP_3 and MTP_4**

Set other resources in the Selected Media Resources*

All other values are default.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Help
Media Resource Group Configuration
Related Links: Back To Find/List Go
Save Delete Copy Add New
Status
Status: Ready
Media Resource Group Status
Media Resource Group: MRG_SW_NoMTP (used by 3 devices)
Media Resource Group Information
Name* MRG_SW_NoMTP
Description With Out MTP
Devices for this Group
Available Media Resources**
MTP_2
MTP_3
MTP_4
Selected Media Resources*
CFB_3 (CFB)
IVR_2 (IVR)
IVR_3 (IVR)
MOH_2 (MOH)
MOH_3 (MOH)
Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)
Save Delete Copy Add New

Cisco Unified Communications Manager Media Resource Group Configuration



Media Resource Group List

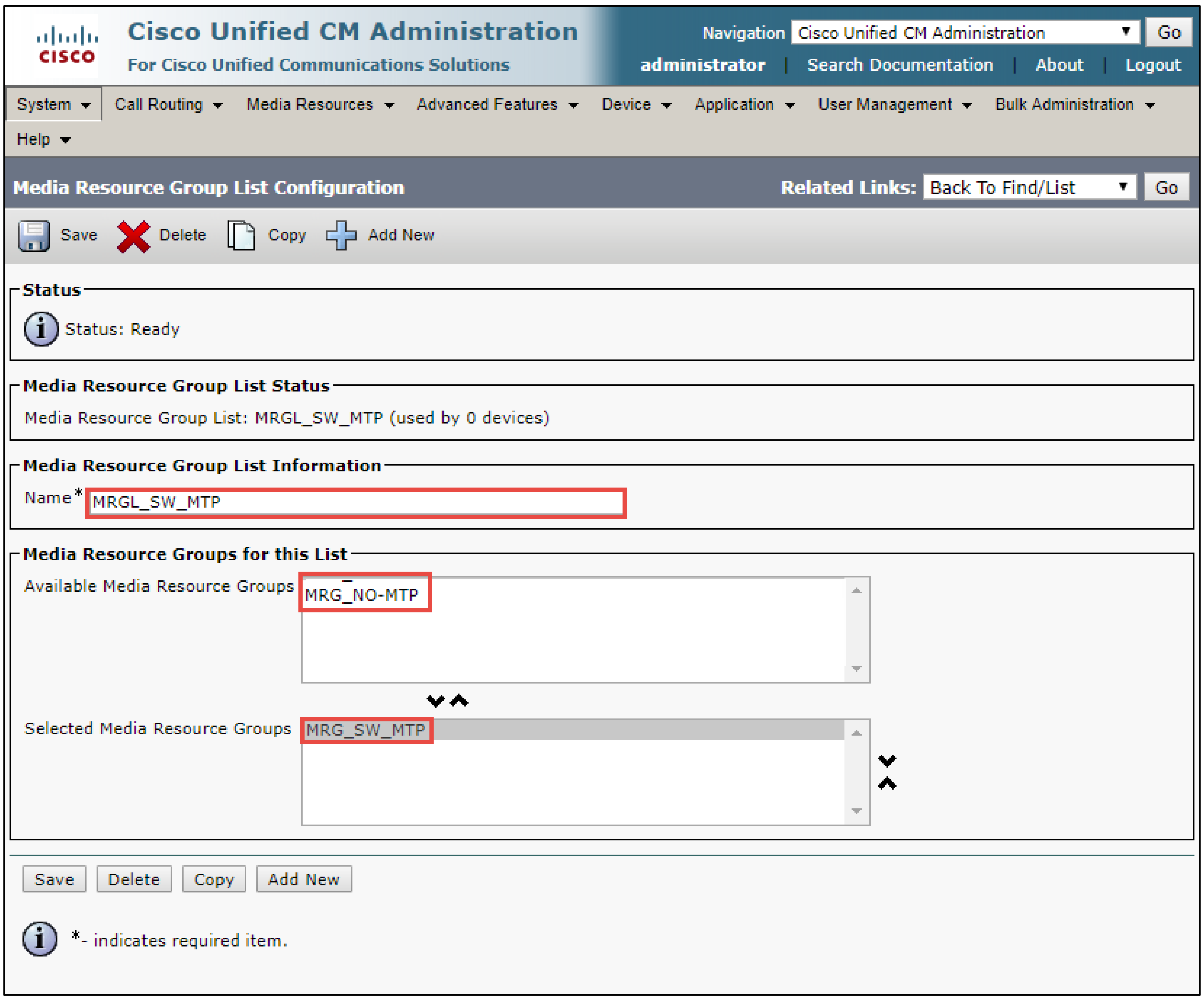
Navigation Path: Media Resources→ Media Resource Group List

Add New

Set **Name*= MRGL_SW_MTP**. This is used for this test.

Set **Available Media Resources = MRG_NO-MTP**

Set **Selected Media Resource Groups= MRGL_SW_MTP**

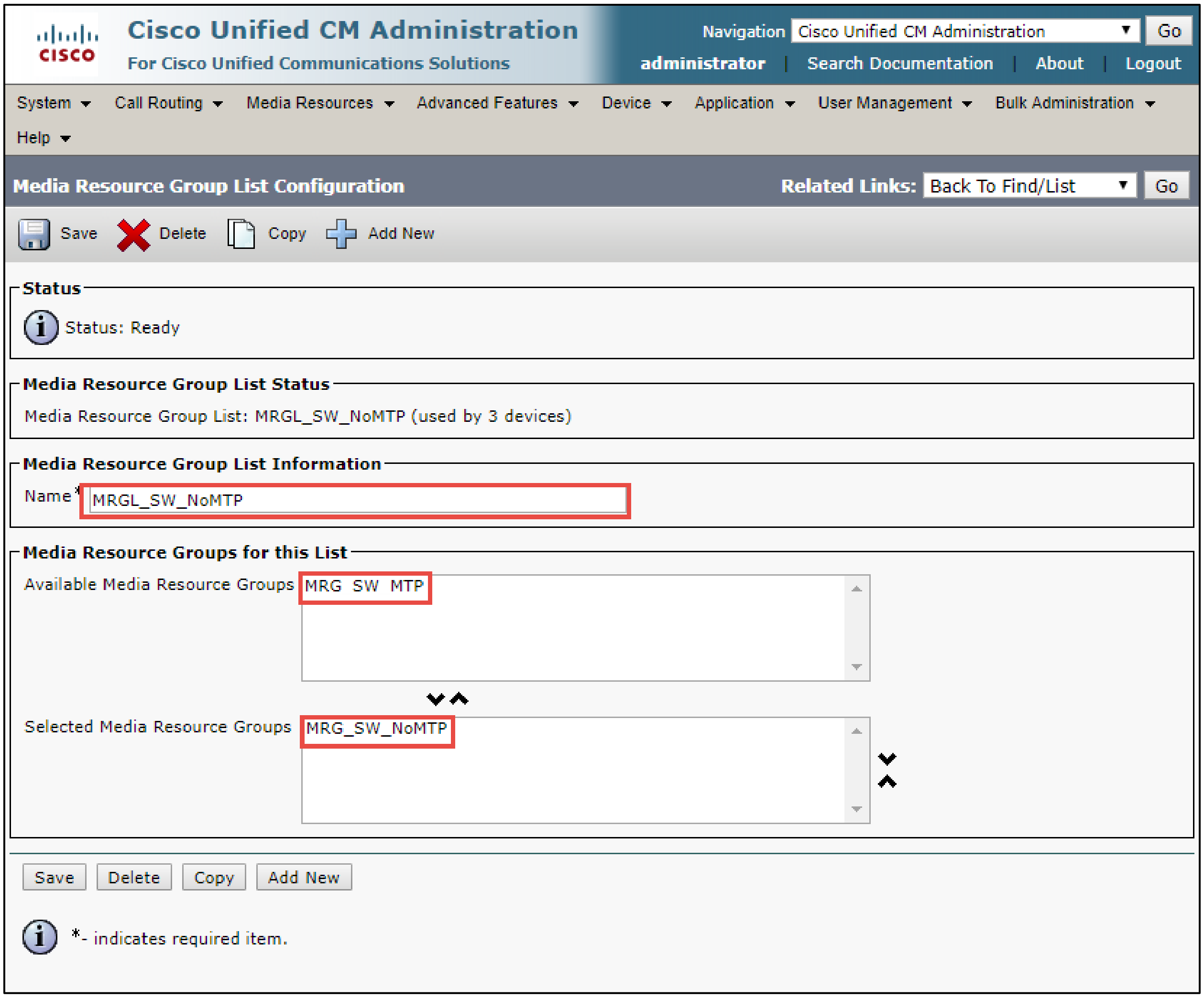


Add new

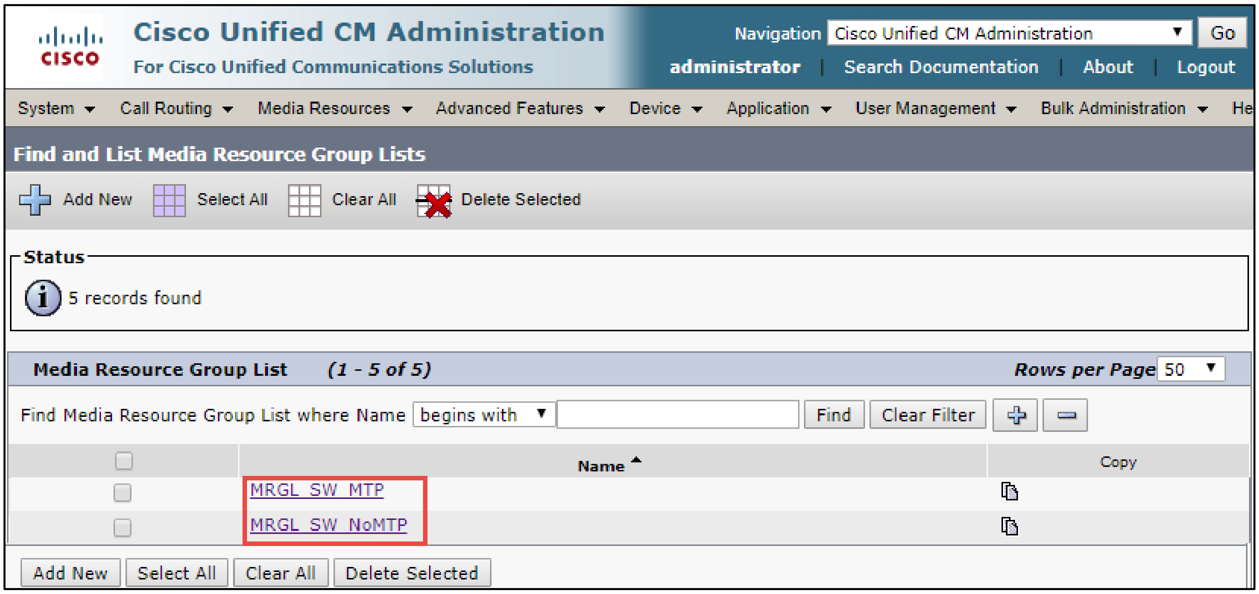
Set **Name*= MRGL_SW_NoMTP**. This is used for the test

Set **Available Media Resources MRG_SW_MTP**

Set **Selected Media Resource Groups= MRGL_SW_NoMTP**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Media Resource Group List Configuration
Related Links: Back To Find/List Go
Save Delete Copy Add New
Status
Status: Ready
Media Resource Group List Status
Media Resource Group List: MRGL_SW_NoMTP (used by 3 devices)
Media Resource Group List Information
Name* MRGL_SW_NoMTP
Media Resource Groups for this List
Available Media Resource Groups MRG_SW_MTP
Selected Media Resource Groups MRG_SW_NoMTP
Save Delete Copy Add New
*- indicates required item.

Cisco Unified Communications Manager Media Resource Group List Configuration



Device Pool Configuration

Device Pool - **G711_Pool** is created in this test.

Navigation Path: System → Device Pool

Add New.

Set **Device Pool Name*= G711_pool**. This is used in the test.

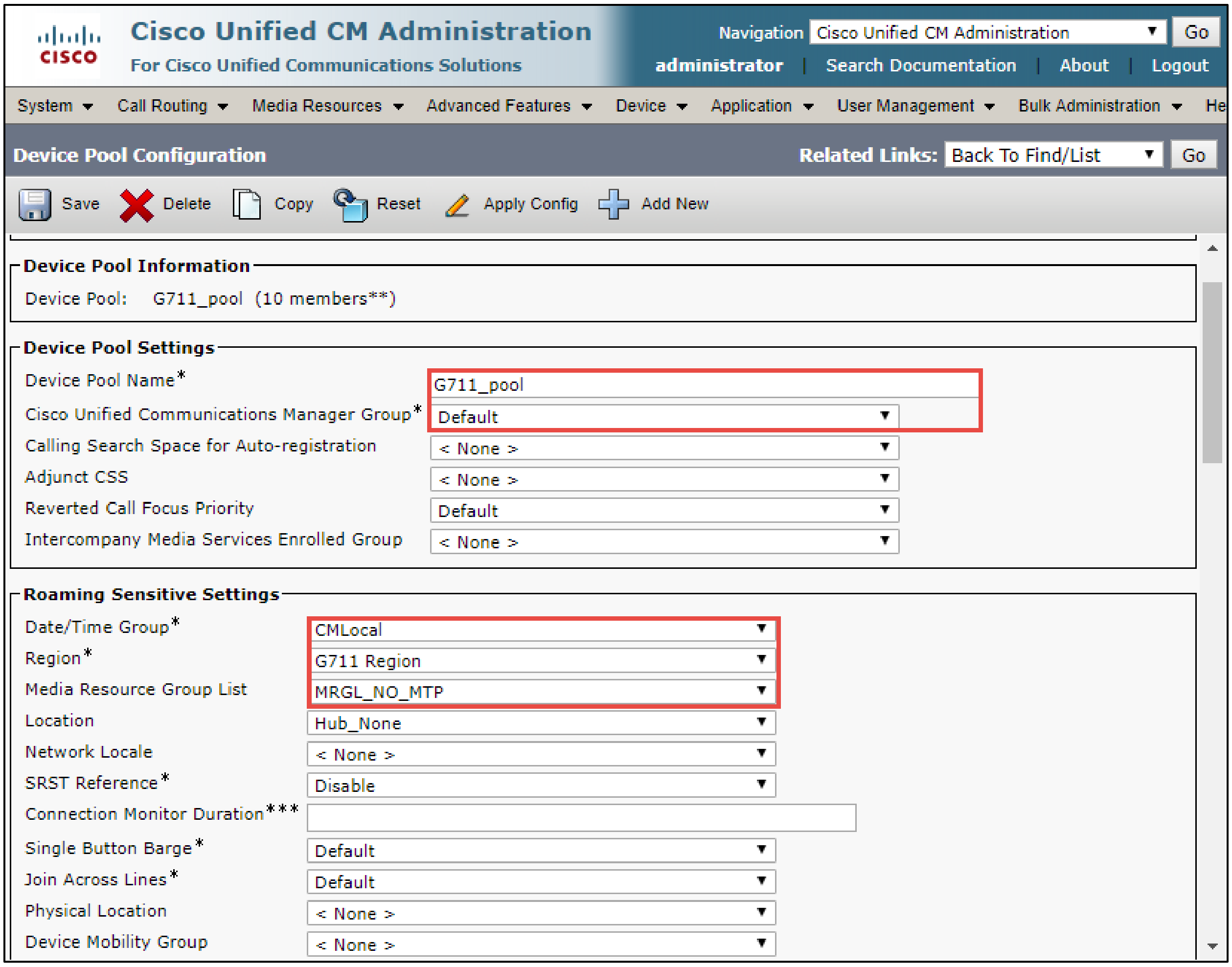
Set **Cisco Unified Communications Manager Group*= Default**

Set **Date/Time Group* = CMLocal**

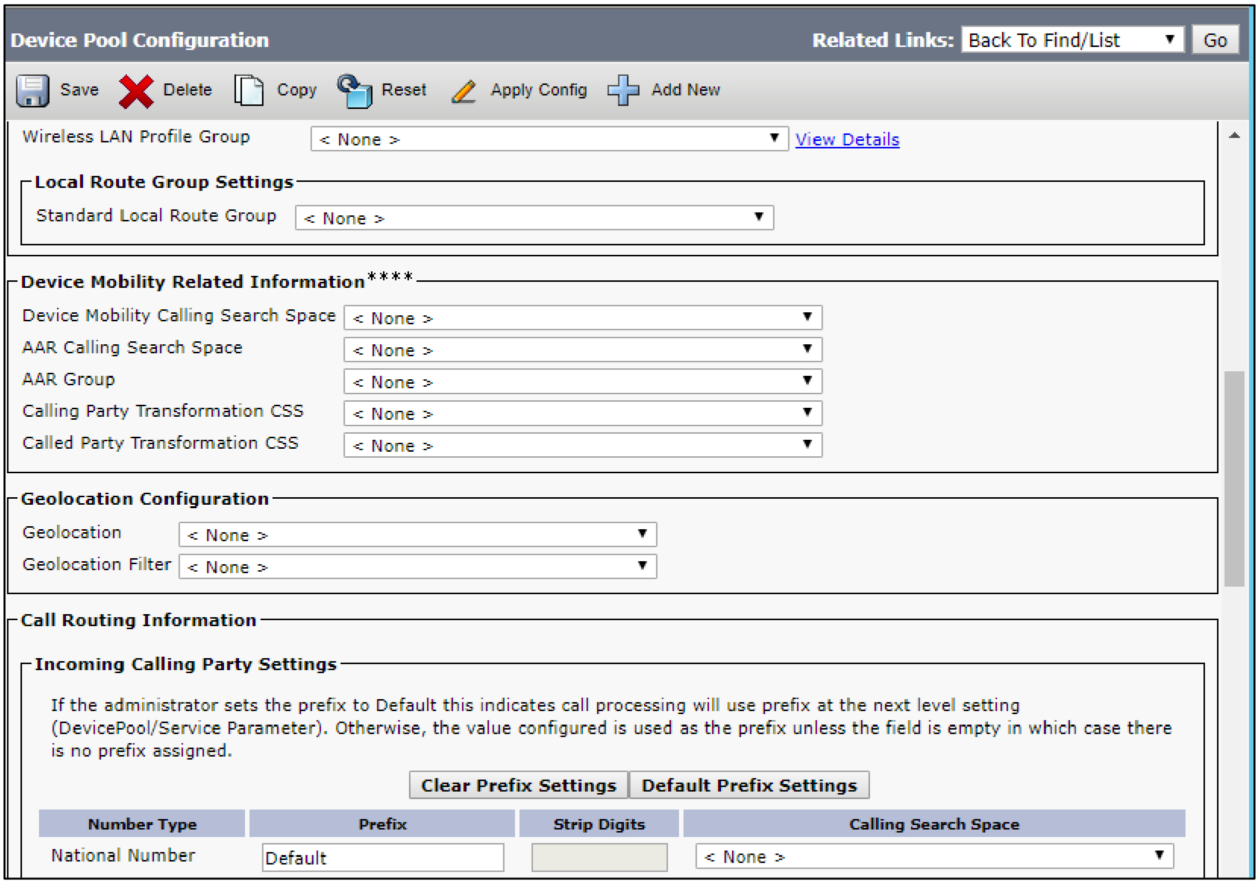
Set **Region* = G711 Region**. This is used in this example

Set **Media Resource Group List =MRGL_NO_MTP**. This is used in this example.

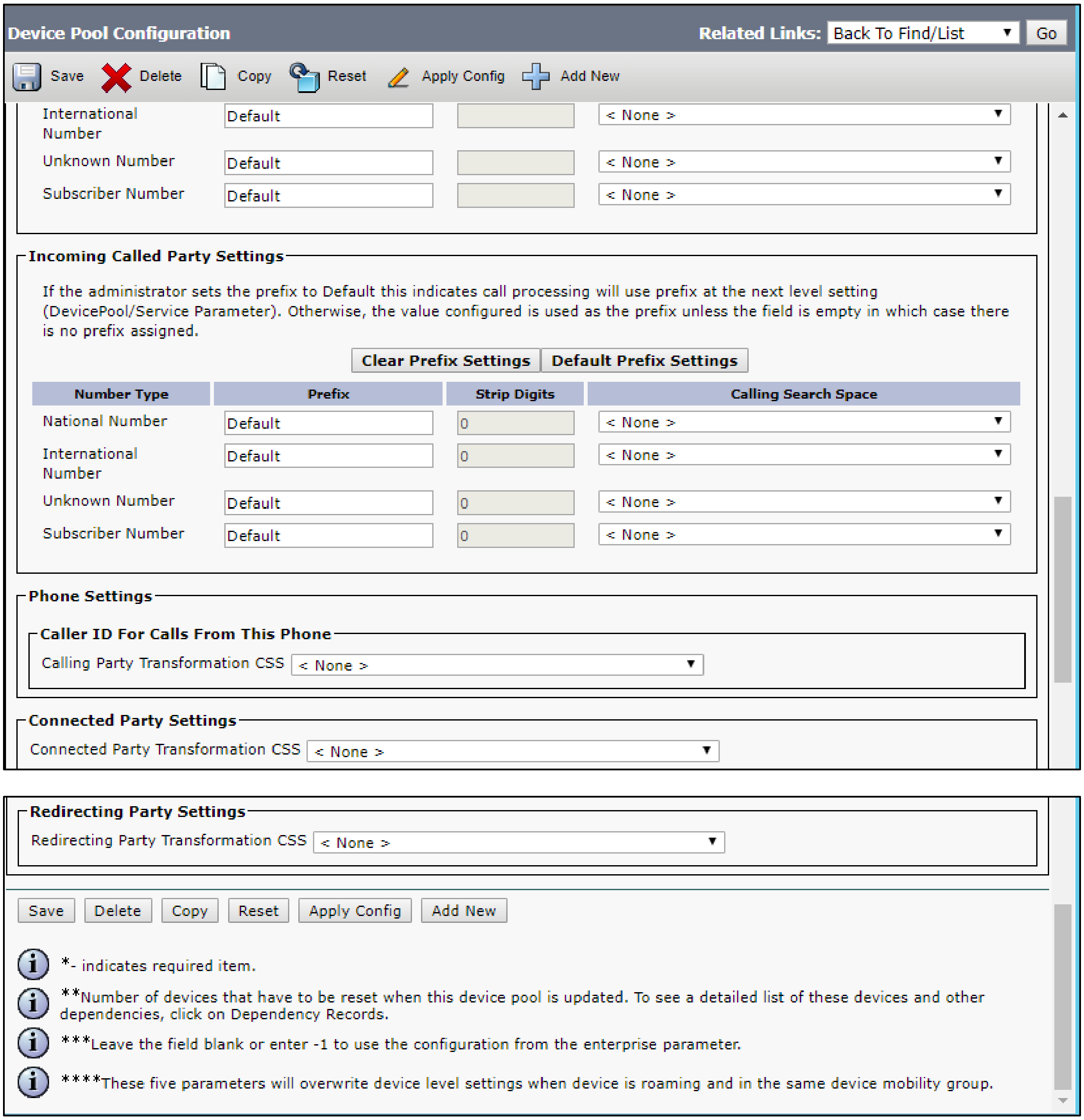
All other values are default.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Device Pool Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
Device Pool Information
Device Pool: G711_pool (10 members**)
Device Pool Settings
Device Pool Name* G711_pool
Cisco Unified Communications Manager Group* Default
Calling Search Space for Auto-registration < None >
Adjunct CSS < None >
Reverted Call Focus Priority Default
Intercompany Media Services Enrolled Group < None >
Roaming Sensitive Settings
Date/Time Group* CMLocal
Region* G711 Region
Media Resource Group List MRGL_NO_MTP
Location Hub_None
Network Locale < None >
SRST Reference* Disable
Connection Monitor Duration***
Single Button Barge* Default
Join Across Lines* Default
Physical Location < None >
Device Mobility Group < None >

Cisco Unified Communications Manager Device Pool Configuration (Continued)



Cisco Unified Communications Manager Device Pool Configuration (Continued)



Region Configuration

Navigation Path: System → Region Information → Region

Add New

G711 Region is created in this test.

Set **Name*= G711 Region**. This is used in this example

Set **Region= G711 Region**. This is used in this example

Set **Audio Codec Preference List= G711_Preferred Codec List**

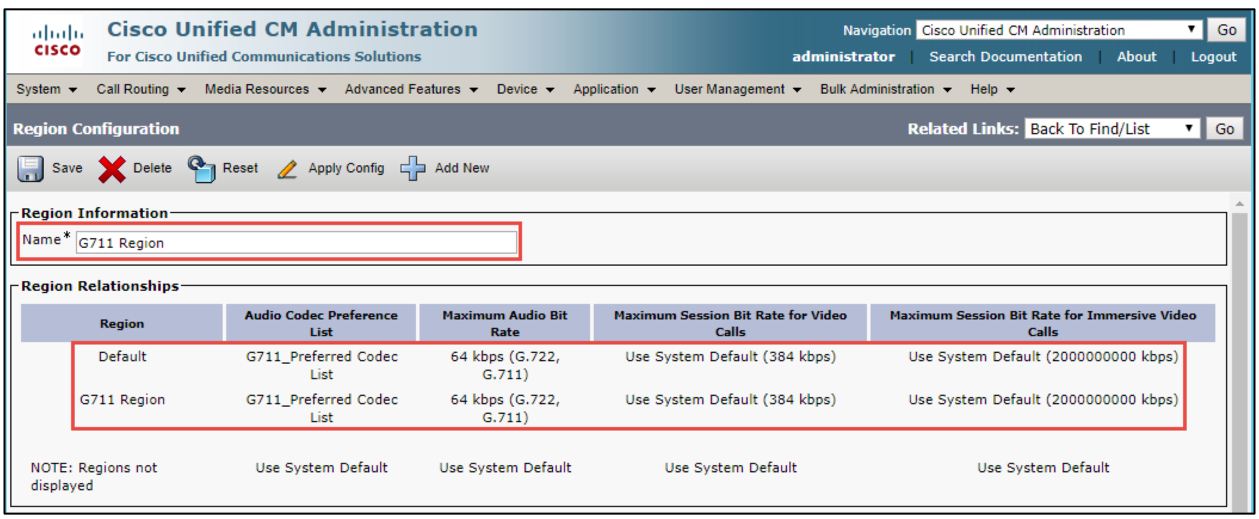
Set **Maximum Audio Bit Rate= 64 Kbps (G7.22, G7.11).** This is used in this example

Set **Region=Default**. This is used in this example

Set **Audio Codec Preference List= G711_Preferred Codec List**. This is used in this example

Set **Maximum Audio Bit Rate= 64 Kbps (G722, G7.11)**. This is used in this example

All other values are default



Normalization Script

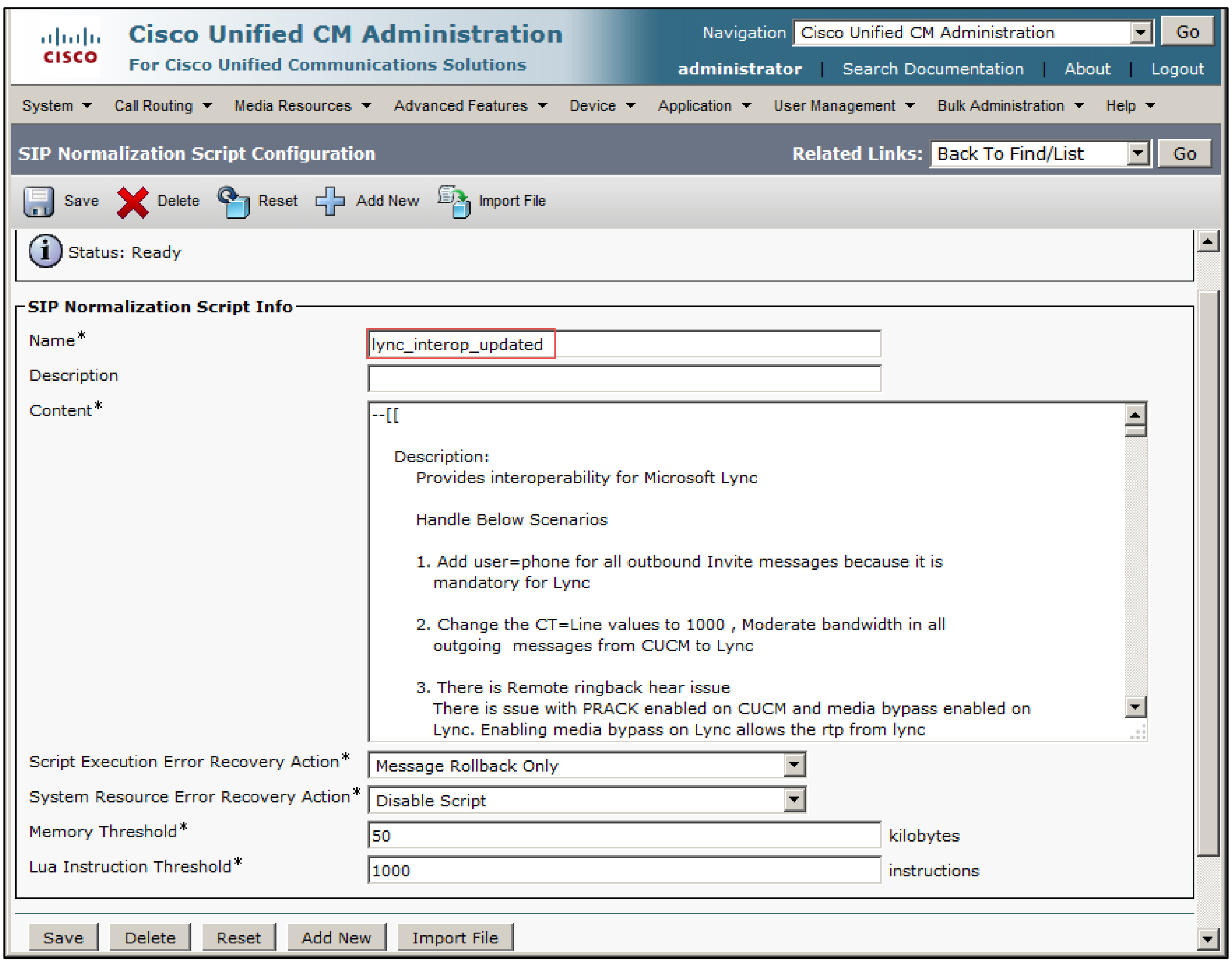
Navigation: Device->Device Settings->SIP Normalization Script

Add New

Set Name = enter text here to identify the normalization script for use on trunk. Lync_interop_updated is used in this test.

Set Content = add script content.

Note: “lync_interop” was the originally provided script by Cisco Support for Cisco UCM-Skype for Business TLS integration. However, with the script activated, the call from Skype for Business to Cisco UCM was not established on SRTP still. Cisco UCM sent AVP (that is, chose RTP instead of SRTP) when Skype for Business sent a=tcap: 1 RTP/SAVP through INVITE SDP. The script was updated to fix this issue and “lync_interop_updated” is the updated script.



Normalization Script

```
--[[

  Description:
    Provides interoperability for Microsoft Lync

    Handle Below Scenarios

    1. Add user=phone for all outbound Invite messages because it is
      mandatory for Lync

    2. Change the CT=Line values to 1000 , Moderate bandwidth in all
      outgoing  messages from CUCM to Lync

    3. There is Remote ringback hear issue
      There is issue with PRACK enabled on CUCM and media bypass enabled on
      Lync. Enabling media bypass on Lync allows the rtp from lync
      endpoint to flow through CUCM directly instead of flowing through
      Mediation server. The problem with PRACK enabled is that Lync end
      point is now not able to answer the incoming call.Looking into the
      traces, it appears that even though Lync sent updated connection
      information in 183 w/sdp, the call manager is still sending rtp to the
      mediation server which seems to be incorrect" So In this scenario
      CUCM expects 180 Ringing not 183 Session progress.
      So added the Script to convert 183 Session Progress to 180 Ringing.

    4. There is incoming Invite from Lync and in From Header there is
      "user=phone" which cause CUCM to send malformed data in to
      different layers which cause call failure.So this is work around for that
      Scenario.

    5. Script modify the AS header which from outgoing messages because call forward
      fails due to bandwith negotiation value is A=64 is not supported

    6. Script convert the History info to diversion Header since call forward to unity
      Is not supported.

    7. Transfer Scenario: Referred-By in Incoming Invite is converted to Diversion Header.



  Script Parameters:

  Release: 9.1(2) , 10.0.(1)

  Copyright (c) 2009-2011 Cisco Systems, Inc. All rights reserved.
  All rights reserved.
```

```
--]]

M = {}

M.allowHeaders = {"History-Info"}

trace.enable()

local function getDisplayName (i_header)
   local position_of_uri=string.find(i_header, "<")
         if position_of_uri <= 2
         then
                  display_name=nil
         else
                  -- save display name which arrives in quotes
                  local display_name_tmp = string.sub(i_header,1, (position_of_uri - 1))
                  -- now remove the quotes
                  display_name_tmp = string.gsub(display_name_tmp,'"','')
                  -- now remove the space
                  display_name = string.gsub(display_name_tmp,' ','')
         end
         return display_name
end

local function modify_CT_bandwidth(msg)
   local sdp = msg:getSdp()
   if sdp
   then
      local b_CT_line = sdp:getLine("b=CT","64")
      if not b_CT_line
      then
         local b_CT_line = sdp:getLine("b=CT","0")
         if not b_CT_line
         then
            return
         end
         b_CT_line = b_CT_line:gsub("0", "1000")
         sdp = sdp:modifyLine("b=CT", "0", b_CT_line)
         msg:setSdp(sdp)
         return
      end
      b_CT_line = b_CT_line:gsub("64", "1000")
      sdp = sdp:modifyLine("b=CT", "64", b_CT_line)
      msg:setSdp(sdp)
   end
end

local function remove_AS_bandwidth(msg)
```

```
   local sdp = msg:getSdp()
   if sdp
   then
          local b_AS_line = sdp:getLine("b=AS","64")
      if b_AS_line
      then
         sdp = sdp:removeLine("b=AS", "64")
         msg:setSdp(sdp)
      end
   end
end

local function process_outbound_request(msg)

   local method, ruri, ver = msg:getRequestLine()

   if string.find(ruri, "@")
   then
      local uri = ruri .. ";user=phone"
      msg:setRequestUri(uri)
   end

   modify_CT_bandwidth(msg)
   remove_AS_bandwidth(msg)

end

local function process_outbound_message(msg)
   modify_CT_bandwidth(msg)
   remove_AS_bandwidth(msg)
end


local function process_inbound_progress(msg)

   msg:setResponseCode(180, "Ringing")
   local sdp = msg:getSdp()

          if sdp then
          sdp = sdp:removeMediaDescription("audio")
          msg:setSdp(sdp)
          end

   local req = msg:getHeader("Require")
   local reqHeader = req
   if req
   then
      msg:removeHeader("Require")
```

```
   end

   local rseq = msg:getHeader("Rseq")
   local rseqPresnt = rseq
   if rseq
   then
      seqVal = msg:getHeaderValues("Rseq")
      msg:removeHeader("Rseq")
   end

   local sdp = msg:getSdp()
   if sdp
   then
      msg:removeUnreliableSdp()
   end

   if reqHeader
   then
      msg:addHeader("Require", "100rel")
   end

   if rseqPresnt
   then
     msg:addHeader("RSeq",seqVal[1])
   end
end

-- Future reference for changing cause values in divertion header scenario
-- local HiCauseToDiversion = { }
-- HiCauseToDiversion["302"] = "unconditional"
-- HiCauseToDiversion["486"] = "user-busy"
-- HiCauseToDiversion["408"] = "no-answer"
-- HiCauseToDiversion["480"] = "deflection"
-- HiCauseToDiversion["487"] = "deflection"
-- HiCauseToDiversion["503"] = "unavailable"
-- HiCauseToDiversion["404"] = "unknown"

function convertHIToDiversion(msg)
   local historyInfos = msg:getHeaderValues("History-Info")

   for i, hi in ipairs(historyInfos)
   do
      hi = string.gsub(hi, "%%3B", ";")
      hi = string.gsub(hi, "%%3D", "=")
      hi = string.gsub(hi, "%%22", "\"")
      hi = string.gsub(hi, "%%20", " ")
```

```
      -- MS format: <sip:+19728522619@med02.lynclabsj.local;user=phone>;index=1;ms-retarget-
reason=forwarding

      local uri, index, reason = string.match (hi, "<(sip:.*@.*)>;index=(.*)reason=(.*)")

      trace.format("hi: uri '%s', reason '%s'", uri or "nil", reason or "nil")


      if uri
      then
         local diversion = string.format("<%s>", uri)
         if reason
         then
            diversion = string.format("<%s>;reason=\"unconditional\"", uri)
         end
         msg:addHeader("Diversion", diversion)
      end
   end
end

function convertReferredByToDiversion(msg)

   local refInfo = msg:getHeader("Referred-By")
   if refInfo
   then
      local diversion = string.format("%s;reason=\"unconditional\"", refInfo)
      msg:addHeader("Diversion", diversion)
   end

end

local function replaceHistoryHeader(msg)

   local hist = msg:getHeader("History-Info")

   if hist
   then
      convertHIToDiversion(msg)

      local di  = msg:getHeader("Diversion")

      if di
      then
         msg:removeHeader("History-Info")
      end
   end

end
```

```
local function replaceReferredByHeader(msg)

   local refby = msg:getHeader("Referred-By")
   if refby
   then
      convertReferredByToDiversion(msg)
   end

end

local function modifyUserFrom(msg)
-- get a data from "From" header and replace
   local removeUser= ""
   local value = msg:getHeader("From")

   if value
   then
      value = value:gsub(";user=phone", removeUser)
      if value
      then
         msg:modifyHeader("From", value)
      end
   end
end

local function process_inbound_request(msg)
   modifyUserFrom(msg)
   replaceHistoryHeader(msg)
   replaceReferredByHeader(msg)
   removecryptoline(msg)
   local sdp = msg:getSdp()
    if sdp
    then

        local tcap = sdp:getLine("a=tcap:", "RTP/SAVP")
if
   tcap
      then
      local a_m_line = sdp:getLine("m=audio", "RTP/AVP")
      a_m_line = a_m_line:gsub("AVP", "SAVP")
      sdp = sdp:modifyLine("m=audio", "RTP/AVP", a_m_line)
      end
       sdp=sdp:removeLine("a=crypto:", "|2^31|")
         msg:setSdp(sdp)
    end
end
```

```
function process_inbound_any_response(msg)
   msg:addHeader("SUPPORTED","X-cisco-srtp-fallback")
   local sdp = msg:getSdp()

   if sdp
   then
      trace.format("Inbound SDP")
      local tcap = sdp:getLine("a=tcap:", "RTP/SAVP")
      if tcap
      then
         local a_m_line = sdp:getLine("m=audio", "RTP/AVP")
         a_m_line = a_m_line:gsub("AVP", "SAVP")
         sdp = sdp:modifyLine("m=audio", "RTP/AVP", a_m_line)
      end
      trace.format("before removing crypto")
      sdp=sdp:removeLine("a=crypto:", "|2^31|")
      trace.format("after removing crypto")
      msg:setSdp(sdp)
   end
end

function removecryptoline(msg)
   local sdp = msg:getSdp()
   if sdp
   then
      trace.format("removecryptoline before removing crypto")
      sdp=sdp:removeLine("a=crypto:", "|2^31|")
      trace.format("removecryptoline after removing crypto")
      msg:setSdp(sdp)
   end

end


function process_inbound_any_request(msg)
  msg:addHeader("SUPPORTED","X-cisco-srtp-fallback")
end

M.outbound_INVITE        = process_outbound_request
M.outbound_ACK           = process_outbound_message
M.outbound_200_INVITE    = process_outbound_message
M.outbound_18X_INVITE    = process_outbound_message

M.inbound_183_INVITE     = process_inbound_progress
M.inbound_INVITE         = process_inbound_request
M.inbound_ANY_ANY        = process_inbound_any_response
M.inbound_ANY            = process_inbound_any_request
```

```
return M
```

SIP Trunk to Skype for Business Configuration

Navigation: Device → Trunk

Set **Device Name*= SFB_2019**. This is used for the test

Set **Device Pool* = G711_pool**. This is used for the test

Set **Call Classification*= Use System Default**. This is used for the test

Set **Media Resource Group List = MRGL_SW_NoMTP**. This is used for the test

Uncheck Media Termination Point Required

Check Run On All Active Unified CM Nodes

Check Redirecting Diversion Header Delivery – Inbound

Set **Destination Address = 172.16.31.99** [FQDN of Skype for Business Mediaition Server] this is used in the test

Set **SIP Trunk Security Profile*= SFB_SECURITY_PROFILE**

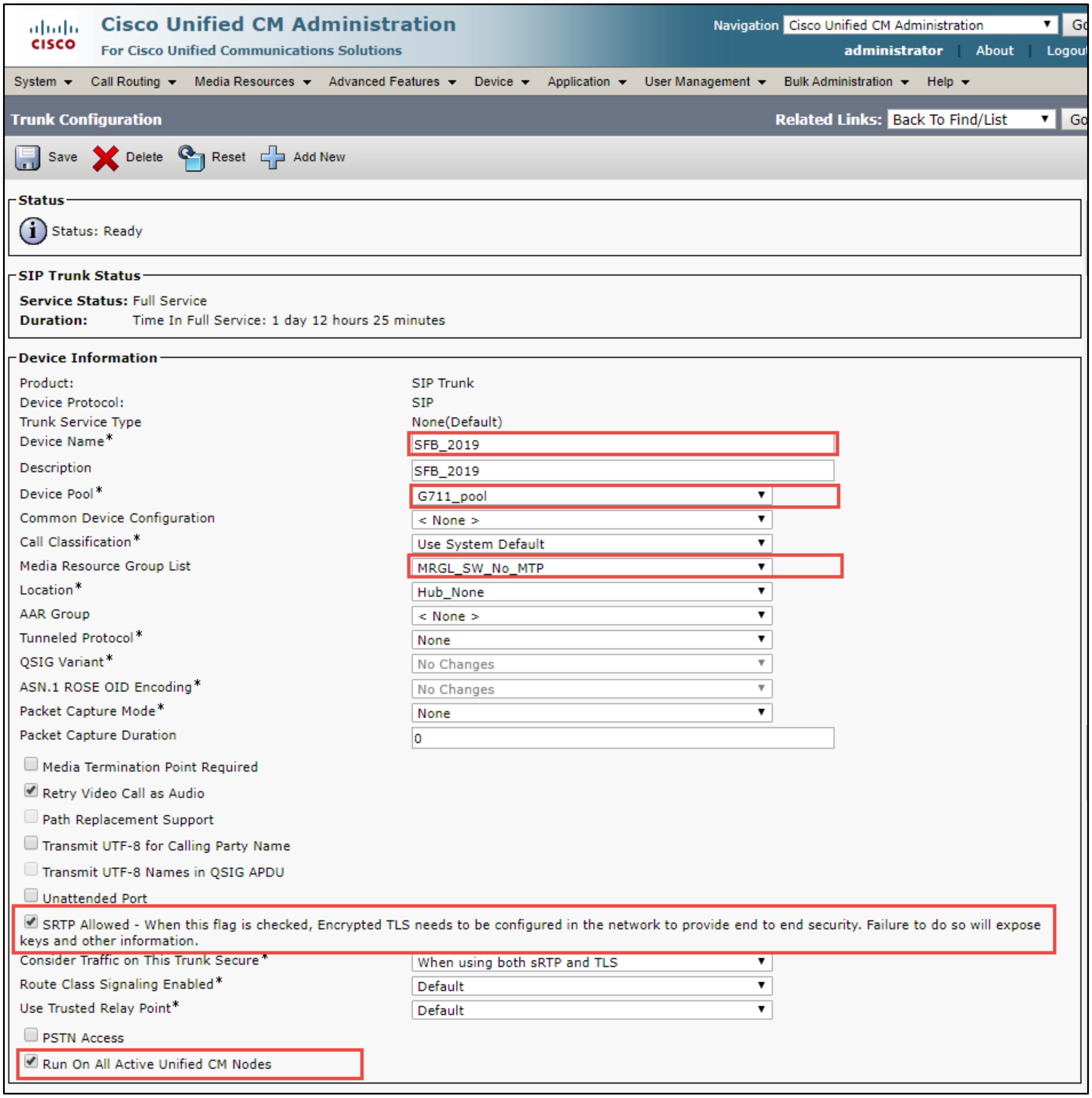
Set **SIP Profile*= SFB_SIP_PROFILE** – Standard SIP Profile

Set **DTMF Signaling Method*= No Preference**

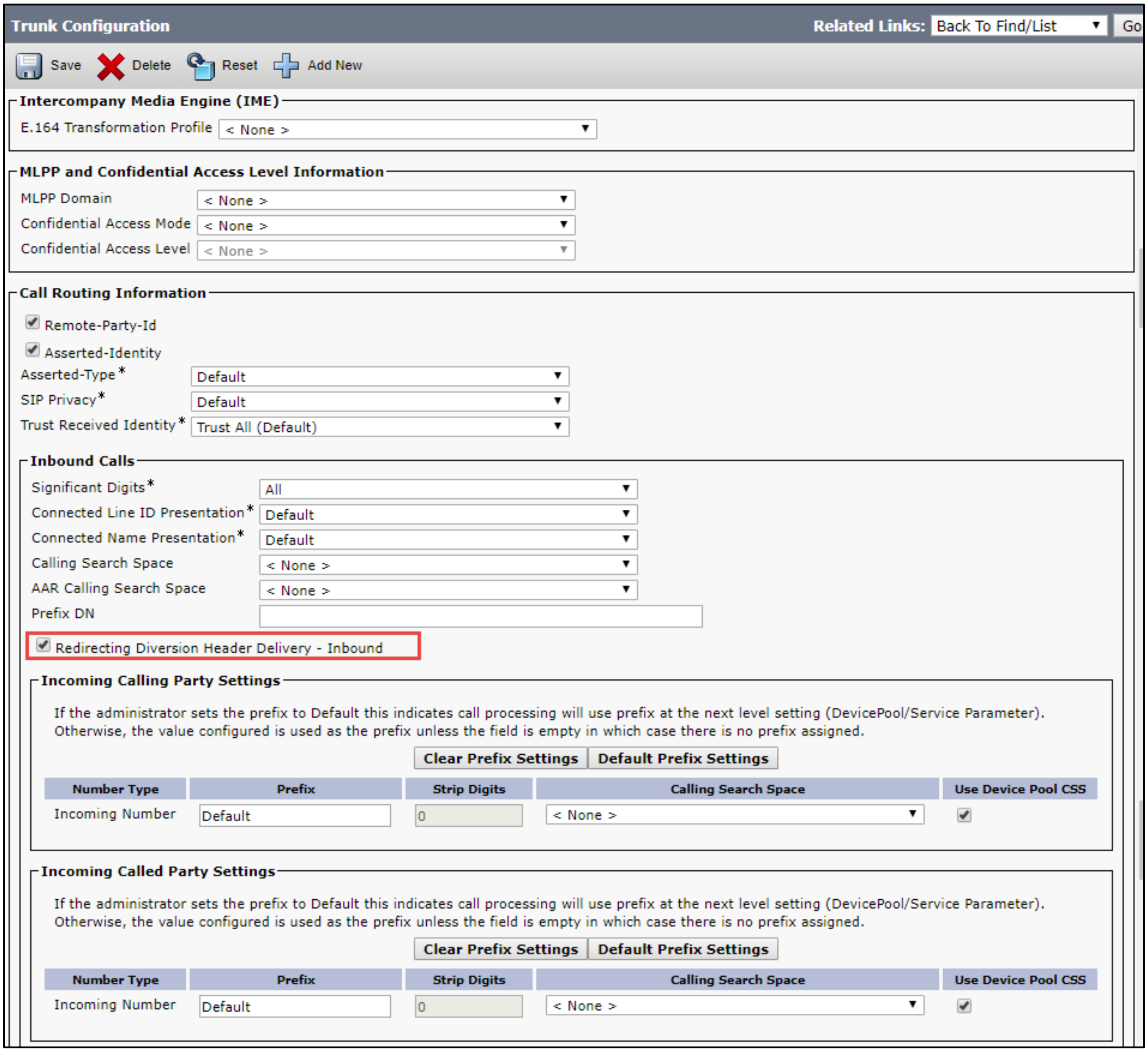
Set **Normalization Script = lync_interop_updated**

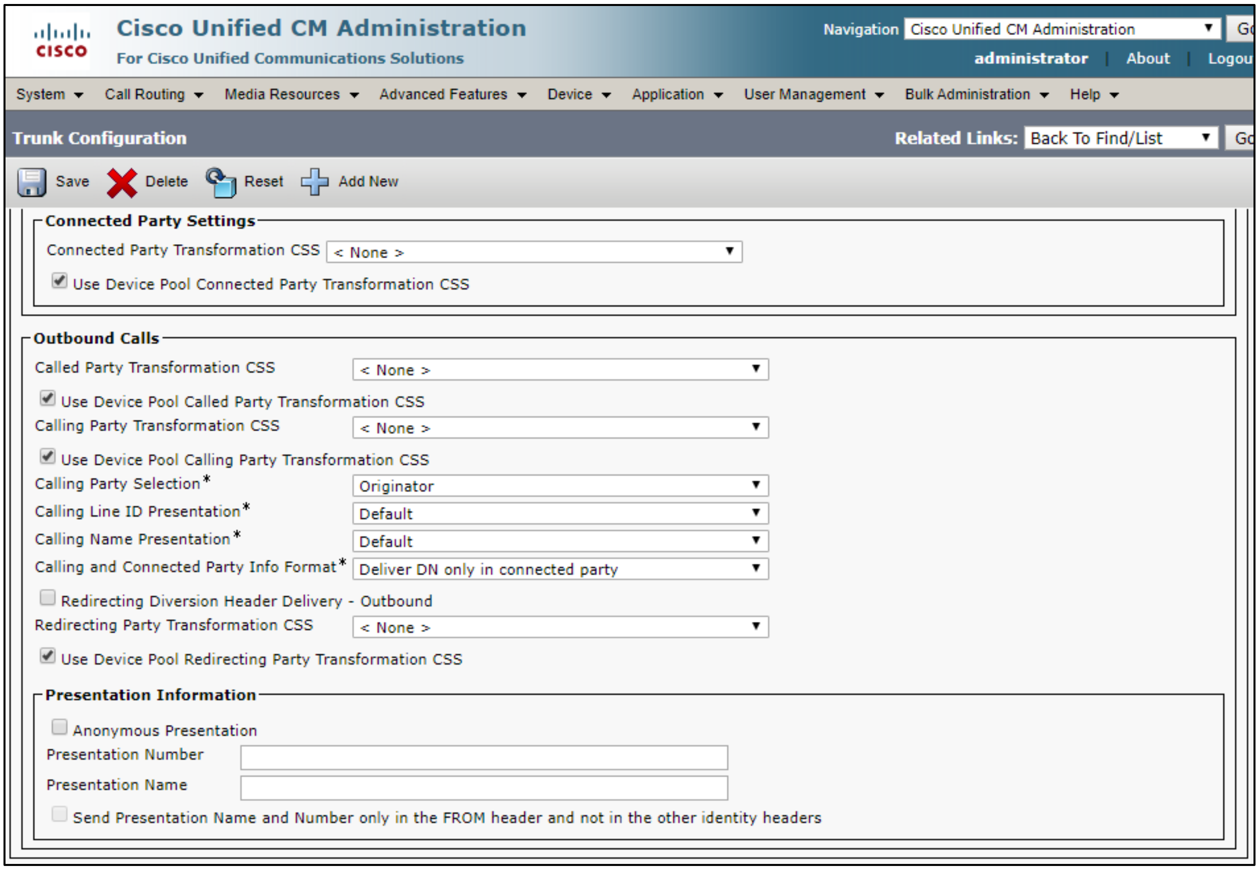
All other values are default.

Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)

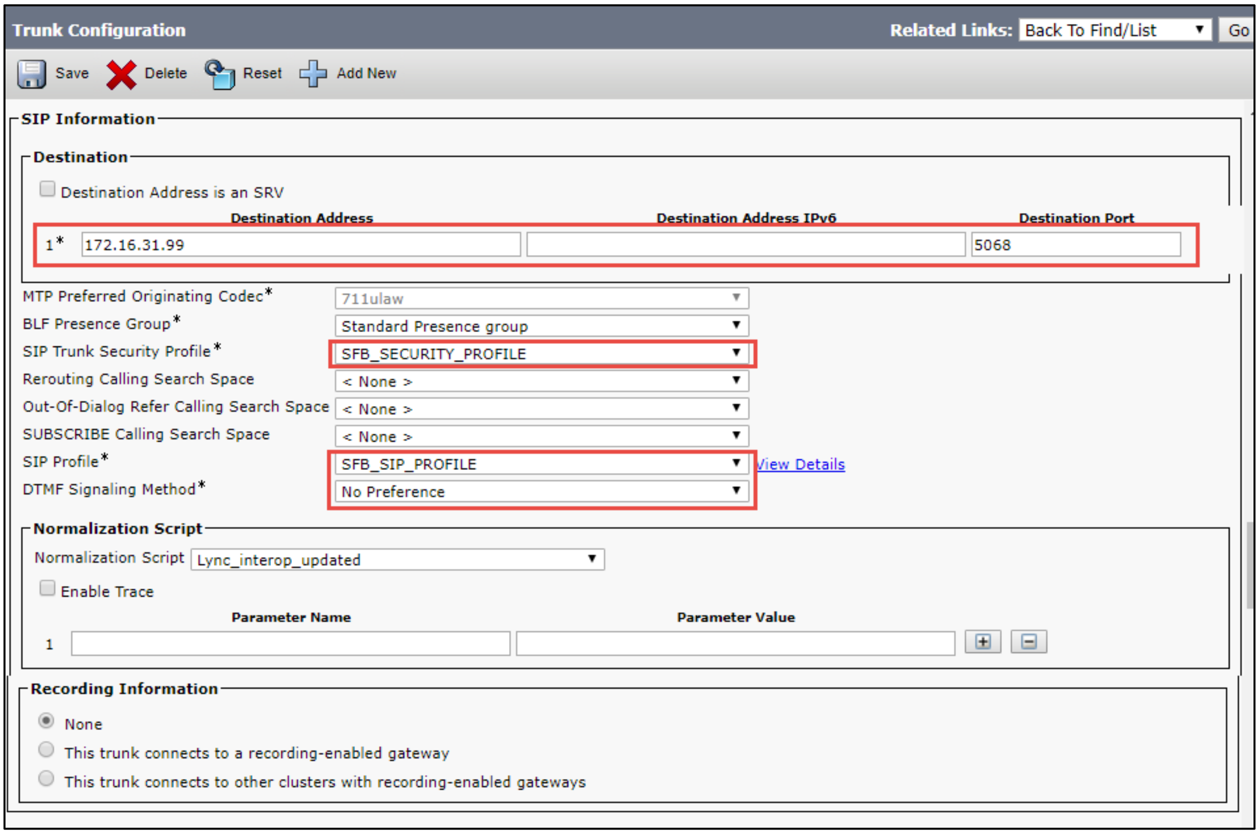


Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)




Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
administrator | About | Logou
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Trunk Configuration
Related Links: Back To Find/List
Save Delete Reset Add New
Connected Party Settings
Connected Party Transformation CSS < None >
Use Device Pool Connected Party Transformation CSS
Outbound Calls
Called Party Transformation CSS < None >
Use Device Pool Called Party Transformation CSS
Calling Party Transformation CSS < None >
Use Device Pool Calling Party Transformation CSS
Calling Party Selection* Originator
Calling Line ID Presentation* Default
Calling Name Presentation* Default
Calling and Connected Party Info Format* Deliver DN only in connected party
Redirecting Diversion Header Delivery - Outbound
Redirecting Party Transformation CSS < None >
Use Device Pool Redirecting Party Transformation CSS
Presentation Information
Anonymous Presentation
Presentation Number
Presentation Name
Send Presentation Name and Number only in the FROM header and not in the other identity headers

Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)



SIP Trunk to Cisco Unity Connection Configuration

Navigation: Device → Trunk

Set **Device Name*= Clus22unity**. This is used for the test.

Set **Device Pool* = Default**

Check Run On All Active Unified CM Nodes

Check Redirecting Diversion Header Delivery – Inbound

Check Redirecting Diversion Header Delivery – Outbound

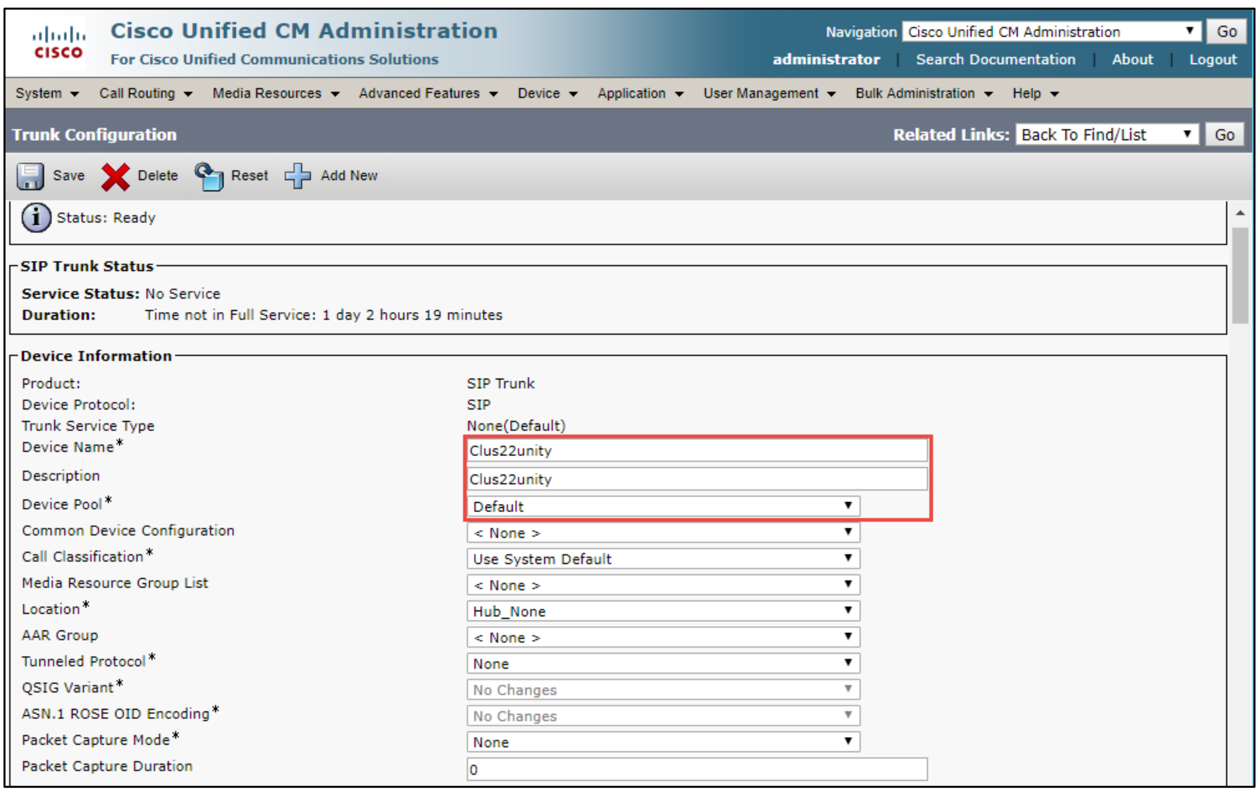
Set **Destination Address = 10.80.12.6**. This is used for the test.

Set **SIP Trunk Security Profile*= TLS_CUC**

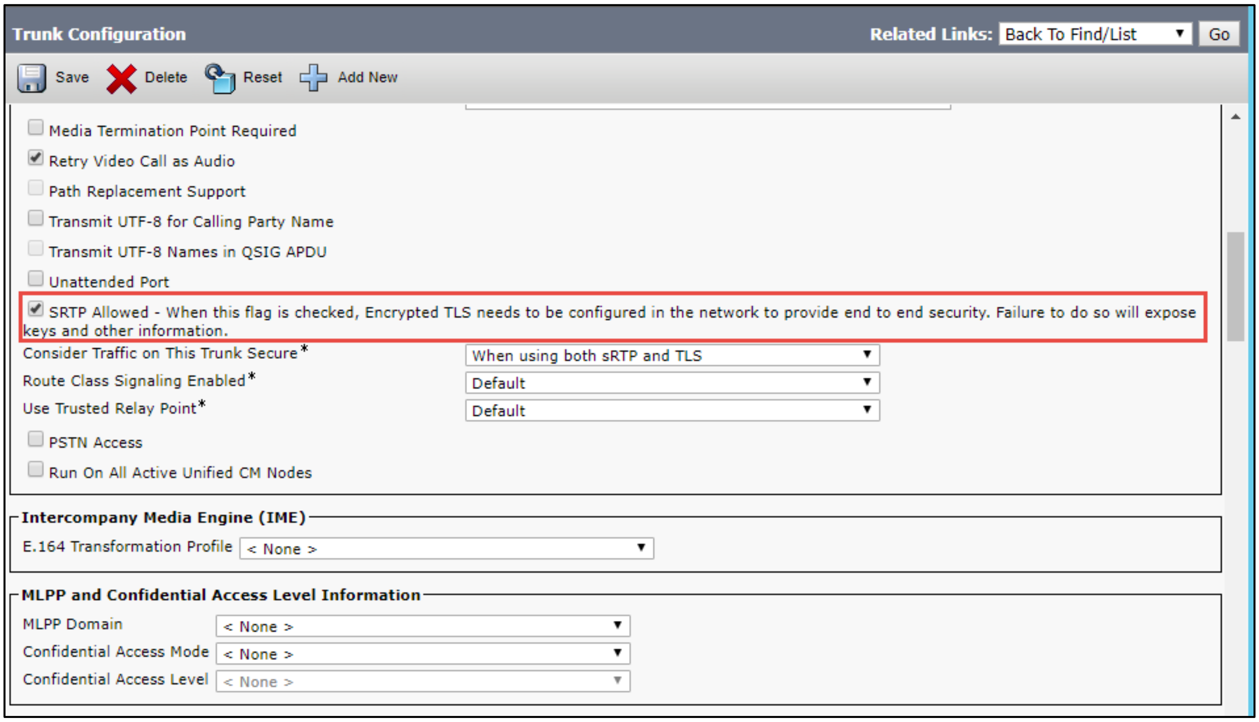
Set **SIP Profile*= Standard SIP Profile - OPTIONS**

Set **DTMF Signaling Method *= No Preference**

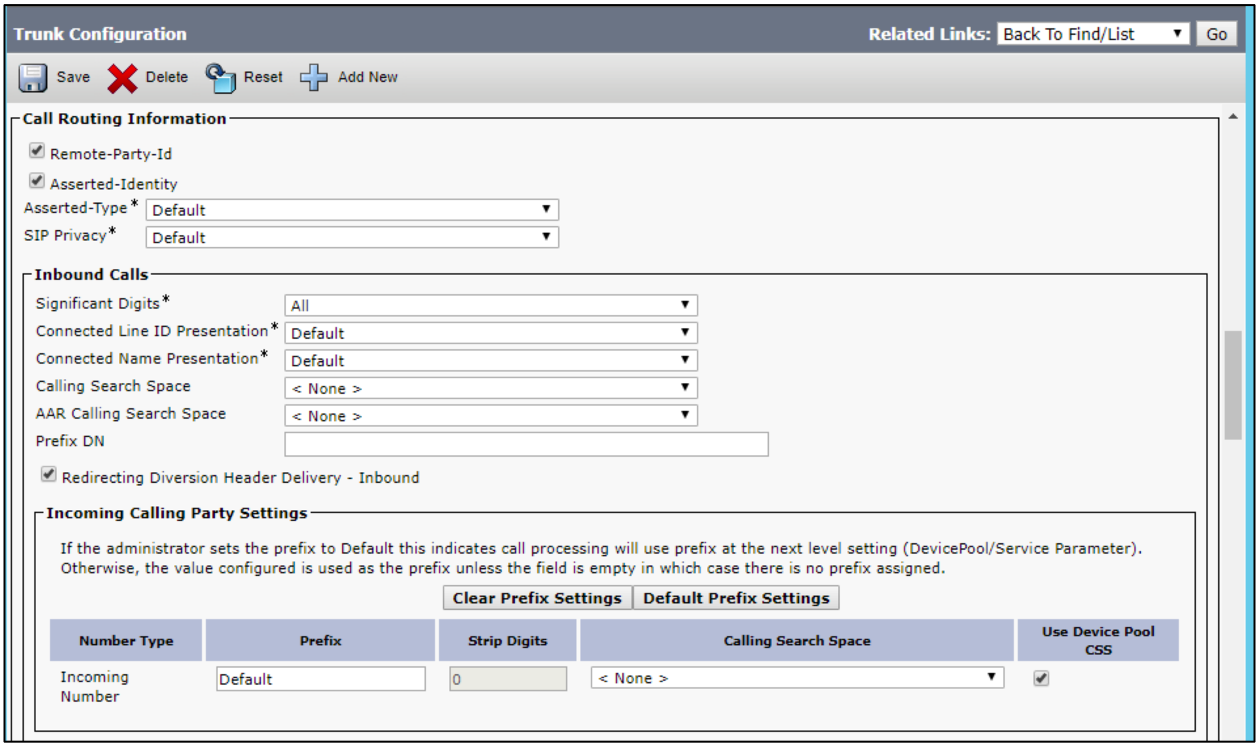
All other values are default



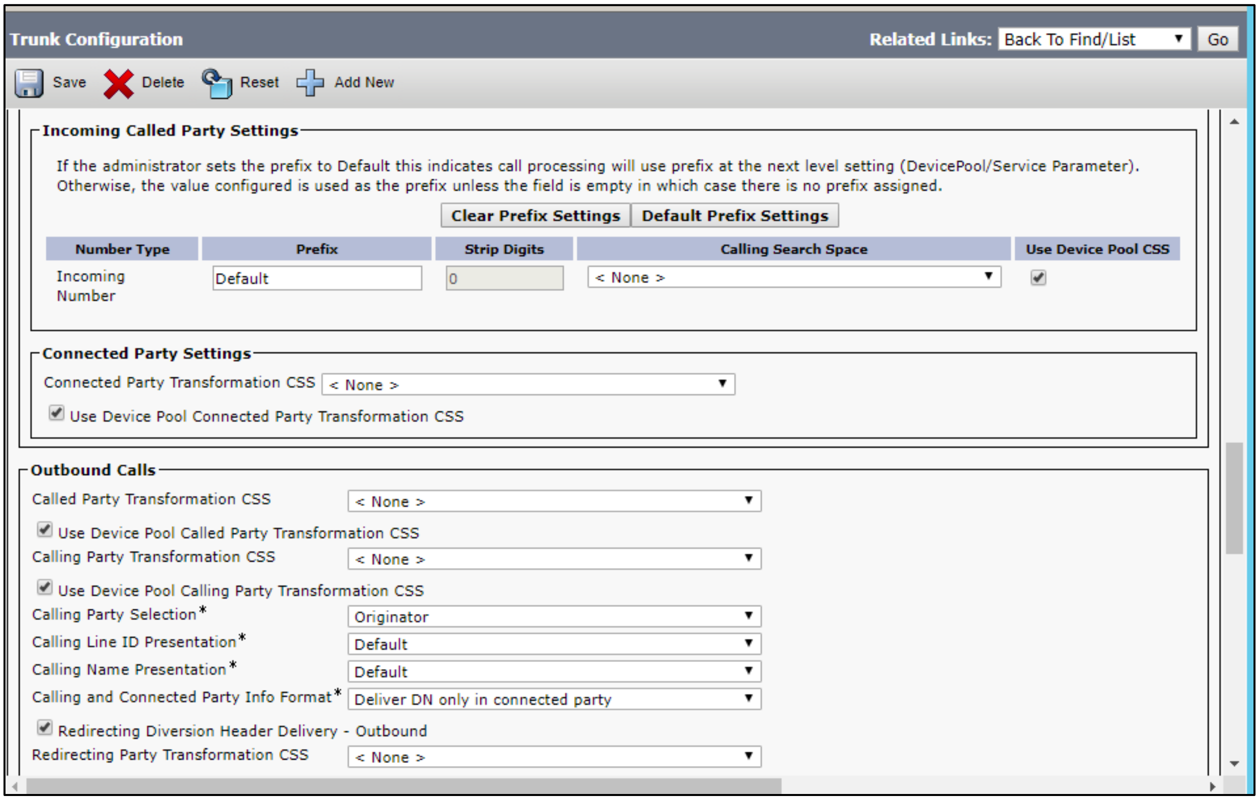
Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)

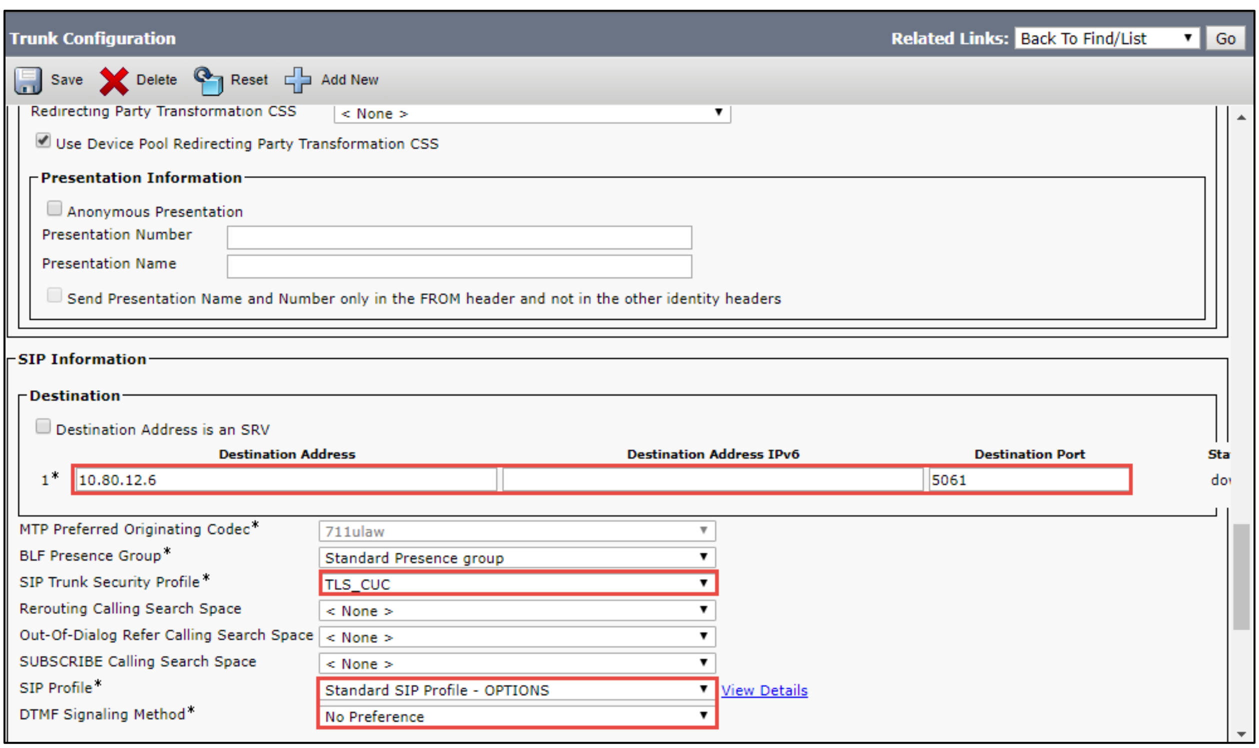


Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)



Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)





Voice Mail Configuration

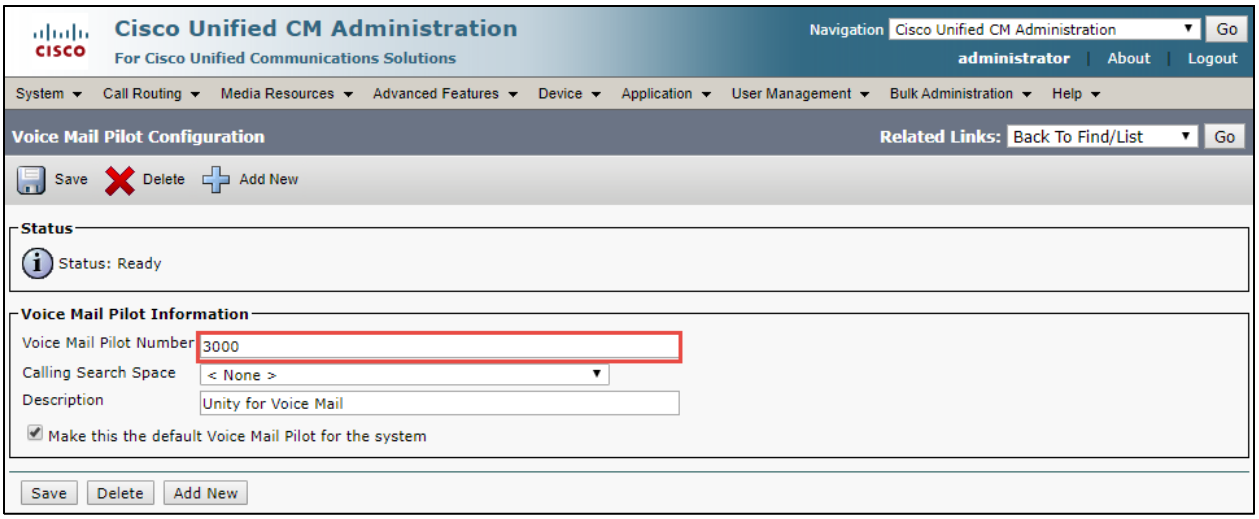
Configure Voice Mail Pilot:

Navigation: Advanced Features → Voice Mail → Voice Mail Pilot

Add new

Set **Voice Mail Pilot Number = 3000** .This is used for the test

Set **Description = Unity for Voice Mail** .This text is used to identify this SIP Profile



Route Pattern to Skype for Business Extensions

Navigation: Call Routing → Route/Hunt → Route Pattern

Add New

Set **Route Pattern* = 5XXX**. This is used to route to the Skype for Business in this test

Set **Gateway/Route List* = SFB_2019**. This is used for the test

Set **Calling Line ID Presentation= Default**

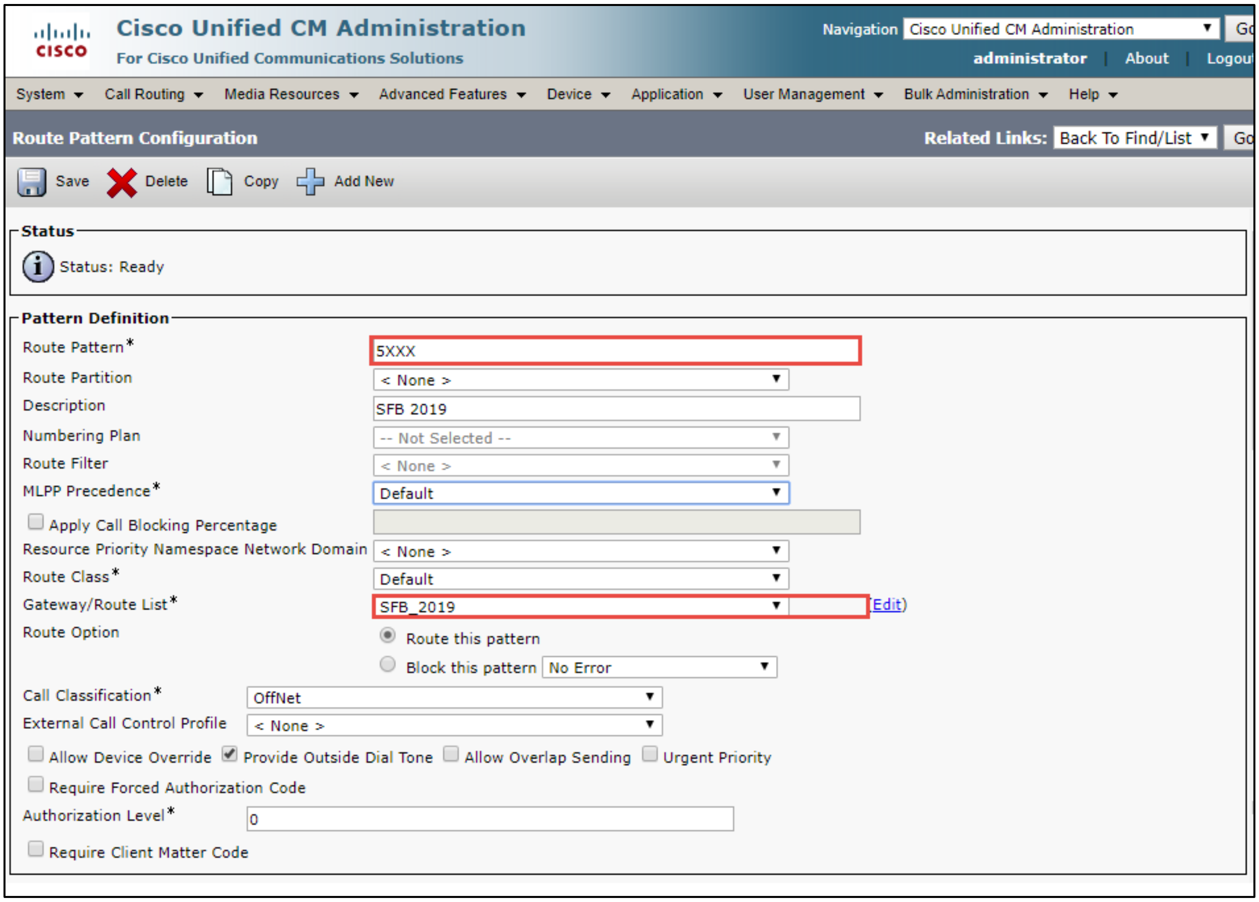
Set **Calling Name Presentation= Default**

Set **Connected Line ID Presentation*= Default**

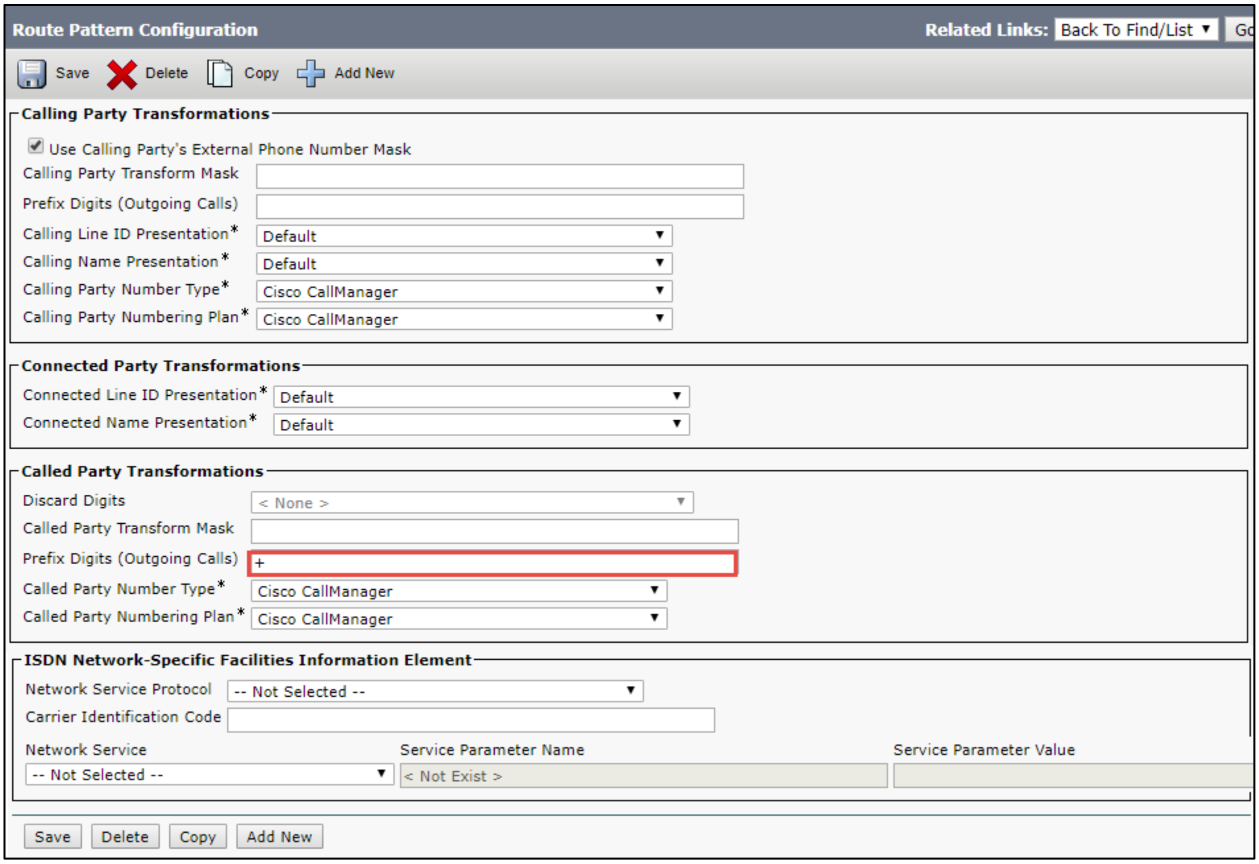
Set **Calling Name Presentation* = Default**

Prefix digit Outgoing Calls (Out Going) = +, Skype user configured + as prefix

All other values are default.


cisco
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
administrator | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Route Pattern Configuration
Related Links: Back To Find/List
Save Delete Copy Add New
Status
Status: Ready
Pattern Definition
Route Pattern*
5XXX
Route Partition
< None >
Description
SFB 2019
Numbering Plan
-- Not Selected --
Route Filter
< None >
MLPP Precedence*
Default
Apply Call Blocking Percentage
Resource Priority Namespace Network Domain
< None >
Route Class*
Default
Gateway/Route List*
SFB_2019
(Edit)
Route Option
Route this pattern
Block this pattern No Error
Call Classification*
OffNet
External Call Control Profile
< None >
Allow Device Override
Provide Outside Dial Tone
Allow Overlap Sending
Urgent Priority
Require Forced Authorization Code
Authorization Level*
0
Require Client Matter Code

Route Pattern Configuration for 2xxx (Continued)



Route Pattern to invoke Jabber client with Remote Destination configured as Skype for Business Extensions

Navigation: Call Routing → Route/Hunt → Route Pattern

Set **Route Pattern* = \+5XXX**. This is used to route to the Skype for Business when using the Extend and Connect functionality in this test

Set **Gateway/Route List* = SFB_2019**. This is used for the test

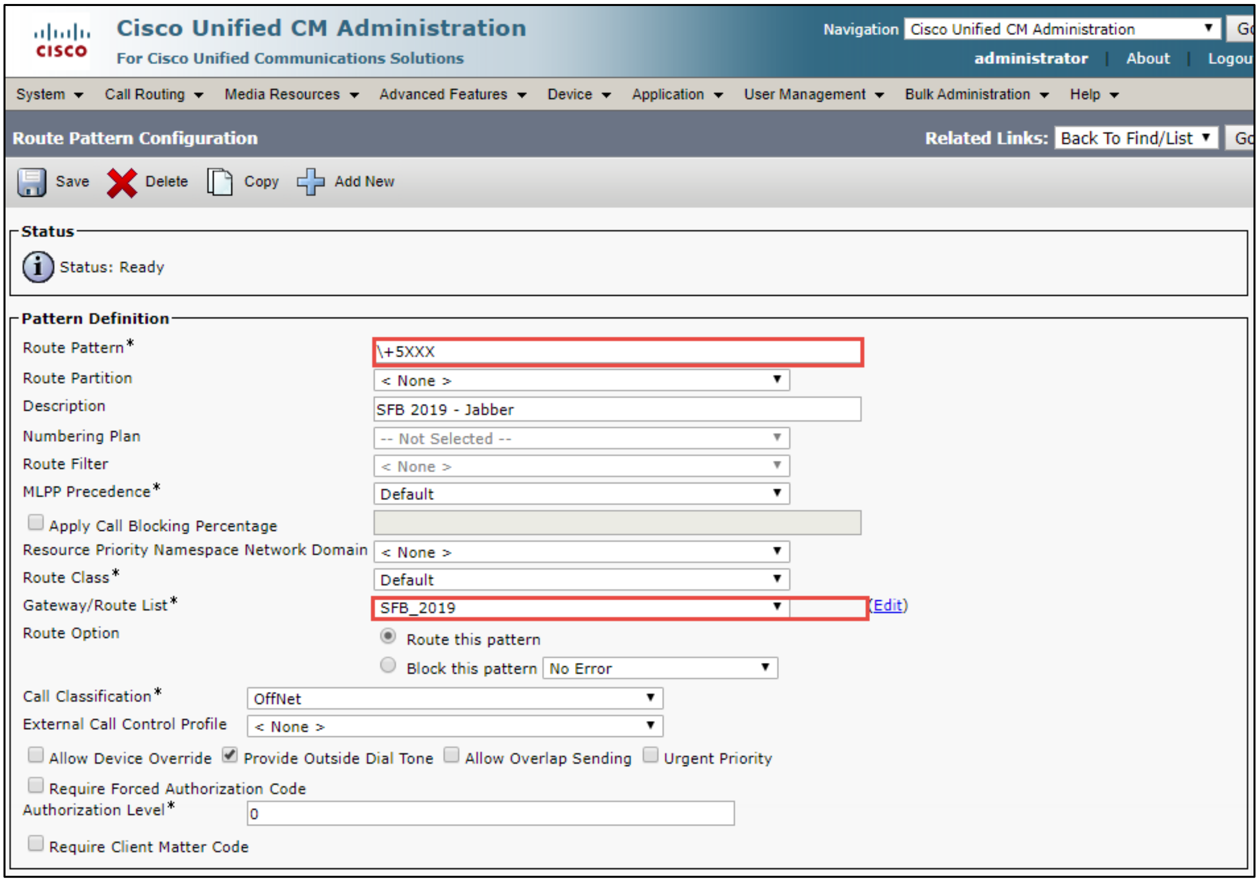
Set **Calling Line ID Presentation= Default**

Set **Calling Name Presentation= Default**

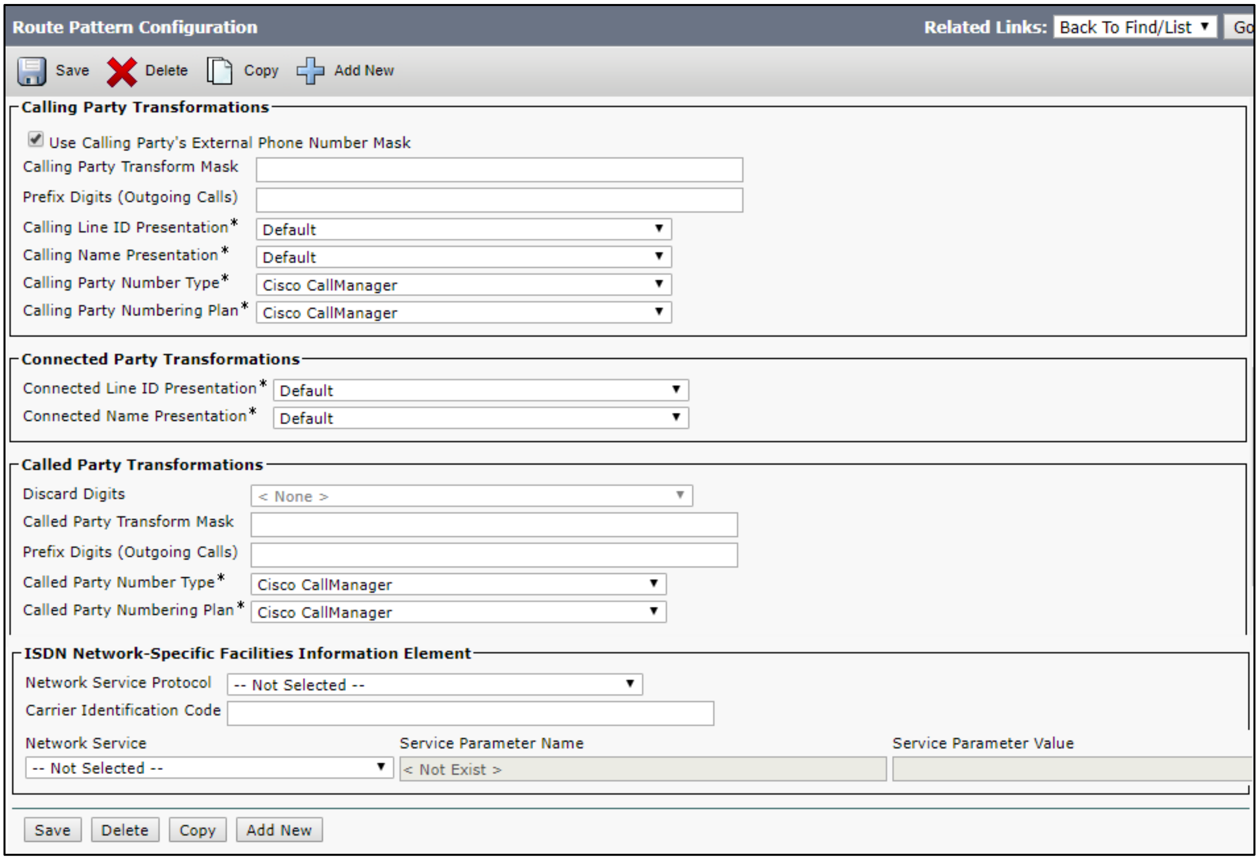
Set **Connected Line ID Presentation*= Default**

Set **Calling Name Presentation* = Default**

All other values are default

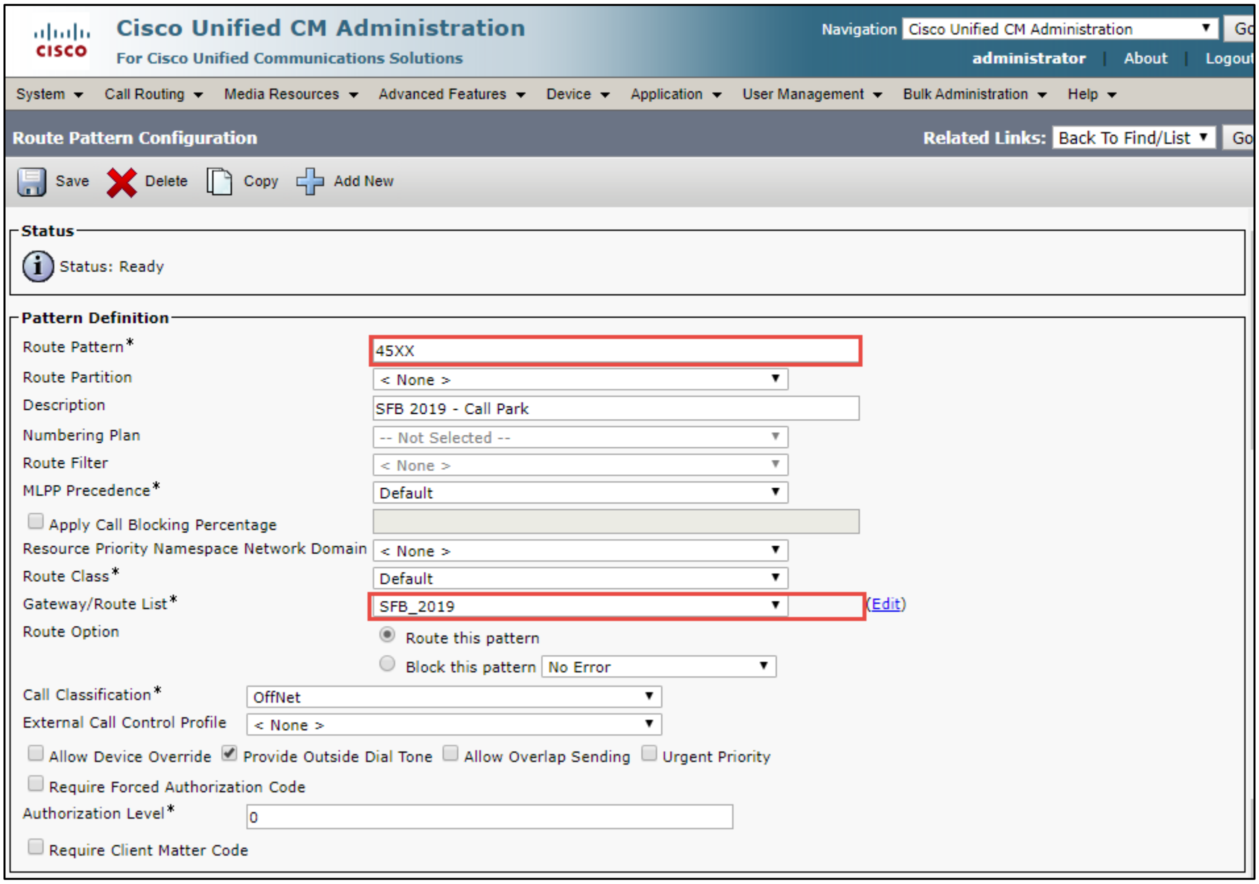

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
administrator | About | Logou
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Route Pattern Configuration
Related Links: Back To Find/List
Save Delete Copy Add New
Status
Status: Ready
Pattern Definition
Route Pattern* \+5XXX
Route Partition < None >
Description SFB 2019 - Jabber
Numbering Plan -- Not Selected --
Route Filter < None >
MLPP Precedence* Default
Apply Call Blocking Percentage
Resource Priority Namespace Network Domain < None >
Route Class* Default
Gateway/Route List* SFB_2019 (Edit)
Route Option
Route this pattern
Block this pattern No Error
Call Classification* OffNet
External Call Control Profile < None >
Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority
Require Forced Authorization Code
Authorization Level* 0
Require Client Matter Code

Cisco Unified Communications Manager Route pattern Configuration (Continued)

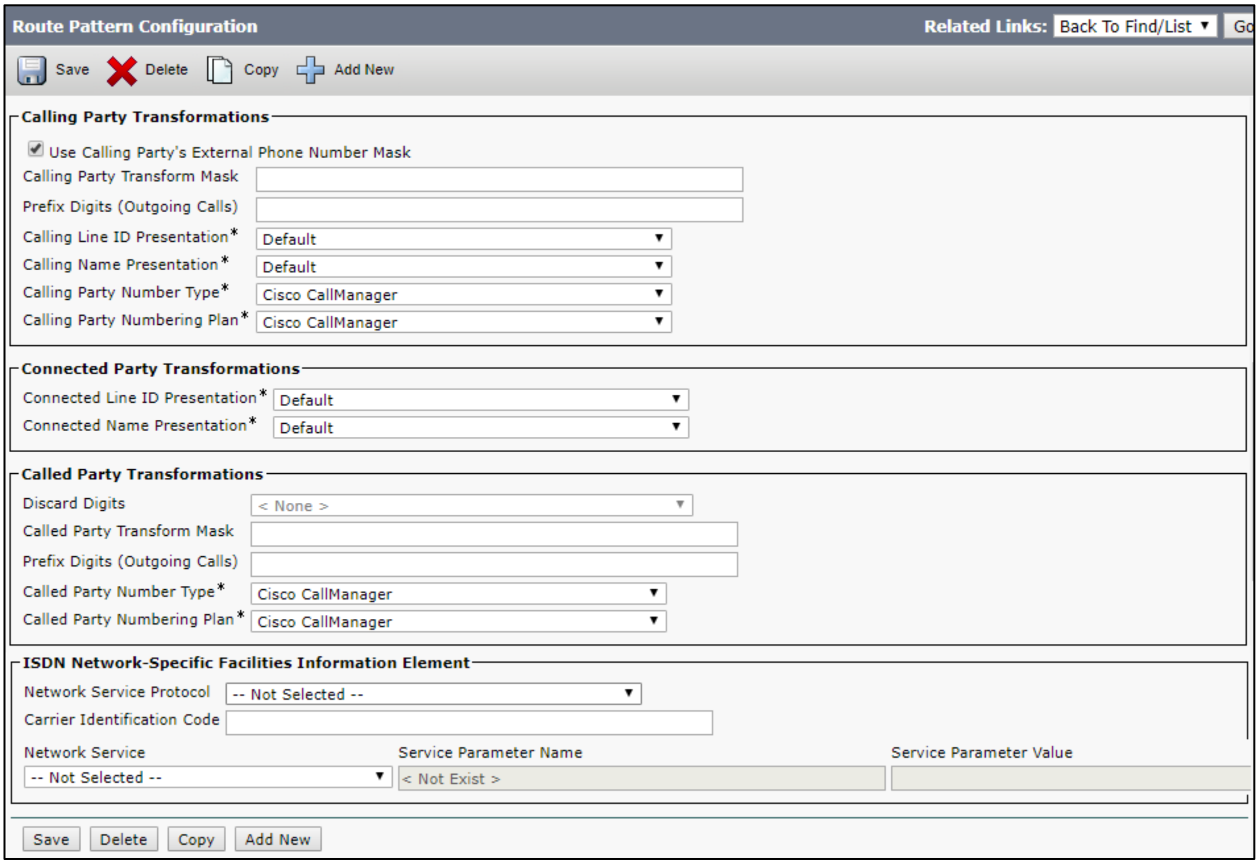


Route Pattern to Skype for Business Call Park range

The Skype for Business Call Park range configured is 1000-1999 .The following route pattern “45XX” is therefore configured to enable a parked call to be retrieved from Cisco UCM.

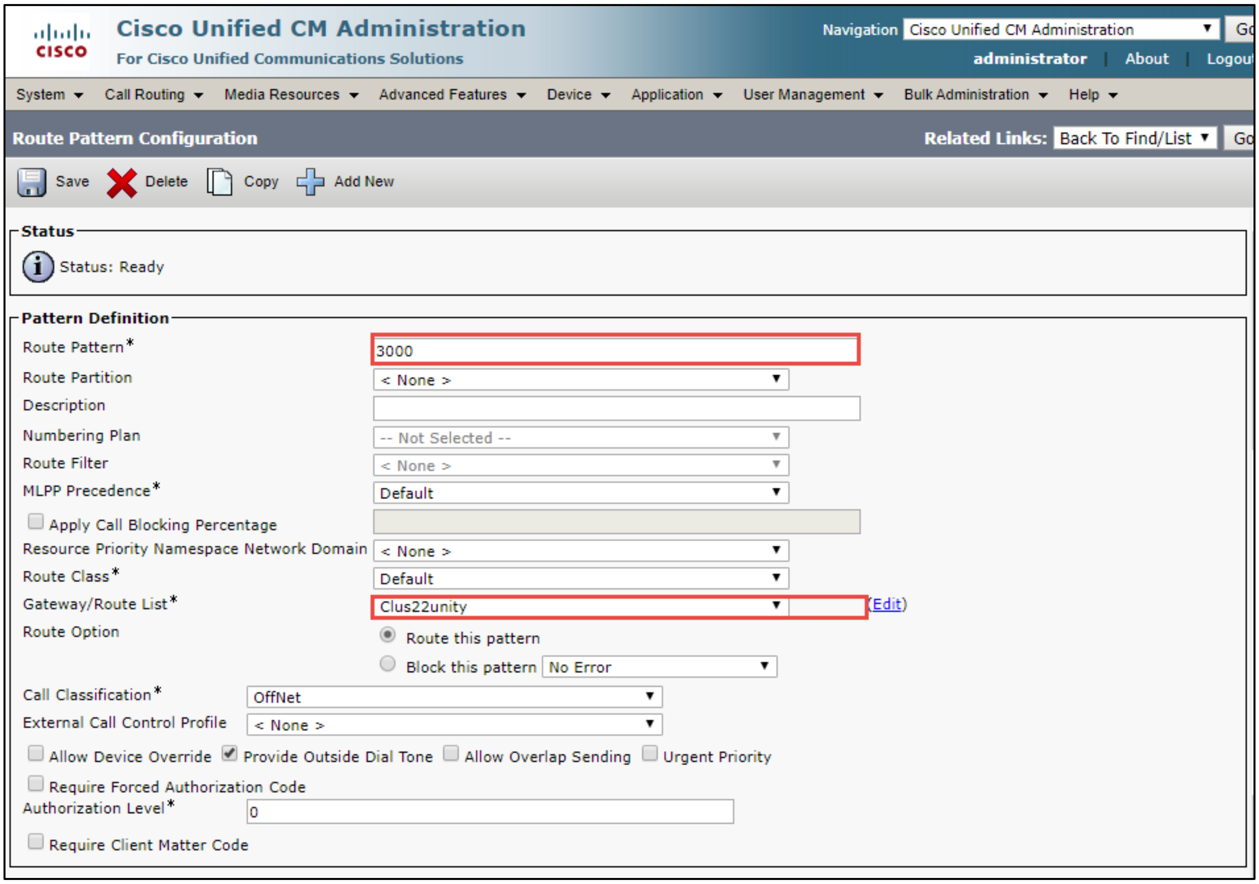


Cisco Unified Communications Manager Call Park Range Configuration (Continued)

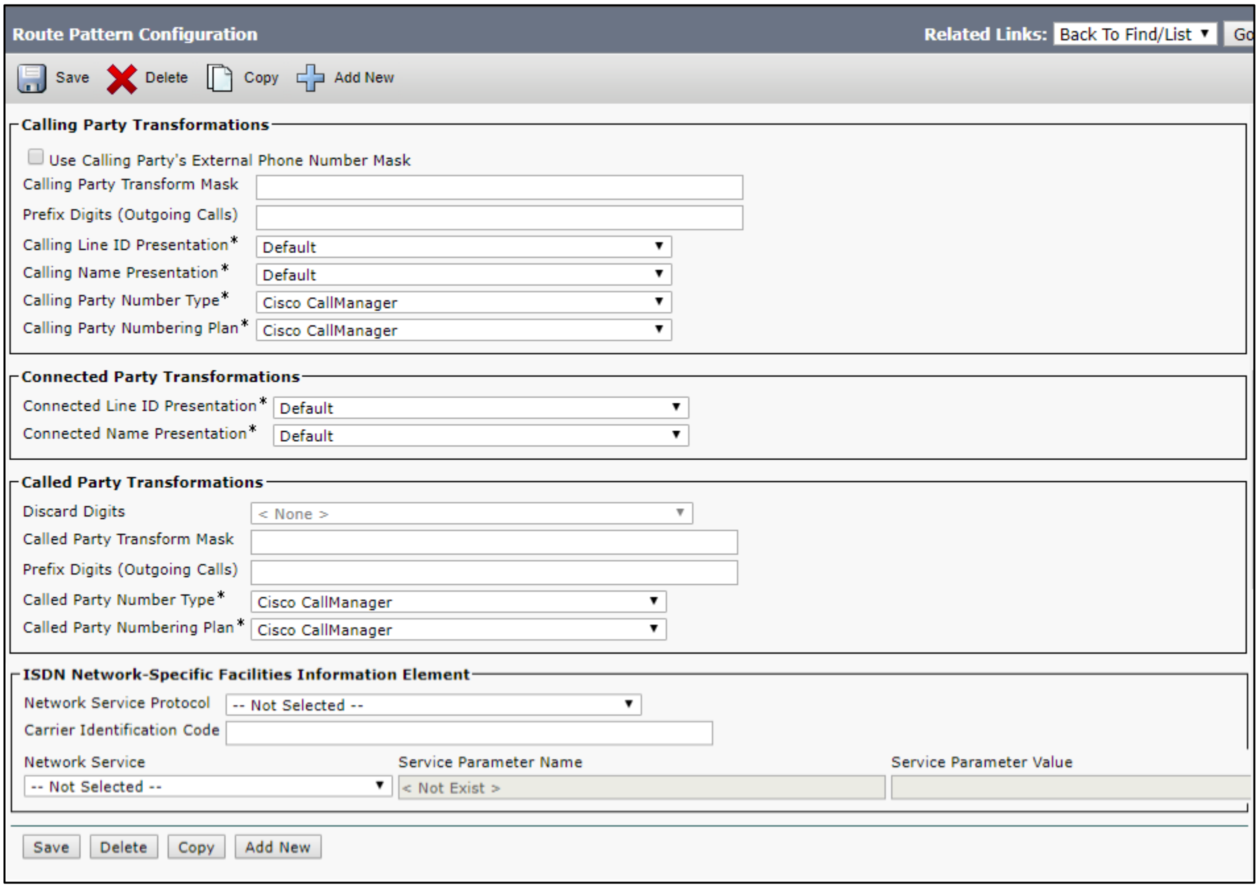


Route Pattern to Unity Connection Voice Mail

A route pattern 3000 (which is the voice mail pilot), is configured to reach Unity Connection Voice Mail.



Cisco Unified Communications Manager Route Pattern Configuration (Continued)



Cisco UCM Extent and Connect

Extend and Connect is a feature that allows administrators to rapidly deploy UC Computer Telephony Integration (CTI) applications, which interoperate with any endpoint. With Extend and Connect, users can leverage the benefits of UC applications from any location using any device. This feature also allows Interoperability between newer UC solutions and legacy systems, so customers can migrate to newer UC Solutions over time as existing hardware is deprecated.

UC service Configuration

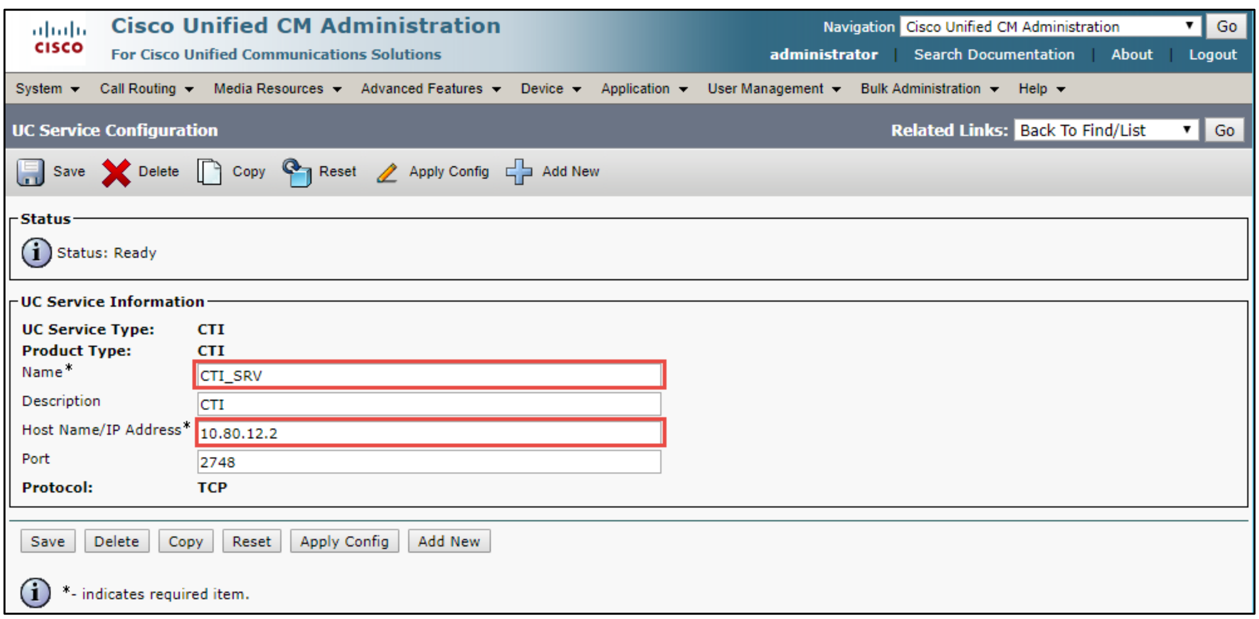
Navigation Path: User Management→ User setting → UC Service

Add New

Select Service Type as CTI

Set **Name = CTI_SRV**

Set **Host Name/IP Address* = 10.80.12.2**; this is the Cisco UCM publisher IP.

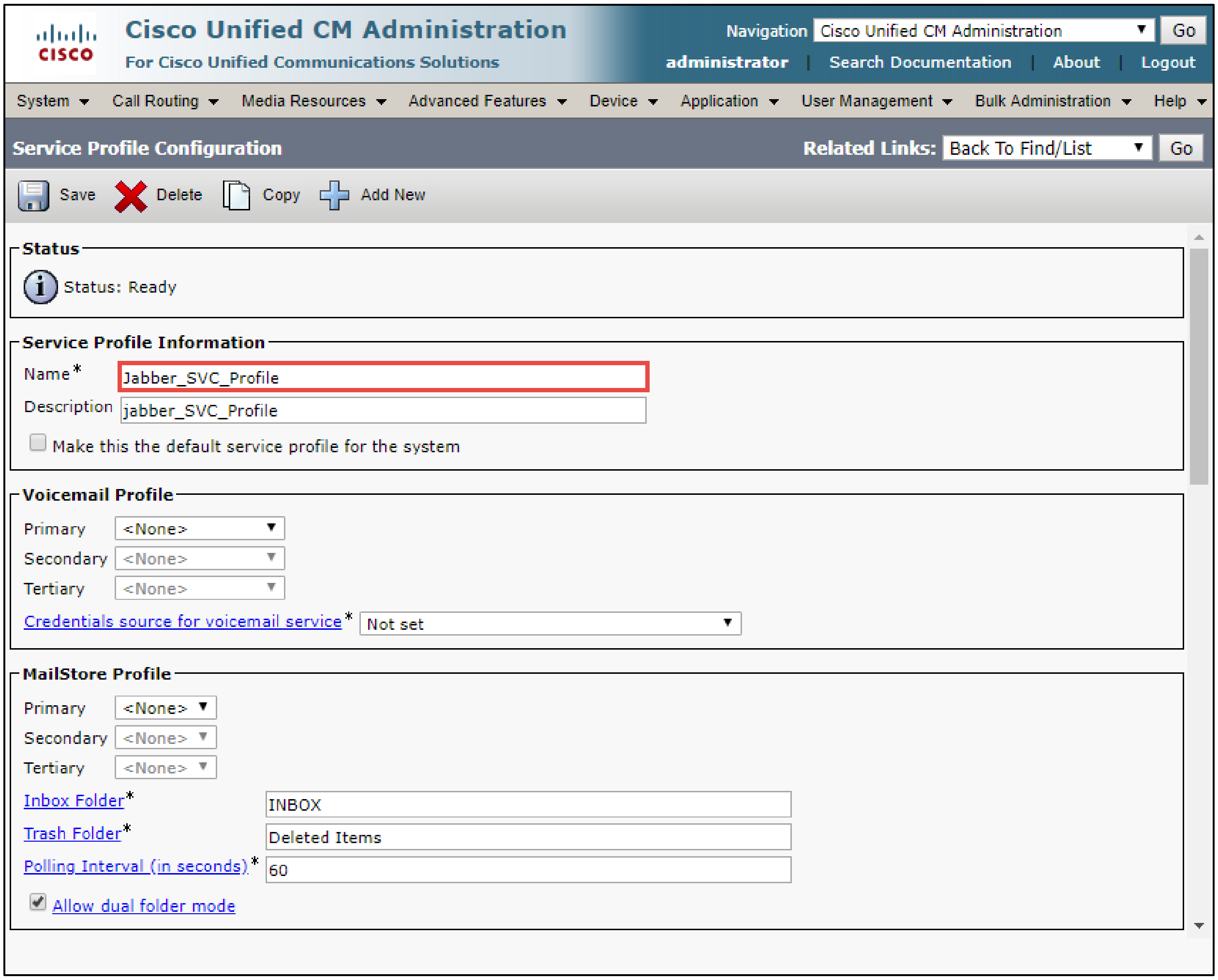


In the same manner, a UC Service is configured for the subscriber also.

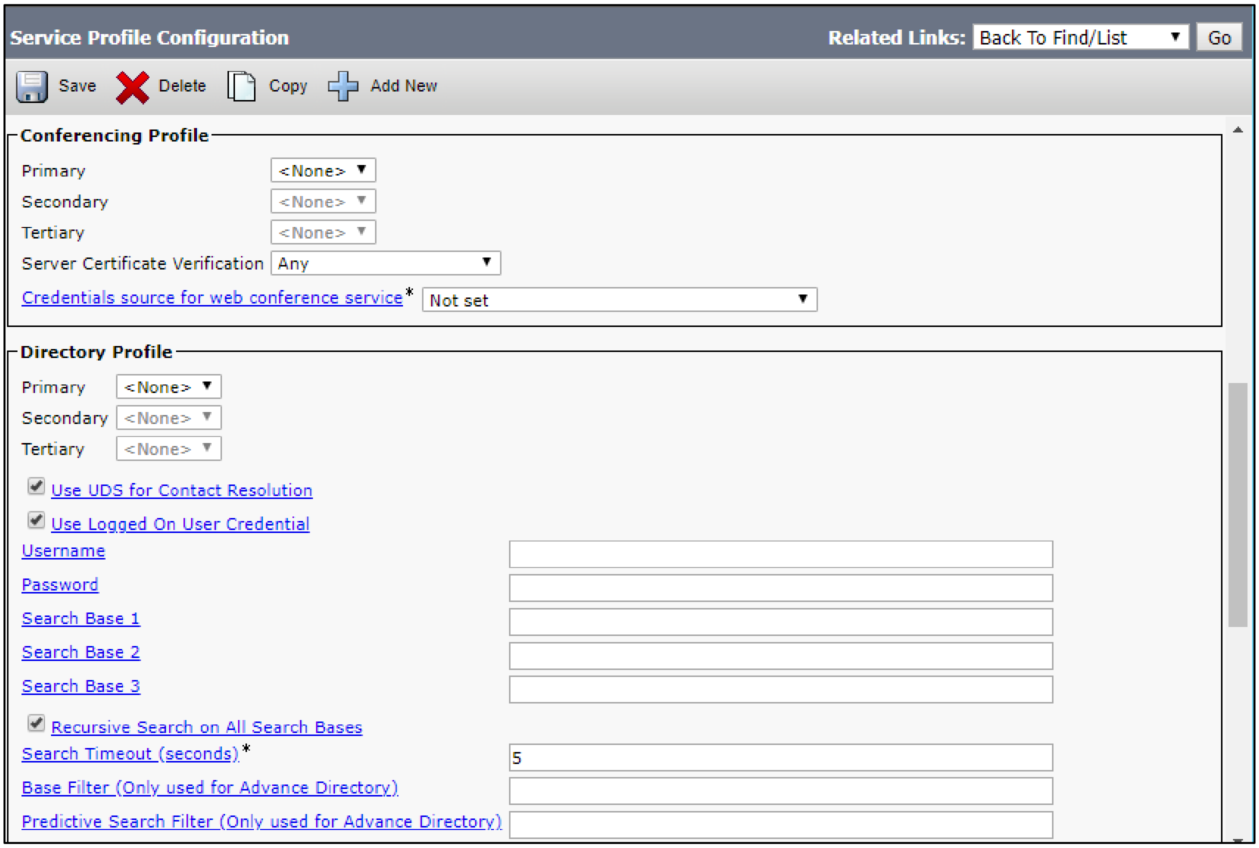
A UC service of Type IM and Presence is configured with the IP of the Presence server.

Service Profile Configuration

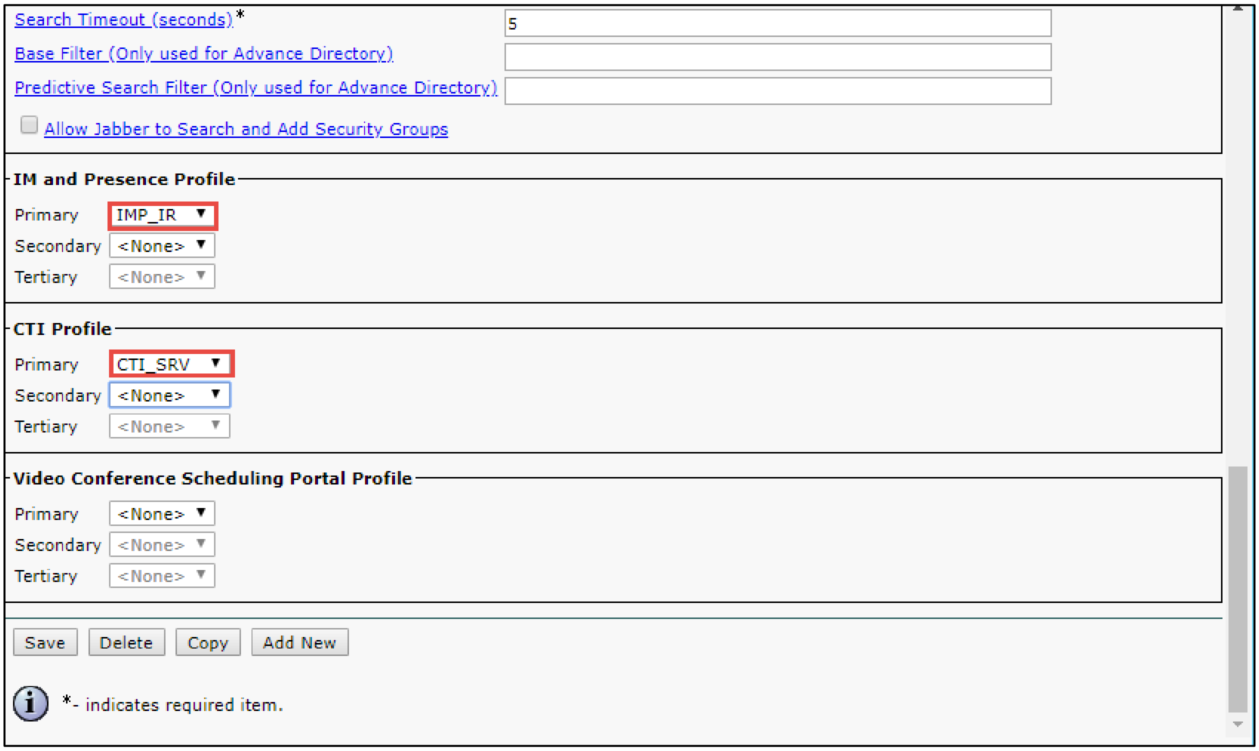
Navigation: User Management→ User setting → Service Profile



Cisco UCM service profile Configuration (Continued)



Cisco UCM service profile Configuration (Continued)



Cisco Unified CM IM Presence – CCMCIP Profile Configuration

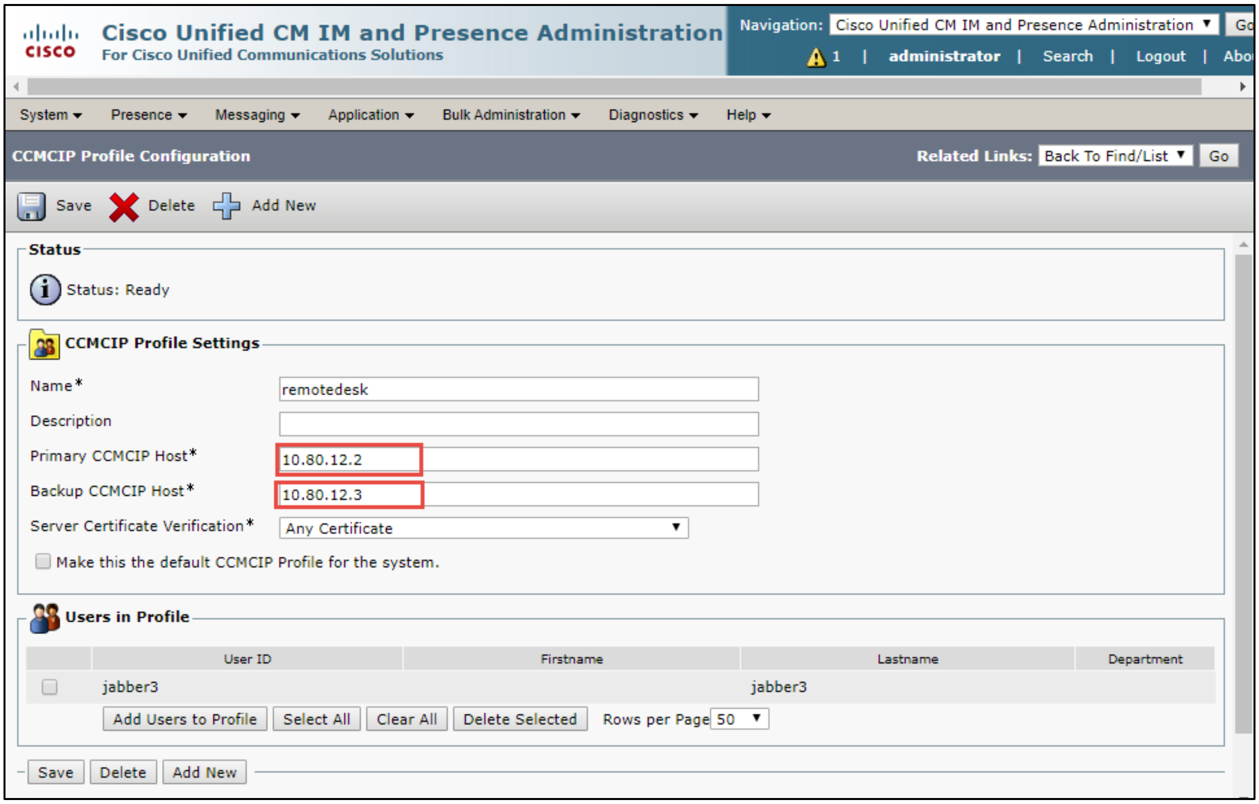
Navigation Path: Application → CCMCIP Profile

Set Name *: remotedesk. This is used in this example.

Set **Primary CCMCIP Host *: 10.80.12.2**.Cisco Publisher IP. This is used in this test.

Set **Backup CCMCIP Host *: 10.80.12.3**.Cisco Publisher IP. This is used in this test.

Add Users to Profile: jabber3.This is used in this test.



SIP trunk to Cisco IM&Presence Trunk Configuration

Navigation Path: Device→ Trunk

Set **Device Name*=IMPTrunk**. This is used for the test.

Set **Device Pool* = Default**. This is used for the test.

Set **Media Resource Group List = MRGL_SW_NoMTP**. This is used for the test.

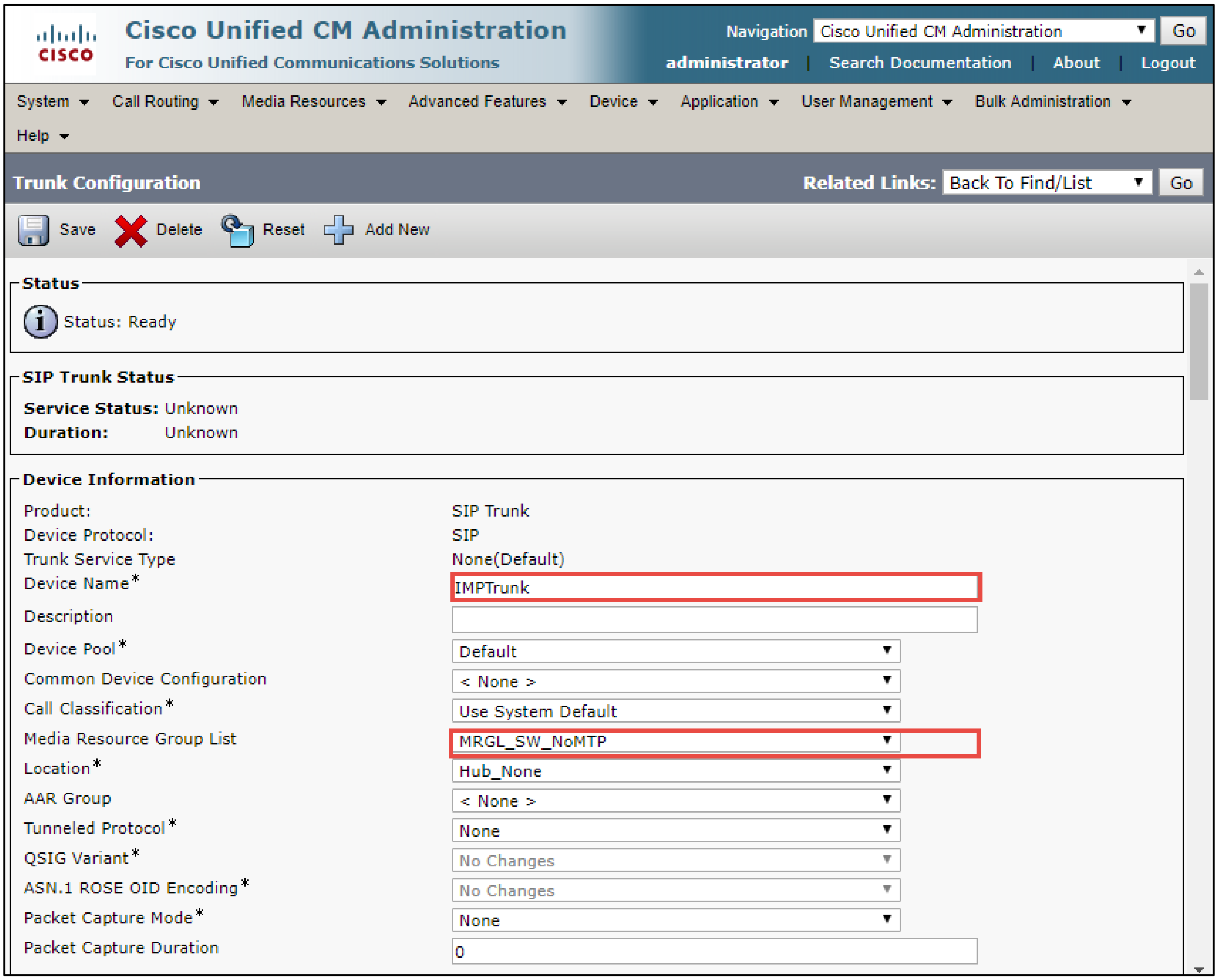
Set **Destination Address = 10.80.12.5**. This is used in this example.

Set **SIP Trunk Security Profile*= Non-Secure SIP Trunk Profile**.

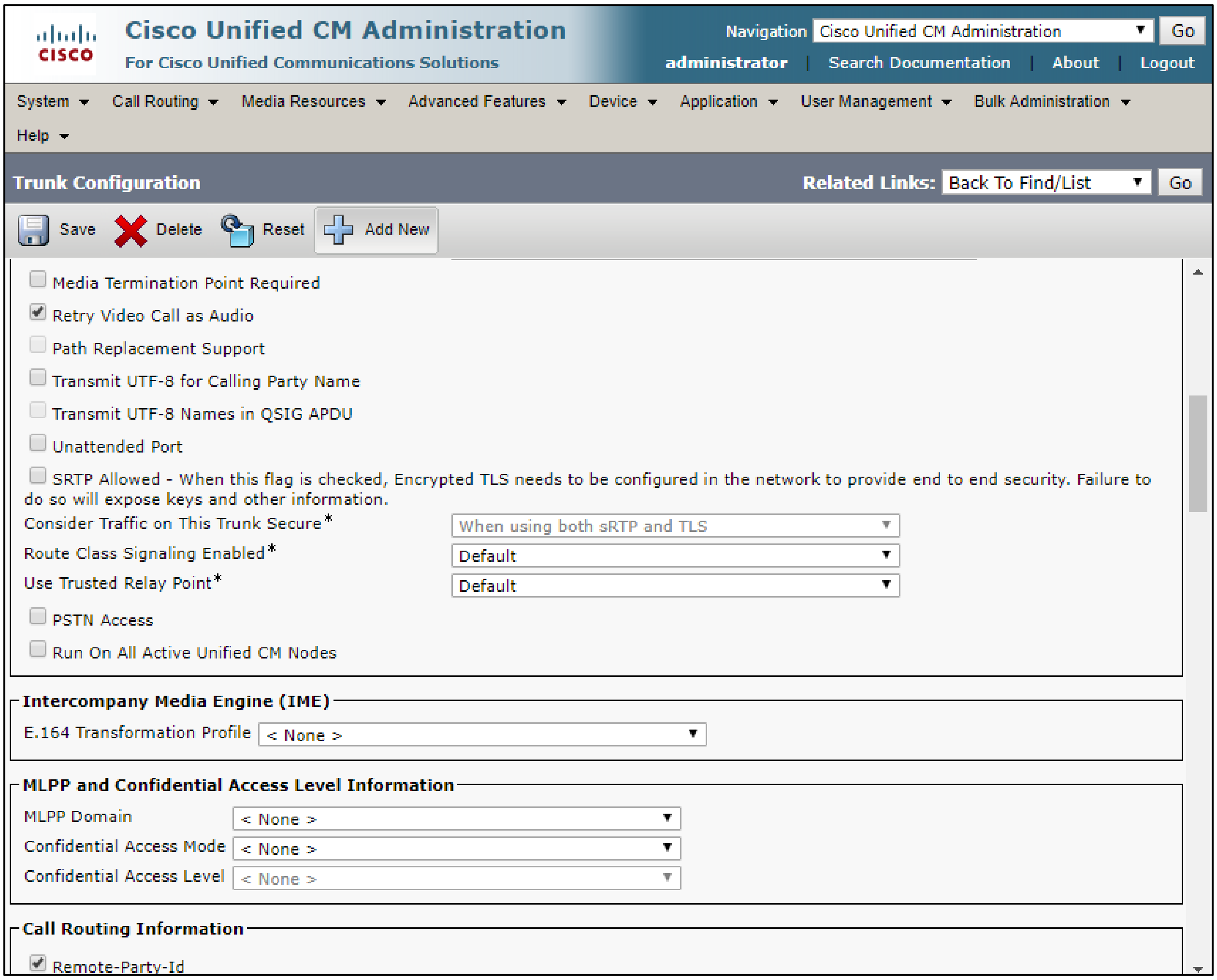
Set **SIP Profile*= Standard SIP Profile.**

Set **DTMF Signaling Method*= No Preference.**

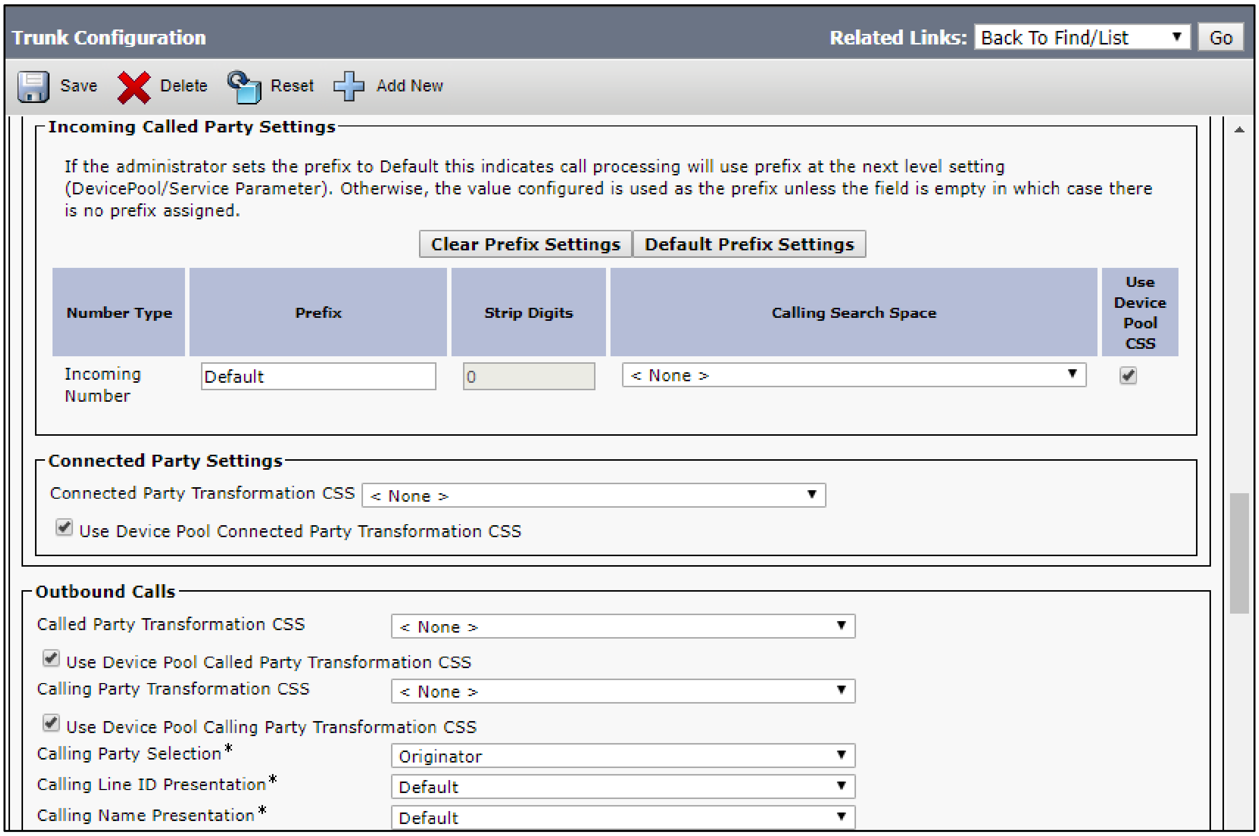
All other values are default.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Help
Trunk Configuration
Related Links: Back To Find/List Go
Save Delete Reset Add New
Status
Status: Ready
SIP Trunk Status
Service Status: Unknown
Duration: Unknown
Device Information
Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type None(Default)
Device Name* IMPTrunk
Description
Device Pool* Default
Common Device Configuration < None >
Call Classification* Use System Default
Media Resource Group List MRGL_SW_NoMTP
Location* Hub_None
AAR Group < None >
Tunneled Protocol* None
QSIG Variant* No Changes
ASN.1 ROSE OID Encoding* No Changes
Packet Capture Mode* None
Packet Capture Duration 0

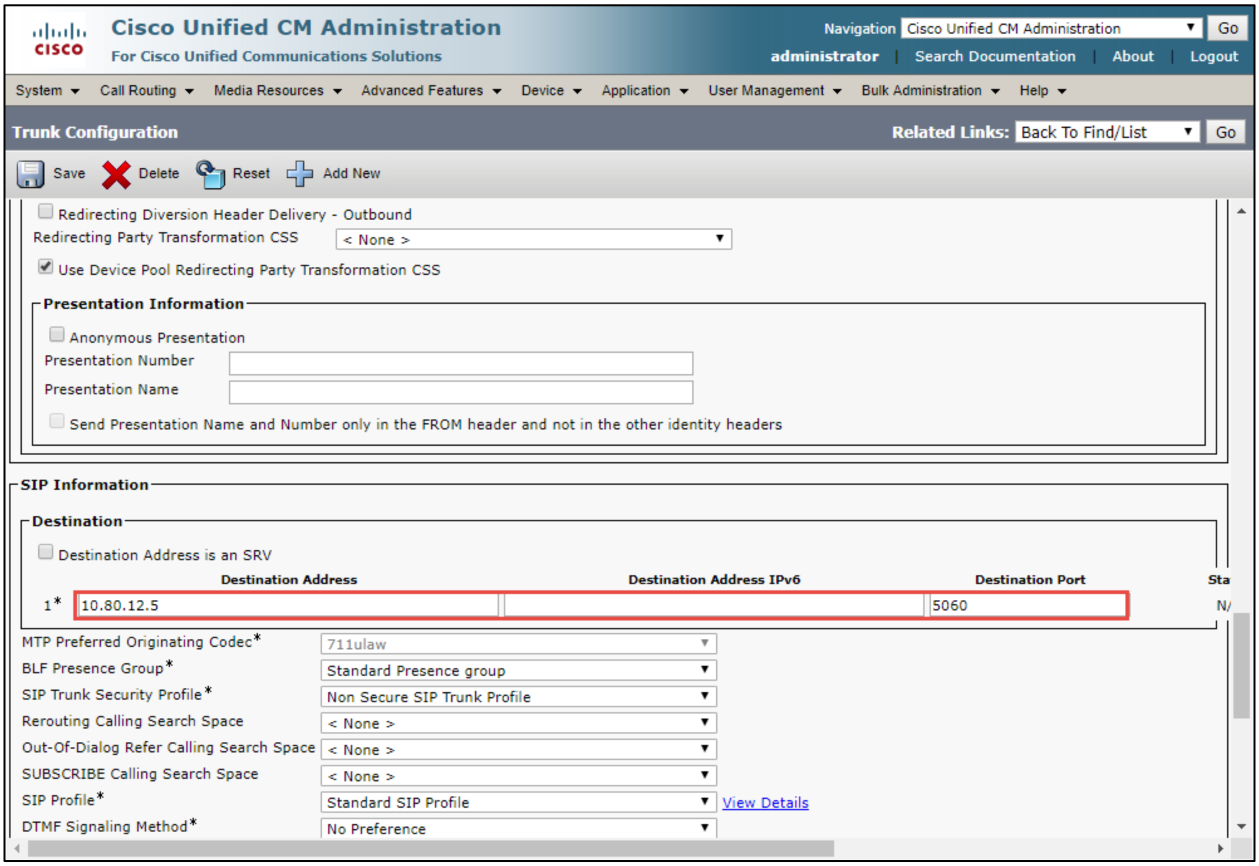
Cisco Unified Communications Manager SIP Trunk to CUP Configuration (Continued)

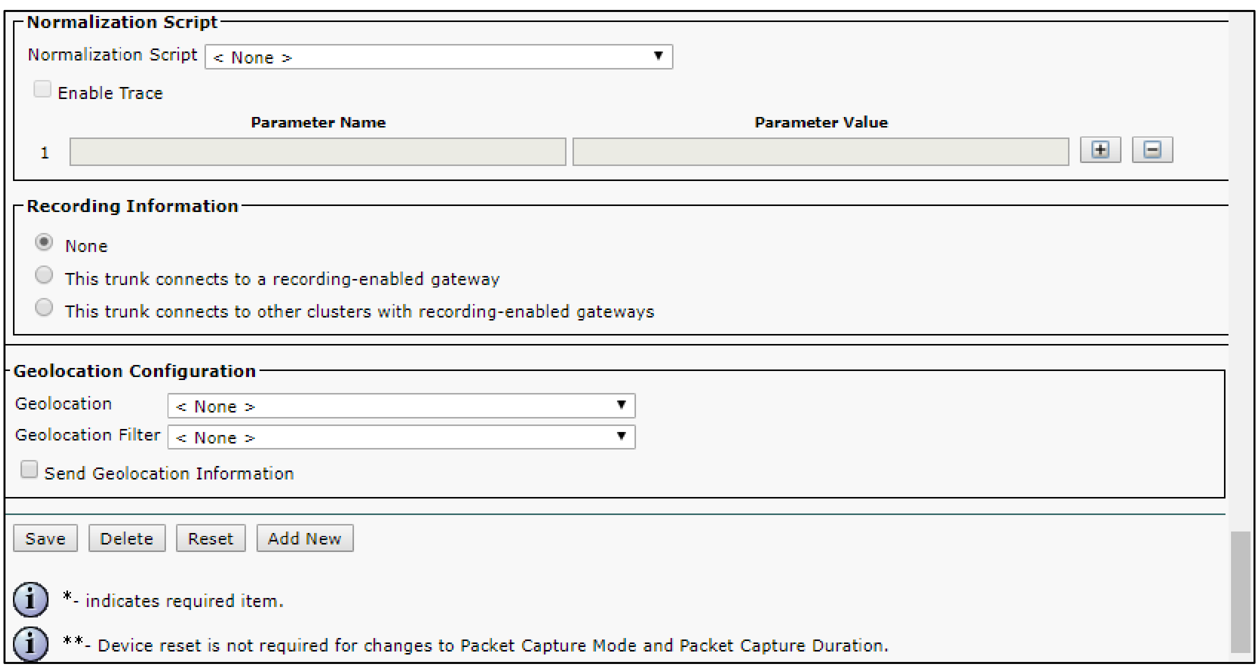


Cisco UCM SIP Trunk to CUP Configuration (Continued)



Cisco UCM SIP Trunk to CUP Configuration (Continued)





End user configuration

Add user to Cisco UCM

Navigation: User Management→ End user

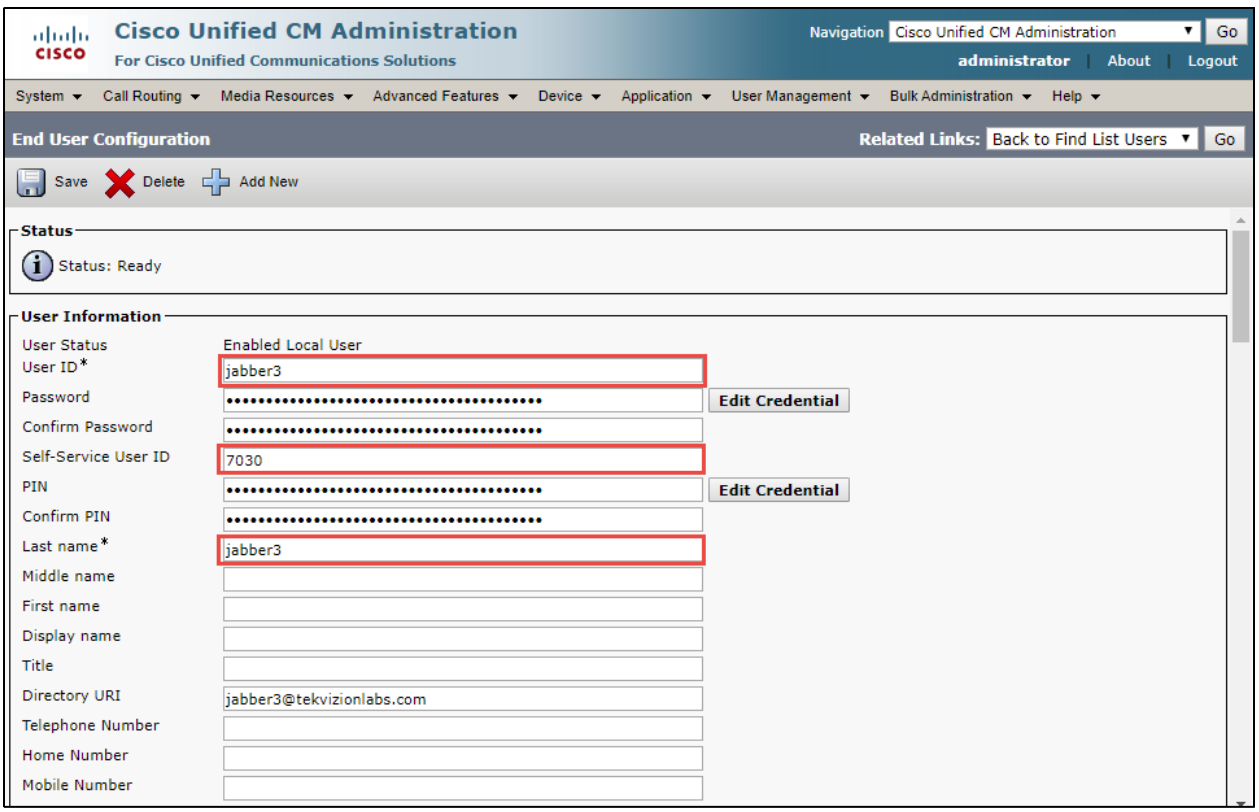
Set **User ID*= jabber3**. This is used for the test.

Set **Last Name = jabber3**. This is used for the test.

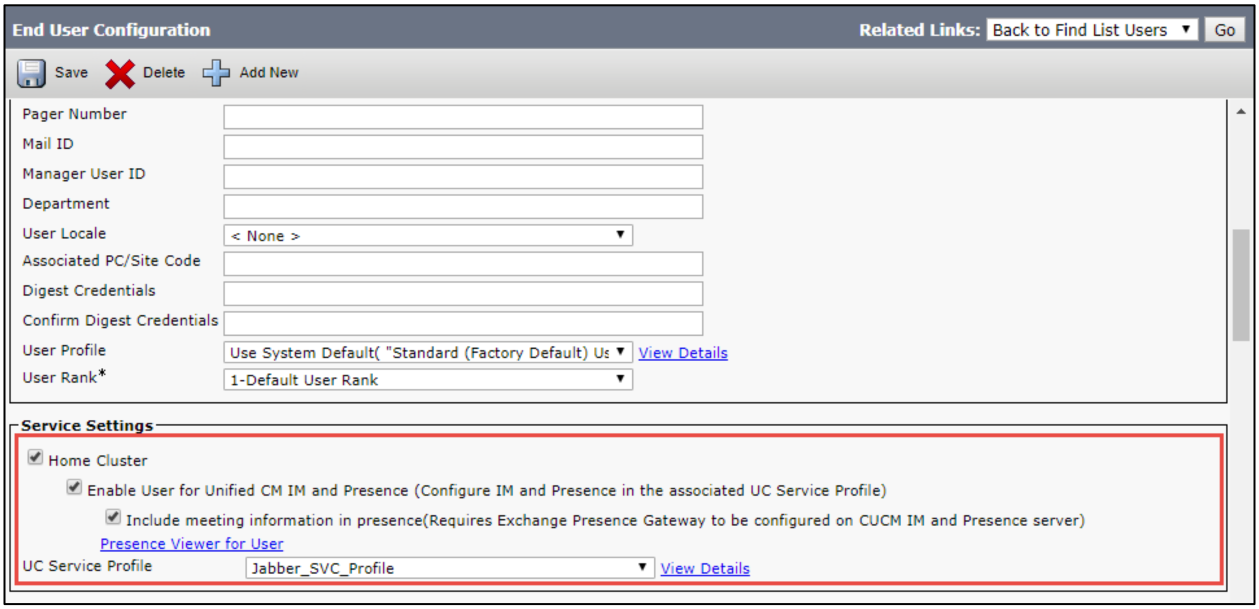
Check Home Cluster.

Click the Device Association

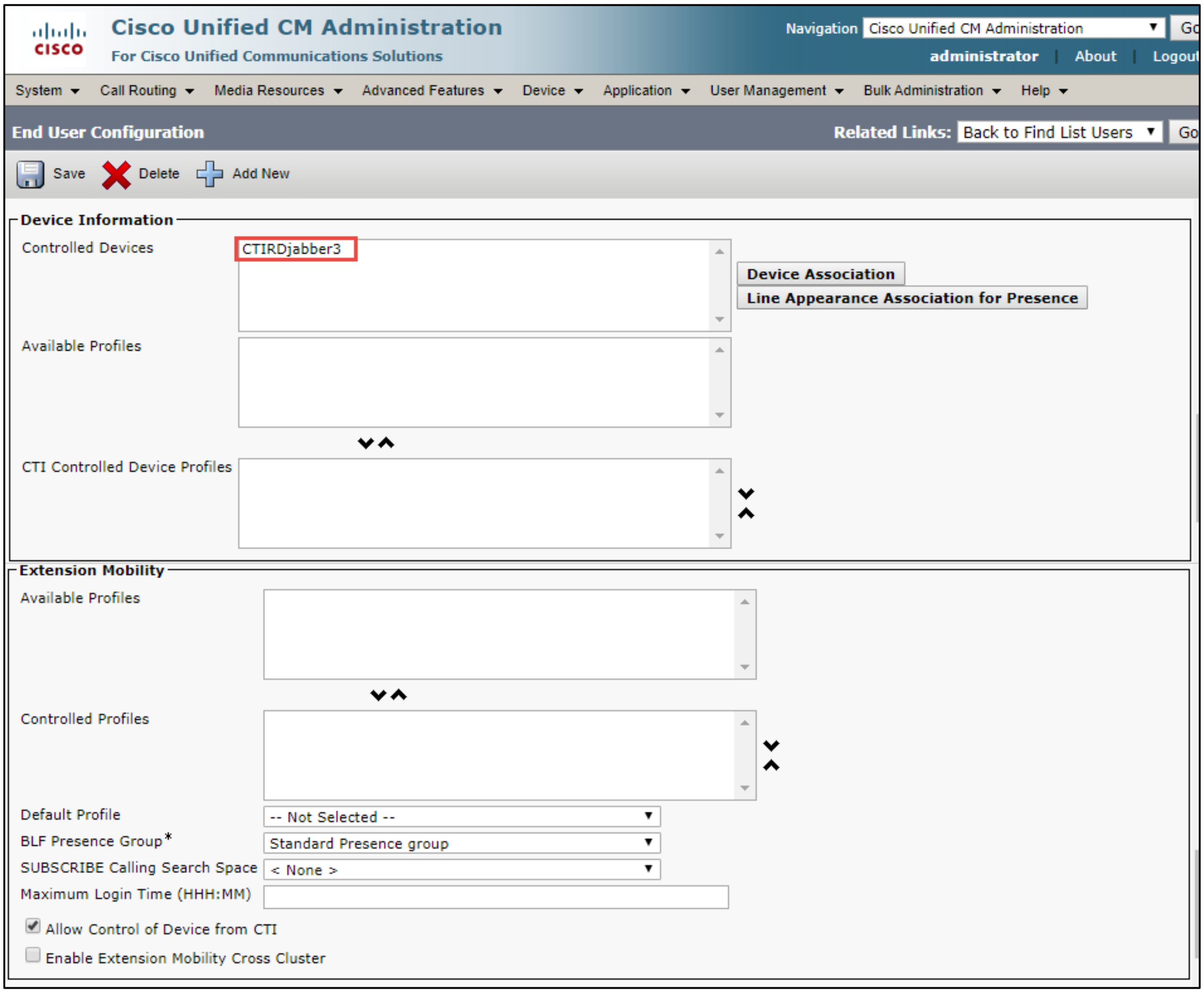
Select CTI1 from User Device Association screen



Cisco UCM end user Configuration (Continued)



Cisco UCM end user Configuration (Continued)



Cisco UCM end user Configuration (Continued)

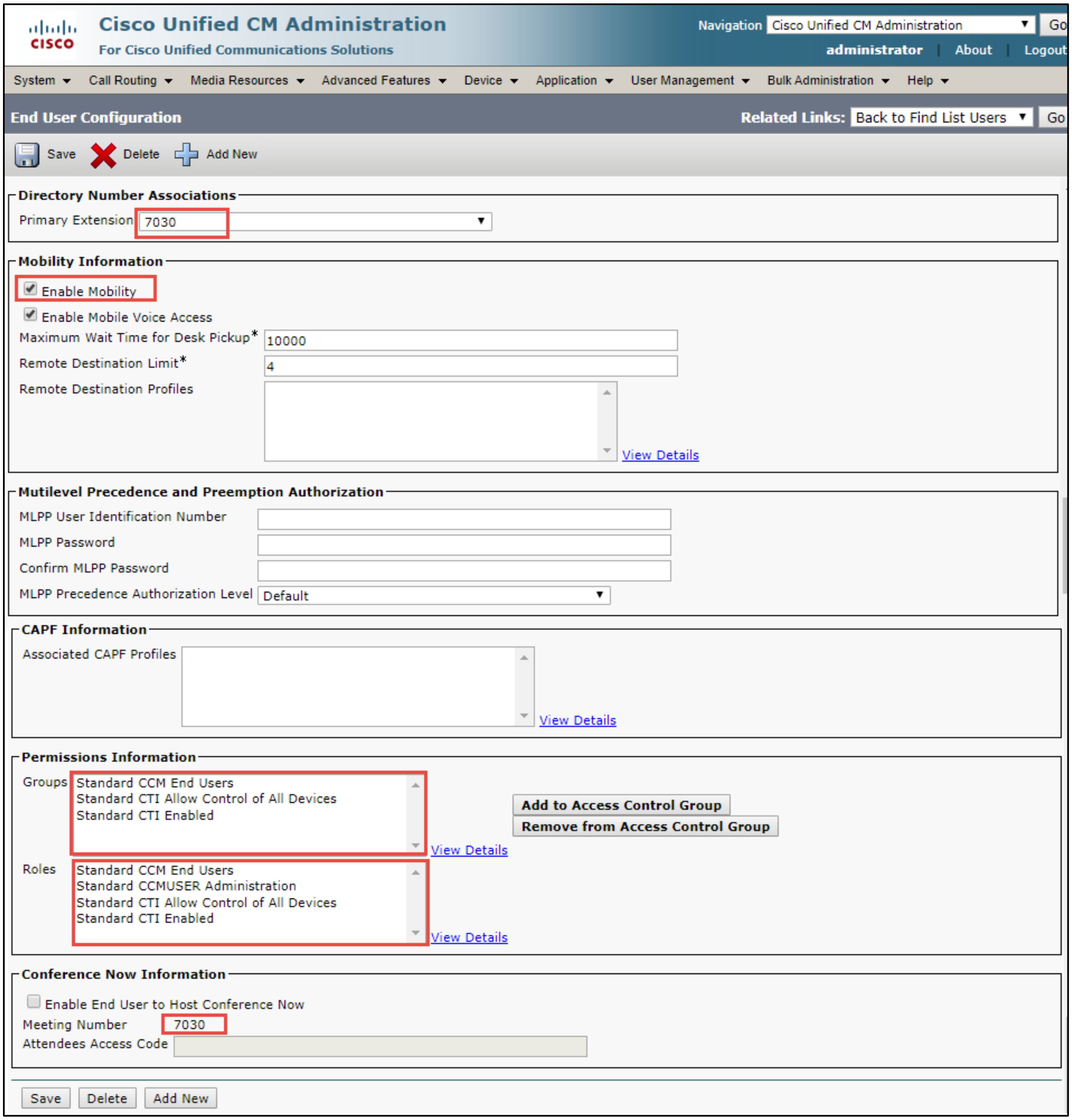
Check Allow Control of Device from CTI
Select the Primary Extension for this user.7030 is used for this example.
Check Enable Mobility.
Add the following permissions for Standard Users:

–Standard CCM End-Users

–Standard CTI Enabled

–Standard CTI Allow Control of All Devices

–Standard CCMUSER Administration



Remote Destination Configuration

Navigation: Device→Remote Destination

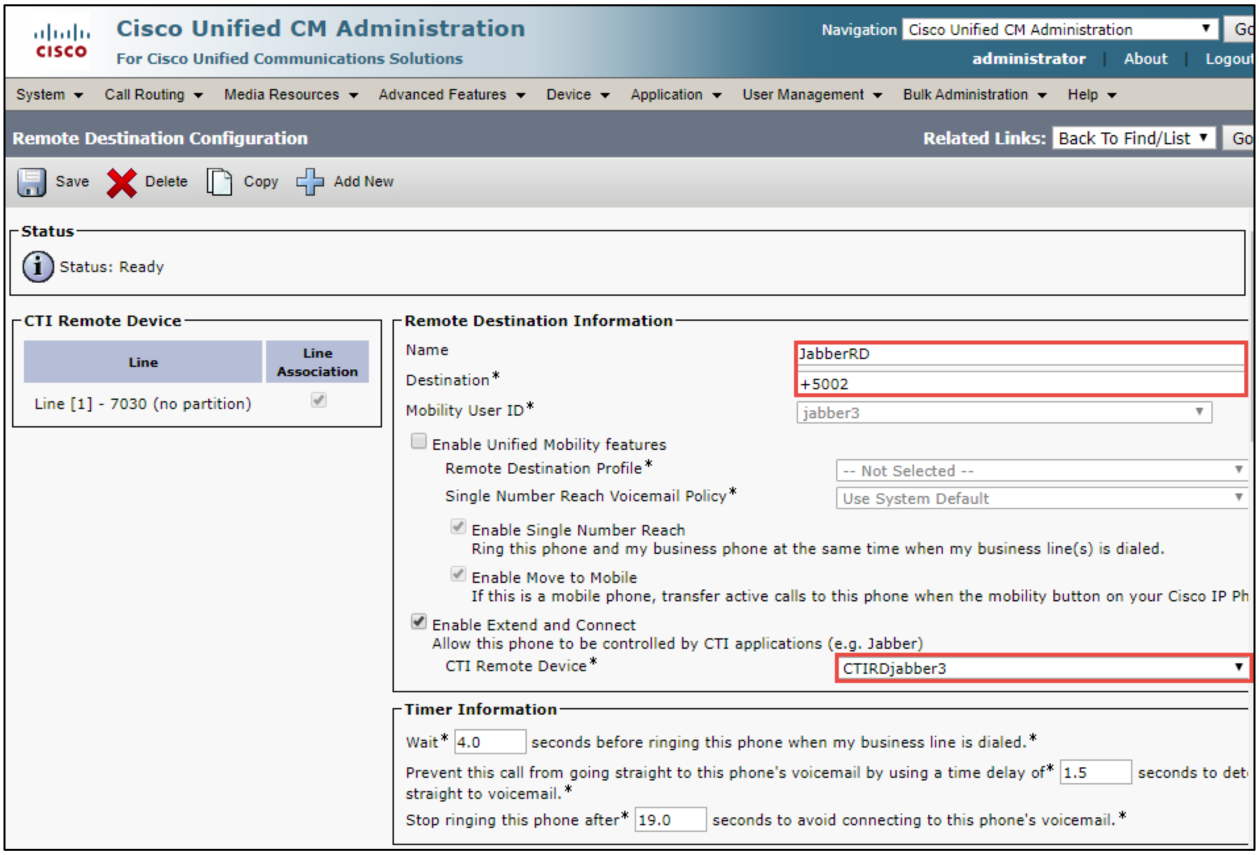
Add New

Set **name = Jabber RD** .This is used for the test

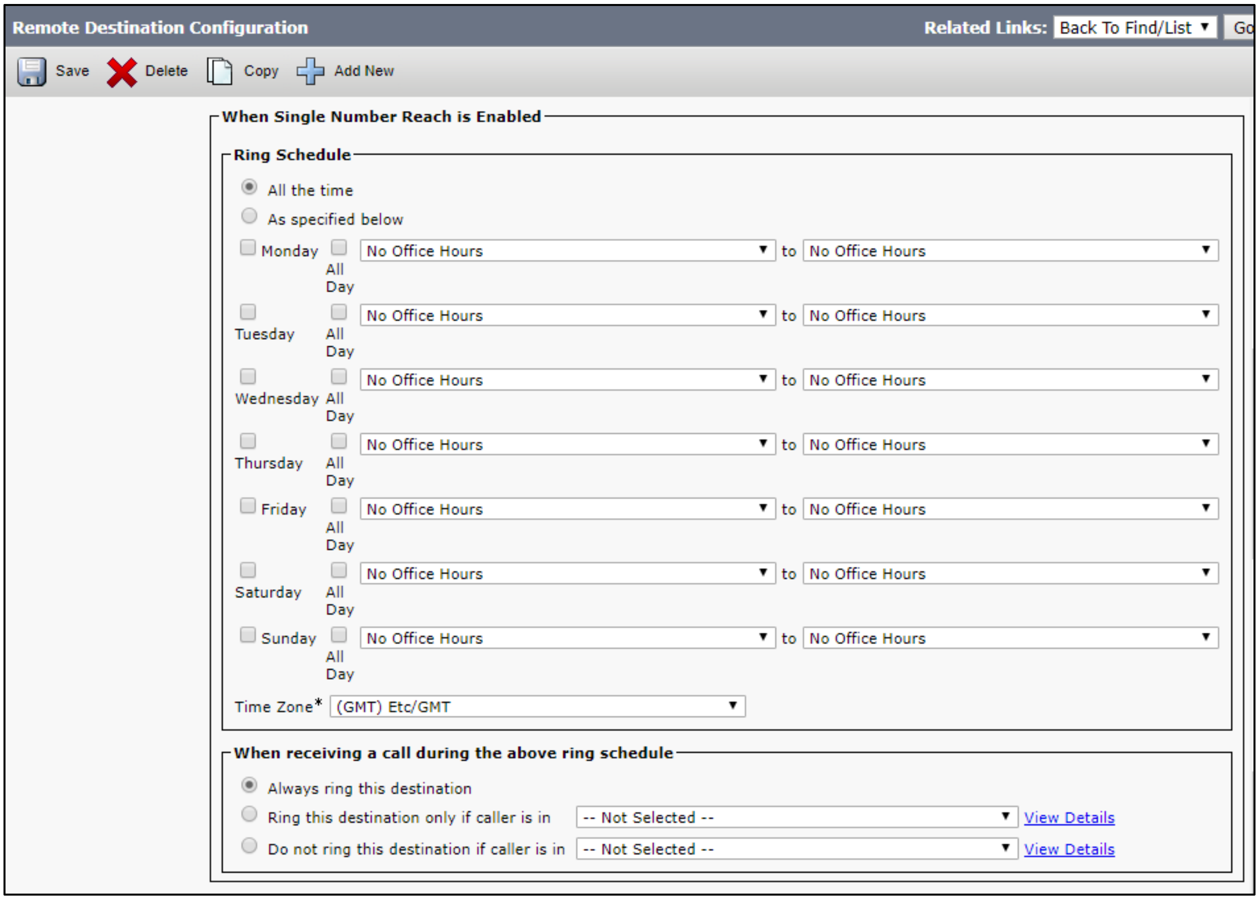
Set **Destination Number*= +5002**. This is used for the test. [7030 is a Skype for Business extension]

Check Enable Extend and Connect.

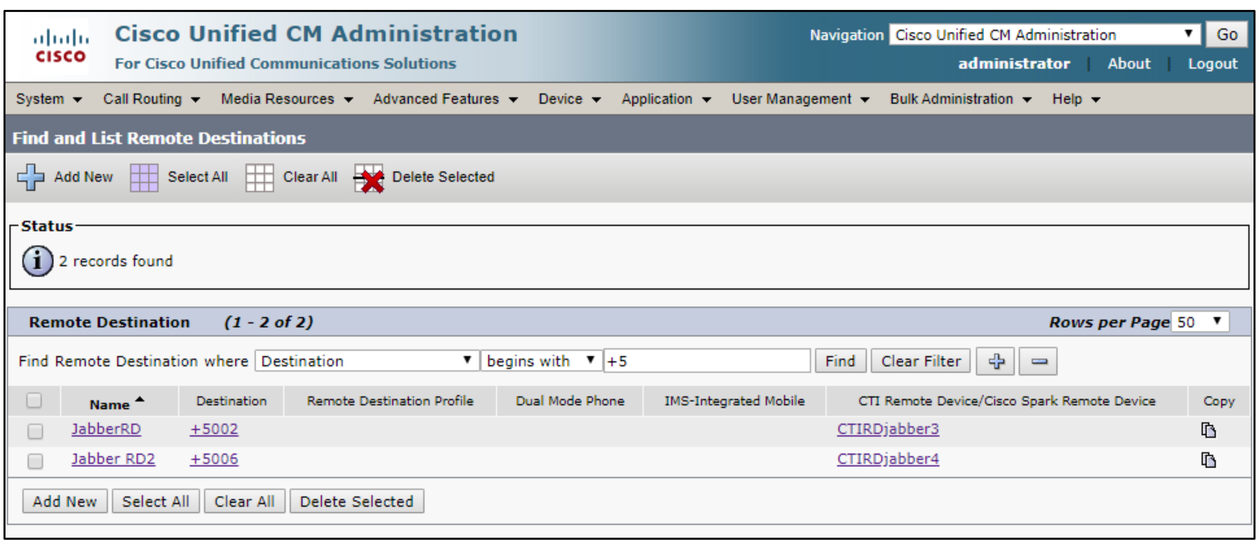
Set **CTI Remote Device = CTIRD1**



The CTI Remote Device configuration is updated with the remote destination:



Two Remote Destinations were configured for this test:



Cisco UCM CTI Remote Device Configuration

Navigation: Device→ Phone

Add New.

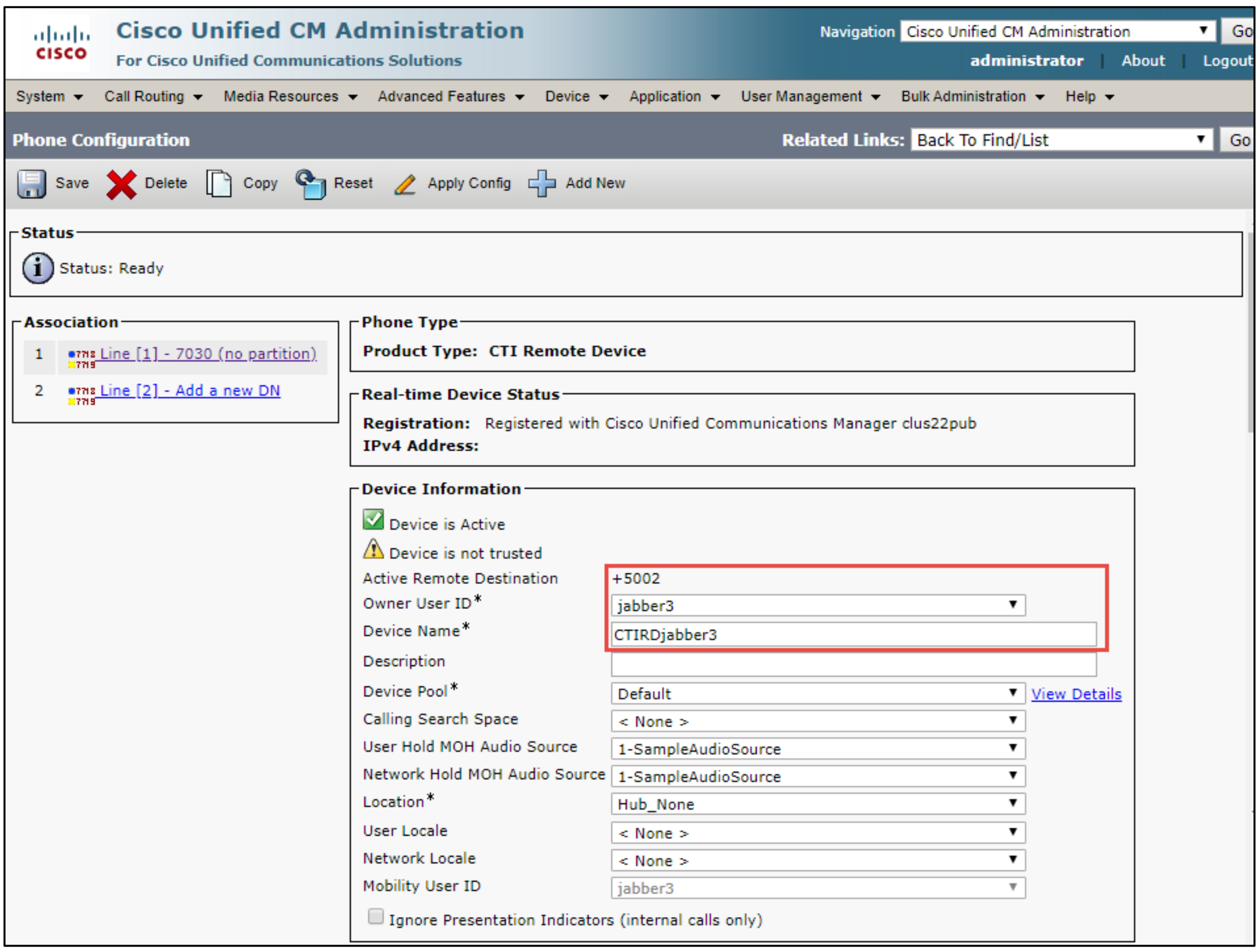
Select **Phone Type * = CTI Remote Device**

The CTI Remote Device type represents the user's remote device(s).

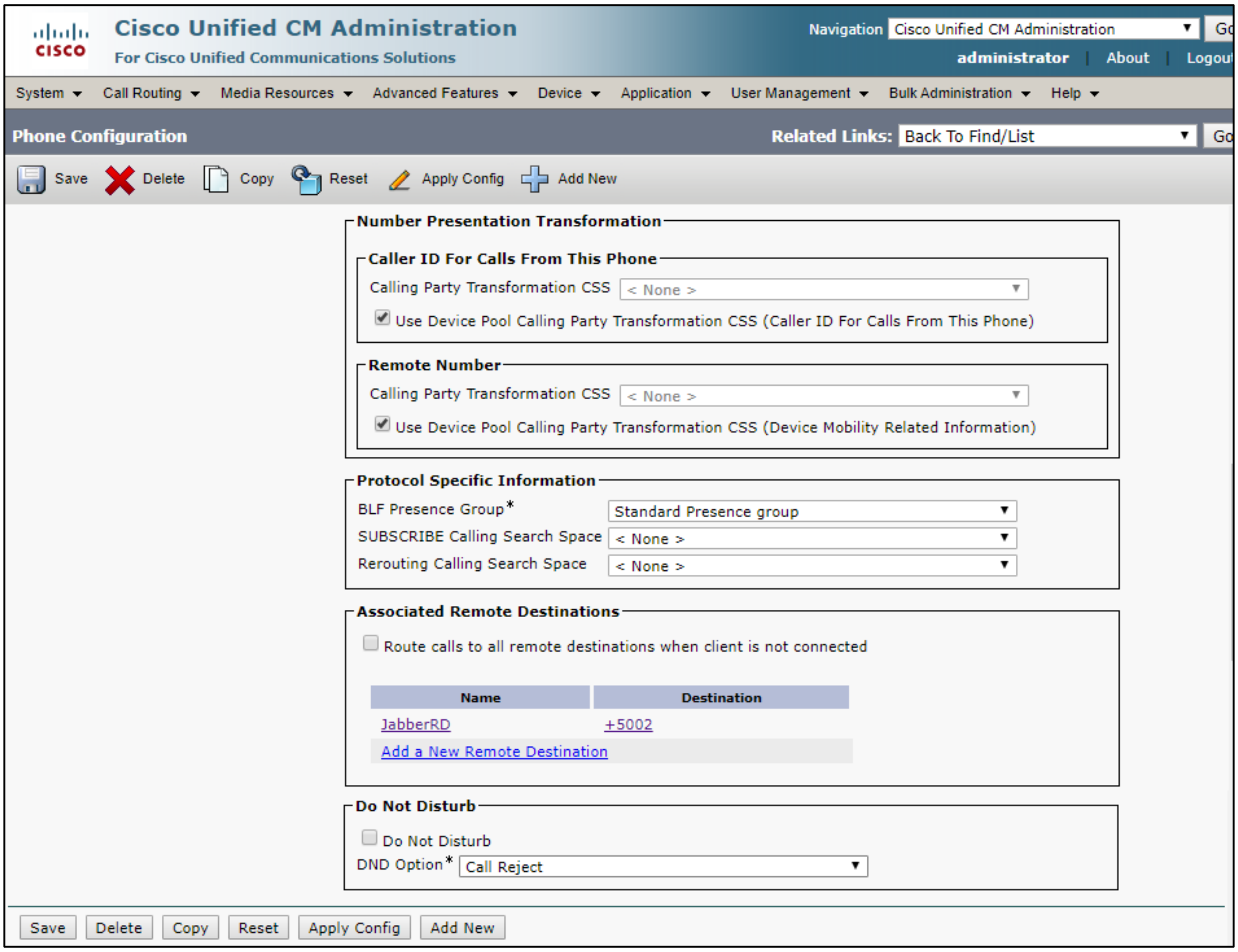
Select the desired Owner User ID. jabber3 is used in this test.

Set Device Pool: Default

Save.



Cisco UCM CTI Remote Device Configuration (Continued)



Add a DN to this device.

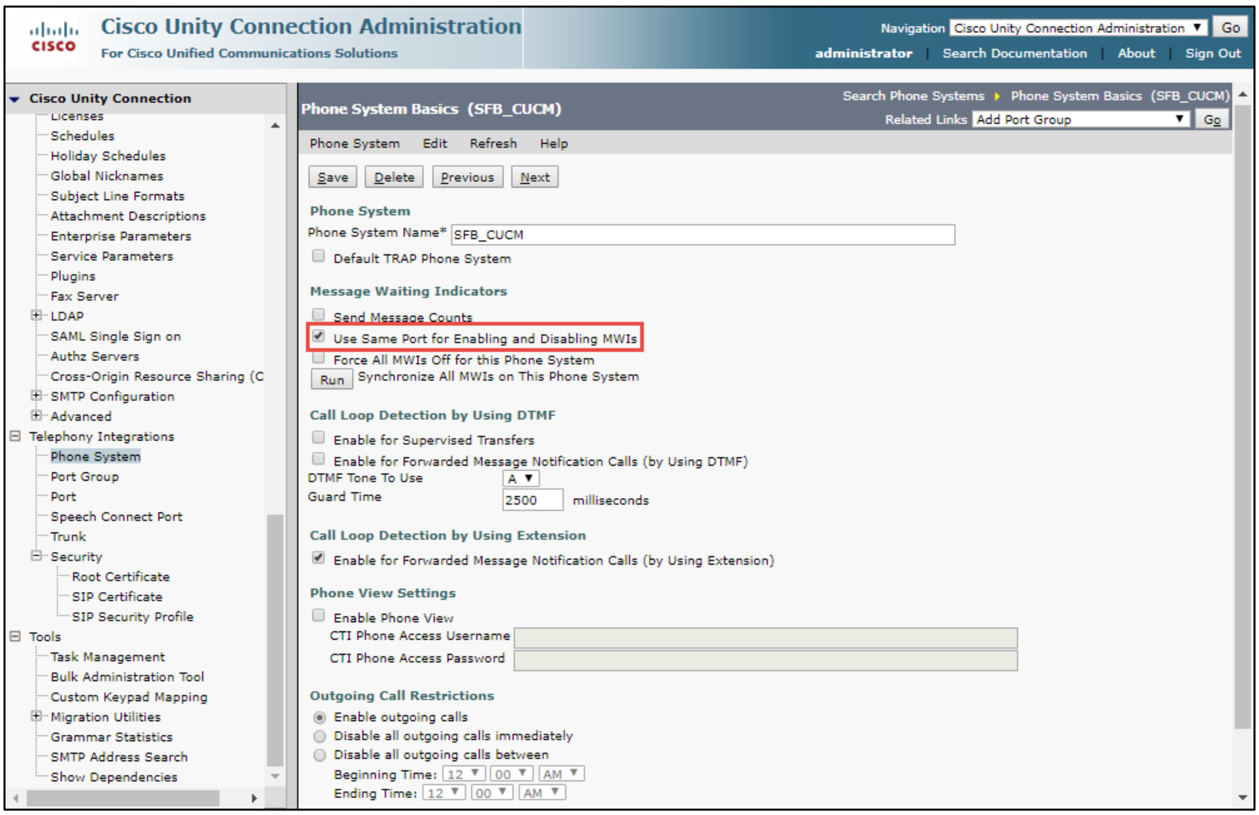
DN +5002 was configured for this test.

Cisco Unity Connection

Telephony Integration – Add Phone System

Navigation: Telephony Integrations → Phone system
Add New
Set Phone **System Name* = SFB_CUCM**. This Name used for this test

Check Use Same Port for Enabling and Disabling MWIs



Telephony Integration – Add Port Group

Navigation: Telephony Integration → Port Group or from previous Screen, Related Links “Add Port Group” Go

Set **Phone System = SFB_CUCM**

Set **Create From – Port group**

Set **Type = SIP**

Set Display Name* = SFB_CUCM-1.This Name used for this example.

Set Ipv4 Address or Host Name = 10.80.12.2 [This is the Cisco UCM publisher IP]

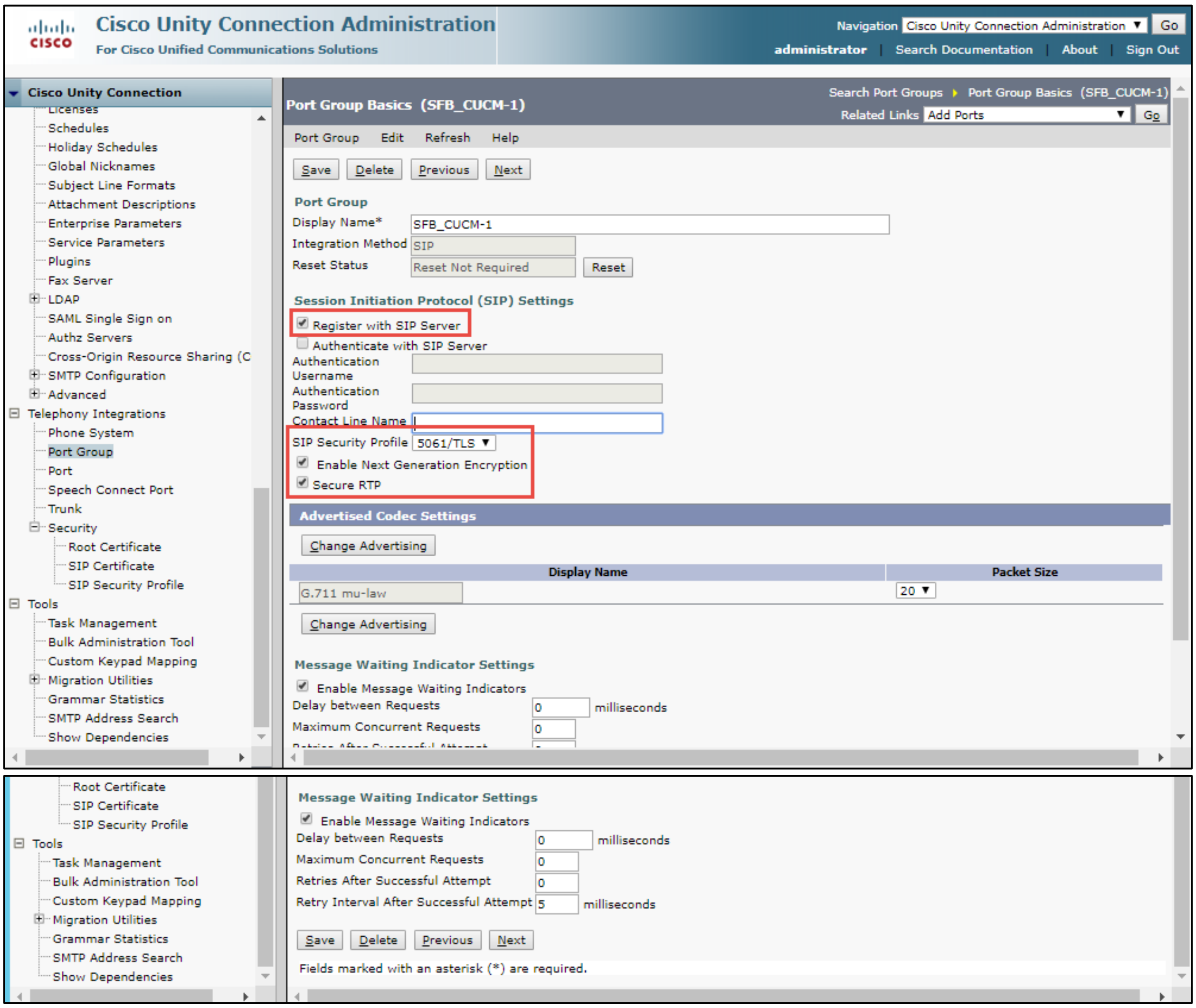
Check Register with SIP server

Set **Security Profile = 5061/TLS**

Set **Security Mode = Encrypted**

Check Secure RTP

Check Enable Message Waiting Indicators



Click Save.

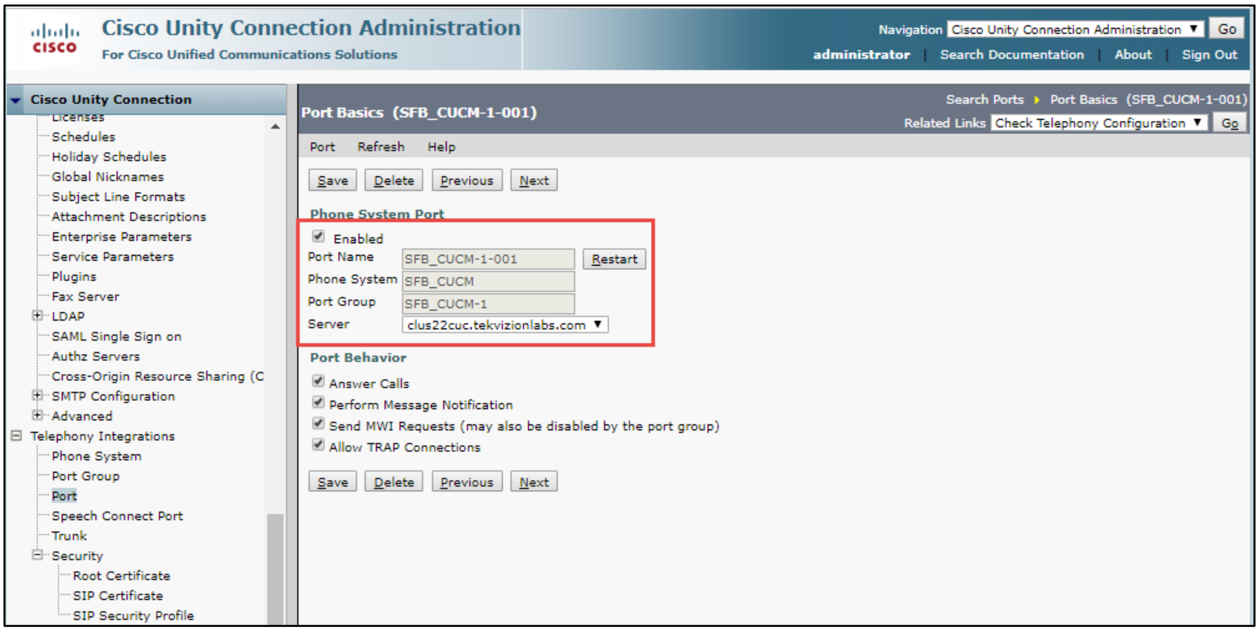
Telephony Integration – Add Ports

Set **Number of Ports = 4**

Set **Phone System = SFB_CUCM-1-001**

Set **Port Group = SFB_CUCM-1**

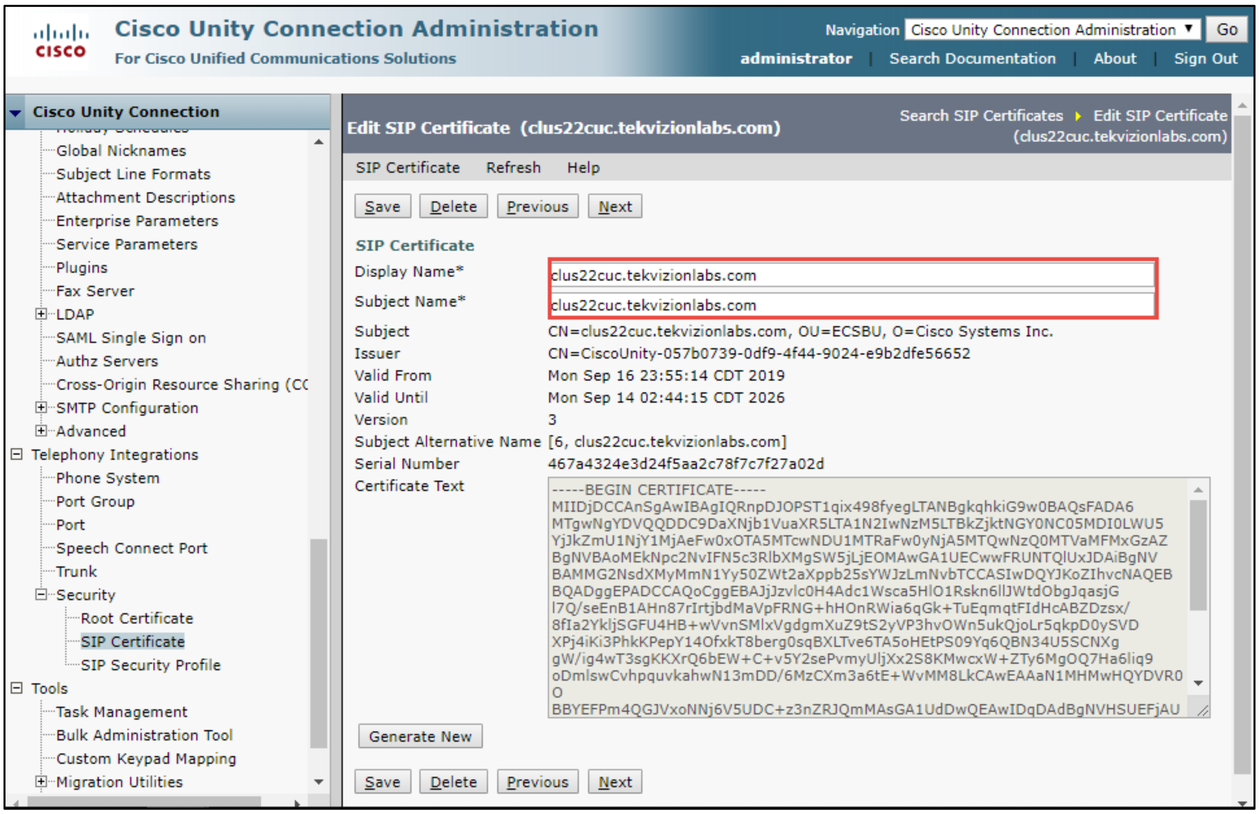
Set **Server = clus22cuc.lab.tekvizion.com** (which is the FQDN of Cisco Unity Server)



SIP Certificate

Navigation: Telephony Integrations → Security → SIP Certificate
Add New
Set **Display Name* = clus22cuc.tekvizionlabs.com**. This Name used for this test

Set **Subject Name* = clus22cuc.tekvizionlabs.com**. Subject Name must match the X.509 Subject Name in SIP trunk security profile in Cisco UCM



User Configuration

Navigation: Cisco Unity Connection → Users → Users

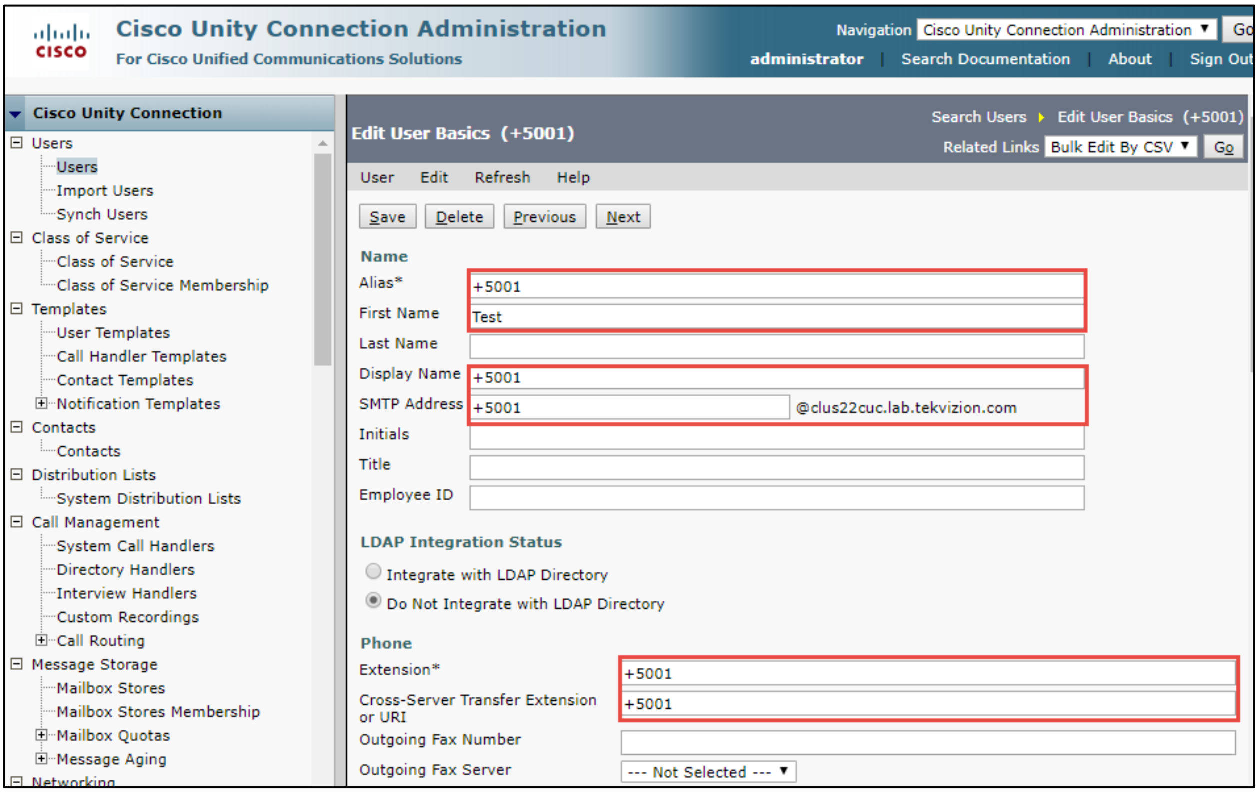
Set **Alias*= +5001** (This is used for the test)

Set **First Name = Test** (This is used to identify the User)

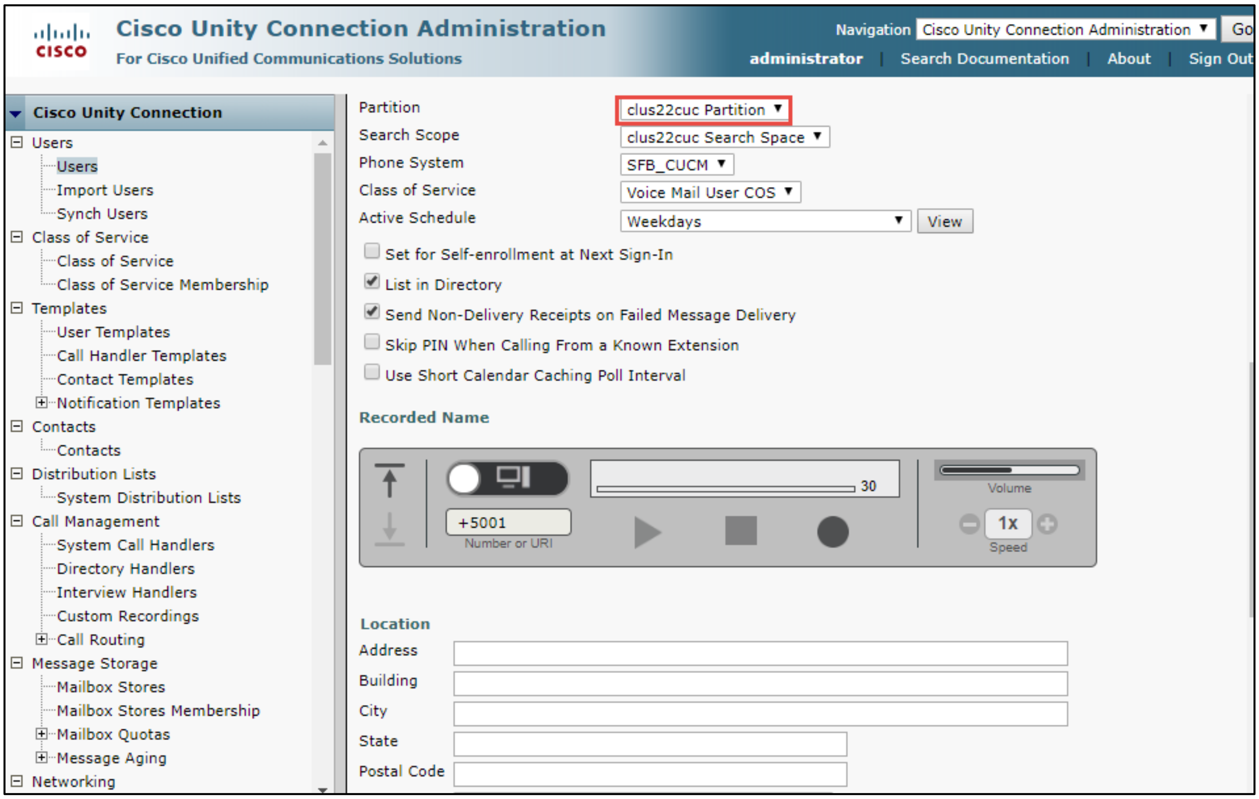
Set **Extension* = +5001** (This is user's extension number)

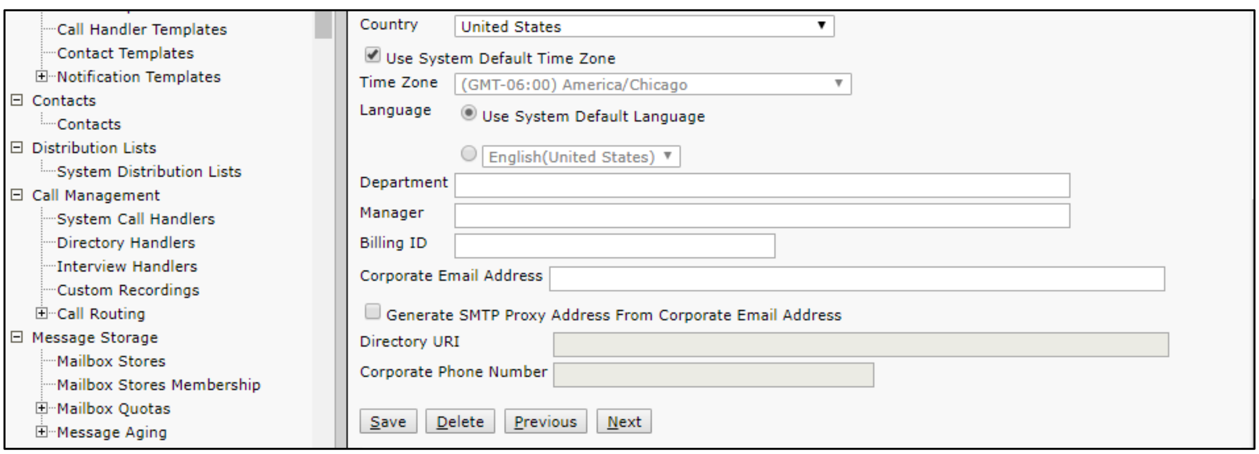
Set **Partition = clus22cucpartition**

Set **Phone System = SFB_CUCM**



Cisco Unity Connection User Configuration (Continued)





Acronyms

Acronym	Definition
CCNR	Call Completion on No Reply
CFB	Call Forwarding on Busy
CFNA	Call Forwarding No Answer
CFU	Call Forwarding Unconditional
Cisco UCM	Cisco Unified Communications Manager
CLIP	Calling Line (Number) Identification Presentation
CLIR	Calling Line (Number) Identification Restriction
CNIP	Calling Name Identification Presentation
CNIR	Calling Name Identification Restriction
COLP	Connected Line (Number) Identification Presentation
COLR	Connected Line (Number) Identification Restriction
CONP	Connected Name Identification Presentation
CONR	Connected Name Identification Restriction
CT	Call Transfer
CUP	Cisco Unified Presence
DNS	Domain Name Server
EXT	Extension
FQDN	Fully Qualified Domain Name
MRGL	Media Resource Group List
MTP	Media Termination Point
MWI	Message Waiting Indicator
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SCCP	Skinny Client Control Protocol
SFB	Skype for Business
SIP	Session Initiated Protocol
UDP	Uniform Dial Plan
VM	Voice Mail