Crestron Mercury® Tabletop Conference System (CCS-UC-1 & CCS-UC-1-X)

Non Secure SIP Endpoint with Cisco® 12.5 Unified Communication Manager (CUCM)

Configuration Guide

Prepared by tekVizion for Crestron Electronics, Inc.

Original Instructions

The U.S. English version of this document is the original instructions.
All other languages are a translation of the original instructions.

Crestron Electronics, Inc.

15 Volvo Drive, Rockleigh, NJ 07647

Tel: 888.CRESTRON

www.crestron.com

tekVizion

3701 W. Plano Parkway

Suite 300, Plano, TX 75075

Tel: + 1 214-242-5900

Contents

Revision History

Revision	Date	Author	Description
1.0	September 29, 2021	tekVizion	Initial Release

Introduction

This configuration guide describes the necessary procedure to configure a Crestron Mercury® device to register to the Cisco® Unify Communication Manager (CUCM) as a Non Secure SIP Endpoint.

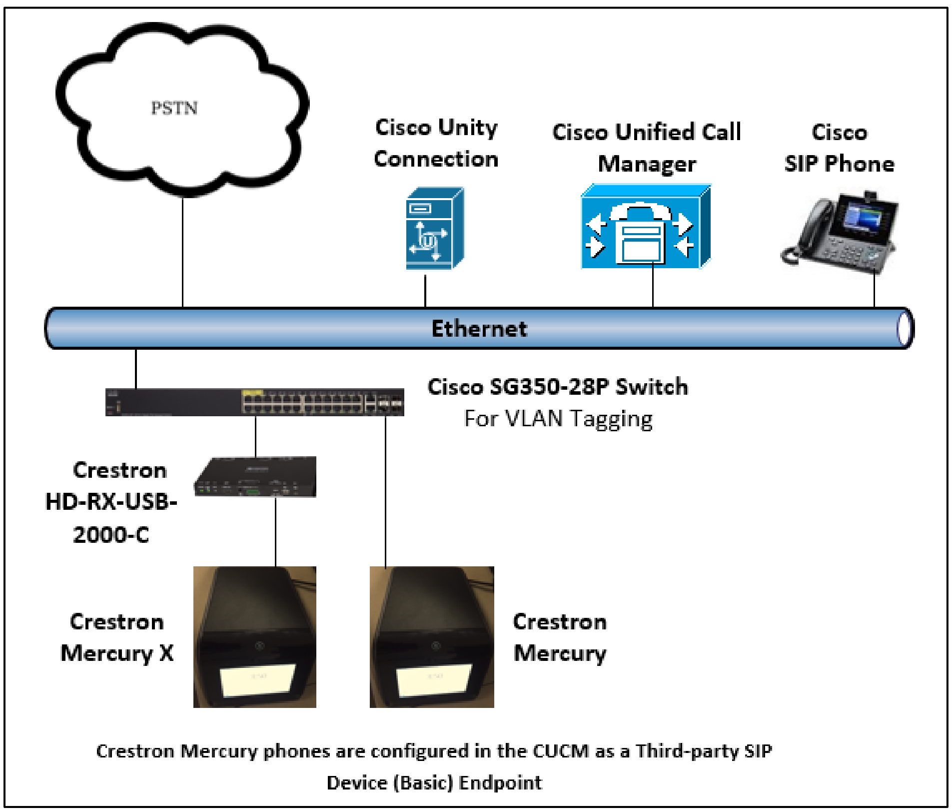
Audience

This document is intended for users attempting to configure and use Crestron Mercury as Secure SIP Endpoints registering to Cisco CUCM 12.5.

Topology

The network topology for the Crestron Mercury Endpoint to operate with Cisco CUCM is shown below.

Crestron Mercury: SIP Endpoint Integration with CUCM: Reference Network



The lab network consists of the following components:

- Cisco Unified Communications Manager (Cisco CUCM) cluster for voice features
- Cisco Unity Connection as the voice mail system
- Cisco SIP phones
- Cisco SG350-28P Switch (For VLAN Tagging Configuration)
- Crestron Mercury and Crestron Mercury X as the SIP Endpoints
- Crestron HD-RX-USB-2000-C – used when connecting to the AUX Port on the Crestron Mercury X

Software Requirements

- Cisco Unified Communication Manager v 12.5.1.12900-115
- Cisco Unity Connection v 12.5.1.12900-56
- Cisco SG350-28P v 2.4.5.71
- Crestron Mercury devices v 1.4736.00054
- Cisco SIP Phone v sip9971.9-4-2SR4-1

Hardware Requirements

- Cisco UCS-C240-M3S VMWare Host running ESXi 5.5
- Cisco 3845 as PSTN Gateway
- Cisco SG350-28P (For VLAN Tagging Configuration)
- Cisco Phone : models - 9971 (SIP)
- Crestron Mercury CCS-US-1
- Crestron Mercury X CCS-US-1-EXT
- Crestron HD-RX-USB-2000-C – Needed when using the AUX Port on the Crestron Mercury X and also provides connections for front of the room displays

Product Description

The Crestron Mercury device is a complete solution for conference rooms. It acts as an all-in-one touch screen, speakerphone and AirMedia® wireless presentation product for conference rooms.

Call dialing options on this device include Bluetooth® connectivity, USB and regular audio using a dial pad, though each dialing option is exclusive.

This device can be discovered via Crestron Toolbox™ software, though most of the configuration is performed via a local web interface. An Ethernet port on the device is used to provide power and network connectivity to make audio calls via SIP.

Summary

The Crestron Mercury devices were configured on the Cisco CUCM as a Basic, Third-party SIP Device, endpoints since they support only a single line/extension. The devices successfully registered to the Cisco CUCM with digest authentication.

The Crestron Mercury CCS-UC-1 & CCS-UC-1-X phones in Non Secure mode are configured on the Cisco CUCM as a Basic, Third-party SIP Device, endpoints since they support only a single line/extension. The devices successfully registered to the Cisco CUCM with digest authentication.

The sections below describe the features that are supported/not supported and known issues/limitations on the Crestron Mercury phone.

Features Supported

- VLAN Tagging
- Registration with Digest Authentication
- Basic Calls with G722, G729, G711u and G711a codecs
- DTMF Out-Of-Band and In-Band DTMF support
- Caller ID (limited to only Calling Number)
- Voice Mail access and interaction
- Early Media support
- Retrieval of a Parked Call
- Transferee in a Call Transfer
- Conference Call Participant
- Member of Shared Line configuration
- Member of a Hunt group

Features Not Supported

- Caller ID Name presentation (Only the calling party number is displayed)
- Call Hold and Resume
- Call Forwarding on the device (Though forwarding can be configured on the PBX for the DN assigned to the endpoint)
- Call Waiting
- Initiating a Conference Call
- Initiating Attended Call Transfer
- Initiating Early Attended Call Transfer
- Initiating Blind Call Transfer
- Shared Line (configuration of shared line on Crestron Mercury device)
- Call Park (Initiating call park)
- DND (Do Not Disturb)
- Message Waiting Indicator

Known Issues and Limitations

- None

Crestron Mercury & Crestron Mercury X Configuration

Crestron Mercury - Power

The LAN port of the Crestron Mercury device needs to be connected to one PoE+ port to power it up for network connectivity with the Cisco CUCM. The PoE switch should have LLDP functionality enabled for the device to power up and be completely functional. By default, the **POEPLUS** configuration is set to **OFF** on the device. In the tekVizion™ lab environment, the Crestron Mercury phones are powered by an AC line universal power pack.

Crestron Mercury X - Power

When using the Crestron Mercury X phone, an AC line universal power pack is needed to power the Crestron Mercury X.

AUX Port on Crestron Mercury X

The AUX Port is used on the Crestron Mercury X phone. When using the AUX Port on the Crestron Mercury X phone, the HD-RX-USB-2000-C converter box is needed in line with the Ethernet connection.

Discover/Access the Crestron Mercury

Crestron has a software tool available to discover and access the Crestron Mercury on the network: The Crestron Toolbox.

The Help menu on this tool assists the user through the discovery and configuration procedure.

The Crestron Mercury IP address, Host Name, MAC Address, Serial Number and Firmware Version can be viewed in the System info screen from the Home Screen by pressing and holding the Info link in the bottom left hand corner of the Crestron Mercury phone screen for 10 seconds.

Crestron Mercury: System Info Screen

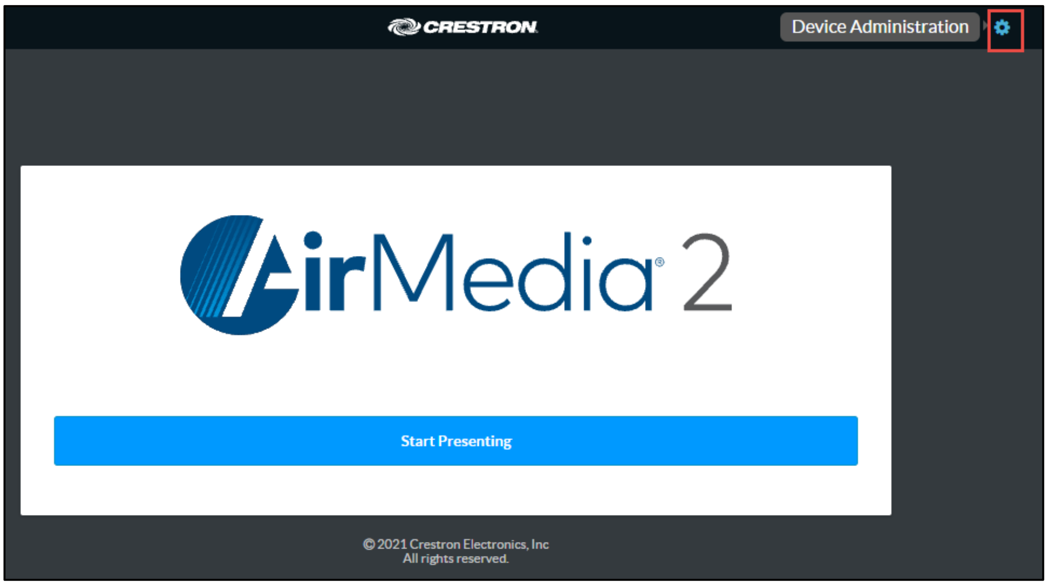
Crestron Mercury Web UI Sign In

Access the Crestron Mercury Web UI for the device by using an http session with the device's IP address.

The initial page that displays is shown below.

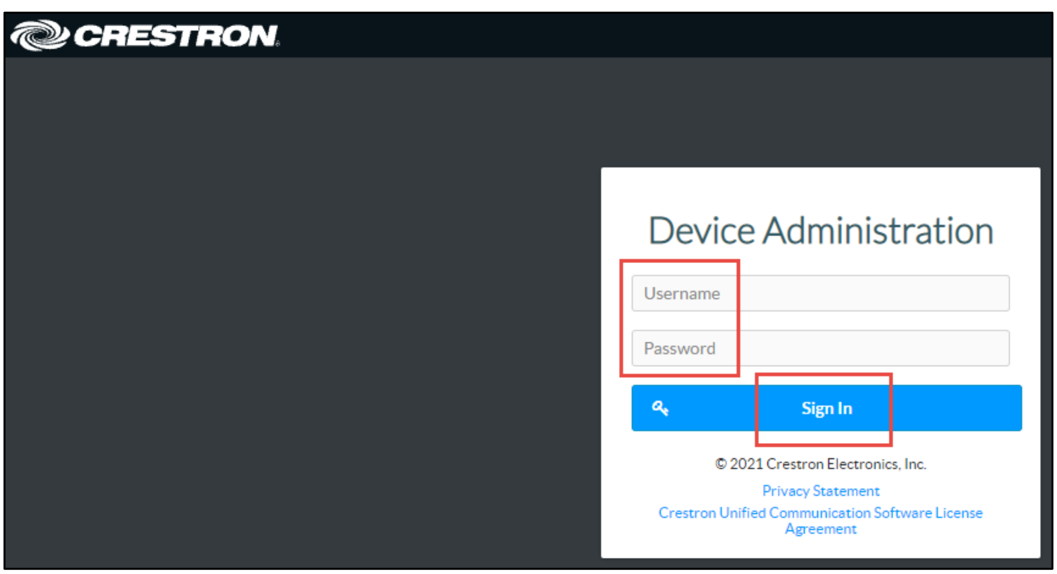
- Select the **Device Administration** link in top right corner.

Crestron Mercury: Device Administration



1. In the pop-up window provide **login credentials.**
2. Default Crestron Mercury Login credentials are **admin/admin**.
3. Click **Sign In.**

Crestron Mercury Web UI: Sign In



Crestron Mercury

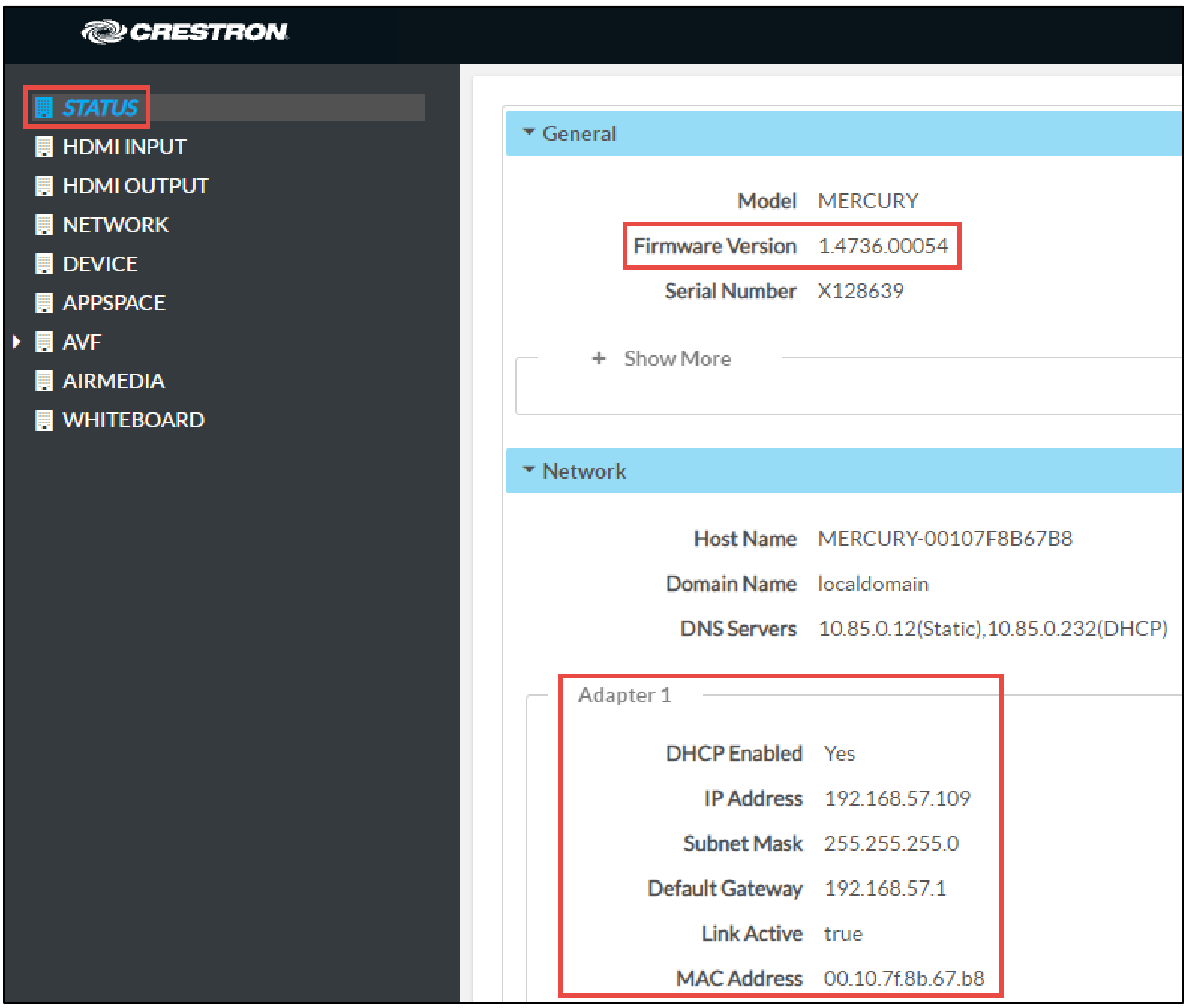
In the tekVizion lab environment, one DUT used as a Crestron Mercury phone with the Ethernet cable connected to the LAN port of the Crestron Mercury. Configuration for this setup is shown below.

Status

The **Status** screen shown below displays basic device information:

- The **Firmware Version** and **Network** info of the Crestron Mercury are shown here.

Crestron Mercury: Status



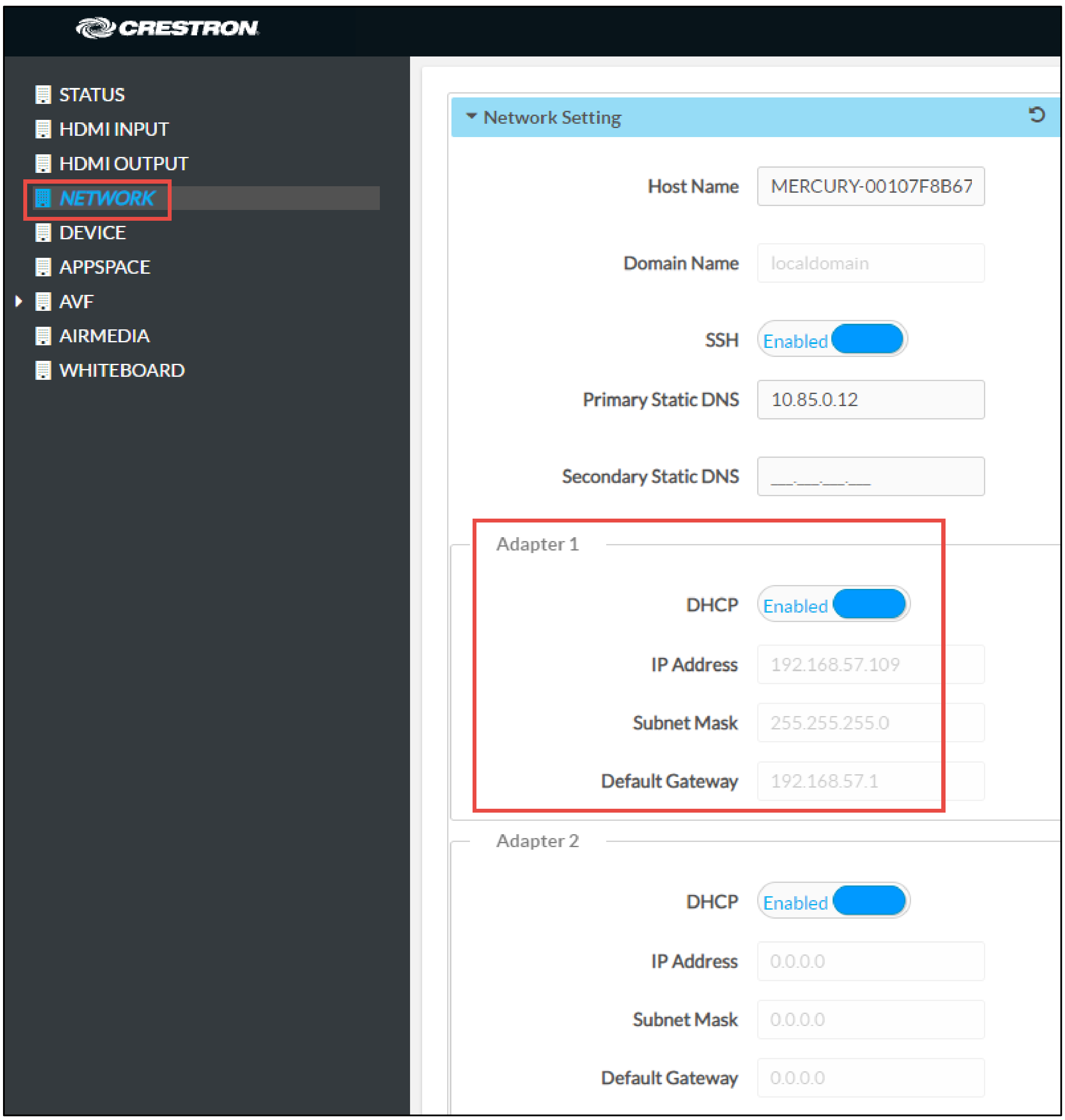
Network Configuration

The Crestron Mercury Network settings can be configured from the Network page.

On the Crestron Mercury Web UI, navigate to **Network.**

1. **DHCP:** The Crestron Mercury is configured as DHCP.
2. The LAN Port is used on the Crestron Mercury, so **Adapter 1** is configured via DHCP.
3. Click **Save Changes.**

Crestron Mercury: Network: DHCP



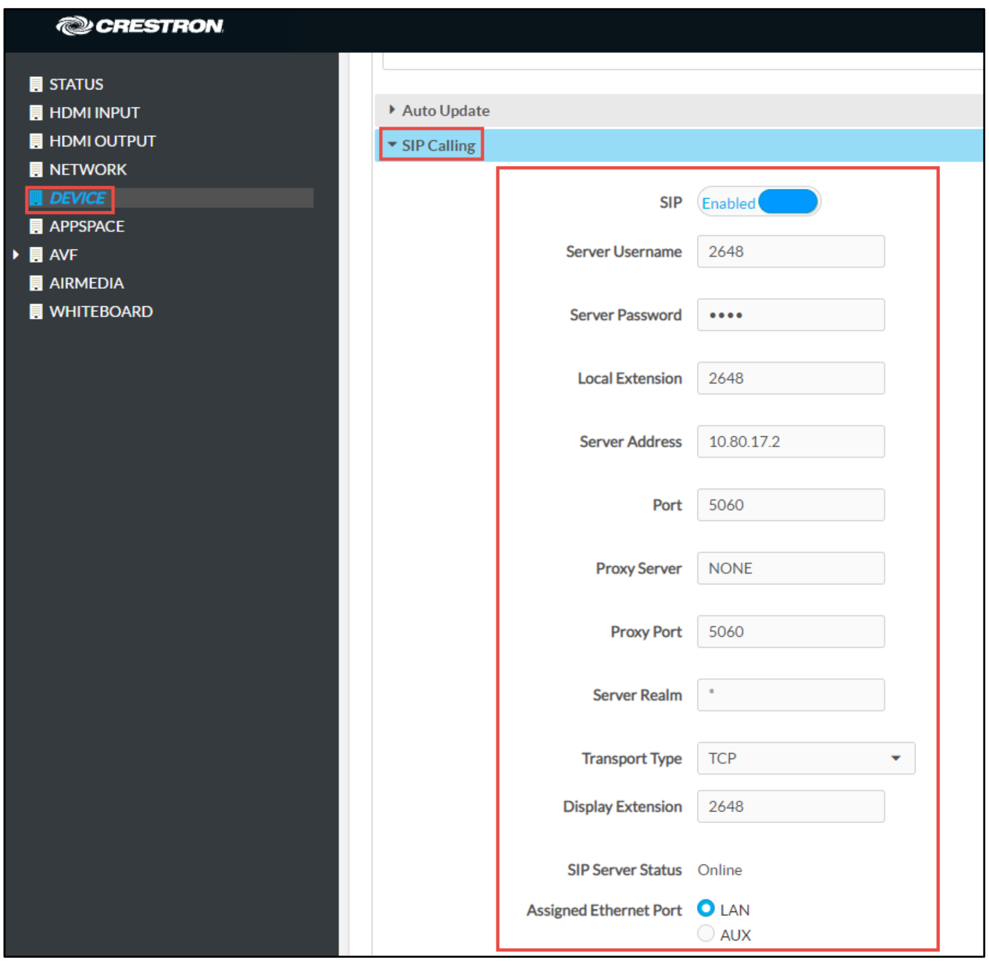
SIP Calling Parameters

Configure the Crestron Mercury SIP Parameters to enable Crestron Mercury communication with the Cisco CUCM.

From the Crestron Mercury Web UI, navigate to **Device → SIP Calling.**

1. **SIP**: click the box to display **Enabled.**
2. **Server Username**: Enter the end user configured on the Cisco CUCM for this device, (**2648**).
3. **Server Password**: User's password as configured on the Cisco CUCM.
4. **Local Extension**: Enter the directory number configured on the Cisco CUCM, (**2648**).
5. **Server Address**: Enter the IP address of the Cisco CUCM, (**10.80.17.2**).
6. **Port**: For the Non Secure TCP setup port **5060** is used.
7. **Transport Type**: For the Non Secure setup, **TCP** Transport is used.
8. **Display Extension**: **2648** is used.
9. **Assigned Ethernet Port** is set to **LAN.**
10. Click **Save Changes.**
11. **SIP Server Status** shows **Online** when successfully registered to the PBX.

Crestron Mercury: Device: SIP Calling



Crestron Mercury X

In the tekVizion lab environment, one DUT is a Crestron Mercury X phone with the Ethernet cable connected to the AUX port y The Crestron HD-RX-USB-2000-C converter box is needed in-line with the Ethernet connection when the AUX port is used. The specific Crestron Mercury X configuration for this setup is shown below, the rest of the configuration is the same as the above Crestron Mercury configuration.

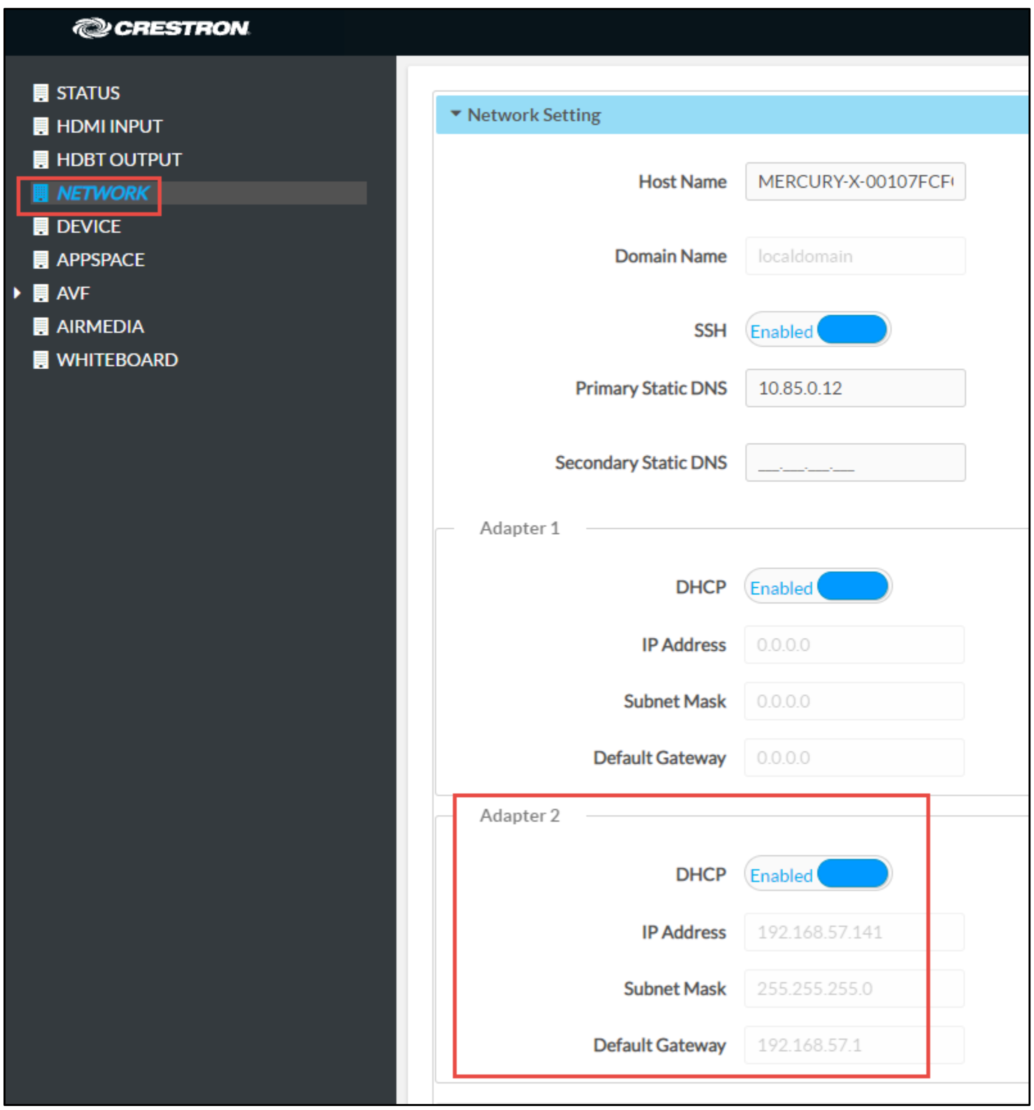
Network Configuration

The Crestron Mercury Network settings can be configured from the Network page.

On the Crestron Mercury Web UI, navigate to **Network.**

1. **DHCP:** The Crestron Mercury is configured as DHCP. The AUX Port is used on the Crestron Mercury X, so **Adapter 2** is configured as **DHCP.**
2. Click **Save Changes.**

Crestron Mercury X: Network



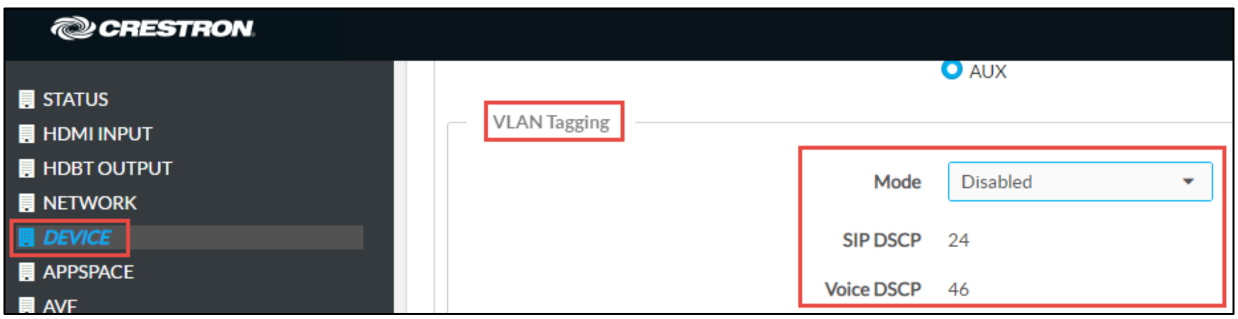
VLAN Tagging

VLAN Tagging on the Crestron Mercury allows you to assign DSCP values to the SIP and Media messages. It also allows you to assign a Priority value to the VLAN used for the SIP and Media messages. When enabled, VLAN Tagging uses a 2nd IP address that is assigned to the Crestron Mercury phone for the SIP and Media messages. The IP address is assigned by a Local Network Cisco switch (Cisco SG350-28P), providing the VLAN Tagging configuration info to the Crestron Mercury.

The available **VLAN Tagging Mode** settings are shown below: From the Crestron Mercury Web UI, navigate to **Device → SIP Calling.**

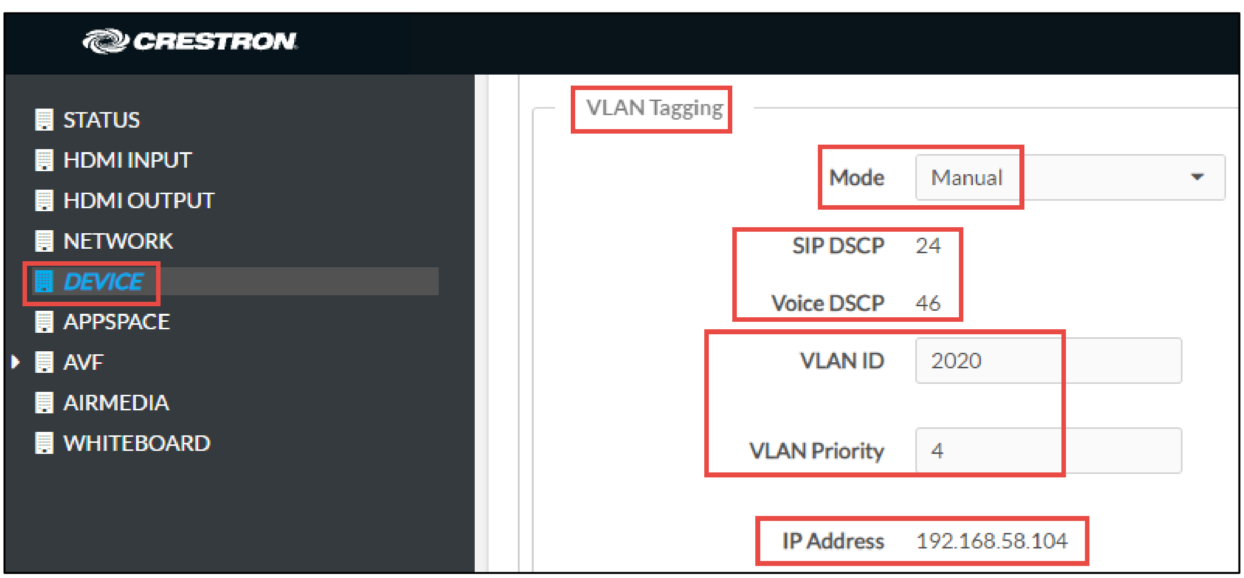
1. **Disabled** – Uses just 1 IP address for the Data IP address SIP and Media. The default DSCP value assigned to SIP is **24** and to Media is **46.** The Priority VLAN value is not assigned to the Messages. The default Crestron Mercury setting is **Disabled**.

Crestron Mercury: Device: SIP Calling: VLAN Tagging - Disabled



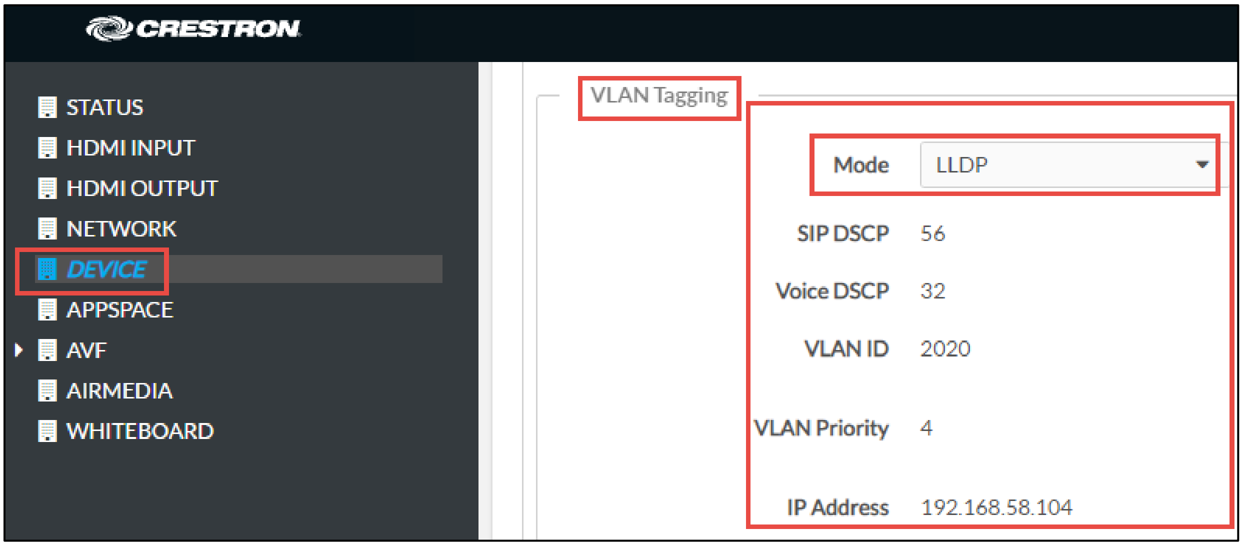
2. **Manual** – Allows you to assign the VLAN ID and VLAN priority to be used by the Crestron Mercury. The default DSCP values (**SIP – 24** and **Voice – 46**) are assigned. The 2nd IP address, used for SIP and Media is assigned to the Crestron Mercury by the local network switch with the VLAN Tagging configuration.

Crestron Mercury: Device: SIP Calling: VLAN Tagging - Manual



3. **LLDP** – Pulls the VLAN Tagging information from the local network switch with the VLAN Tagging configuration.

Crestron Mercury: Device: SIP Calling: VLAN Tagging - LLDP



VLAN Tagging Local Network Switch – Cisco SG350-28P

The tekVizion lab environment used a Cisco SG350-28P switch to provide the 2nd IP address used for SIP & Media, and the VLAN Tagging configuration for the Crestron Mercury and Crestron Mercury X phone when **LLDP** is set as the **Mode** for the Crestron Mercury.

The Crestron Mercury phones are connected directly to the Cisco SG350-28P switch in the lab setup.

The Running Configuration for the VLAN Tagging switch is provided below. The following configuration settings are used in the tekVizion lab VLAN Tagging environment.

1. **Voice Vlan ID 2020**
2. **LLDP Med Network-Policy**
   - 3 voice-signaling vlan 2020 vlan-type tagged up 4
   - 4 voice vlan 2020 vlan-type tagged up 4 dscp 32
   - 9 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 32
   - 10 voice vlan 2020 vlan-type tagged up 4 dscp 32
   - 15 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 56
   - 16 voice vlan 2020 vlan-type tagged up 4 dscp 32
3. **Interface Port 4 - Crestron Mercury phone**
   - interface GigabitEthernet4
   - description Crestron Mercury2
   - switchport mode trunk
   - lldp med network-policy add 15
   - lldp med network-policy add 16
4. **Interface Port 7 - Crestron Mercury phone**
   - interface GigabitEthernet7
   - description Crestron Mercury 5
   - switchport mode trunk
   - lldp med network-policy add 15
   - lldp med network-policy add 16

Cisco SG350_28P – Running Configuration

switch94214e#show run

config-file-header

switch94214e

v2.4.5.71 / RTESLA2.4.5_930_181_144

CLI v1.0

file SSD indicator encrypted

@

ssd-control-start

ssd config

ssd file passphrase control unrestricted

no ssd file integrity control

ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0

!

!

unit-type-control-start

unit-type unit 1 network gi uplink none

unit-type-control-end

!

vlan database

vlan 2,10-11,15,200,2018-2020,4030

exit

voice vlan id 2020

voice vlan oui-table add 0001e3 Siemens_AG_phone________

voice vlan oui-table add 00036b Cisco_phone_____________

voice vlan oui-table add 00096e Avaya___________________

voice vlan oui-table add 000fe2 H3C_Aolynk______________

voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone

voice vlan oui-table add 00d01e Pingtel_phone___________

voice vlan oui-table add 00e075 Polycom/Veritel_phone___

voice vlan oui-table add 00e0bb 3Com_phone______________

no lldp med network-policy voice auto

lldp med network-policy 3 voice-signaling vlan 2020 vlan-type tagged up 4

lldp med network-policy 4 voice vlan 2020 vlan-type tagged up 4 dscp 32

```
lldp med network-policy 9 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 32
lldp med network-policy 10 voice vlan 2020 vlan-type tagged up 4 dscp 32

lldp med network-policy 15 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 56
lldp med network-policy 16 voice vlan 2020 vlan-type tagged up 4 dscp 32

link-flap prevention disable
bonjour interface range vlan 1
hostname switch94214e
no passwords complexity enable
ip ssh server
ip telnet server
!
interface vlan 2
 name Data
!
interface vlan 15
 name "RSPAN VLAN"
 remote-span
!
interface GigabitEthernet1
 description PoE1
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_1 | no_ip_phone_desktop                                  |
ip_phone_desktop"
 no macro auto smartport
 macro auto smartport type ip_phone_desktop
!
```

```
interface GigabitEthernet2
 description PoE2
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_2 | no_ip_phone_desktop                    |
ip_phone_desktop"
 macro auto smartport type ip_phone_desktop
!
interface GigabitEthernet3
 description Crestron Mercury1
 switchport mode trunk
 lldp med network-policy add 15
 lldp med network-policy add 16
!
interface GigabitEthernet4
 description Crestron Mercury2
 switchport mode trunk
 lldp med network-policy add 15
 lldp med network-policy add 16
!
interface GigabitEthernet5
 shutdown
 description Crestron Mercury3
 switchport mode trunk
!
interface GigabitEthernet6
 description Crestron Mercury4
 switchport mode trunk
 lldp med network-policy add 3
```

```
 lldp med network-policy add 4
!
interface GigabitEthernet7
 description Crestron Mercury5
 switchport mode trunk
 lldp med network-policy add 15
 lldp med network-policy add 16
!
interface GigabitEthernet13
 description PoE3
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_3 | no_ip_phone_desktop                    |
ip_phone_desktop"
 macro auto smartport type ip_phone_desktop
!
interface GigabitEthernet14
 description PoE4
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_4 | no_ip_phone_desktop                                 |
ip_phone_desktop"
 !next command is internal.
```

```
 macro auto smartport dynamic_type ip_phone_desktop
!
interface GigabitEthernet24
 description Wireshark
 bridge multicast unregistered filtering
 switchport trunk native vlan none
 ip igmp version 2
 ip igmp query-interval 60
!
interface GigabitEthernet25
 description DHCP
 spanning-tree link-type point-to-point
 switchport mode trunk
 macro description switch
!
interface GigabitEthernet26
 shutdown
 description dhcp1
 spanning-tree link-type point-to-point
 switchport mode trunk
!
exit
monitor session 1 destination remote vlan 15 reflector-port GigabitEthernet24 network
monitor session 1 source interface GigabitEthernet4 both
monitor session 1 source interface GigabitEthernet7 both
monitor session 1 source interface GigabitEthernet13 both
monitor session 1 source interface GigabitEthernet14 both
```

Crestron Mercury & Crestron Mercury X - RFC 2833 Support

To configure the RFC 2833 support on the Crestron Mercury, the **Sipaudiomode RFC2833** command is used from the Crestron Mercury CLI and accessed from the Crestron Toolbox. There are 2 options: **ON** or **OFF**.

1. **ON** (TRUE): Considered Out-of-band, RTP DTMF Events are viewable in the RTP stream. This is the Default setting.
2. **OFF** (FALSE): Considered In-band, RTP DTMF Events are not viewable in the RTP Stream.

SipAudioMode RFC2833 On

Sipaudiomode RFC2833 on command is used to enable RFC2833 Out-of-band support. The RFC2833 setting can be viewed from the **Sipstate** command.

Crestron Mercury X: CLI: RFC 2833 Support

```
MERCURY>sipaudiomode rfc2833 on
RFC2833 support has been turned on.

MERCURY>sipstate

Current SIP States
------------------------------
Server registered   = TRUE
Door station mode   = FALSE
Call in progress    = FALSE
Call hold           = FALSE
Push-To_Talk        = FALSE
Do not disturb      = FALSE
Video started       = FALSE
Video blocked       = FALSE
Video can show      = FALSE
Default ringer      = TRUE
Ring state          = FALSE
Ringback state      = FALSE
Group call flag     = FALSE
User Mute state     = FALSE
Local Mute state    = FALSE
Multicast flag      = FALSE
Support answer      = FALSE
Request auto        = FALSE
Request urgent      = FALSE
RFC 2833 support    = TRUE
Call timeout        = 120 (secs)
Answer timeout      = 0 (secs)
Rewrite CONTACT     = TRUE
Rewrite SDP         = FALSE
Rewrite VIA         = TRUE
Voice-AutoListen    = FALSE
Sound device        = not active
SIP DSCP codepoint = 56
RTP DSCP codepoint = 32
Verify server       = FALSE
Verify client       = FALSE
SRTP                = mandatory
Session Timer       = optional
Early Media         = auto
Video Enable        = auto
Invite Response     = 183
Interface           = LAN_SIPVLAN
Reg Timeout         = 300
```

Crestron Mercury & Crestron Mercury X - SIP Interface Port

To configure the Crestron Mercury X Assigned Ethernet Port to use the LAN or RX OUT Ethernet ports, use the SIPINTERFACE CLI command. When the HD-RX-USB-2000-C Receiver is connected to the Crestron Mercury X, the **AUX** (RX OUT) port is used.

The **Assigned Ethernet Port** can also be configured from the Crestron Mercury Web UI, in the **SIP Calling** section.

SipInterFace AUX

Sipinterface AUX is used in the Crestron Mercury X CLI to activate the RX OUT Ethernet port as the SIP Interface port to be used. Using the RX OUT Ethernet port allows the internet connection to be routed through the HD-RX-USB-2000-C receiver and then connected to the RX OUT port on the Crestron Mercury X.

Crestron Mercury X: CLI: SIPINTERFACE Support

```
MERCURY-X>sipinterface aux
Success: New SIP interface has been set.

MERCURY-X>sipinfo
SIP Parameters
-------------------------------
SIP: ENABLED
-------------------------------
SIP audio mode: FD
SIP auto mode: NONE
SIP local ext: 2645
SIP local name: CRESTRON
SIP local port: 5060
SIP connection mode: SERVER
SIP page group(s): CRESTRON
SIP realm: *
SIP remote config file: NONE
SIP server name: NONE
SIP server port: 5060
SIP server ip address: 10.80.17.2
SIP server username: 2645
SIP server password: ****
SIP Name server: NONE
SIP proxy server: NONE:5060
SIP STUN server: NONE
SIP STUN domain: NONE
SIP multicast address: 227.1.1.1
SIP multicast port: 1234
SIP transport type: TCP
SIP protocol qos: 24
SIP media port: 40000
SIP rtp qos: 46
SIP session timer: optional
SIP Interface: AUX
SIP registration timeout: 300
```

Cisco Unified Communications Manager (CUCM)

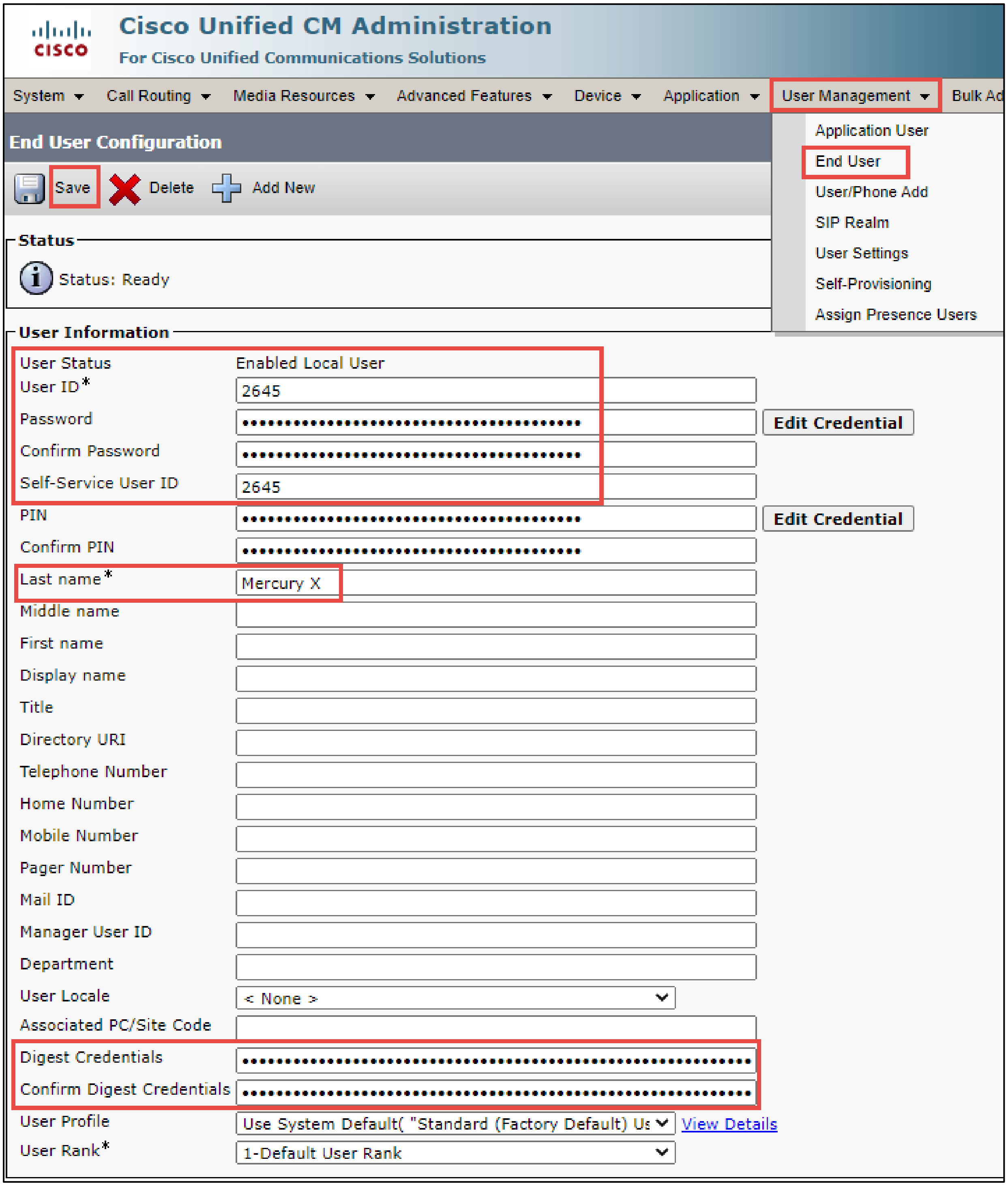
This section describes the Cisco CUCM configuration necessary to integrate the Crestron Mercury and Crestron Mercury X as a SIP Endpoint.

NOTE: It is assumed that the general installation and basic CUCM configuration has already been administered.

User Configuration

1. Navigate to **User Management** -> **End User.**
2. Click **Add New**. The End User configuration window appears.
3. **User ID**: Enter a unique end user identification name. Two users were configured for this test: ***2645*** *(Crestron Mercury X)* and ***2648*** *(Crestron Mercury).*
4. **Last Name**: Enter the end user last name, **Mercury X.**
5. **Digest Credentials**: This same password will be entered on the Crestron Mercury device for the SIP Server Password. The extension number (**2645** & **2648**) is used for the Password.
6. **Confirm the Digest Credentials**: Re-enter the password configured above.
7. **Password**: the **Digest Credentials** were also used for the **Password**.
8. **Confirm Password**: Re-enter the same password configured above.
9. Click **Save.**

Cisco CUCM: End User Configuration



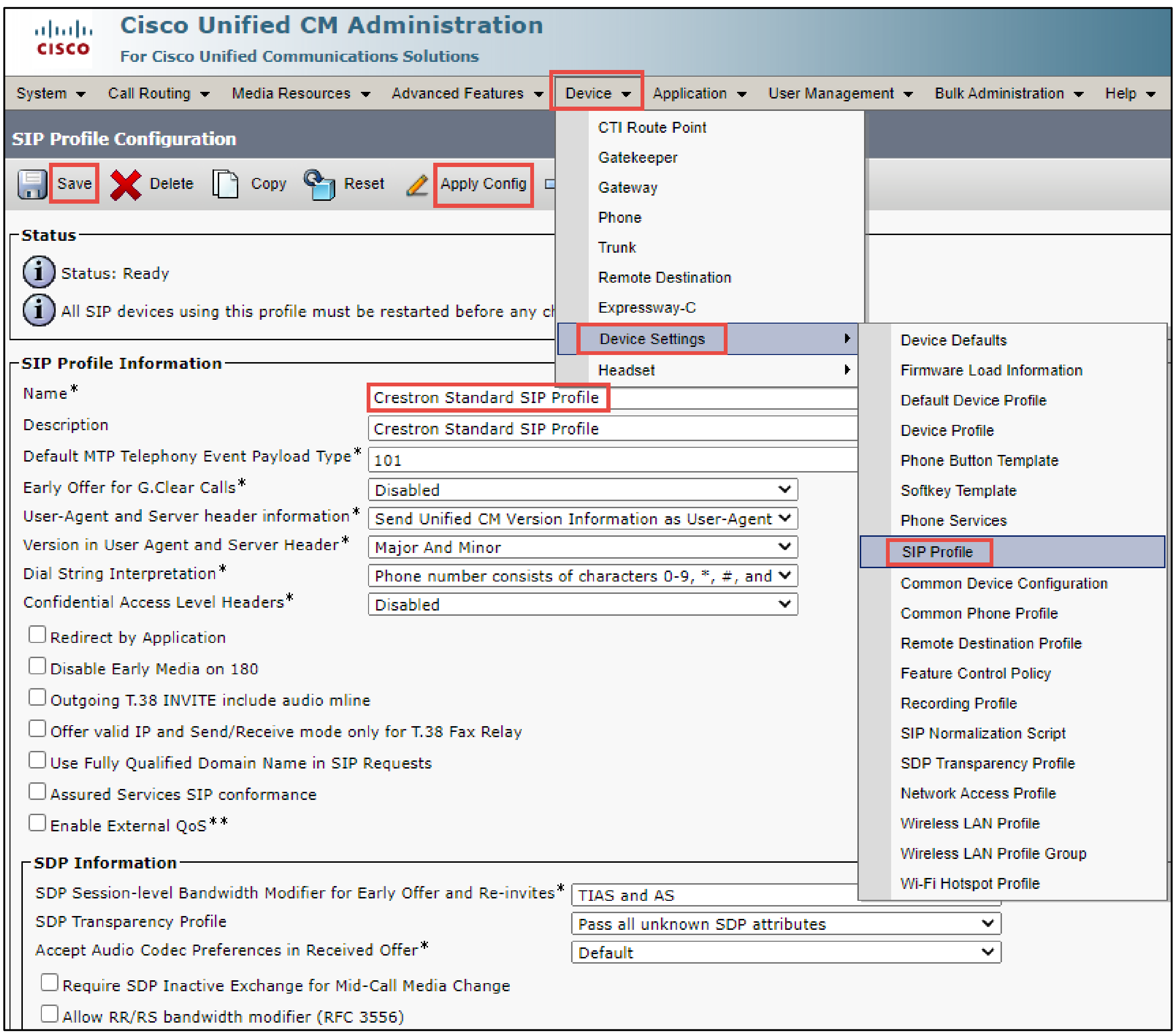
SIP Profile

SIP Profile is configured for the Crestron Mercury and Crestron Mercury X phones. The Standard SIP Profile is used for the Cisco PBX phone.

Crestron Standard SIP Profile – Crestron Mercury phones

1. To add a new SIP Profile, Navigate to **Device** -> **Device Settings-> SIP Profile**.
2. On the screen that appears, click **Add New** and configure the SIP Profile as below.
3. **Name**: **Crestron Standard SIP Profile.**
4. Configure **Early offer support for voice and video calls** * as **Best Effort(no MTP inserted)**
5. Retain all other default configuration settings.
6. Then click **Save** and then **Apply Config**.

Cisco CUCM: Crestron Standard SIP Profile (1/4)

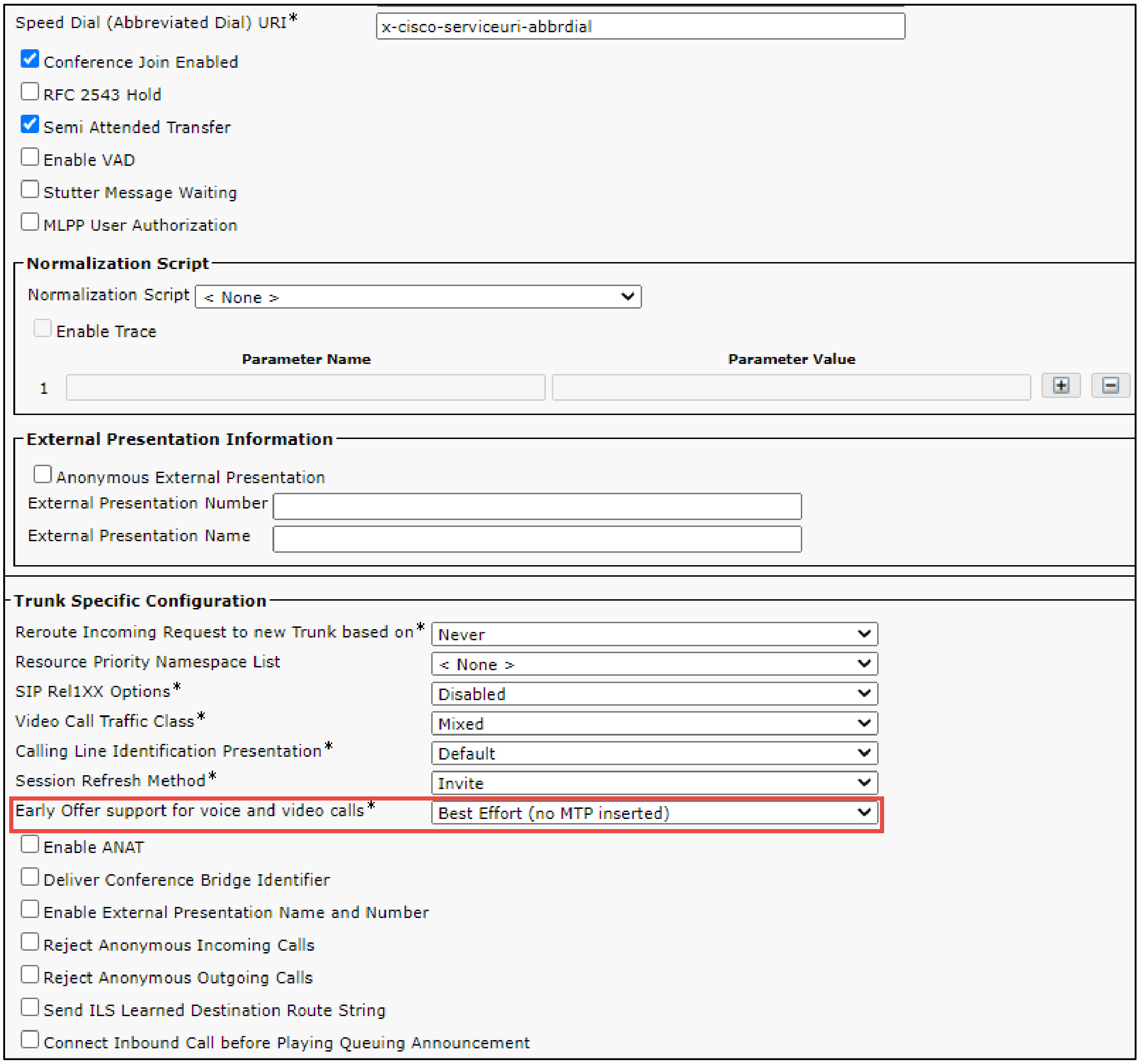


Cisco CUCM: Crestron Standard SIP Profile (2/4)

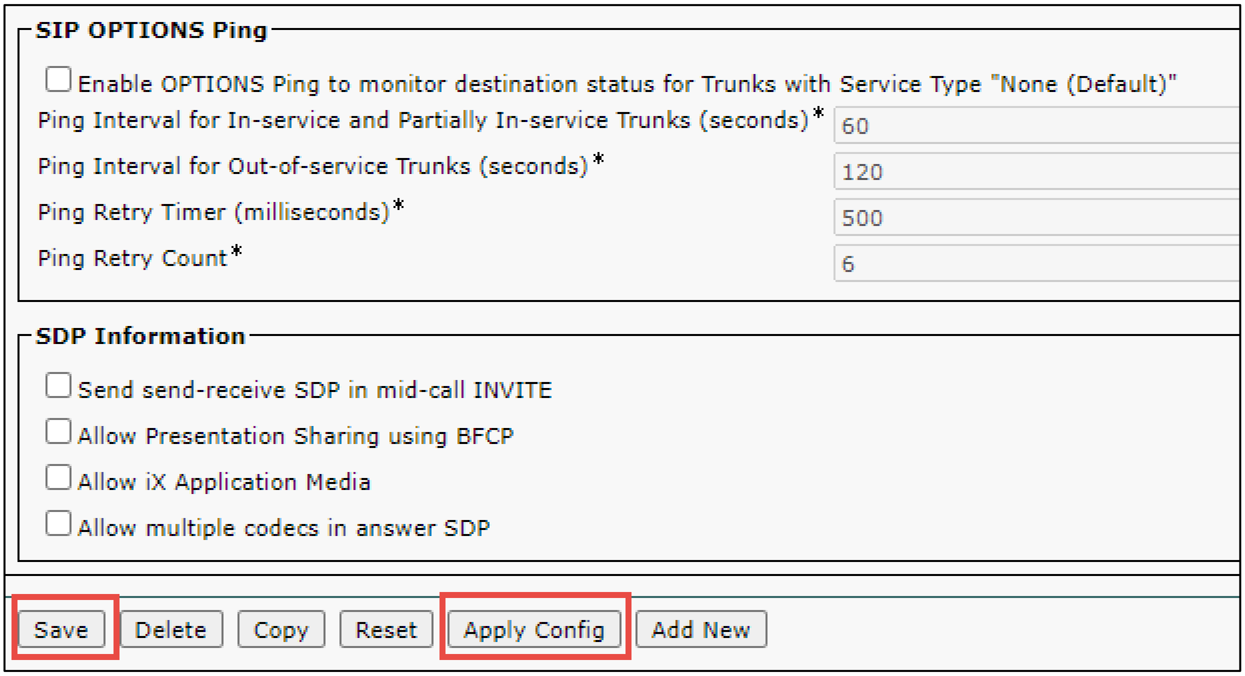
Parameters used in Phone

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	(selected) 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
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 CUCM: Crestron Standard SIP Profile (3/4)



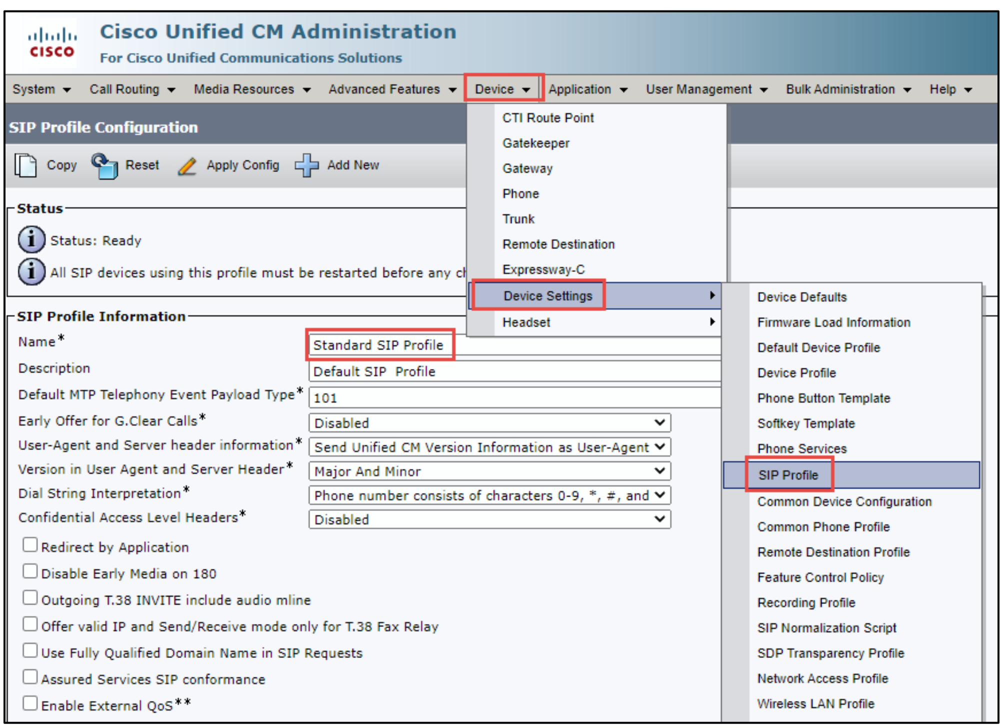
Cisco CUCM: Crestron Standard SIP Profile (4/4)



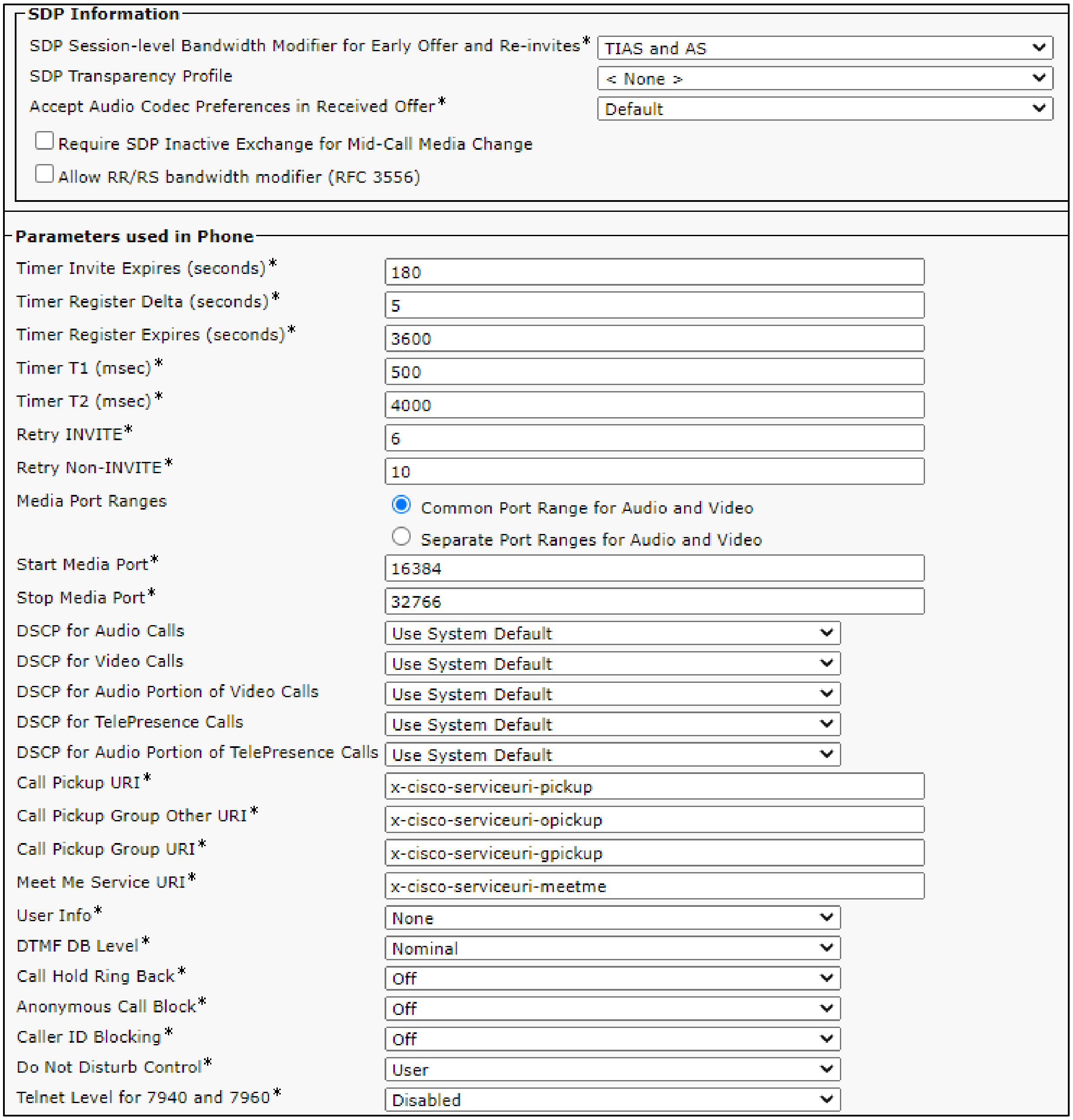
Standard SIP Profile – Cisco PBX phone

- To view the Standard SIP Profile, Navigate to **Device** -> **Device Settings**-> **SIP Profile**.
- The Default Standard SIP Profile is shown below.

Cisco CUCM: Standard SIP Profile (1/4)



Cisco CUCM: Standard SIP Profile (2/4)



SDP Information

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
SDP Transparency Profile	< None >
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
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

Cisco CUCM: Standard SIP Profile (3/4)

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
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial

- [x] Conference Join Enabled
- [ ] RFC 2543 Hold
- [x] Semi Attended Transfer
- [ ] Enable VAD
- [ ] Stutter Message Waiting
- [ ] MLPP User Authorization

Normalization Script

Normalization Script: < None >

- [ ] Enable Trace

	Parameter Name	Parameter Value
1		

External Presentation Information

- [ ] Anonymous External Presentation

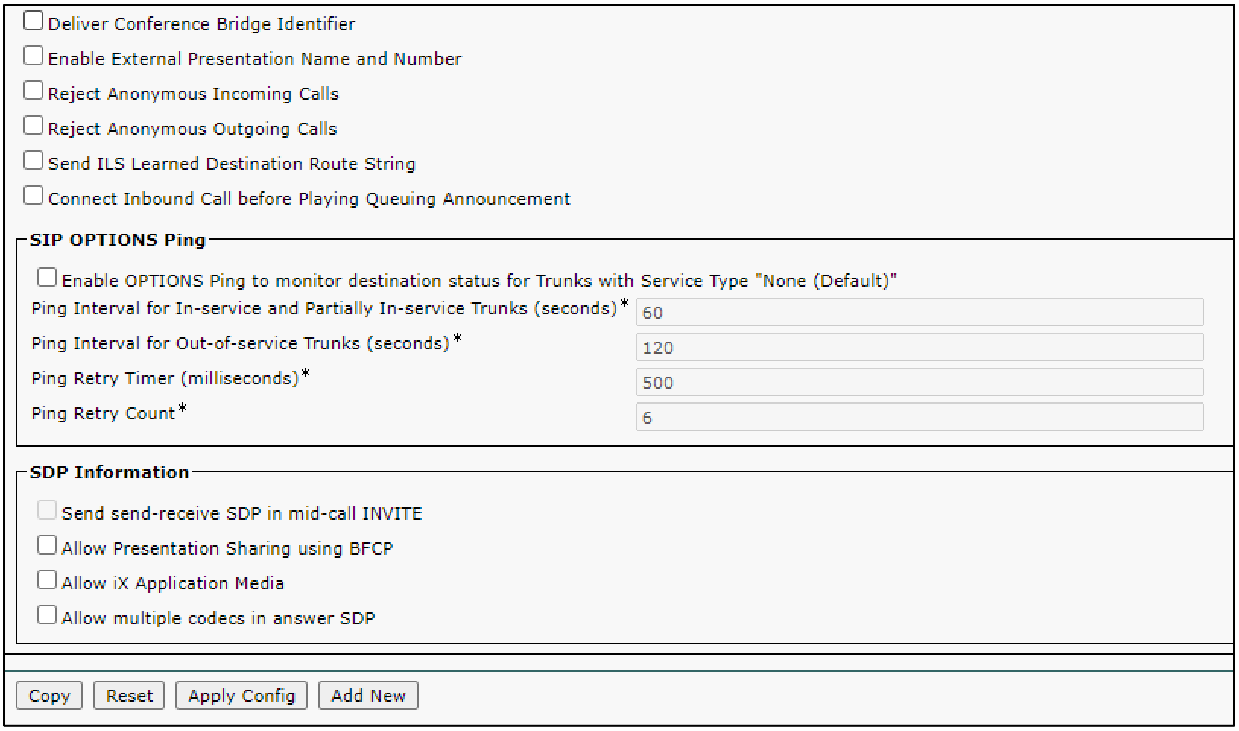
External Presentation Number	
External Presentation Name	

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*	Never
Resource Priority Namespace List	< None >
SIP Rel1XX Options*	Disabled
Video Call Traffic Class*	Mixed
Calling Line Identification Presentation*	Default
Session Refresh Method*	Invite
Early Offer support for voice and video calls*	Disabled (Default value)

- [ ] Enable ANAT

Cisco CUCM: Standard SIP Profile (4/4)



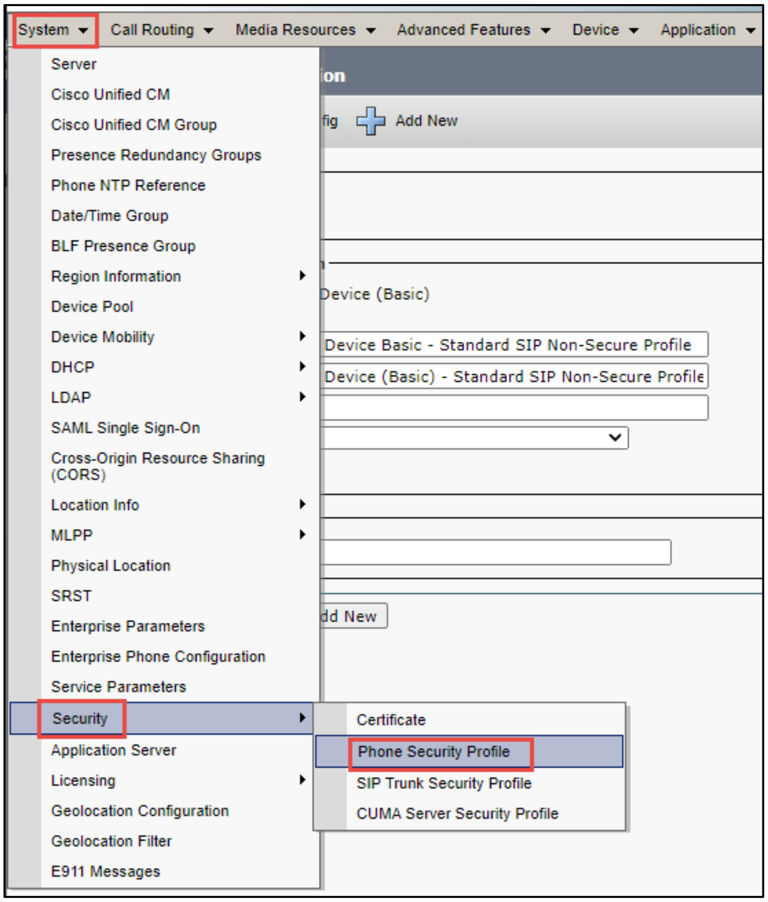
Security Profiles

Three Security Profiles were created, one for the Crestron Mercury phones, one for the Cisco 9971 PBX phone and one for the PSTN Trunk.

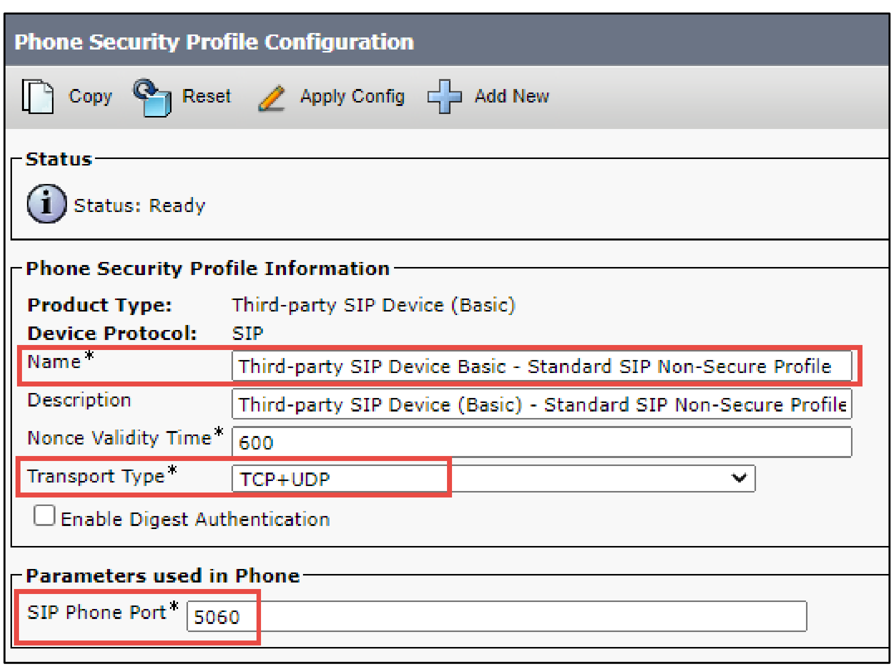
Crestron Mercury Phone Security Profile

1. Navigate to **System**->**Security**-> **Phone Security Profile.**
2. Click **Add New.**
3. Provide a **Name**: ***Third-party SIP Device Basic - Standard SIP Non-Secure Profile.***
4. **Transport Type**: **TCP+UDP**
5. Check the Enable Digest Authentication checkbox
6. Make sure the **SIP Phone Port** is set to **5060**
7. Click **Save**

Cisco CUCM: Crestron Mercury Security Profile (1/2)



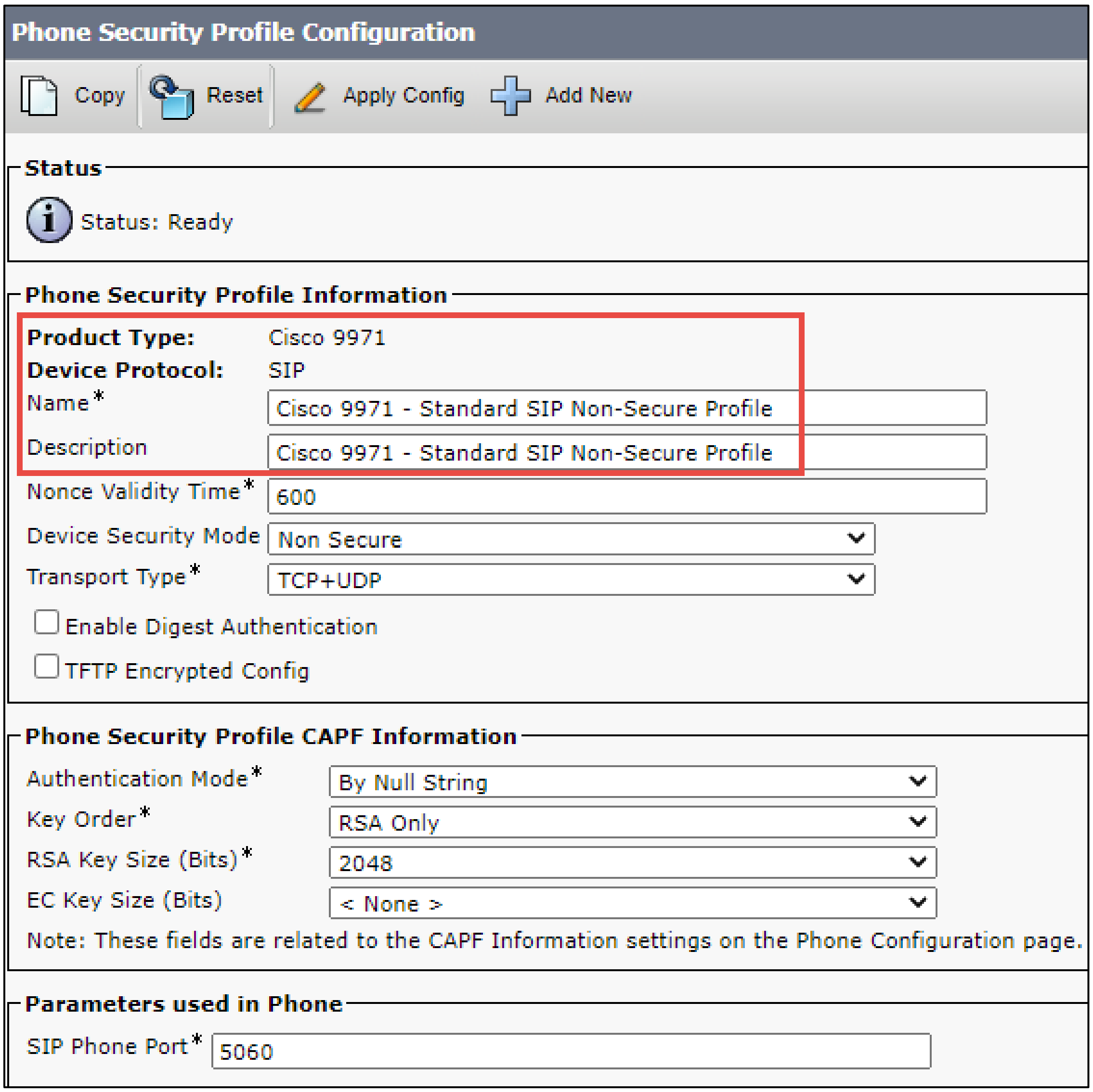
Cisco CUCM: Crestron Mercury Security Profile (2/2)



Cisco 9971 – Security Profile

- Navigate to **System->Security-> Phone Security Profile**
- The Default **Cisco 9971 - Standard SIP Non-Secure Profile** is shown below.

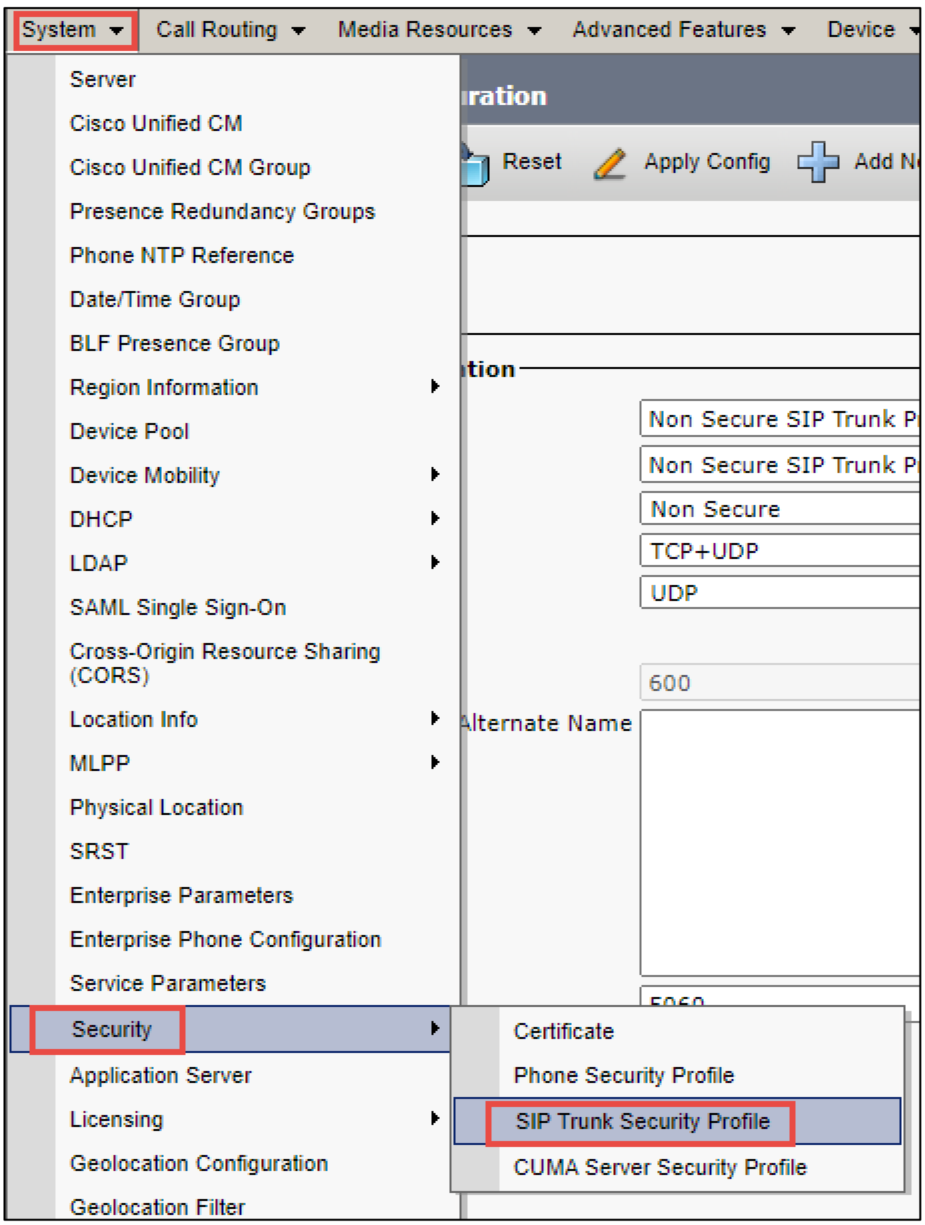
Cisco CUCM: Cisco 9971 – Standard SIP Non-Secure Profile



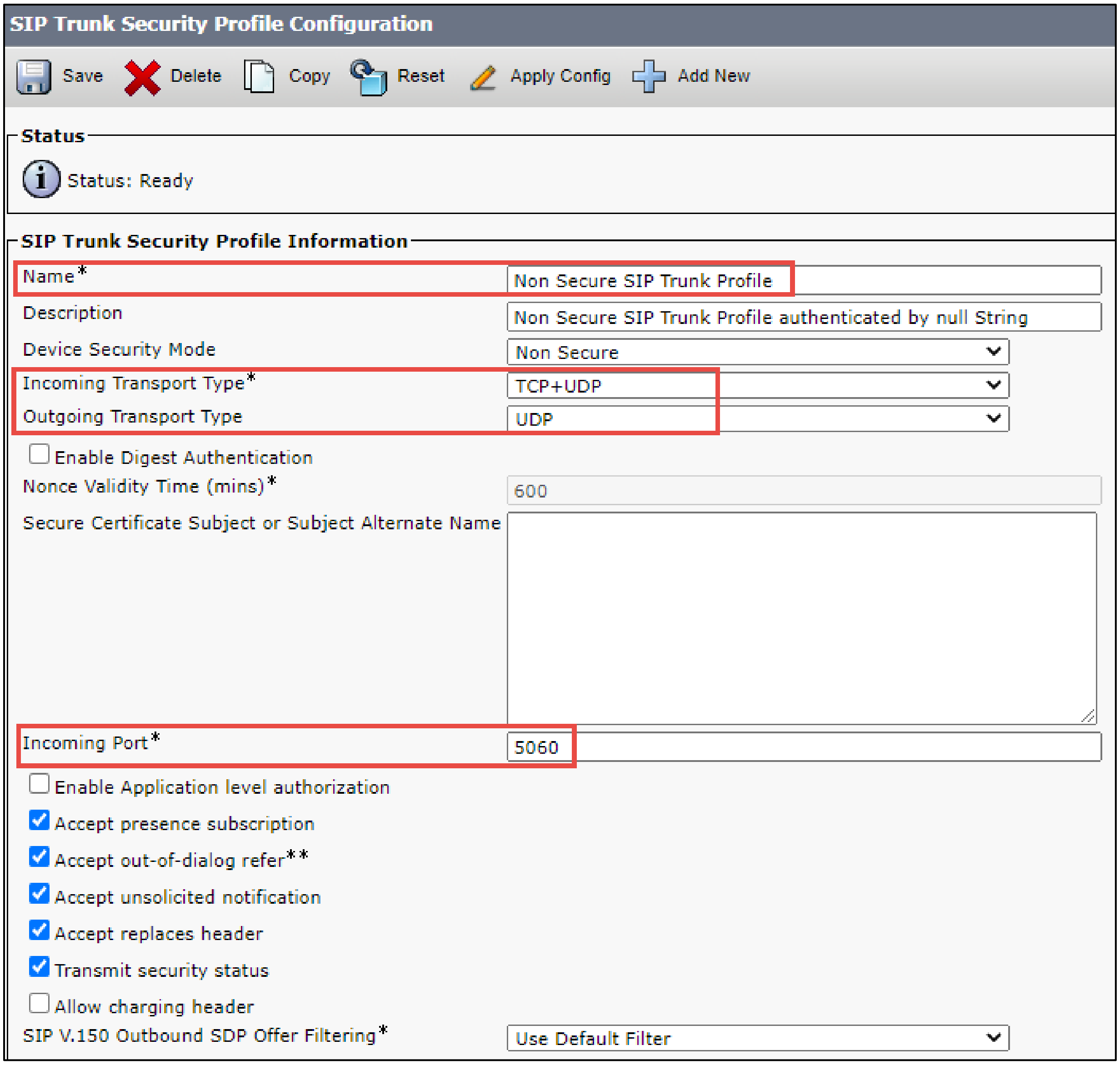
PSTN Trunk - SIP Trunk Security Profile

1. Navigate to **System->Security-> SIP Trunk Security Profile.**
2. Click **Add New.**
3. **Name**: ***Non-Secure SIP Trunk Profile***.
4. **Incoming Transport Type**: **TCP+UDP**
5. **Outgoing Transport Type: UDP**
6. Make sure the **Incoming Port** is set to **5060**

Cisco CUCM: PSTN Trunk – SIP Trunk Security Profile (1/2)



Cisco CUCM: PSTN Trunk – SIP Trunk Security Profile (2/2)

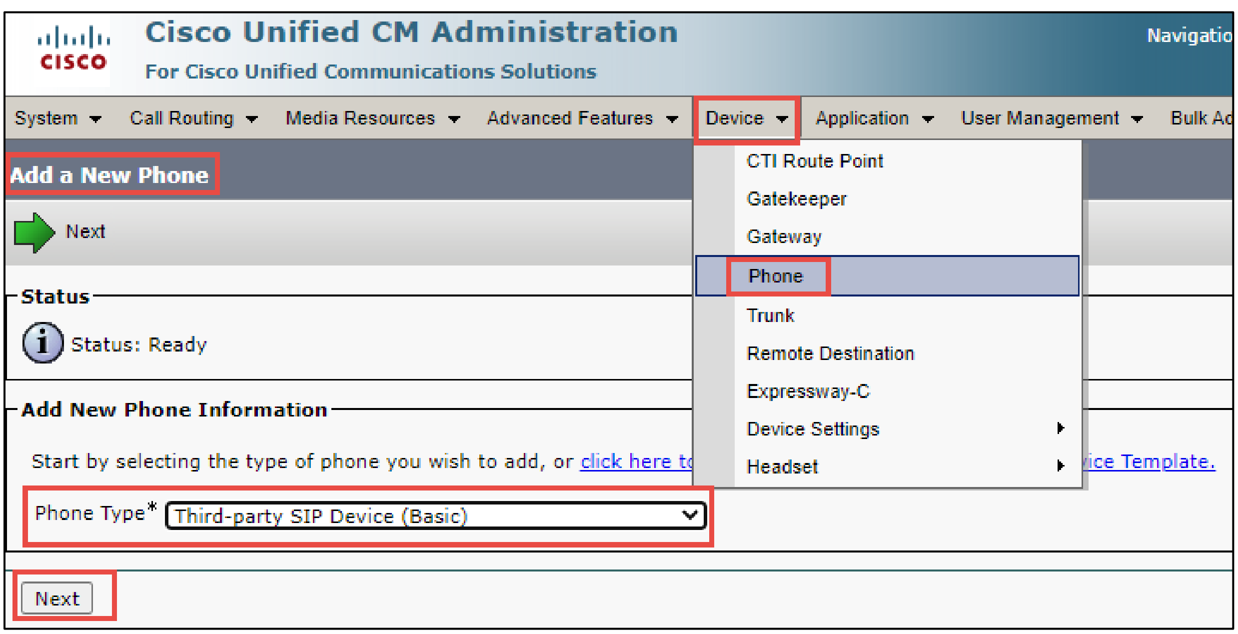


Crestron Mercury devices Configured as Third Party SIP Device (Basic)

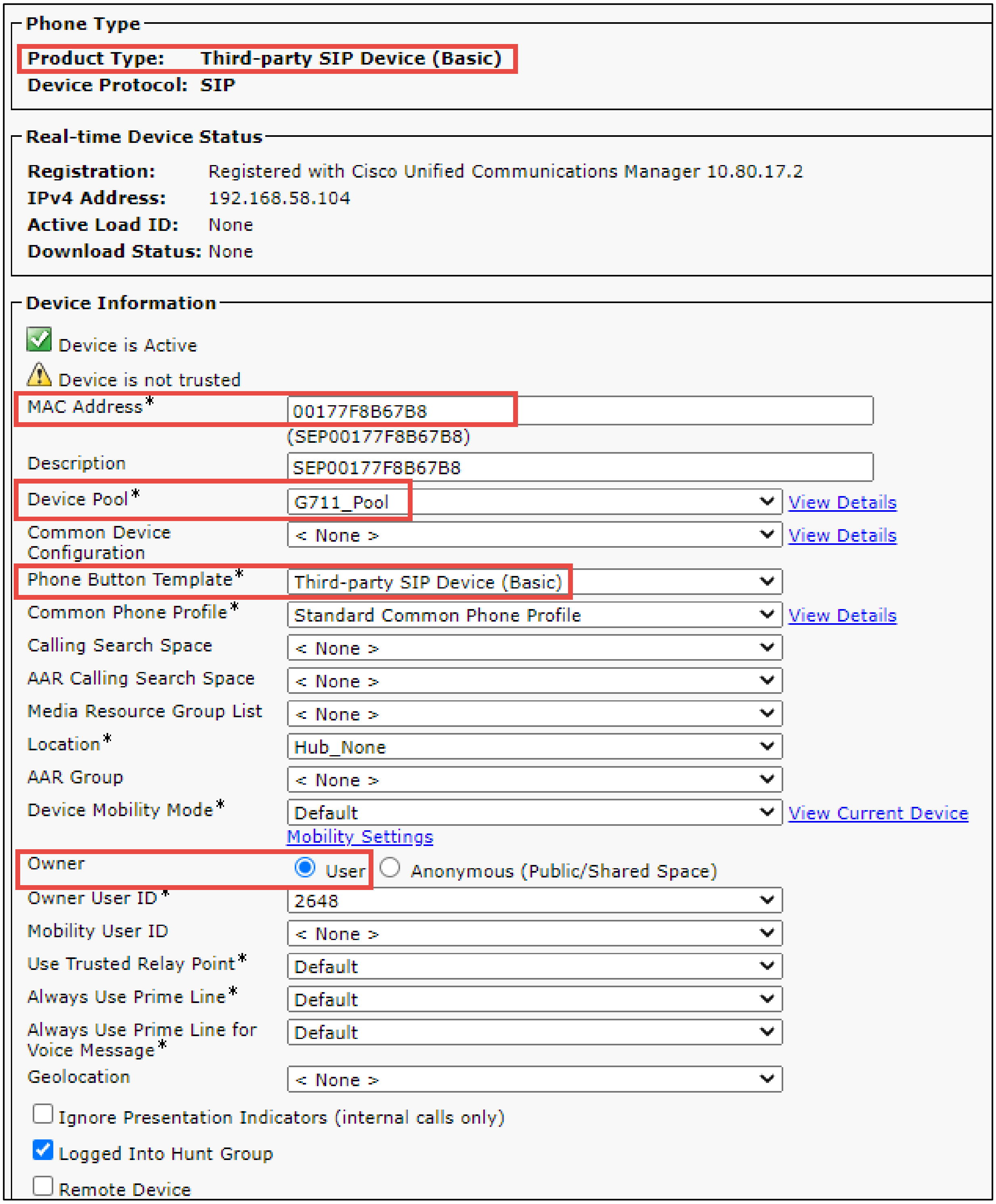
The Crestron Mercury devices are configured as a Third Party SIP Device (Basic) in the Cisco CUCM Phone Configuration

1. Navigate to **Device->Phone.**
2. Click **Add New.**
3. **Phone Type** as **Third-party SIP Device (Basic).**
4. Click **Next**
5. **MAC Address:** Enter MAC Address of the Crestron Mercury - **00177F8B67B8.**
6. **Device Pool: G711_pool**.
7. **Phone Button Template:** as **Third-party SIP Device (Basic).**
8. **Common Phone Template:** as **Standard Common Phone Profile.**
9. **Owner**: click the **User** radio button.
10. **Owner User ID:** select the End User configured earlier from the drop down. **2648** is selected for the Crestron Mercury, **2645** is selected for the Crestron Mercury X.
11. **Device Security Profile** as **Third-party SIP Device Basic - Standard SIP Non-Secure Profile**.
12. **SIP Profile** as configured earlier from the drop down menu - **Crestron Standard SIP Profile**.
13. **Digest User ID:** select the End User configured earlier from the drop down. **2648** is selected for the Crestron Mercury and **2645** is for the Crestron Mercury X
14. Click **Save**

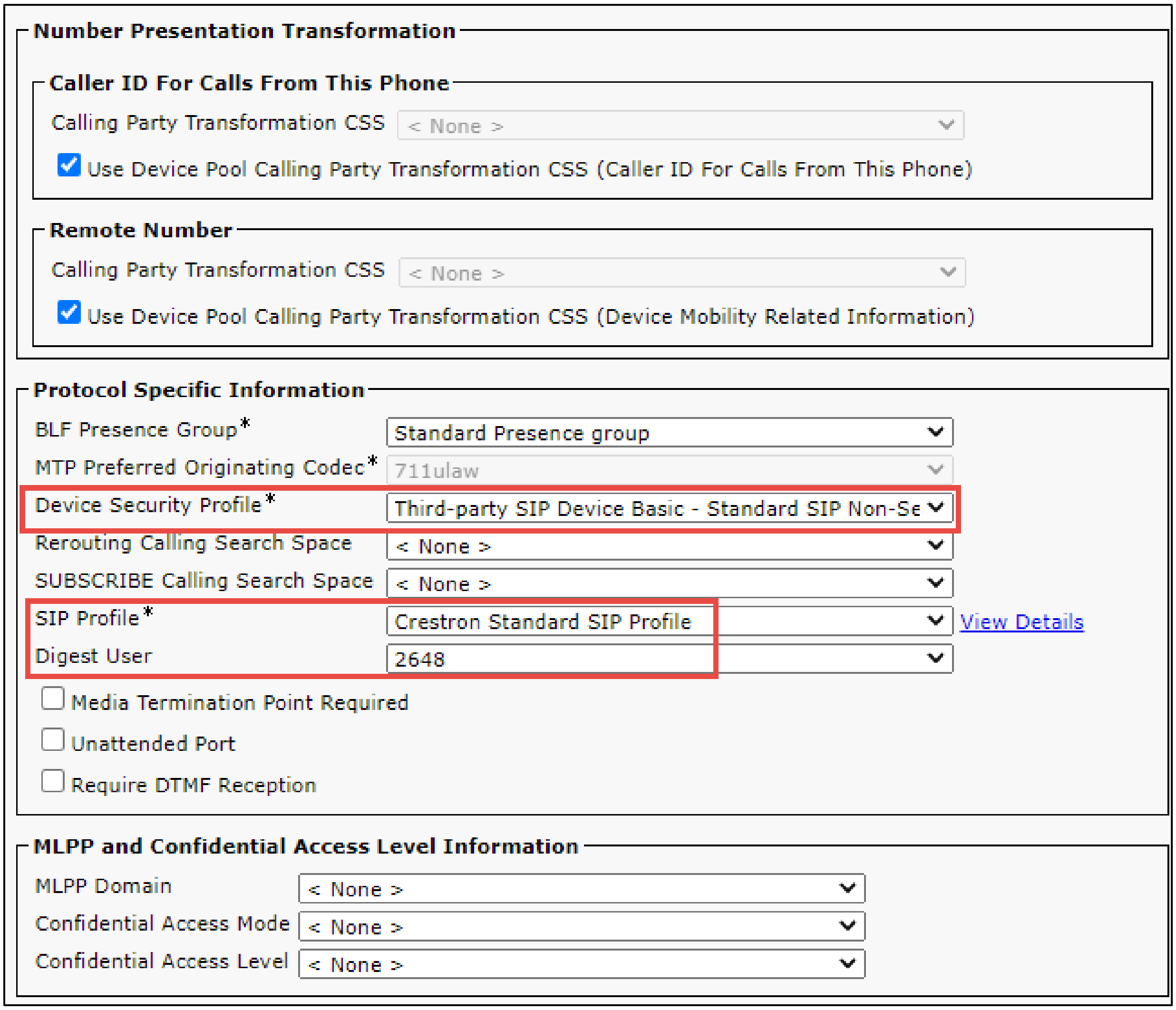
Cisco CUCM: Third Party SIP Device (Basic) (1/3)



Cisco CUCM: Third Party SIP Device (Basic) (2/3)



Cisco CUCM: Third Party SIP Device (Basic) (3/3)

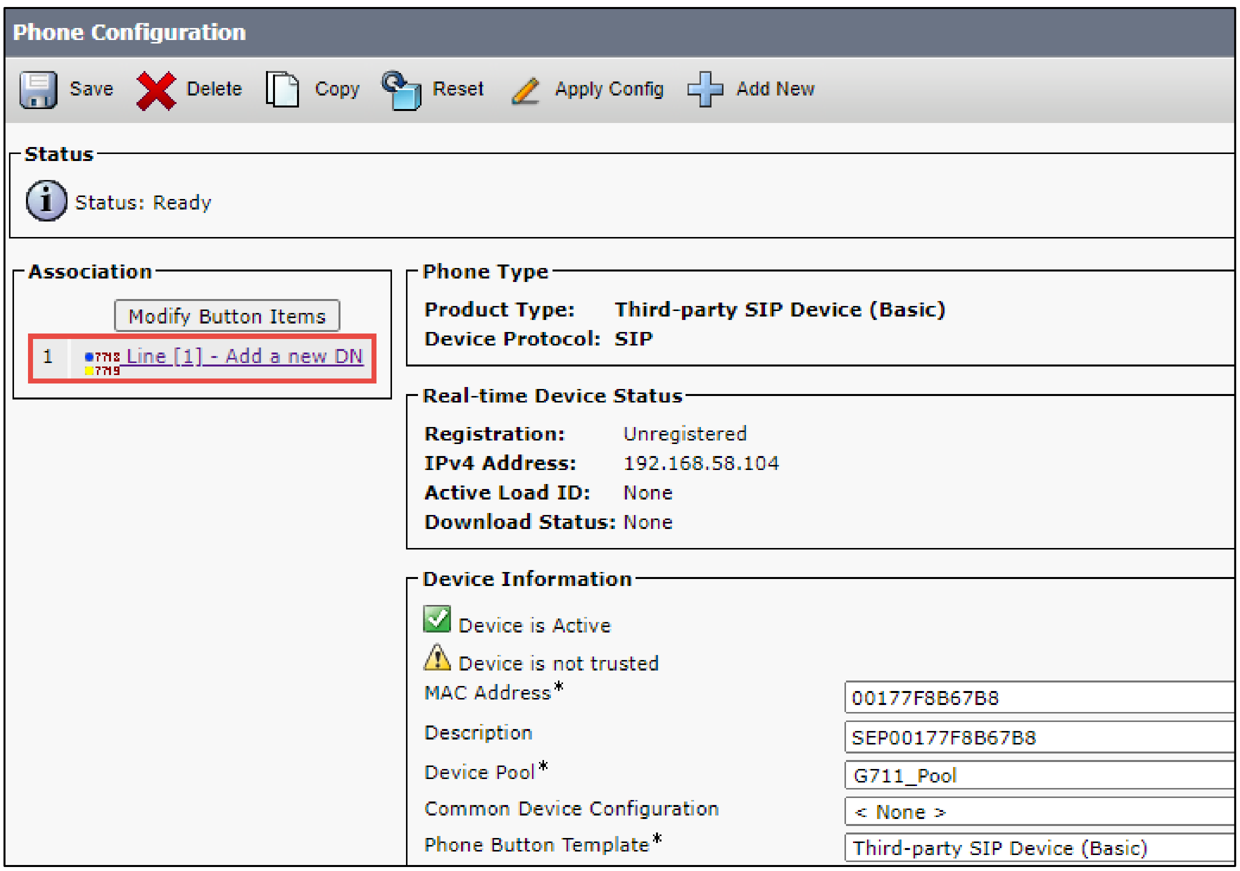


Directory Number

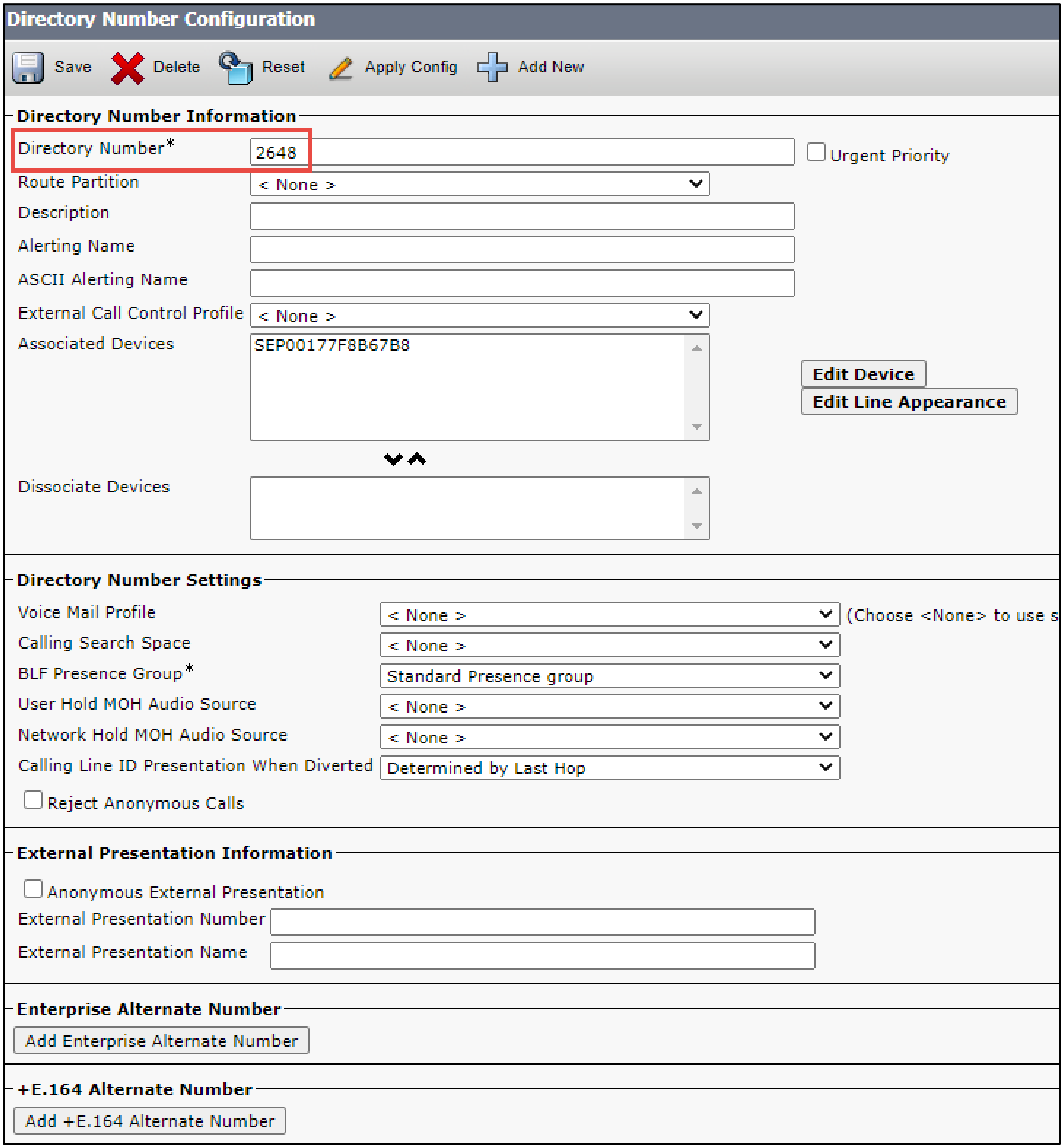
Assign a Directory Number to the Crestron Mercury devices.

1. From the Crestron Mercury Phone Configuration, (**Device**->**Phone).**
2. Click on **Add a new DN.**
3. **Directory Number: 2648** is used for the Crestron Mercury and DN **2645** is used for Crestron Mercury X.
4. The 10 Digit DID is entered for the **Display (Caller ID), ASCII Display (Caller ID)** and the **External Phone Number Mask.**

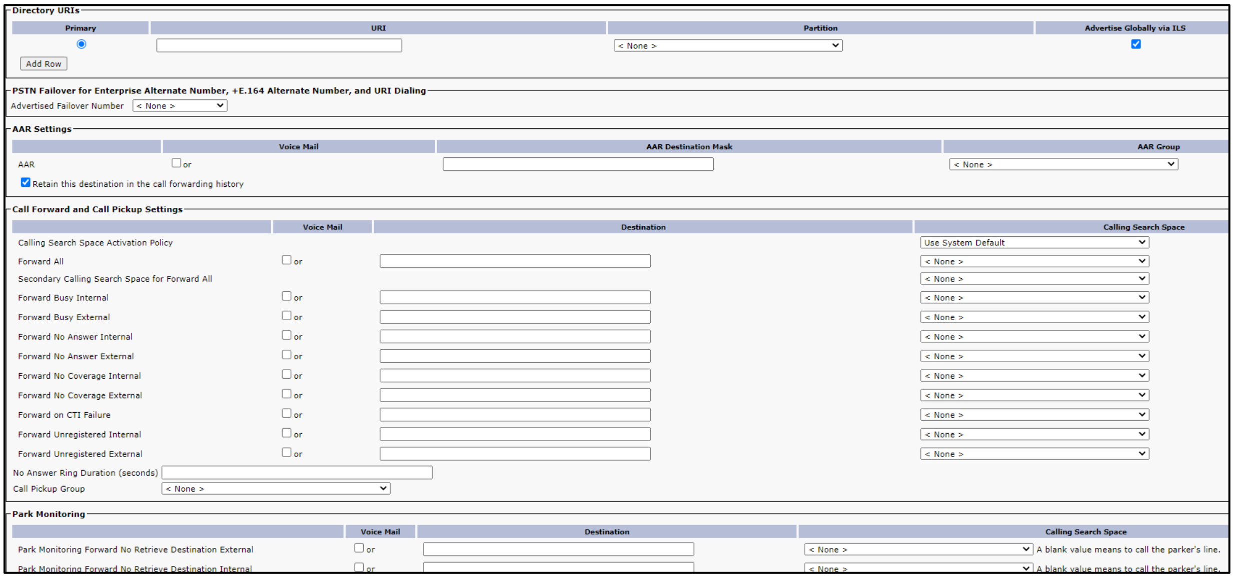
Cisco CUCM: Crestron Mercury Directory Number (1/4)



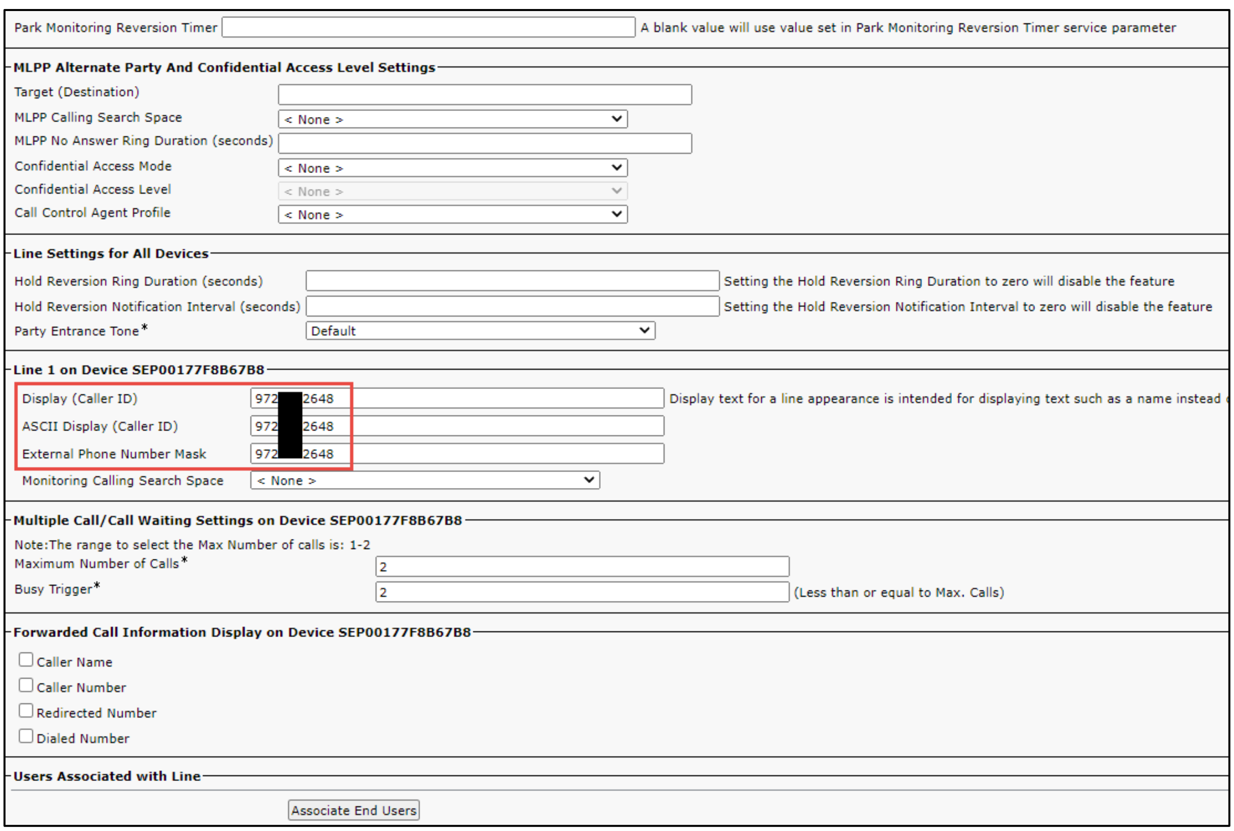
Cisco CUCM: Crestron Mercury Directory Number (2/4)



Cisco CUCM: Crestron Mercury Directory Number (3/4)



Cisco CUCM: Crestron Mercury Directory Number (4/4)

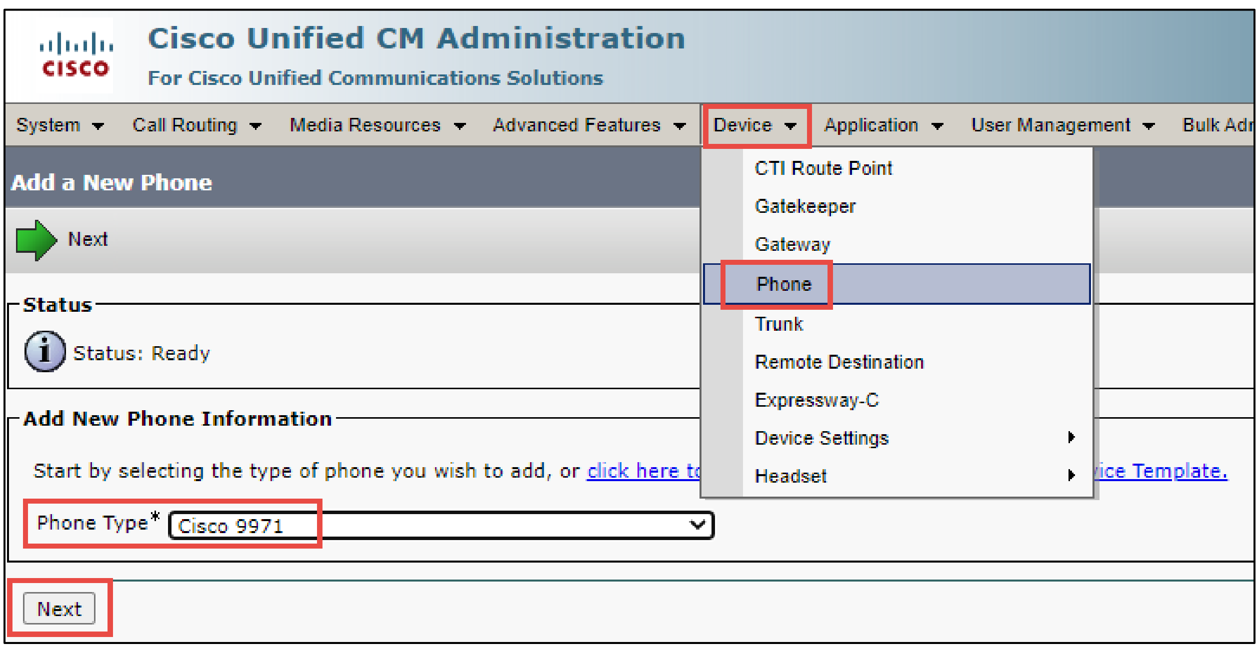


Cisco 9971 SIP PBX Phone

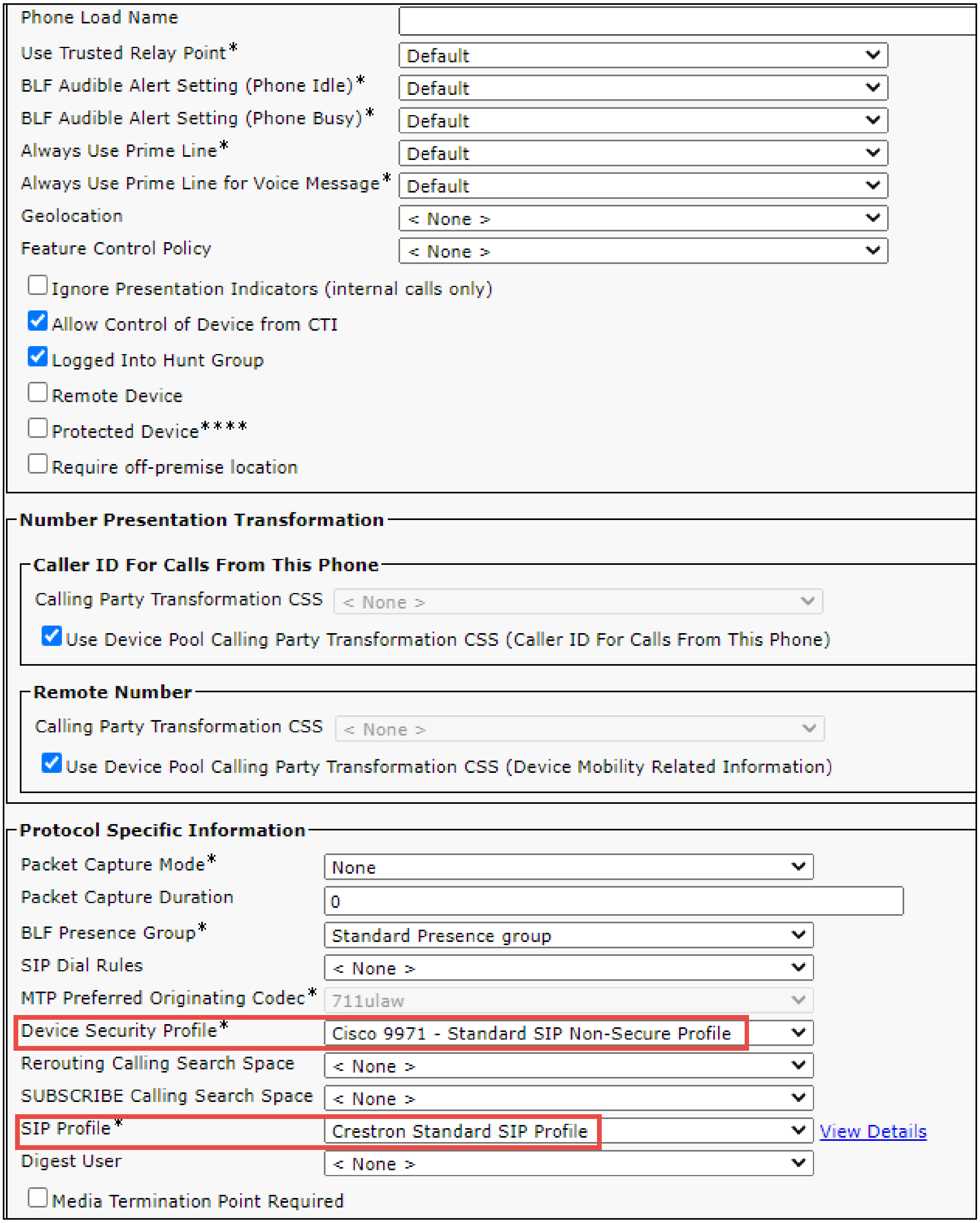
The Cisco 9971 PBX phone is SIP PBX phone.

1. Navigate to **Device->Phone**
2. Click **Add New**
3. Select **Phone Type** as **Cisco 9971**
4. Click **Next**
5. **MAC Address:** Enter MAC Address of the Cisco 9971 SIP Phone - **1C17D337D08D.**
6. **Device Pool** – **G711_pool**.
7. **Phone Button Template** as **Standard 9971 SIP.**
8. **Media Resource Group List:** **Crestron**, (created below).
9. **Owner:** select the **Anonymous** radio button.
10. **Device Security Profile** from the drop down – **Cisco 9971 - Standard SIP Non-Secure Profile**.
11. **SIP Profile** from the drop down select **Crestron Standard SIP Profile**.
12. Click **Save**

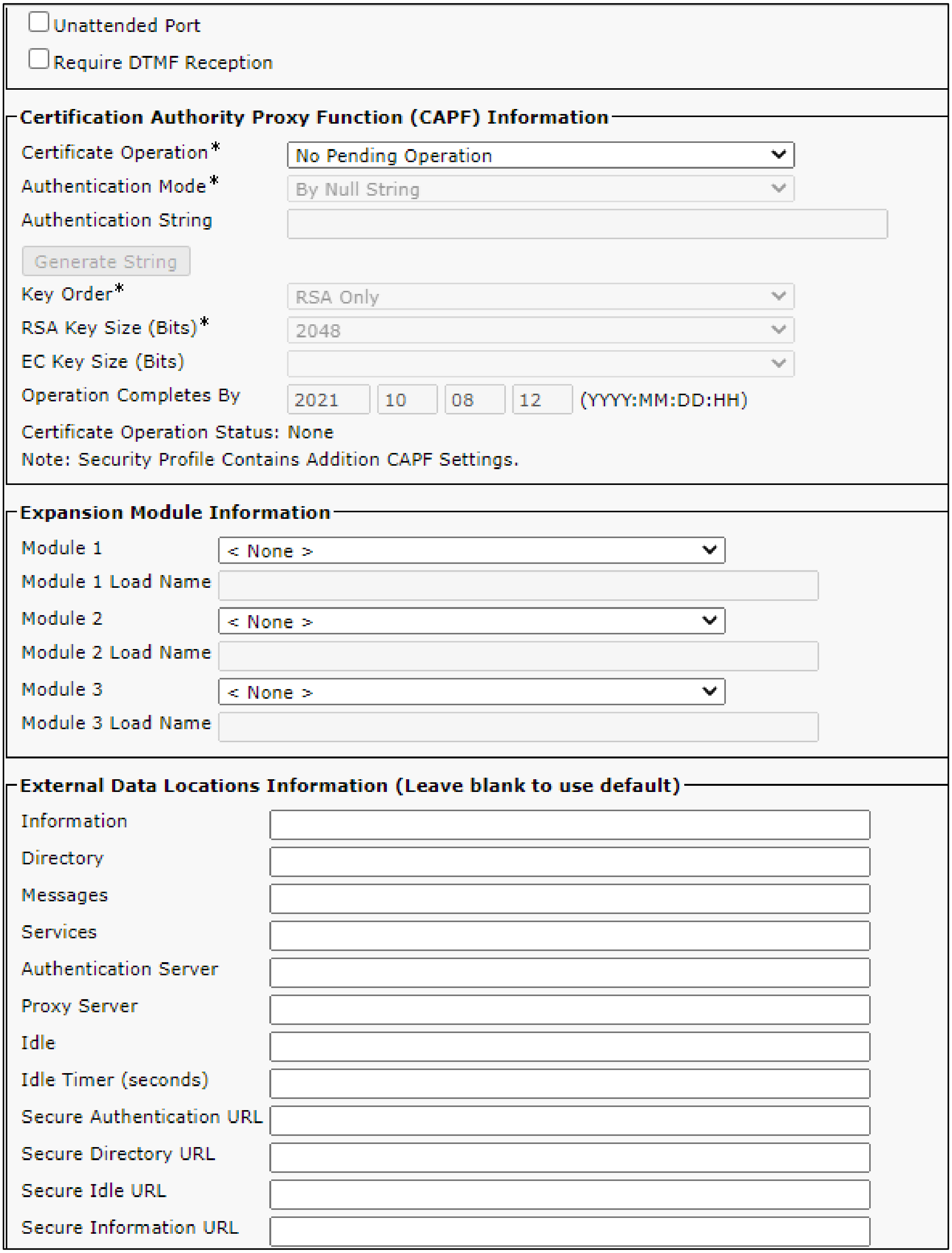
Cisco CUCM: Cisco 9971 SIP Phone (1/7)



Cisco CUCM: Cisco 9971 SIP Phone (2/7)



Cisco CUCM: Cisco 9971 SIP Phone (3/7)



☐ Unattended Port

☐ Require DTMF Reception

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	By Null String
Authentication String	
Generate String	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2021 10 08 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

Expansion Module Information

Module 1	< None >
Module 1 Load Name	
Module 2	< None >
Module 2 Load Name	
Module 3	< None >
Module 3 Load Name	

External Data Locations Information (Leave blank to use default)

Information	
Directory	
Messages	
Services	
Authentication Server	
Proxy Server	
Idle	
Idle Timer (seconds)	
Secure Authentication URL	
Secure Directory URL	
Secure Idle URL	
Secure Information URL	

Cisco CUCM: Cisco 9971 SIP Phone (4/7)

Secure Messages URL
Secure Services URL

Extension Information

☐ Enable Extension Mobility
Log Out Profile: -- Use Current Device Settings --
Log in Time: < None >
Log out Time: < None >

MLPP and Confidential Access Level Information

MLPP Domain	< None >
MLPP Indication*	Default
MLPP Preemption*	Default
Confidential Access Mode	< None >
Confidential Access Level	< None >

Do Not Disturb

☐ Do Not Disturb

DND Option*	Use Common Phone Profile Setting
DND Incoming Call Alert	< None >

Secure Shell Information

Secure Shell User
Secure Shell Password

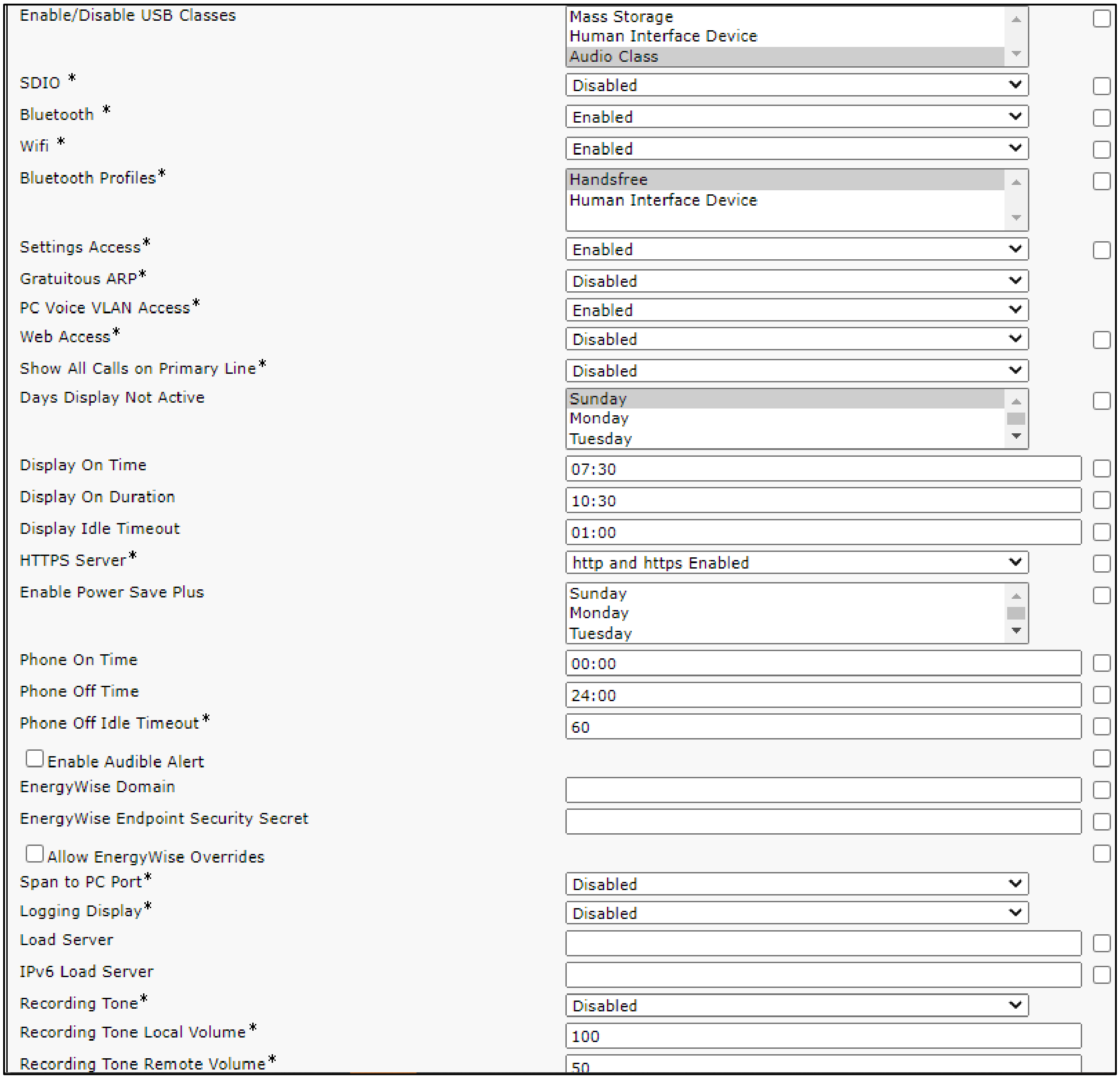
Product Specific Configuration Layout

Parameter Value

☐ Disable Speakerphone
☐ Disable Speakerphone and Headset

PC Port *	Enabled
Back USB Port*	Enabled
Side USB Port*	Enabled
Cisco Camera*	Disabled
Console Access*	Disabled
Video Capabilities*	Disabled
Enable/Disable USB Classes	Mass Storage Human Interface Device

Cisco CUCM: Cisco 9971 SIP Phone (5/7)



Cisco CUCM: Cisco 9971 SIP Phone (6/7)

Recording Tone Duration	
Display On When Incoming Call*	Enabled
RTCP*	Disabled
Log Server	
IPv6 Log Server	
Remote Log*	Disabled
Log Profile	Default Preset Telephony
Advertise G.722 and iSAC Codecs *	Use System Default
Wideband Headset UI Control*	Enabled
Wideband Headset*	Enabled
Peer Firmware Sharing*	Enabled
Cisco Discovery Protocol (CDP): Switch Port*	Enabled
Cisco Discovery Protocol (CDP): PC Port*	Enabled
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*	Enabled
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled
LLDP Asset ID	
LLDP Power Priority*	Unknown
802.1x Authentication*	User Controlled
FIPS Mode*	Disabled
Detect Unified CM Connection Failure*	Normal
Switch Port Remote Configuration*	Disabled
PC Port Remote Configuration*	Disabled
Automatic Port Synchronization*	Disabled
Power Negotiation*	Enabled
Restrict Data Rates*	Disabled
SSH Access*	Disabled
Incoming Call Toast Timer*	5
Provide Dial Tone from Release Button*	Disabled

Cisco CUCM: Cisco 9971 SIP Phone (7/7)

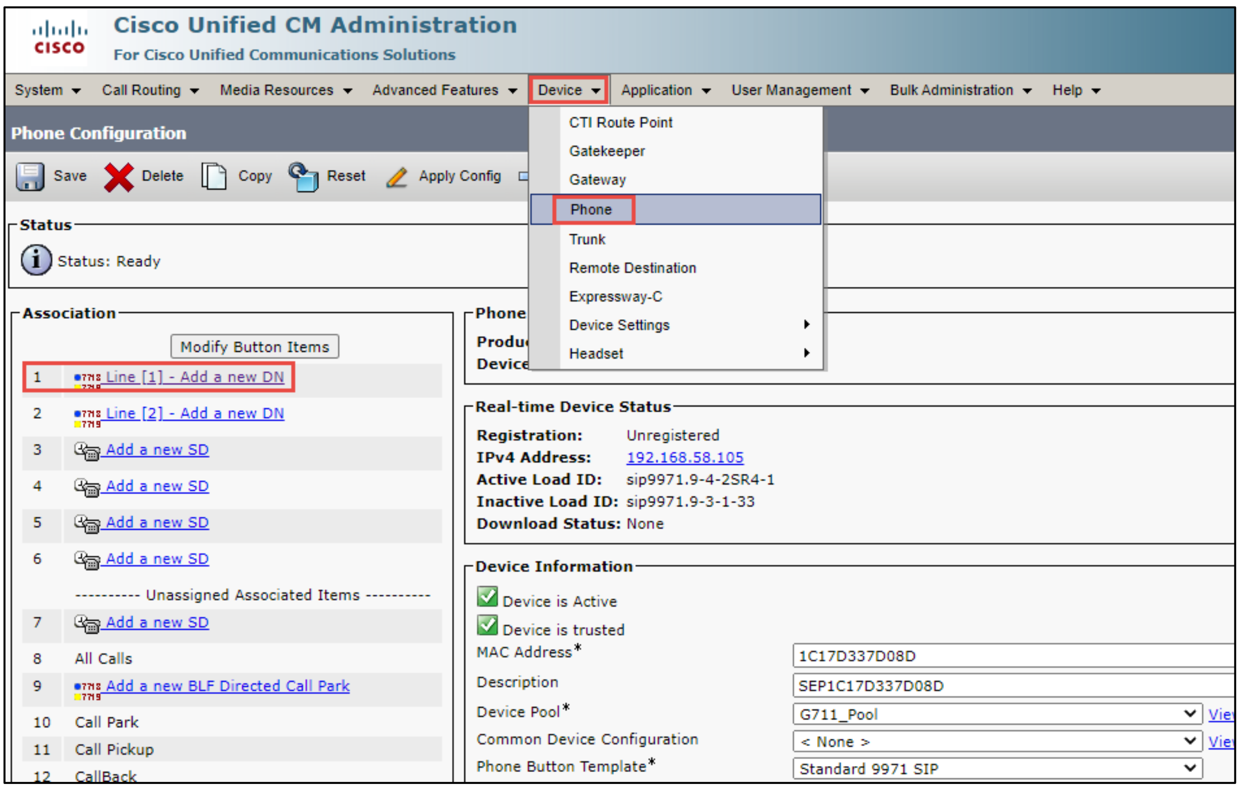
Hide Video By Default*	Disabled
Background Image	
Simplified New Call UI*	Disabled
Enable VXC VPN for MAC	
VXC VPN Option*	Dual Tunnel
VXC Challenge*	Challenge
VXC-M Servers	
Revert to All Calls*	Disabled
RTCP for Video*	Enabled
Record Call Log from Shared Line*	Disabled
Show Remote Private Calls*	Disabled
Record Call Log For Remote Private Calls*	Enabled
Show Call History for Selected Line Only.*	Disabled
Actionable Incoming Call Alert*	Disabled
DF bit*	0
Default Line Filter	
Separate Audio and Video Mute*	Disabled
Softkey Control*	Feature Control Policy
Start Video Port	
Stop Video Port	
Lowest Alerting Line State Priority*	Disabled
TLS Resumption Timer*	3600
Audio EQ*	Default : Default

Directory Number

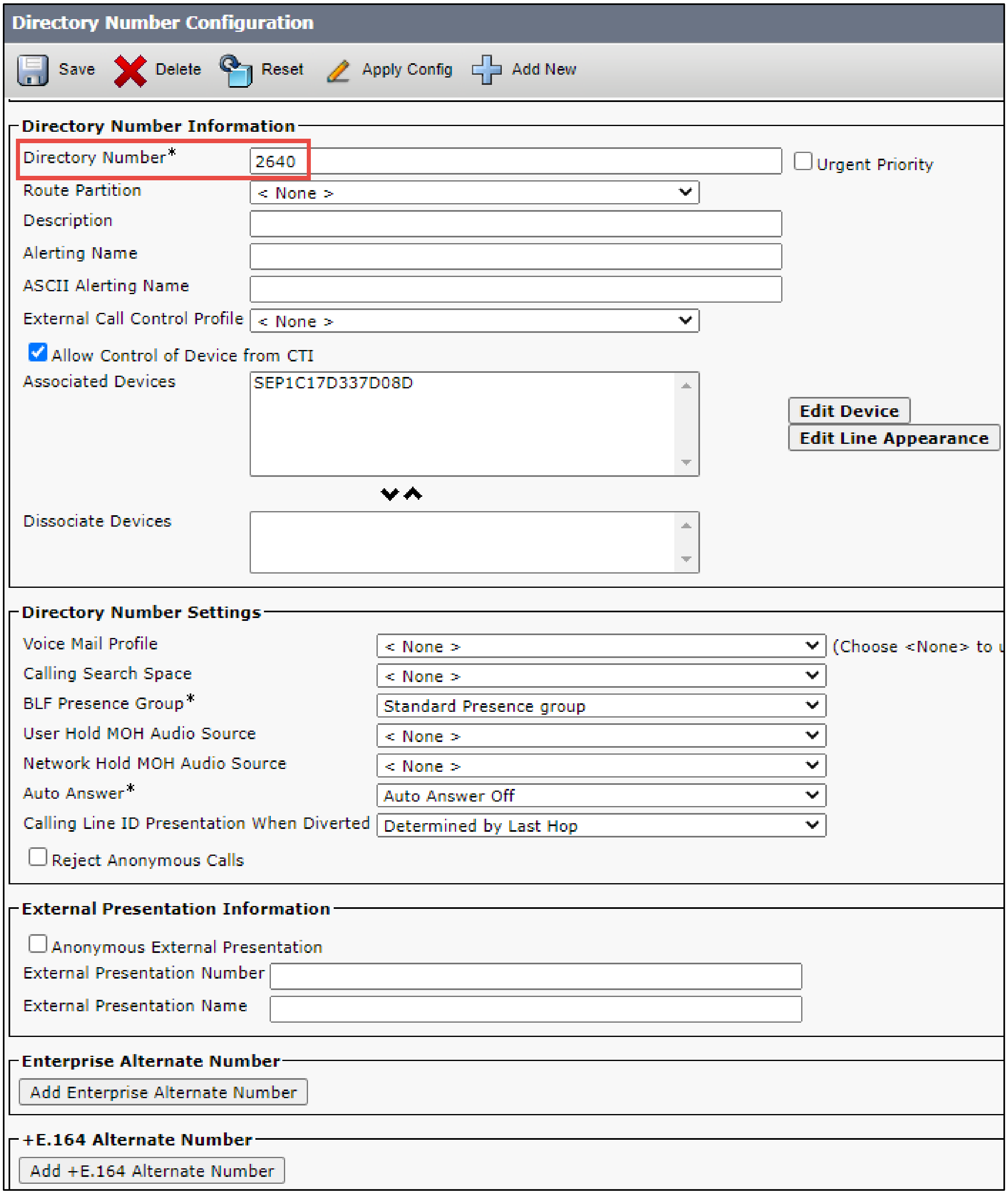
Assign a Directory Number to the Cisco PBX phone.

1. From the Cisco PBX Phone Configuration, (**Device->Phone).**
2. Click on **Add a new DN.**
3. **Directory Number: 2640** is configured for the Cisco 9971 SIP Phone
4. The 10 Digit DID is entered for the **Display (Caller ID), ASCII Display (Caller ID)** and the **External Phone Number Mask.**

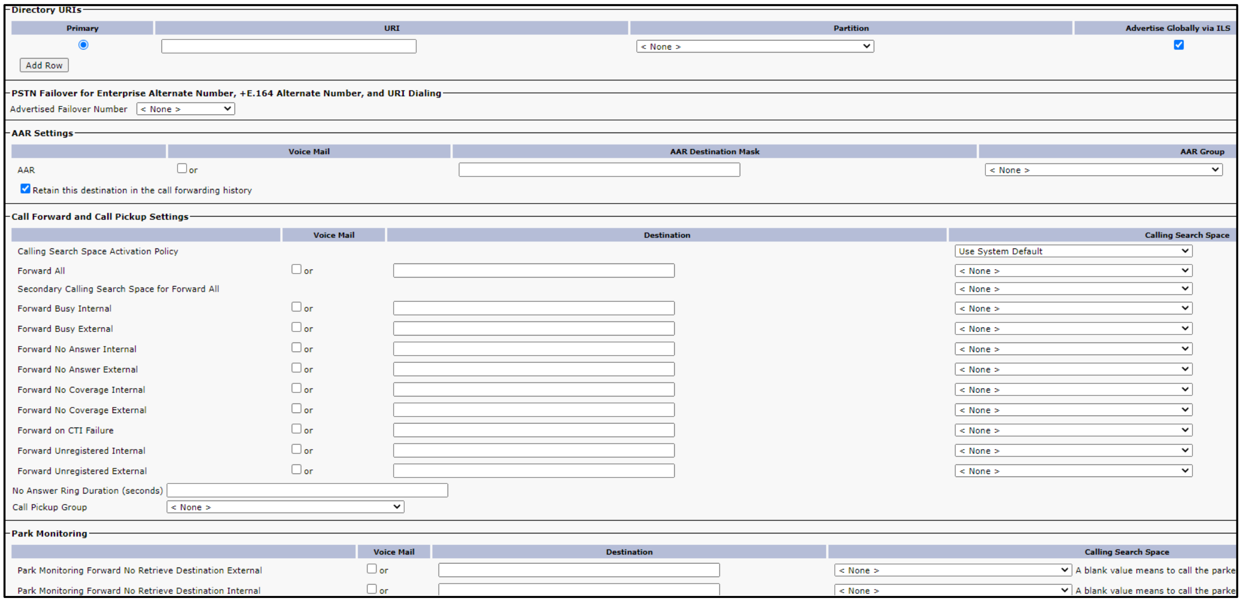
Cisco CUCM: Cisco 9971 SIP Phone Directory Number (1/5)



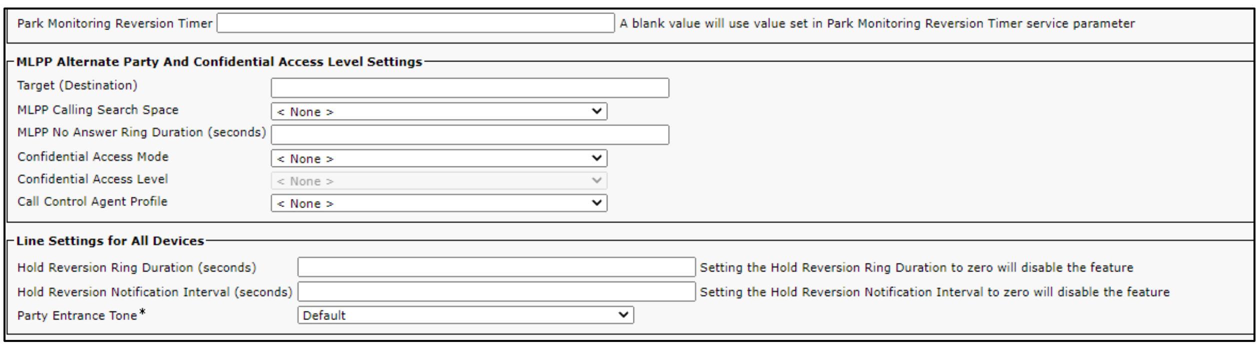
Cisco CUCM: Cisco 9971 SIP Phone Directory Number (2/5)



Cisco CUCM: Cisco 9971 SIP Phone Directory Number (3/5)



Cisco CUCM: Cisco 9971 SIP Phone Directory Number (4/5)



Cisco CUCM: Cisco 9971 SIP Phone Directory Number (5/5)

Line 1 on Device SEP1C17D337D08D

Display (Caller ID)	972[redacted]2640 the [redacted]r.	Display text for a line appearance is intend
ASCII Display (Caller ID)	972[redacted]2640	
Line Text Label		
External Phone Number Mask	972[redacted]2640	
Visual Message Waiting Indicator Policy*	Use System Policy	
Audible Message Waiting Indicator Policy*	Default	
Ring Setting (Phone Idle)*	Use System Default	
Ring Setting (Phone Active)	Use System Default	Applies to this line when any line on the phone has a
Call Pickup Group Audio Alert Setting(Phone Idle)	Use System Default	
Call Pickup Group Audio Alert Setting(Phone Active)	Use System Default	
Recording Option*	Call Recording Disabled	
Recording Profile	< None >	
Recording Media Source*	Gateway Preferred	
Monitoring Calling Search Space	< None >	

☑ Log Missed Calls

Multiple Call/Call Waiting Settings on Device SEP1C17D337D08D

Note:The range to select the Max Number of calls is: 1-200

Maximum Number of Calls*	4	
Busy Trigger*	2	(Less than or equal to Max. Calls)

Forwarded Call Information Display on Device SEP1C17D337D08D

☐ Caller Name
☐ Caller Number
☐ Redirected Number
☐ Dialed Number

Users Associated with Line

Associate End Users

Save | Delete | Reset | Apply Config | Add New

Media Resource Group and Media Resource Group List

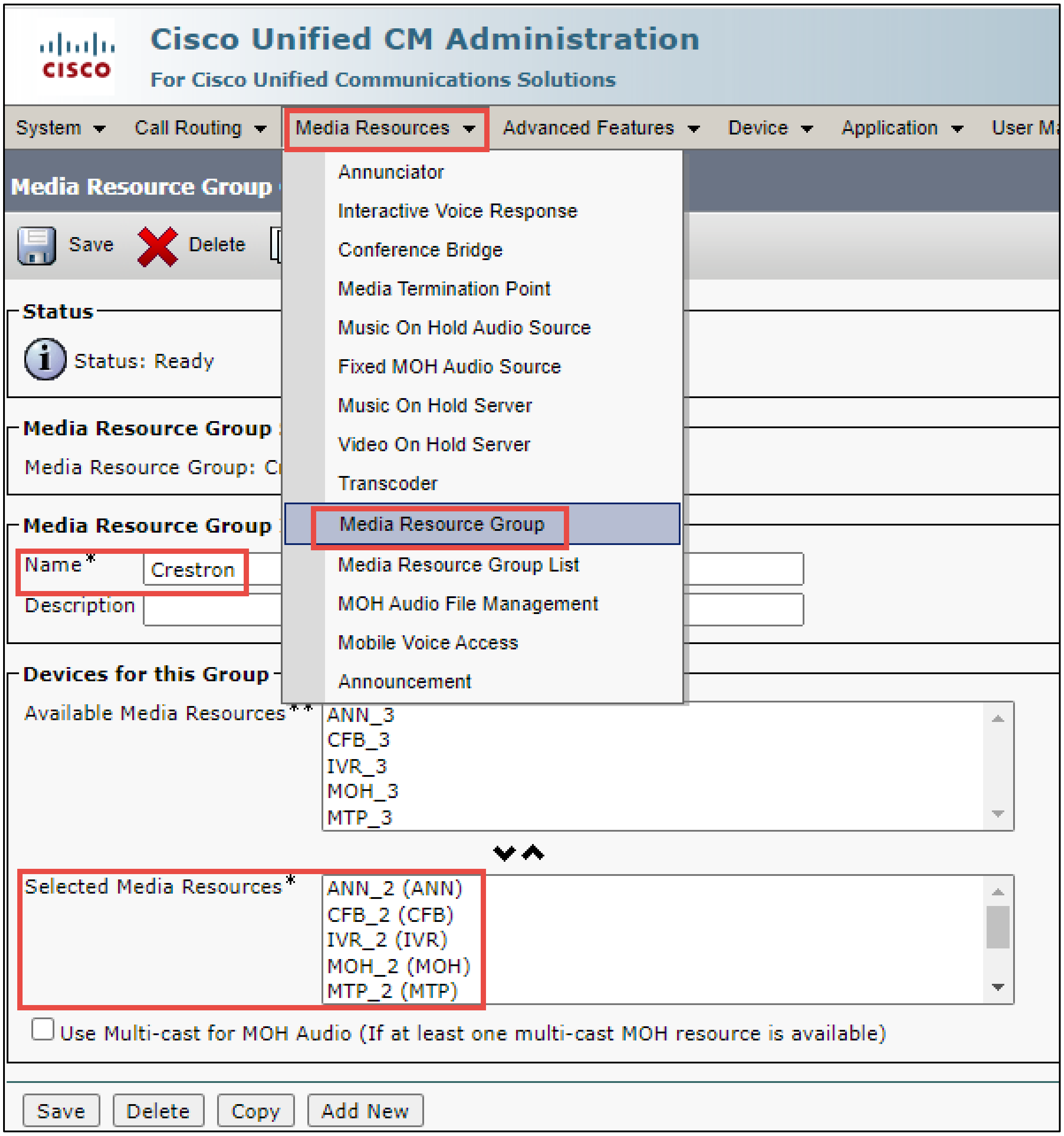
A Media Resource Group and Media Resource Group List are required to include Music on Hold, (MOH) servers Conference Bridges and Media Termination Points that may be required for the Cisco CUCM MOH features.

Media Resource Group

Media Resource Group "**Crestron**" is configured for the MOH features.

1. Navigate to **Media Resources** -> **Media Resource Group**.
2. Select **Add New**.
3. Provide a **Name**: **Crestron**.
4. Move the Media Resources from the **Available Media Resources** box to the **Selected Media Resources** box. (These are assumed to have been added earlier and are available for use /registered with this Cisco CUCM).
    a. **ANN_2 (ANN)**
    b. **CFB_2 (CFB)**
    c. **IVR_2 (IVR)**
    d. **MOH_2 (MOH)**
    e. **MTP_2 (MTP)**
    f. **SRTP-MTP (MTP)**
    g. **XCoder (XCODE)**
    h. **Crestron (CFB)**
5. Click **Save.**

Cisco CUCM: Media Resource Group

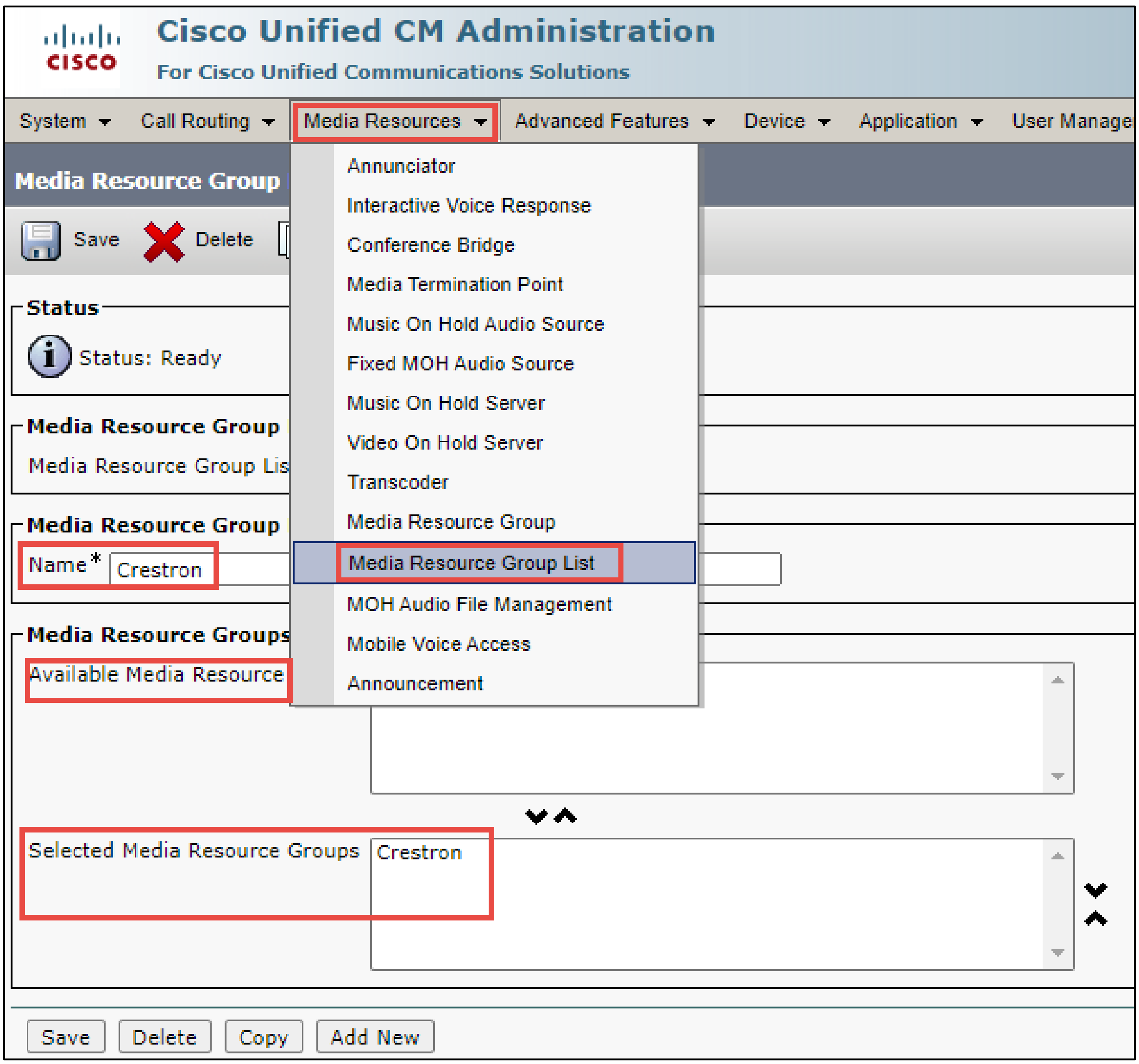


Media Resource Group List

Media Resource Group List "**Crestron**" is configured for the MOH features.

1. Navigate to **Media Resources** -> **Media Resource Group List.**
2. Select **Add New**.
3. Provide a **Name: Crestron**
4. Move the **Crestron** Media Resource Group from the **Available Media Resource Groups** box to the **Selected Media Resource Groups** box.
5. Click **Save.**

Cisco CUCM: Media Resource Group



Trunks

Two trunks were configured.

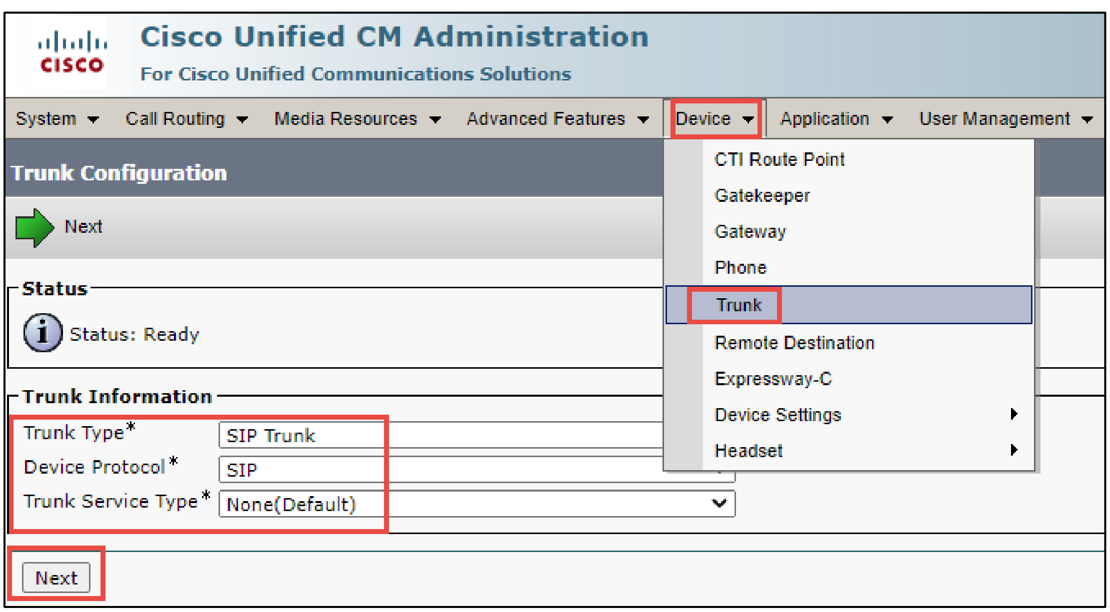
- Between the Cisco CUCM and the PSTN Gateway for calls to and from the PSTN.
- Between the Cisco CUCM and Cisco Unity Connection for Voicemail.

PSTN Gateway <-> Cisco CUCM Trunk

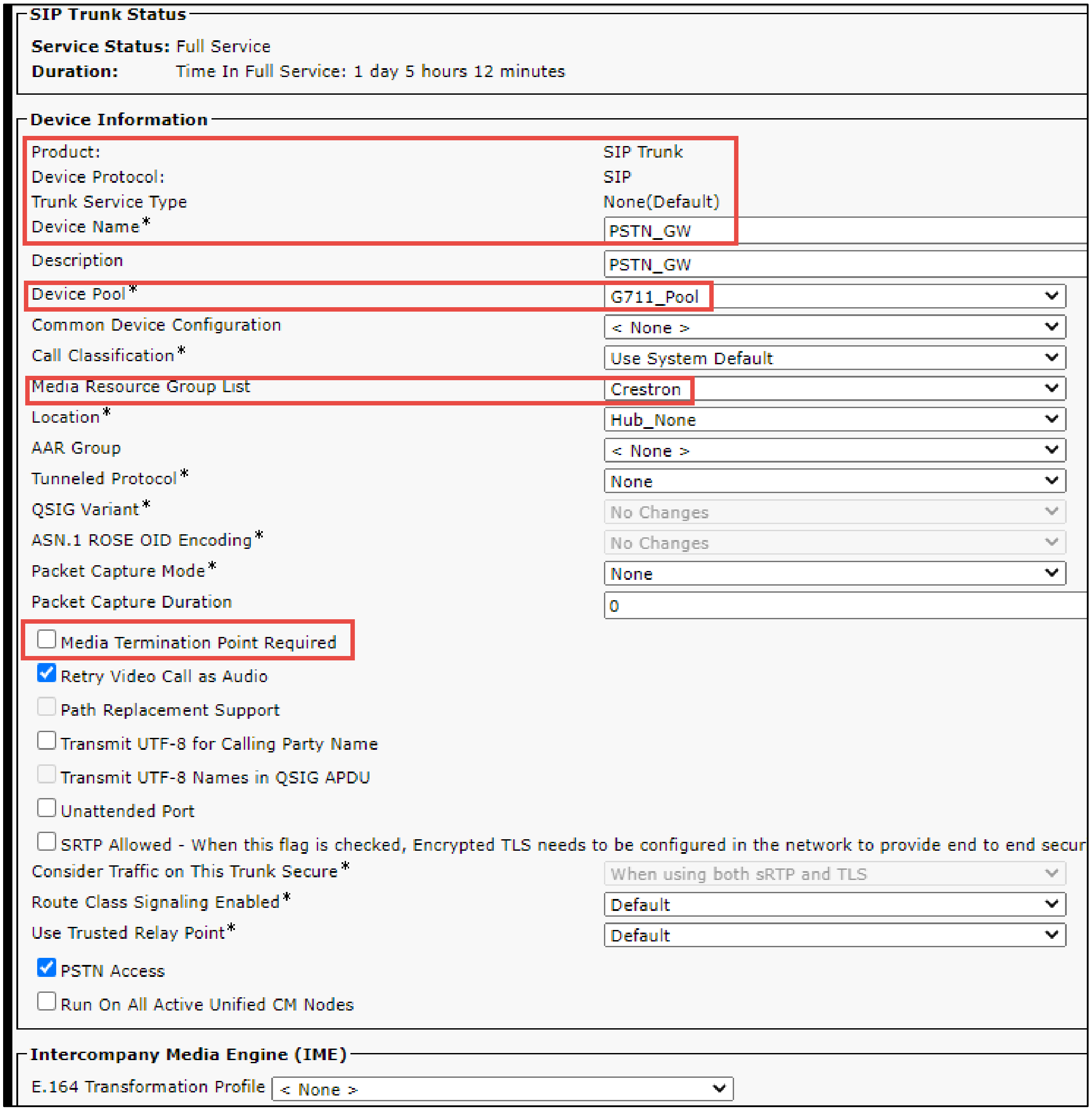
For the connection between the Cisco CUCM and the PSTN Gateway a Trunk is created.

1. Navigate to **Device** ->**Trunk**.
2. Click **Add New**.
3. **Trunk Type** as **SIP Trunk** , **Device Protocol** as **SIP** and **Trunk Service Type** as **None(Default)**
4. Click **Next**.
5. **Device Name** – ***PSTN*_GW.**
6. **Device Pool - *G711_Pool*.**
7. **Media Resource Group List**, select **Crestron**.
8. Ensure that the **Media Termination Point Required** is unchecked.
9. **Significant Digits**: set to **4**
10. Select the **Redirecting Diversion Header Delivery – Inbound** check box.
11. Select the **Redirecting Diversion Header Delivery – Outbound** check box.
12. **SIP Information** - Destination Address "**10.64.1.72**" and port "**5060**" of the PSTN Gateway.
13. Select the **Non Secure SIP Trunk Profile** as the SIP Trunk Security Profile.
14. Select the configured **Standard SIP Profile** SIP Profile.
15. Click **Save**.

Cisco CUCM: PSTN Gateway Trunk (1/5)



Cisco CUCM: PSTN Gateway Trunk (2/5)



SIP Trunk Status

Service Status: Full Service
Duration: Time In Full Service: 1 day 5 hours 12 minutes

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	PSTN_GW
Description	PSTN_GW
Device Pool*	G711_Pool
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	Crestron
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

- [ ] Media Termination Point Required
- [x] Retry Video Call as Audio
- [ ] Path Replacement Support
- [ ] Transmit UTF-8 for Calling Party Name
- [ ] Transmit UTF-8 Names in QSIG APDU
- [ ] Unattended Port
- [ ] SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end secur

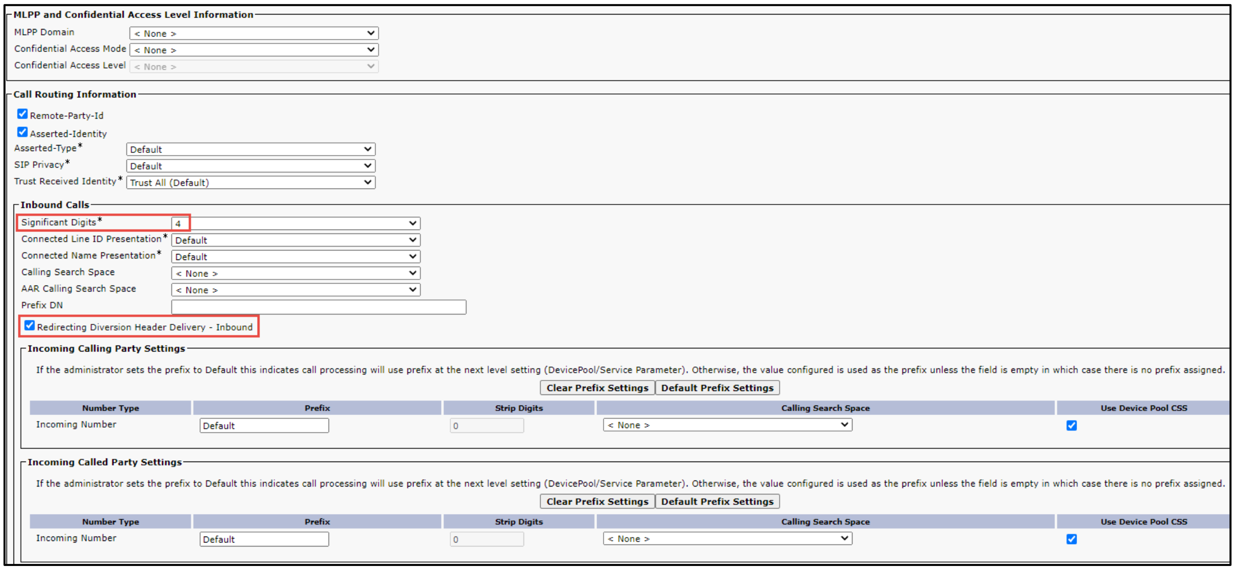
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

- [x] PSTN Access
- [ ] Run On All Active Unified CM Nodes

Intercompany Media Engine (IME)

E.164 Transformation Profile	< None >

Cisco CUCM: PSTN Gateway Trunk (3/5)



MLPP and Confidential Access Level Information
MLPP Domain < None >
Confidential Access Mode < None >
Confidential Access Level < None >

Call Routing Information
Remote-Party-Id
Asserted-Identity
Asserted-Type* Default
SIP Privacy* Default
Trust Received Identity* Trust All (Default)

Inbound Calls
Significant Digits* 4
Connected Line ID Presentation* Default
Connected Name Presentation* Default
Calling Search Space < None >
AAR Calling Search Space < None >
Prefix DN
Redirecting Diversion Header Delivery - Inbound

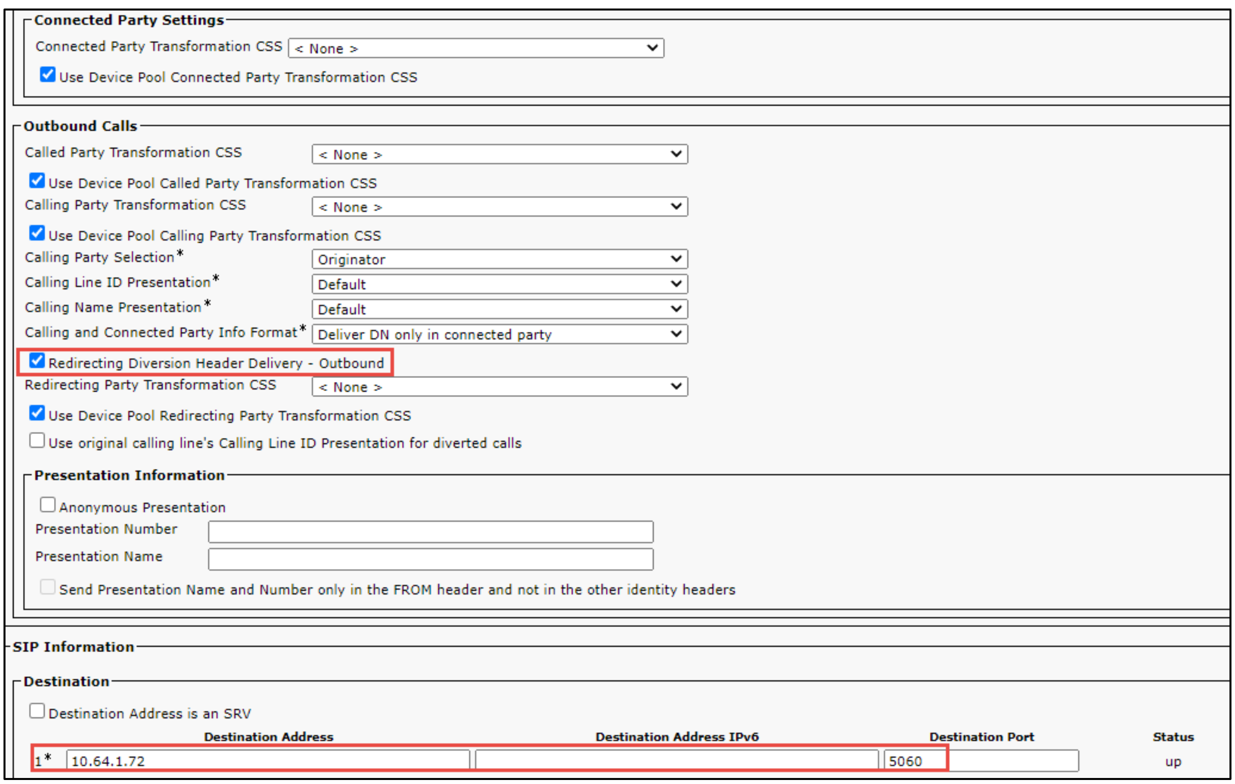
Incoming Calling Party Settings
If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.
Clear Prefix Settings | Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default	0	< None >	☑

Incoming Called Party Settings
If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.
Clear Prefix Settings | Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default	0	< None >	☑

Cisco CUCM: PSTN Gateway Trunk (4/5)



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
Use original calling line's Calling Line ID Presentation for diverted calls

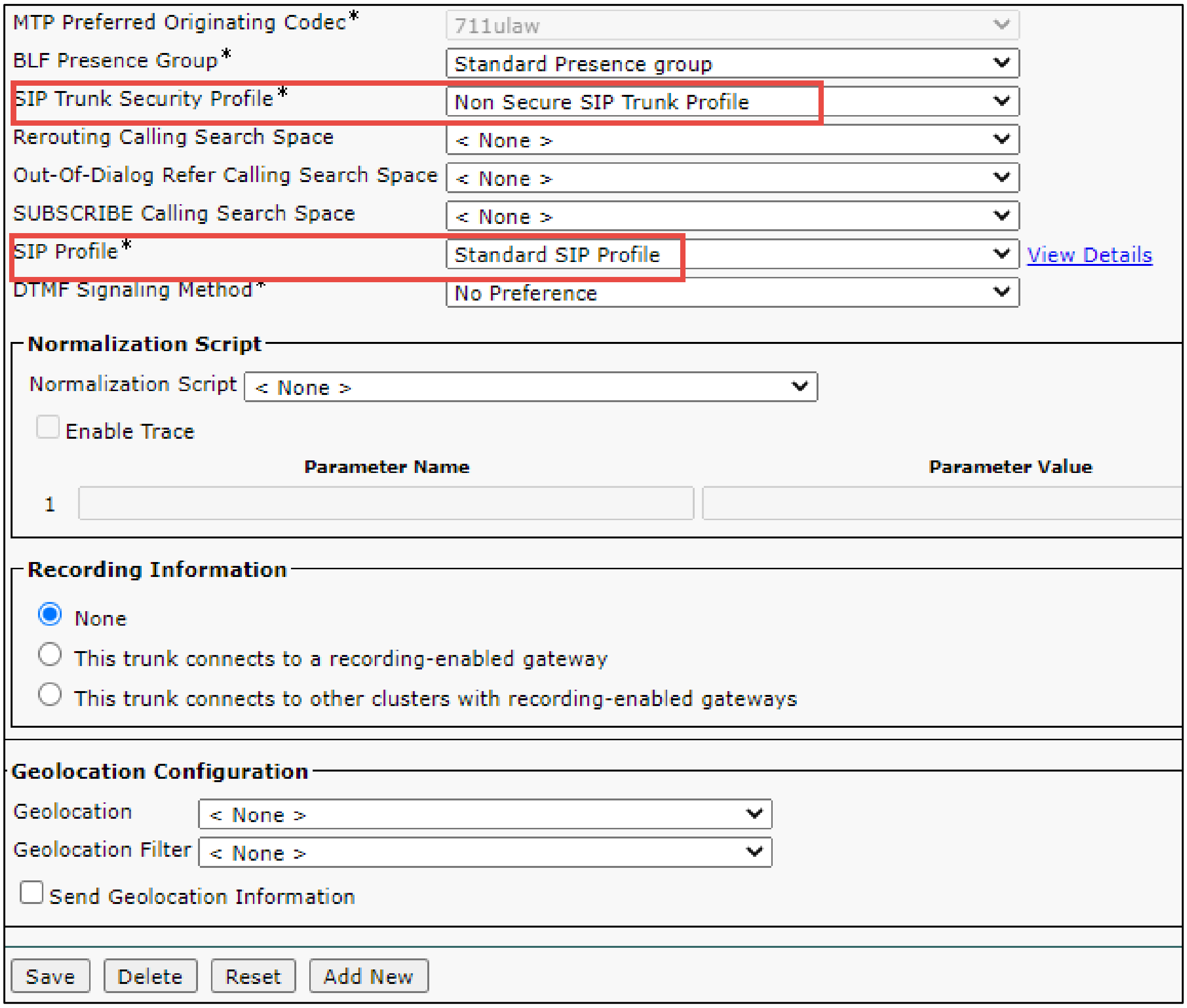
Presentation Information
Anonymous Presentation
Presentation Number
Presentation Name
Send Presentation Name and Number only in the FROM header and not in the other identity headers

SIP Information

Destination
Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status
1*	10.64.1.72		5060	up

Cisco CUCM: PSTN Gateway Trunk (5/5)

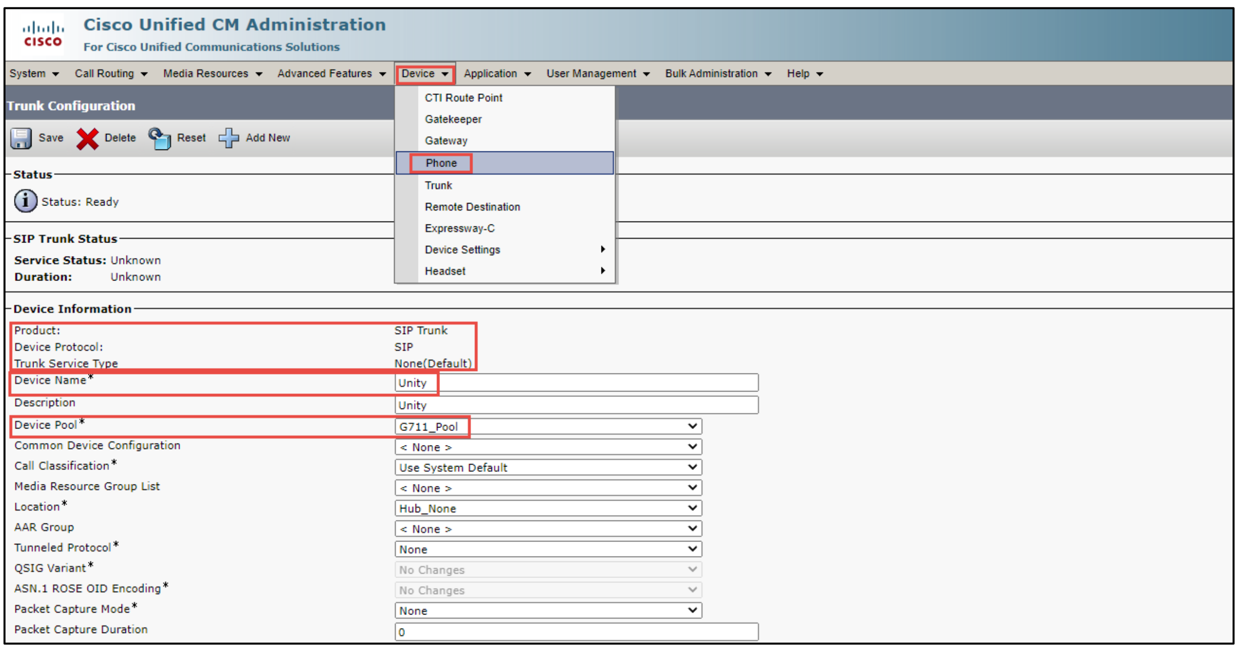


Cisco CUCM <–> Cisco Unity Connection Trunk

For the connection between the Cisco CUCM and the Cisco Unity Connection, a Trunk is created.

1. Navigate to **Device** ->**Trunk**.
2. Click **Add New**.
3. **Trunk Type** as **SIP Trunk** , **Device Protocol** as **SIP** and **Trunk Service Type** as **None(Default)**
4. Click **Next**.
5. **Device Name** – ***Unity*.**
6. **Device Pool -** ***G711_Pool***.
7. **SIP Information** - Destination Address “**10.64.1.72**” and port “**5060**” of the PSTN Gateway.
8. Select the **Non Secure SIP Trunk Profile** as the SIP Trunk Security Profile.
9. Select the configured **Standard SIP Profile** SIP Profile.
10. Click **Save**.

Cisco CUCM: Cisco Unity Connection Trunk (1/4)



CRESTRON® tekVizion™

Cisco CUCM: Cisco Unity Connection Trunk (2/4)

- [ ] Media Termination Point Required
- [x] Retry Video Call as Audio
- [ ] Path Replacement Support
- [ ] Transmit UTF-8 for Calling Party Name
- [ ] Transmit UTF-8 Names in QSIG APDU
- [ ] Unattended Port
- [ ] SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure t

Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

- [ ] PSTN Access
- [ ] Run On All Active Unified CM Nodes

Intercompany Media Engine (IME)

E.164 Transformation Profile	< None >

MLPP and Confidential Access Level Information

MLPP Domain	< None >
Confidential Access Mode	< None >
Confidential Access Level	< None >

Call Routing Information

- [ ] Remote-Party-Id
- [x] Asserted-Identity

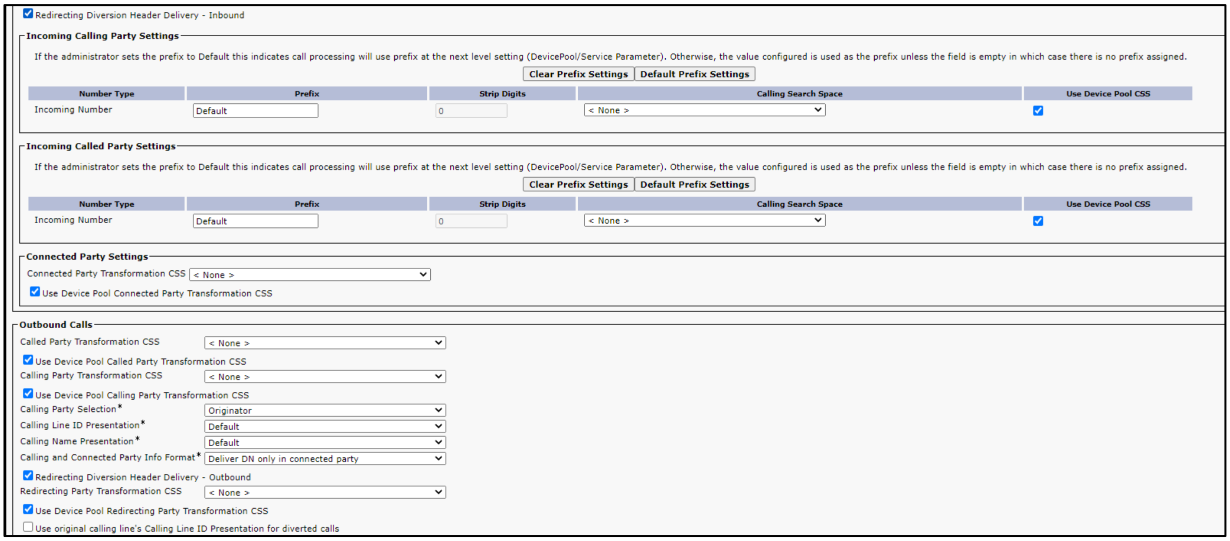
Asserted-Type*	Default
SIP Privacy*	Default
Trust Received Identity*	Trust All (Default)

Inbound Calls

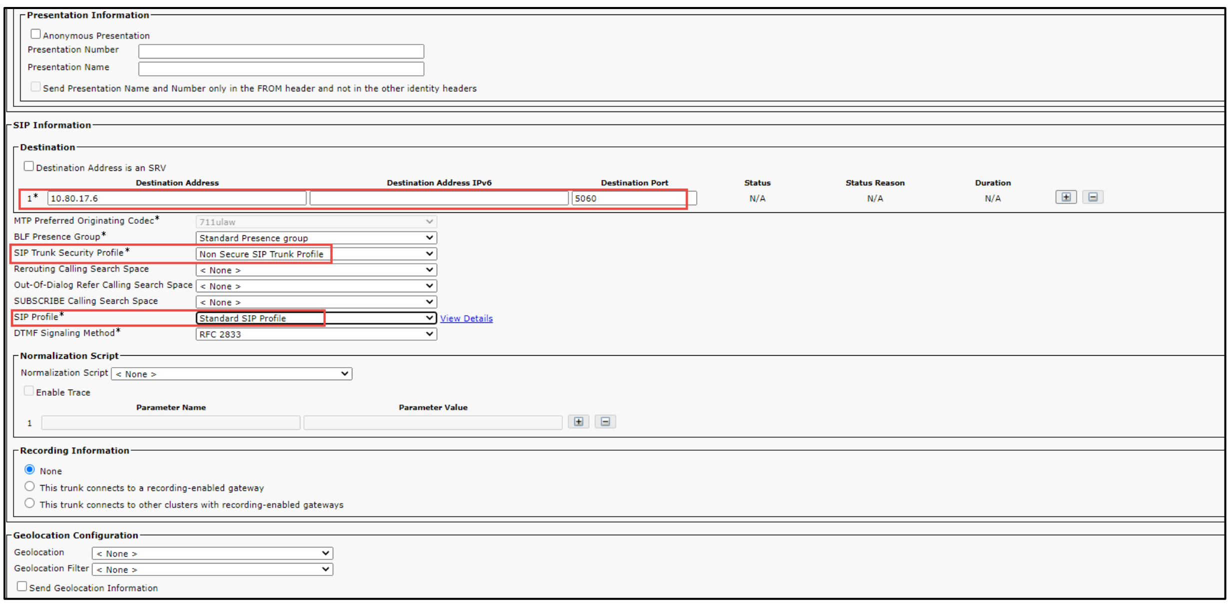
Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	

- [x] Redirecting Diversion Header Delivery - Inbound

Cisco CUCM: Cisco Unity Connection Trunk (3/4)



Cisco CUCM: Cisco Unity Connection Trunk (4/4)



Route Patterns

Route patterns were configured for the following:

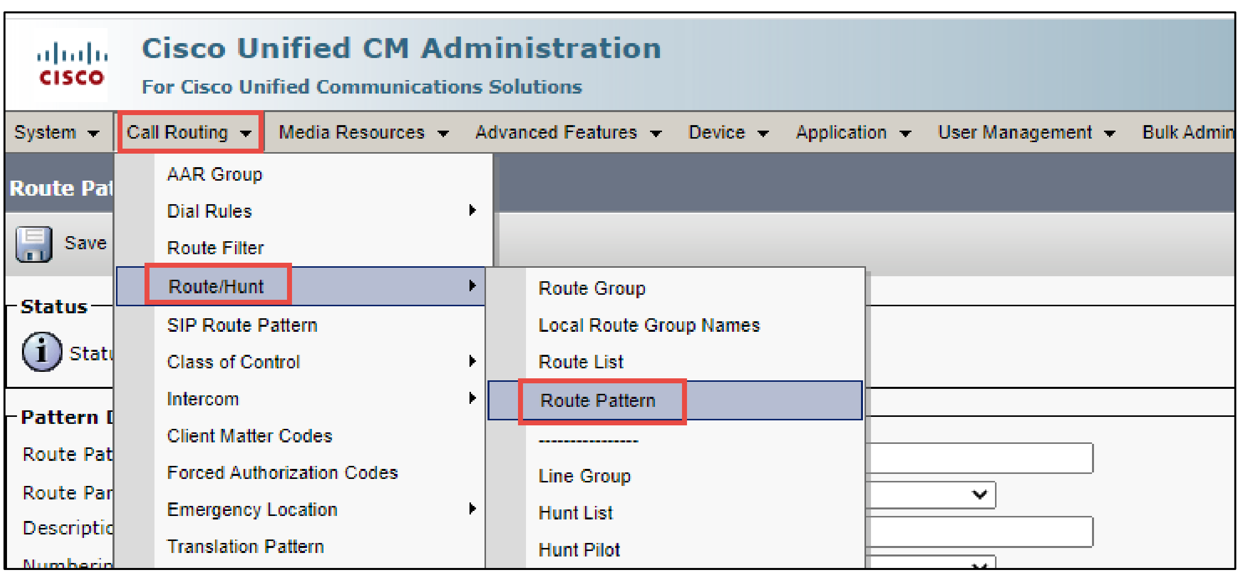
- To route calls from the Cisco CUCM to the PSTN.
- To restrict caller id on outgoing calls.
- To access the voicemail system.

PSTN Access - 7.@

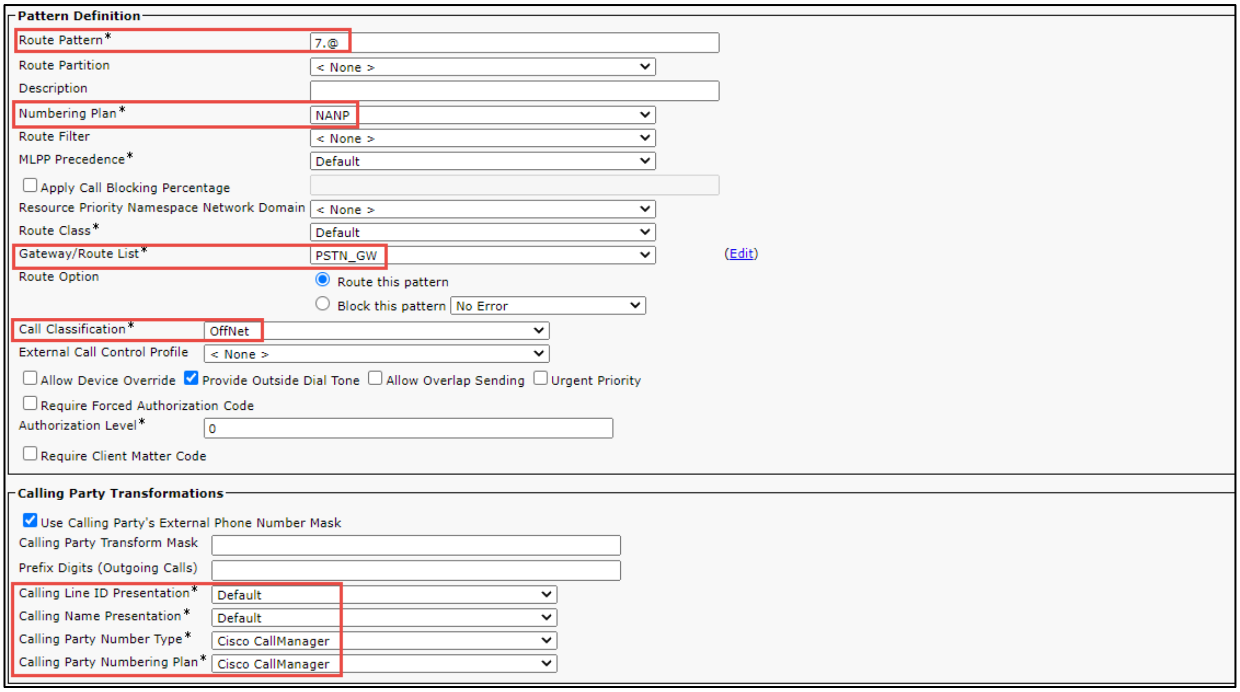
The route pattern **7.@** is used to enable outbound dialing from the phones to PSTN using the access code "**7**", before dialing the phone number.

1. Navigate to **Call Routing -> Route/Hunt-> Route Pattern**
2. **Add New**
3. **Route Pattern – 7.@**
4. **Numbering Plan – NANP**
5. **Gateway/Route List – PSTN_GW**
6. **Call Classification – OffNet**
7. **Calling Line ID Presentation – Default**
8. **Calling Name Presentation – Default**
9. **Calling Party Number Type – Cisco CallManager**
10. **Calling Party Numbering Plan – Cisco CallManager**
11. **Discard Digits - PreDot**

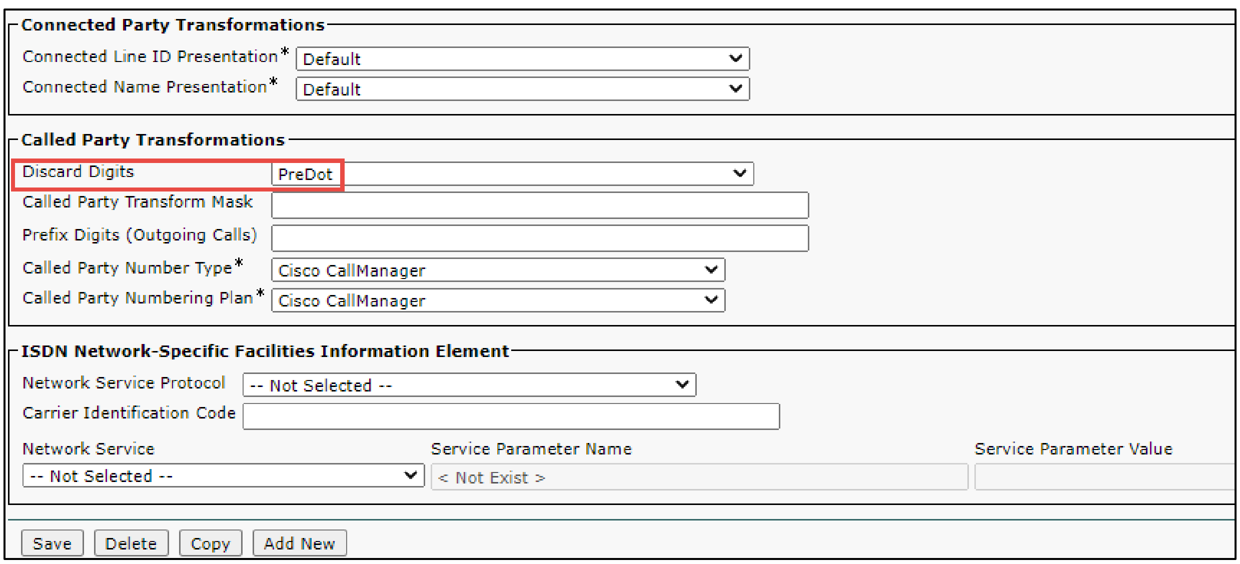
Cisco CUCM: PSTN Route Pattern (1/3)



Cisco CUCM: PSTN Route Pattern (2/3)



Cisco CUCM: PSTN Route Pattern (3/3)

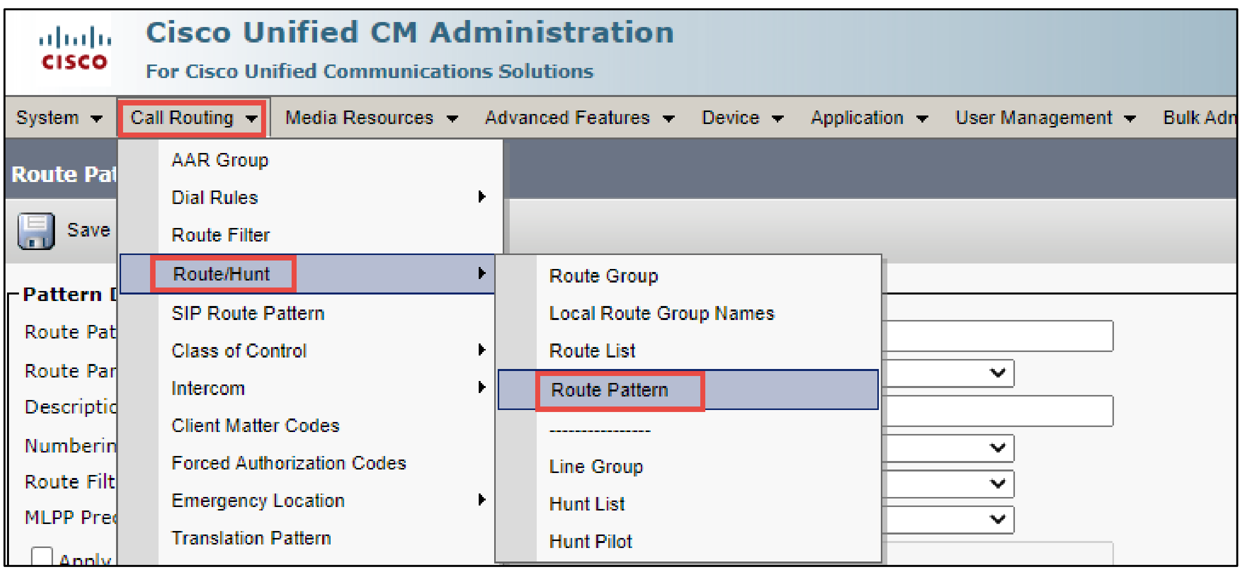


Restrict Outbound Caller ID - 767.@

The route pattern of **767.@** is used to restrict caller id on outbound calls to the PSTN using the access code "**767**", before dialing the phone number.

1. Navigate to **Call Routing -> Route/Hunt-> Route Pattern**
2. **Add New**
3. **Route Pattern – 767.@**
4. **Numbering Plan – NANP**
5. **Gateway/Route List – PSTN_GW**
6. **Call Classification – OffNet**
7. **Calling Line ID Presentation – Restricted**
8. **Calling Name Presentation – Restricted**
9. **Discard Digits - PreDot**

Cisco CUCM: Caller ID Restricted PSTN Route Pattern (1/3)



Cisco CUCM: Caller ID Restricted PSTN Route Pattern (2/3)

Route Pattern Configuration

Save

Pattern Definition

Route Pattern*	767.@
Route Partition	< None >
Description	PSTN Restricted Call
Numbering Plan*	NANP
Route Filter	< None >
MLPP Precedence*	Default
☐ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	PSTN_GW (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 CUCM: Caller ID Restricted PSTN Route Pattern (3/3)

Calling Party Transformations

☐ Use Calling Party's External Phone Number Mask

Calling Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Calling Line ID Presentation*	Restricted
Calling Name Presentation*	Restricted
Calling Party Number Type*	Cisco CallManager
Calling Party Numbering Plan*	Cisco CallManager

Connected Party Transformations

Connected Line ID Presentation*	Default
Connected Name Presentation*	Default

Called Party Transformations

Discard Digits	PreDot
Called Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Called Party Number Type*	Cisco CallManager
Called Party Numbering Plan*	Cisco CallManager

ISDN Network-Specific Facilities Information Element

Network Service Protocol	-- Not Selected --
Carrier Identification Code	

Network Service	Service Parameter Name	Service Parameter Value
-- Not Selected --	< Not Exist >	

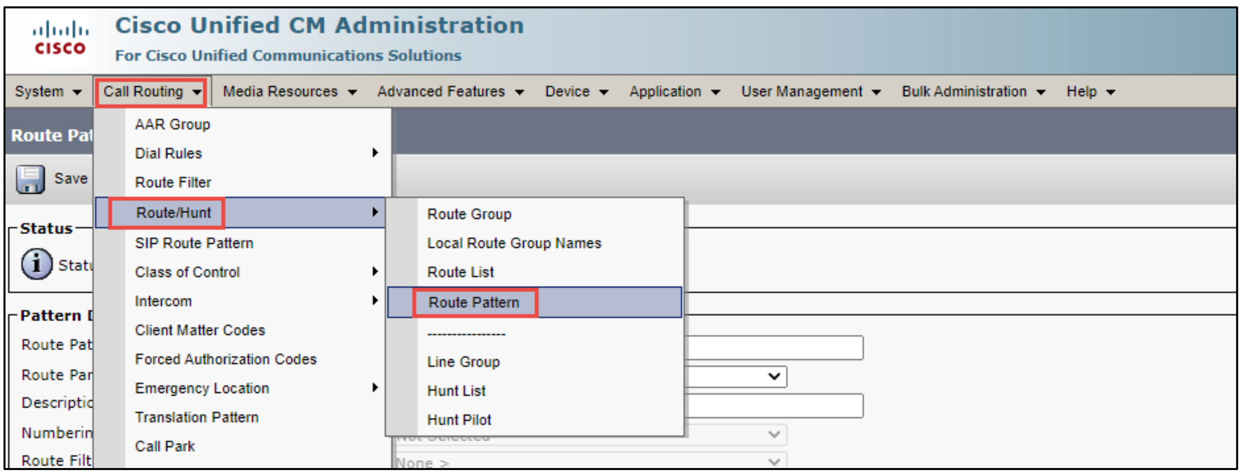
Save

Voicemail Access - 5555

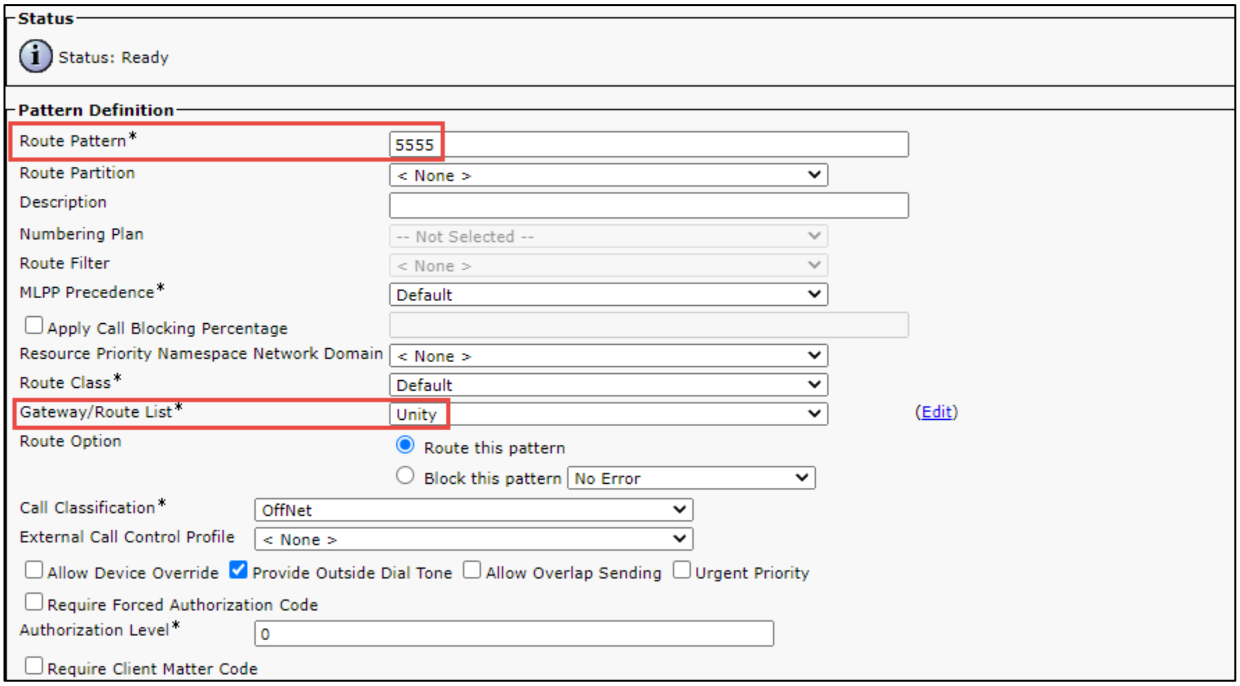
Route pattern **5555** is used to route the voice mail pilot number 5555 to the Cisco Unity Connection server.

1. Navigate to **Call Routing -> Route/Hunt-> Route Pattern**
2. **Add New**
3. **Route Pattern – 5555**
4. **Gateway/Route List – Unity**

Cisco CUCM: Cisco Unity Connection Route Pattern (1/3)



Cisco CUCM: Cisco Unity Connection Route Pattern (2/3)



Cisco CUCM: Cisco Unity Connection Route Pattern (3/3)