DSP-1282 & DSP-1283
Crestron Avia™ DSP with Cisco® Unified Communications Manager 11.5 (Secure)

Configuration Guide

Crestron Electronics, Inc.

The product warranty can be found at www.crestron.com/warranty.

The specific patents that cover Crestron products are listed at patents.crestron.com.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/opensource.

Contents

DSP-1282 & DSP-1283: SIP Endpoint with Cisco® Unified Communications Manager 11.5 (Secure)

Introduction

This configuration guide describes the procedures required to configure Crestron Avia™ Digital Signal Processor (DSP) devices in a secure mode. The devices operate on the Cisco® Unified Communications Manager (UCM) as Assured Service Session Initiation Protocol (AS-SIP) endpoints .

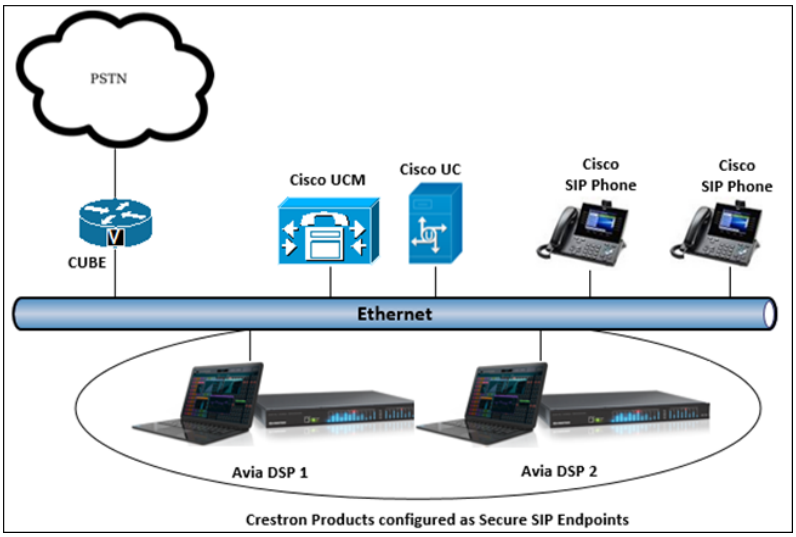
Audience

The intended audience includes those attempting to configure and use Crestron Avia DSP devices as secure SIP endpoints registered to the Cisco Unified Communications (Cisco UCM).

Topology

The diagram below shows the network topology for integration of a Crestron Avia DSP endpoint with the Cisco UCM.

Secure SIP Endpoint Integration with Cisco UCM - Reference Network



The lab network consists of the following components:

- Cisco UCM cluster for voice features
- Cisco SIP phones
- Crestron DSP as the secure SIP endpoint
- Cisco Unified Border Element (UBE) to ensure secure signaling and media within the enterprise for Public Switched Telephone Network (PSTN) calls

Software Requirements

- Cicso Unified Communications Manager v11.5.1.13902-2
- Cisco Unity Connection v 11.0.1.20000-2
- Cisco Unified Border Element v15.7(3)M
- Crestron Avia DSP devices v1.00.251.000

Hardware Requirements

- Cisco UCS-C240-M3S VMWare Host running ESXi 5.5
- Cisco 3845 as PSTN gateway
- Cisco UBE as a Session Border Controller (SBC)
- Cisco Phones: models - 9951 (SIP), 9971 (SIP)
- Crestron Avia DSP devices (2)

Product Description

The Crestron Avia DSP products (DSP-1282 and DSP-1283, specifically) consist of a family of programmable digital audio signal processors intended for the commercial sound market. Each version provides 12 analog mic/line inputs and eight analog line outputs. The devices include a Local Area Network (LAN) connection and a Universal Serial Bus (USB) connection for programming and control. The programmable signal flow is a fixed topology with user-configurable input and output processing chains using a library of preset signal-specific DSP blocks.

Use the Crestron Avia too to:

- Discover the device on the network
- Configure the SIP parameters
- Configure the mixers to allow 2-way communication on a SIP call

Save the audio configuration along with the SIP configuration as a project file. The project file can be loaded onto all of the DSPs that receive similar settings on a given project. Minor modifications may be necessary.

Use the Crestron Toolbox™ software to discover and control all Crestron devices on the network.

During the integration test, Crestron Toolbox can:

- Discover devices on the network
- Console connect to the devices
- Configure the Ethernet settings
- Upgrade firmware

Summary

This document describes how to configure the Crestron Avia DSP devices in secure mode on the Cisco UCM as AS-SIP endpoints. It also provides information on how to register devices to the Cisco UCM with digest authentication.

Supported features include:

- Secure mode: establishing a secure SIP and Secure Real-Time Transport Protocol (SRTP) session with the Cisco UCM
- Registration with digest authentication
- Basic calls with G711Ulaw, G711Alaw, and G729 codecs
- Dual-Tone Multi-Frequency (DTMF) support
- Early media support
- Retrieval of a parked call
- Transferee in a call transfer
- Conference participant
- Member of hunt group

Unsupported features include:

- Calls with non-secure (Real-time Transport Protocol (RTP) only) devices
- Codec G722
- Caller ID presentation with name and number display
- Call hold and resume
- Call forwarding on the device (forwarding can be configured on the Private Branch Exchange (PBX) for the Domain Name (DN) assigned to the endpoint)
- Call waiting
- Initiating a conference
- Initiating call transfer
- Shared line
- Initiating call park

Known issues and limitations include:

- The device under test (DUT) configured with static Internet Protocol (IP) network setting (Domain name System (DNS) server field) failed to perform name resolution and therefore, failed to validate the certificate during the Transport Layer Security (TLS) handshake. The device Linux file did not contain the assigned DNS server setting. This issue was tracked via Bugzilla™ software defect: 143019.
- The DUT involved in a G729 negotiated call contained audio with a garbled voice. This issue was tracked via Bugzilla defect: 141481.
- The DUT did not play Music on Hold (MoH) when a Cisco UCM phone placed the call on hold. The Cisco UCM sent an MOH stream after acknowledgement (ACK) from the Session Description Protocol (SDP), but DSP did not play it. This issue was tracked via Bugzilla defect: 116049.
- The DUT did not play MOH/ringback while an unattended call transfers from the Cisco UCM phone. Transfer worked fine and heard two-way audio. This issue was tracked via Bugzilla defect: 146058.
- DTMF digits pressed on the DUT during a call with an Interactive Voice Response (IVR) produced duplicate entries. This issue was tracked via Bugzilla defect: 143570.

Crestron Avia DSP Configuration

This section provides the following details:

- How to set up connections to the amplifier and speaker
- How to access the DSP on the network (once powered)
- How to configure the DSP for registration and integration with the PBX

Connections

Make the following connections:

- Connect microphone to DSP MIC/LINE INPUTS port 1
- Connect DSP LINE OUTPUTS port 1 to "Audio In" on amplifier
- Connect "Audio Out" of amplifier to speaker
- Connect LAN port to network

Device Discovery/Access

Use the Crestron Toolbox and the Crestron Avia tool to discover and access the connected LAN and/or VOIP ports) DSP devices.

Use the Help menu to assist when performing the discovery and configuration procedure.

Set Up SIP Interface and Routes

The DSP units have separate network interfaces for Voice over Internet Protocol (VoIP) and LAN on the rear panel. Configure either one for SIP calling. The default configuration binds SIP calling to the LAN interface. An optional console command binds the SIP interface to the VoIP connector. Configure all VoIP connections on a separate Virtual Local Area Network (VLAN) or subnet. VoIP connections cannot be on the same subnet as the LAN connection.

Ethernet

Use the **Ethernet** command to turn the VoIP port on/off.

```
DSP-1281>Ethernet ?
ETHERNET [<device_num> ON | OFF [/now]]
Device_num - 0  n
ON - enables VoI
OFF - disables VoIP
/now - take effect without a reboot
No parameter - displays the current setting
```

The VoIP port is off by default. The LAN port is not selectable.

```
<device_num> = 0 selects the LAN port
<device_num> = 1 selects the VoIP port
```

SIP Interface

Use the **sipinterface** command to bind all SIP activity, data, and traffic to the selected port. If a VLAN or exclusive VoIP network is available, bind to the VoIP port (recommended).

```
DSP-1281>sipinterface ?
Get or Set SIP Interface
SIPINTERFACE [LAN | VOIP]
LAN - normal LAN port
VOIP - VOIP port
No Parameter - Displays current setting
```

Routes

If the configured VoIP port is the SIP interface, add a static route to ensure that all SIP routing is via the VoIP port.

The following console commands (**routeadd**, **routedel**, **routeprint**, and **routetrace**) support the static IP routing configuration:

```
DSP-1282>routeadd ?
ROUTEADD <destination> <netmask> <gateway> [/FORCE]
   destination - destination IP address in dot decimal notation
   netmask - netmask in dot decimal notation
   gateway - gateway in dot decimal notation
   /FORCE - force to add/delete even if failed to persist to NVRAM

DSP-1282>routedel ?
ROUTEDELETE <destination> <netmask> <gateway> [/FORCE]} | </ALL>
   destination - destination IP address in dot decimal notation
   netmask - netmask in dot decimal notation
   gateway - gateway in dot decimal notation
   /FORCE - force to add/delete even if failed to persist to NVRAM
   /ALL - delete all routes from NVRAM

DSP-1282>routeprint ?
ROUTEPRINT - shows current routes

DSP-1282>routetrace ?
ROUTETRACE <IPaddress>
   IPaddress - IP address in dot decimal notation
```

Secure SIP Configuration Commands

Some of the console commands used to setup TLS on the DSP include:

`SIPTRANSPORT TLS` - enable TLS instead of TCP/UDP
`SIPSERVERPORT <port>` - to configure the SIP server port, such as 5060
`SIPTLS VSOFF` - disable SIP server certificate verification
`SIPTLS VSON` - enable SIP server certificate verification
`SIPTRUStedcas` - select/list SIP trusted Certification Authority (CA) certificates

Configure TLS Settings on the Device

Configure the following settings on the DSP console to enable TLS:

```
SIPTRANSPORT TLS
SIPSERVERPORT 5060
SIPTLS VSON
```

Device Configuration

The basic setup for a phone call requires:

- An analog input (such as from a microphone) routed out through the phone line
- Audio coming in from the phone line routed to an analog output (such as to an amplifier or speaker)

Configure the DSP Device

Use the Crestron Avia tool to select and configure the DSP device.

Input Configuration

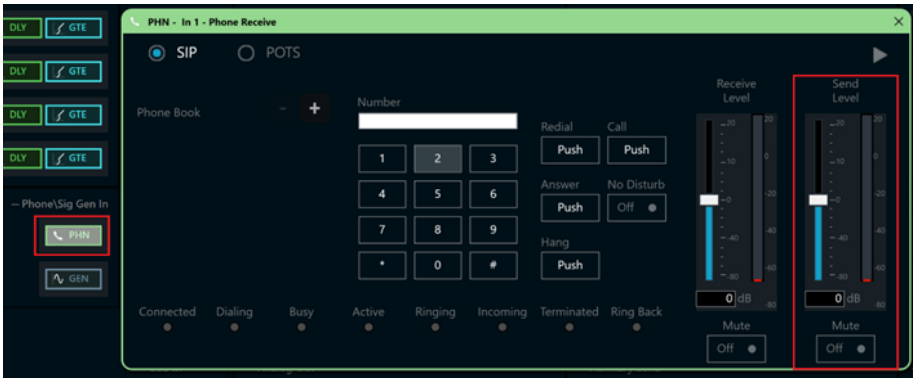
To configure the analog input:

1. Click **Signal**.
   Crestron Avia tool: Audio Input Configuration (1/4)
   

2. Under **Analog In 1** (first row), double click **Gain**. In the new window set the following:
   a. Click **Mute** to **Off**.
   b. Select **33** for the **Analog Gain**.
   c. If a condenser microphone is being used, click **+48V** (phantom power) to **On**.
   Crestron Avia Tool: Audio Input Configuration (2/4)
   

3. Under **Analog In 1** (first row), click **Ref/Phone Out** (right-most column) and enter **0** as the decibel value.
   Crestron Avia Tool: Audio Input Configuration (3/4)
   

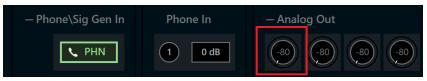
4. Under **Phone\Sig Gen In**, click **PHN**. In the new window set the following:
    a. Move the **Send Level** slider to **0 db**.
    b. Click **Mute** to **Off**.
    Crestron Avia Tool: Audio Input Configuration (4/4)



Output Configuration

To configure the analog output:

1. Under **Phone In 1** (first row), click **Analog Out** (left-most column) and enter **0** as the decibel value.
    Crestron Avia Tool: Audio Output Configuration (1/3)



2. Under **Analog Out 1**, double click **LVL**. In the new window set the following:
    a. Move the **Level** slider to **0 db**.
    b. Click **Mute** to **Off**.
    Crestron Avia Tool: Audio Output Configuration (2/3)

3. Under **Phone\Sig Gen In**, click **PHN**. In the new window set the following:
    a. Move the **Receive Level** slider to **0 db**.
    b. Click **Mute** to **Off**.

Crestron Avia Tool: Audio Output Configuration (3/3)

Configure the SIP Parameters

From the open **PHN - In 1 - Phone Receive** window, select and configure the SIP parameters.

1. With **SIP** selected, click the chevron at the right top corner to expand the window.

Crestron Avia Tool: Phone Dialer, SIP Parameters Configuration

2. Enter the extension configured on Cicso UCM for the **Local Extension** for this device. This example uses **2501**.
3. Enter the Cisco UCM PBX for the **SIP Server IP Address**. This example uses **clus35pub.skypelabsj.local**.
4. Enter the SIP server port (**5061**) for the **Port**.
5. Enter the same end user name configured for the Cisco UCM PBX for the **SIP Server User Name**. This example uses **DSP2**.
6. Enter the same password as configured for the Cisco UCM PBX end user digest credentials for the **SIP Server Password**.

Certificates

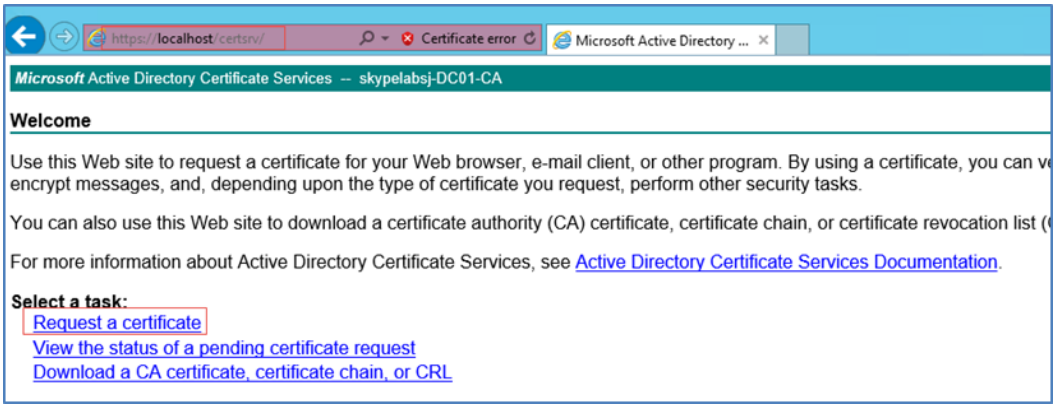
For a successful TLS handshake between the DSP device and the Cisco UCM, add the following certificates to the DSP.

- A rootCA certificate (root_cer)
  Download this certificate from the certificate authority that serves the Cisco UCM (the DNS IP configured on the Cisco UCM and Mercury device). The DSP requires the certificate to permit Cisco UCM validation, if enabled.
- A SIP certificate (sip-cert.pfx)
  Download this specific device certificate from the same certificate authority that serves the Cisco UCM. This certificate contains information on the Certificate Authority (CA) that the Cisco UCM identifies/recognizes and enables a successful TLS handshake. This certificate is a signed certificate from the CA with the signing request generated on the same CA, using a specific device certificate request with server and client authentication.

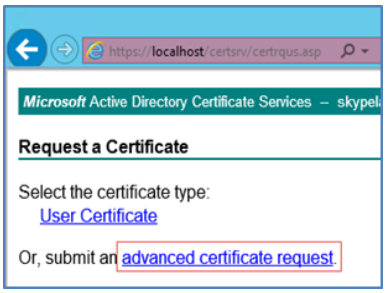
Generate Device Certificate Request and Download the Certificate

On the CA, open a browser and access the Certificate Services. This example uses a Microsoft Active Directory to generate a specific device certificate request.

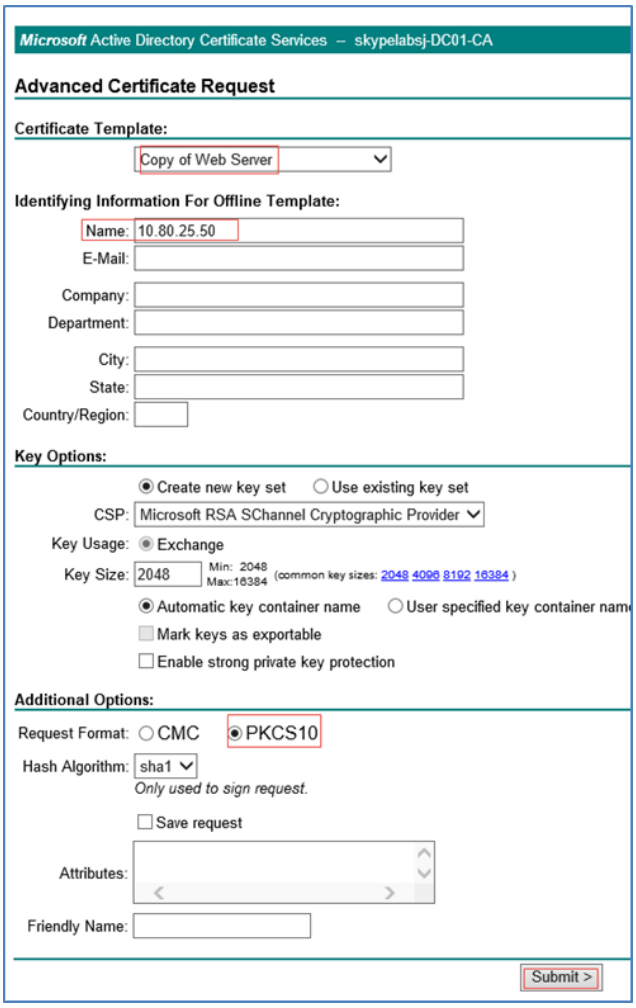
1. Click **Request a certificate**.
   Certificate Authority: Request a Certificate



2. Click **advanced certificate request**.
   Certificate Authority: Advanced Certificate Request

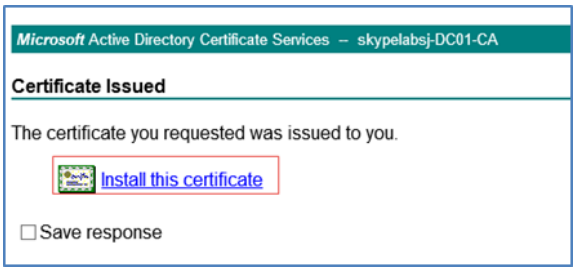


3. On the screen that follows, click **Create and Submit** a request to this CA.
Certificate Authority: Submit Device Specific Certificate Request



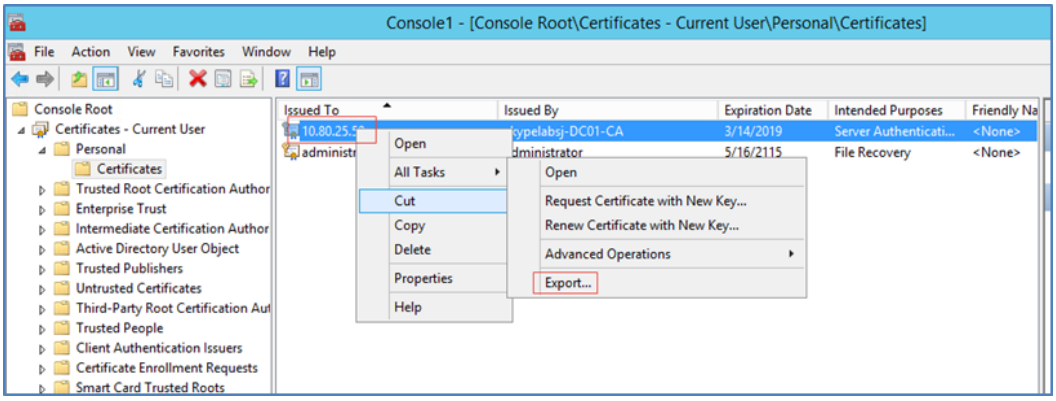
4. Select a template that does client and server authentication for the **Certificate Template**. This example uses **Copy of Web Server**.
5. In the **Identifying Information For Offline Template** section , enter the DSP device IP for the **Name**. This example uses **10.80.25.50**.
6. Click **PKCS10** for the **Request Format** (for this example) to configure additional options.
7. Click **Submit**.

8. On the screen that follows, click **Install this certificate**.
Certificate Authority: Install Certificate



Export the certificate from the certificate store as **crestron256.pfx** with the following conditions:

- Export the private key (optional)
- Save with .pfx extension
- Assign a password (same password entered when importing this SIP certificate on the DSP)
- Name the certificate **crestron256** (for this example)
Certificate Authority: Export Device Certificate



Copy Certificates

Copy the Root Certificate and SIP Certificate into the DSP device under the directory /user/cert **by doing SFTP**.

Import and Assign Root Certificate

Use the Crestron Toolbox text console utility (in the Crestron Avia DSP console) to import and assign the root certificate.

1. Type the command `certificate addf "RootCA.cer" root` (where `RootCA` is the name of the root certificate uploaded in the previous section).
   Root Certificate - Successful Import

```
DSP-1282>certificate addf Rootcert256.cer root
Import successful.
```

2. Verify the uploaded root certificate and note the # of the certificate.
   List of Trusted Root Certificates in the Device

```
DSP-1282>siptrustedcas listn
TableStart: [Sip Trusted Certification Authorities]

#   | Name                                                    | UID                                      | In Use
|
----+---------------------------------------------------------+------------------------------------------+-------
+
000 | Baltimore CyberTrust Root                               | 020000B9                                 | No
|
001 | skypelabsj-DC01-CA                                      | 509D8F67E96E78AE43BE80573A7FEE1A         | No
|
002 | skypelabsj-DC01-CA                                      | 343E63A0387235A1449ABB5676612403         | No
|
```

3. Use the command `siptrustedcas use #`, but replace # with the certificate number assigned in the previous step.
   Root Certificate - Assignment

```
DSP-1282>siptrustedcas use 002
Sip Trusted Certification Authorities USING skypelabsj-DC01-CA
343E63A0387235A1449ABB5676612403
```

Add SIP Certificate

Use the Crestron Toolbox text console utility (in the Crestron Avia DSP console) to add the SIP certificate.

Type the command `certificate addf crestron256.pfx SIP 123456`.

This example uses **crestron256** as the name and **123456** as the password (same as the password entered while exporting the certificate from CA).

SIP Certificate - Successful Import

```
DSP-1282>certificate addf crestron256.pfx SIP 123456
Import successful.
```

Cisco UCM Configuration

This section describes the Cisco UCM configuration necessary to integrate Crestron devices as secure SIP endpoints.

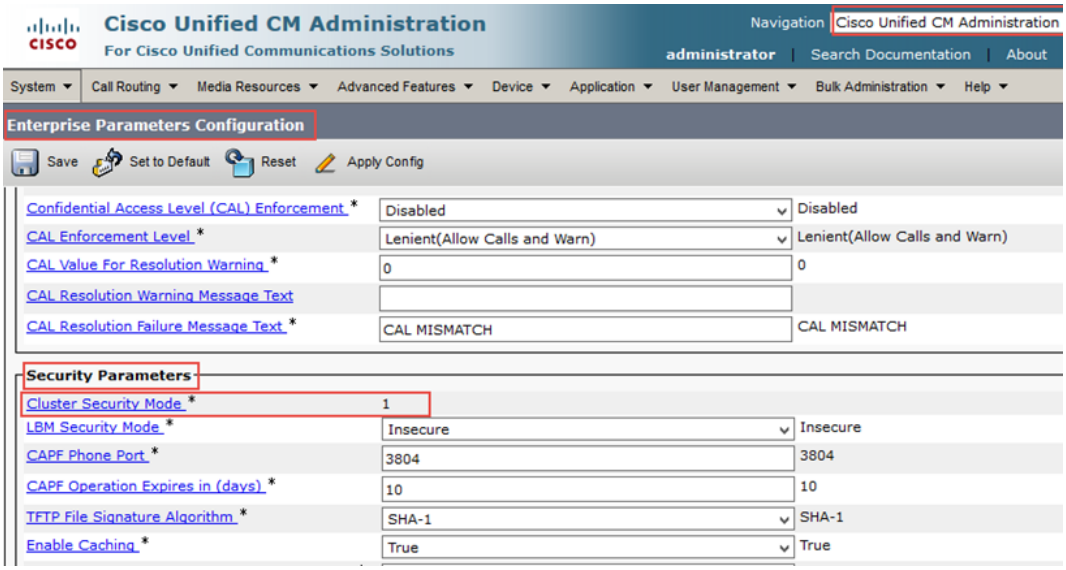
NOTES:

- Confirm that the general installation and basic Cisco UCM configuration have been administered.
- Cisco UCM's Certificate Management has the CallManager certificate signed by the CA. It and the Root CA certificate upload to the CallManager-trust store, which is a repository of X.509 certificates that the application explicitly trusts.

Set up Cisco UCM's cluster security mode in mixed mode to register phones securely (TLS) with Cisco UCM. Refer to Cisco documentation to set up cluster security mode.

To verify Cisco UCM's cluster security mode:

1. Click **Cisco Unified CM Administration** > **System** > **Enterprise Parameters Configuration**.
   Cluster Security Mode



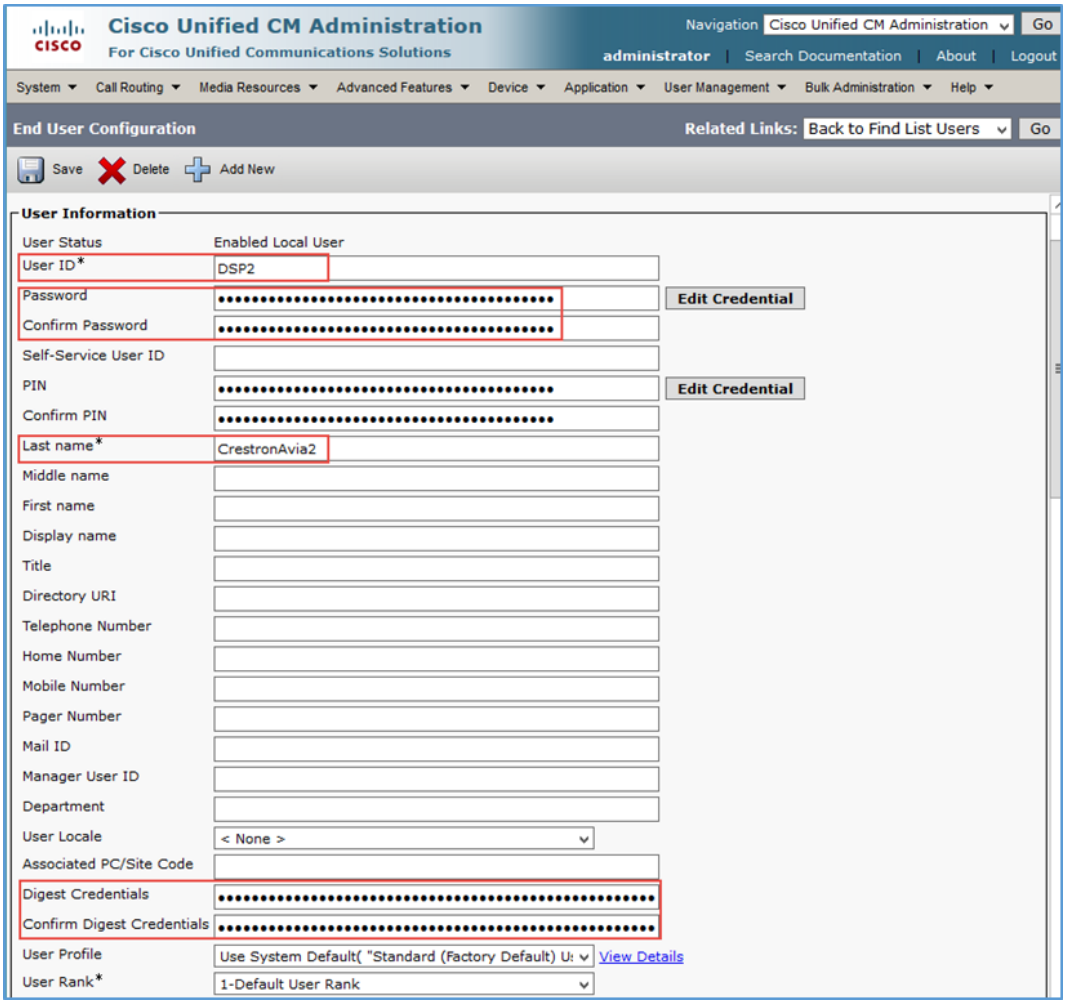
2. In the **Security Parameters** section, select **1** for the **Cluster Security Mode**.

NOTE: The default setting for cluster security mode on the Cisco UCM is insecure mode.

Configure the User

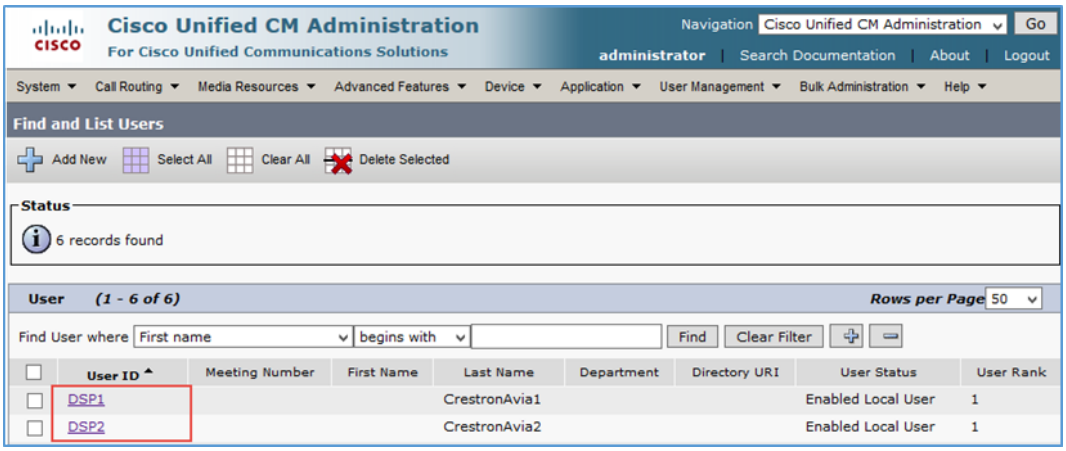
To configure the end user:

1. Click **User Management** > **End User**.
2. Click **Add New**.
   Cisco UCM: End User Configuration



3. Enter a unique end user identification name for the **User ID**. This example uses **DSP1** and **DSP2** for the two DSP devices.
4. Enter a **Password**. This example uses **123456**, which is the same password used on the device against the SIP server password.
5. Enter the same password for **Confirm Password**.
6. Enter the end user's last name for the **Last Name**. This example uses **CrestronAvia2**.
7. Enter a string of alphanumeric characters for the **Digest Credentials**.
8. Enter the same string for **Confirm Digest Credentials**.
9. Click **Save**.

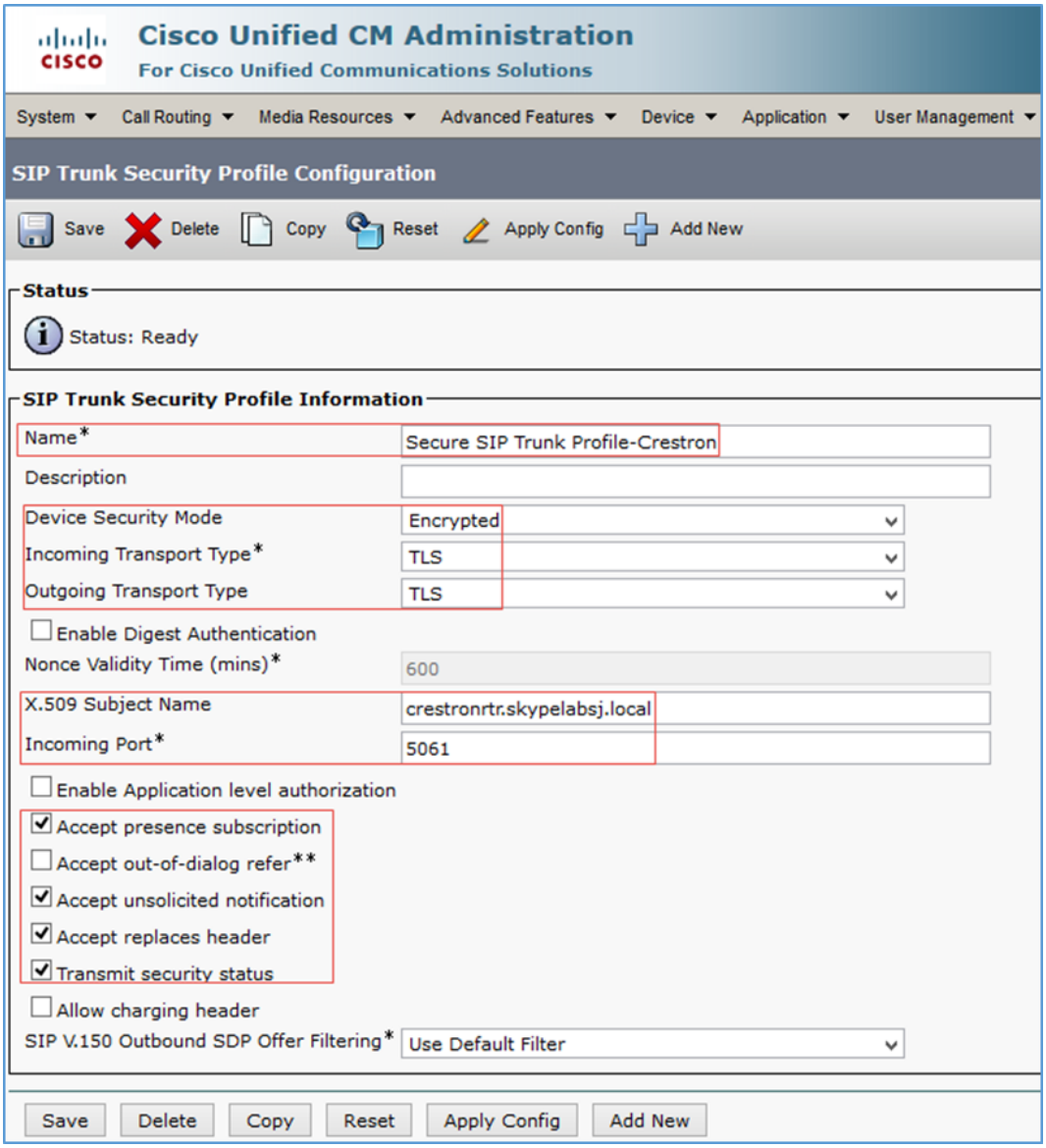
Cisco UCM: End Users Configured for all DSP Devices



Configure a Secure SIP Trunk Security Profile

To configure a new SIP Trunk Security Profile:

1. Click **System** > **Security** > **SIP Trunk Security Profile**.
2. Click **Add New**.
   Cisco UCM: SIP Trunk Security Profile Configuration



3. Enter **Secure SIP Trunk Profile-Crestron** for the **Name** (for this example).
4. Select **Encrypted** for the **Device Security Mode**.
5. Select **TLS** for the Incoming **Transport Type**.
6. Select **TLS** for the **Outgoing Transport Type**.
7. Enter the fully qualified domain name (FQDN) of the Cisco UBE for the **X.509 Subject Name**. This example uses **crestronrtr.skypelabsj.local**.

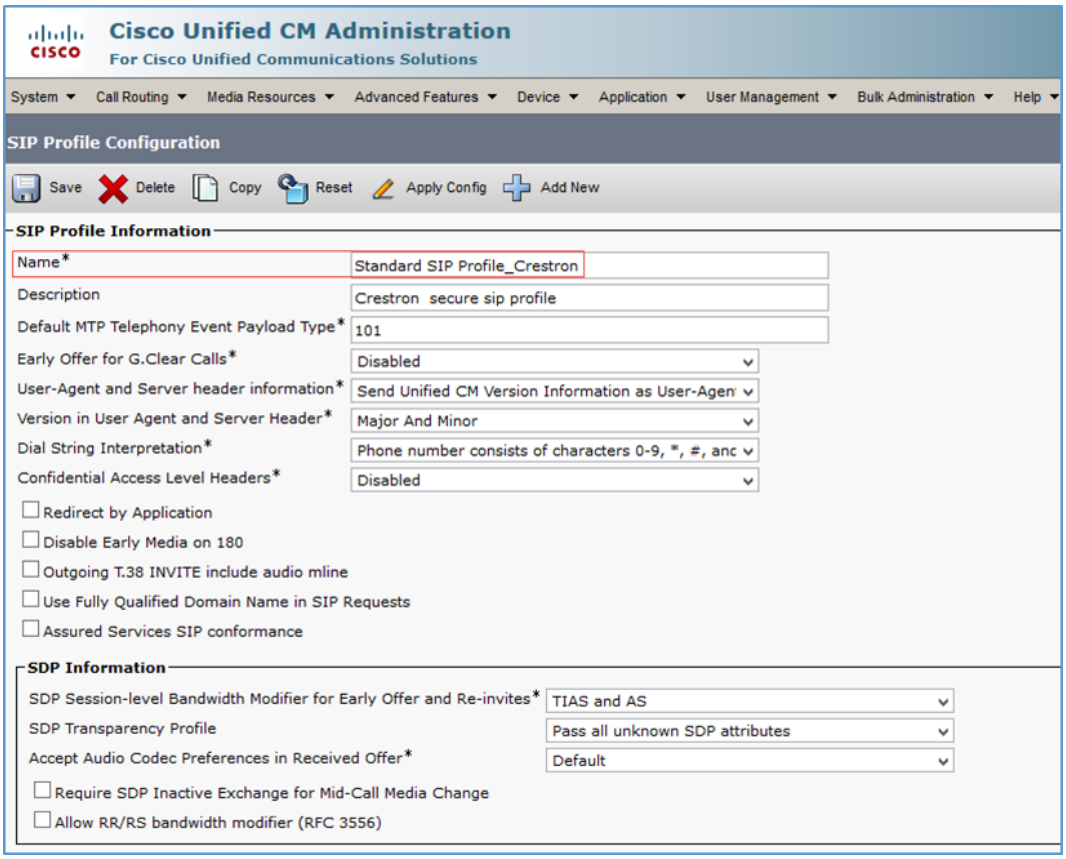
8. Enter **5061** for the **Incoming Port** (for this example).
9. Check **Transmit security status**.
10. Click **Save**.

Configure a Secure SIP Profile

This example configures a new SIP Profile: **Standard SIP Profile_Crestron**.

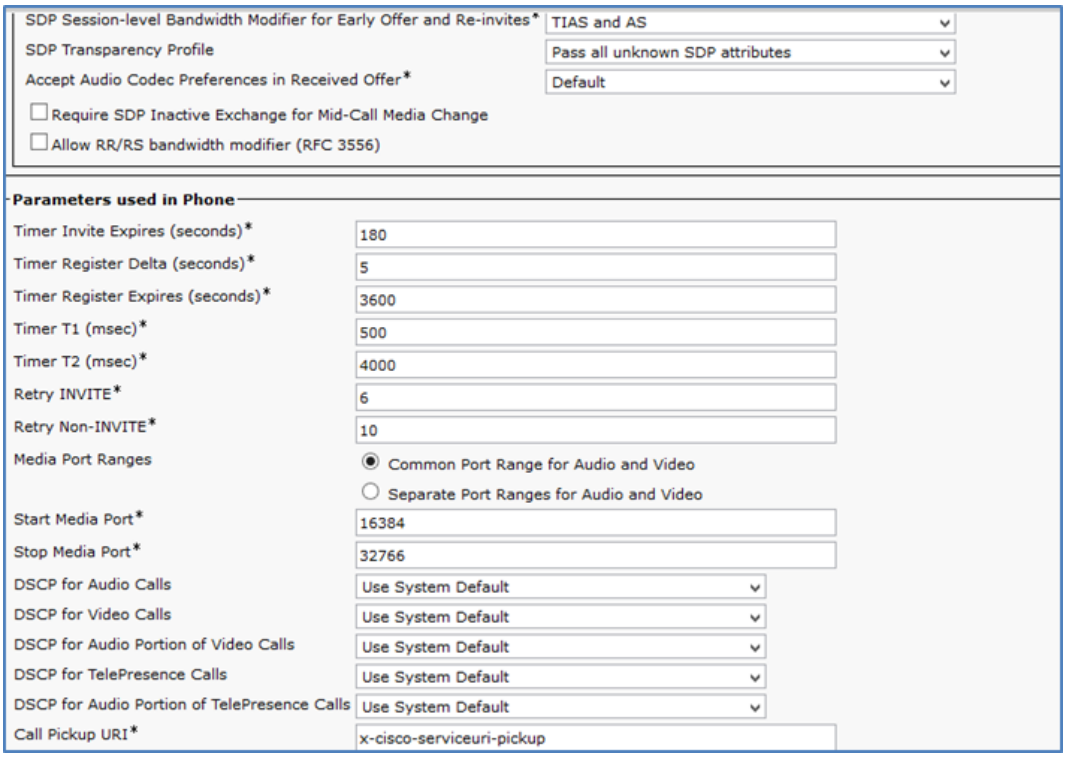
To add a new SIP Profile:

1. Click **Device** > **Device Settings** > **SIP Profile**.
2. Click **Add New**.
   Cisco UCM: SIP Profile Configuration (1/4)

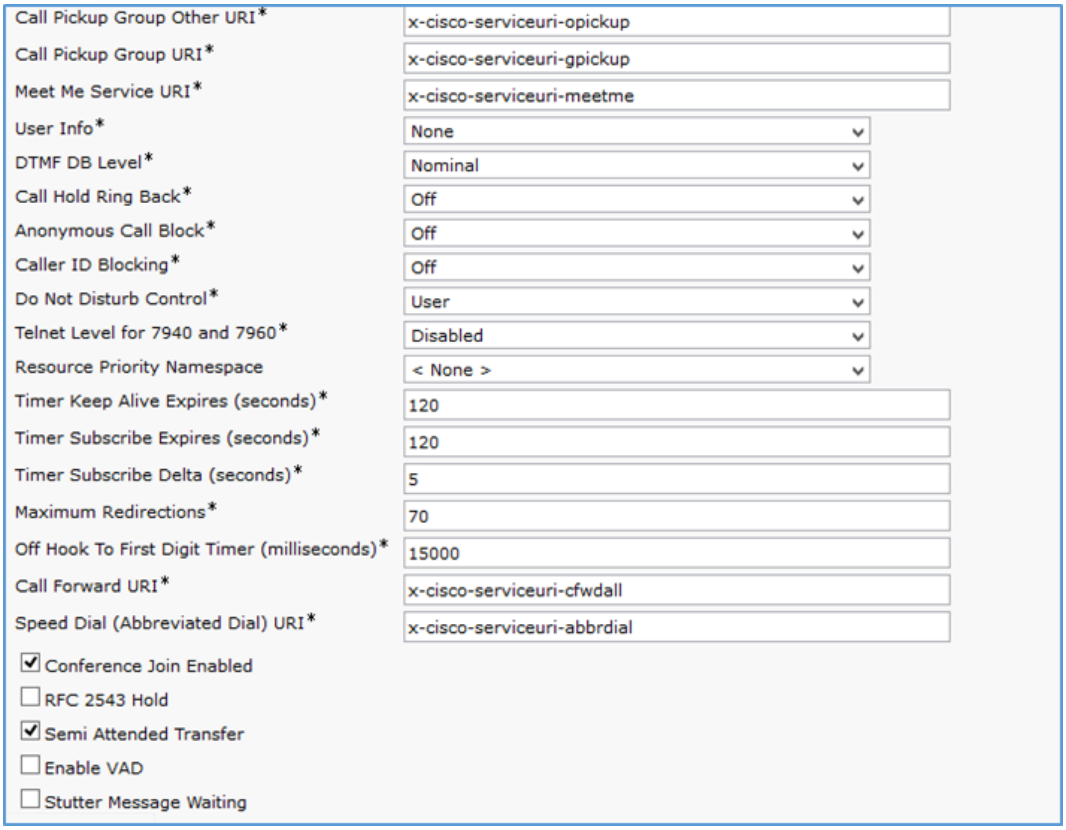


3. Enter **Standard SIP Profile_Crestron** for the **Name** (for this example).

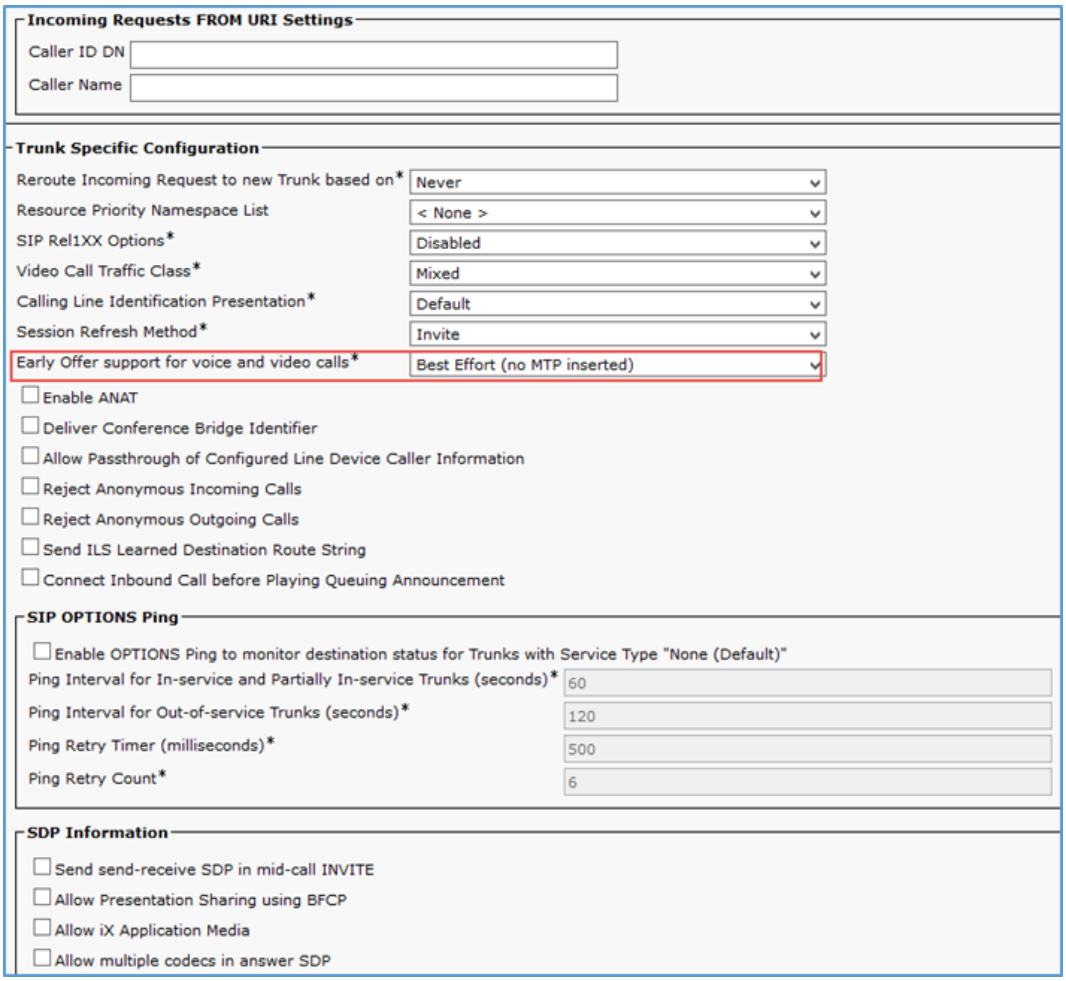
Cisco UCM: SIP Profile Configuration (2/4)



Cisco UCM: SIP Profile Configuration (3/4)



Cisco UCM: SIP Profile Configuration (4/4)



4. Select **Best Effort (no MTP inserted)** for **Early Offer support for voice and video calls**.
5. Leave all other fields at the default values.
6. Click **Save**.
7. Click **Apply Config**.

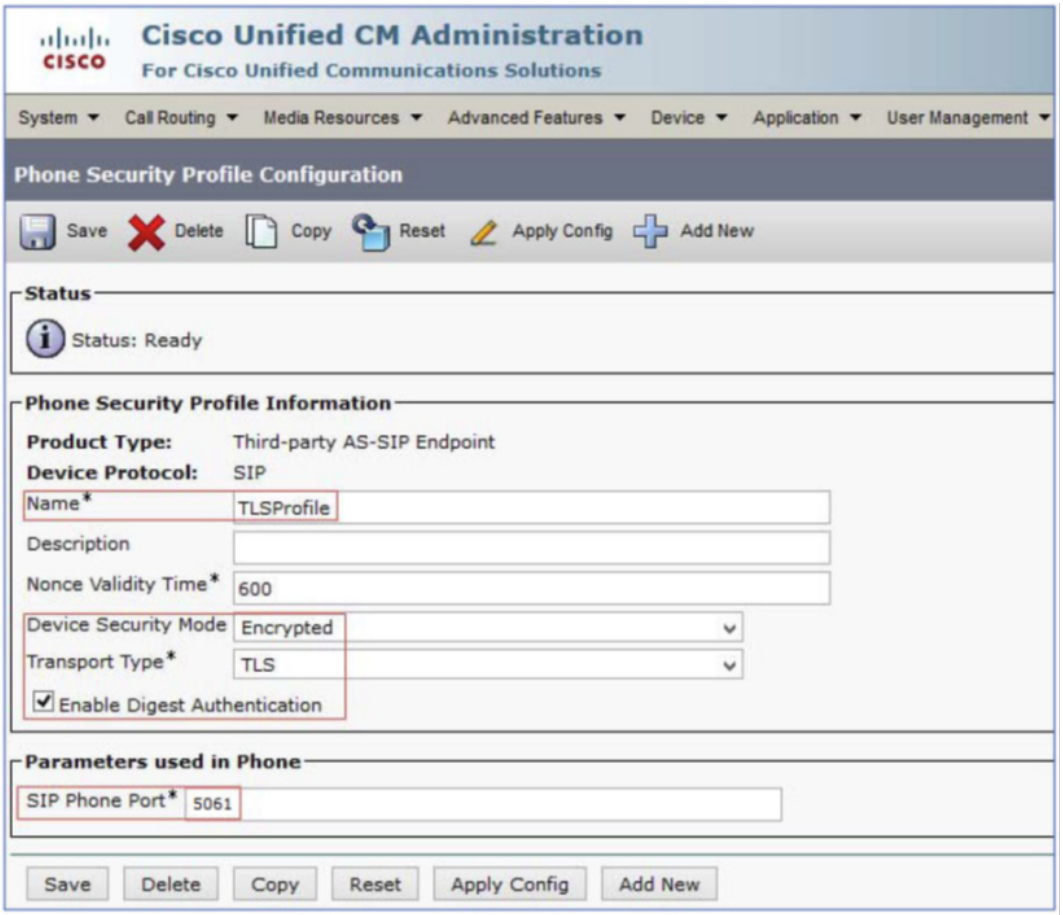
Configure Phone Security Profile

Each phone type requires its own Phone Security Profile. The following procedure configures a profile for the DSP device using 9951 and 9971 phone types.

To configure the Phone Security Profile:

1. Click **System** > **Security** > **Phone Security Profile**.
2. Click **Add New**.

Cisco UCM: Phone Security Profile

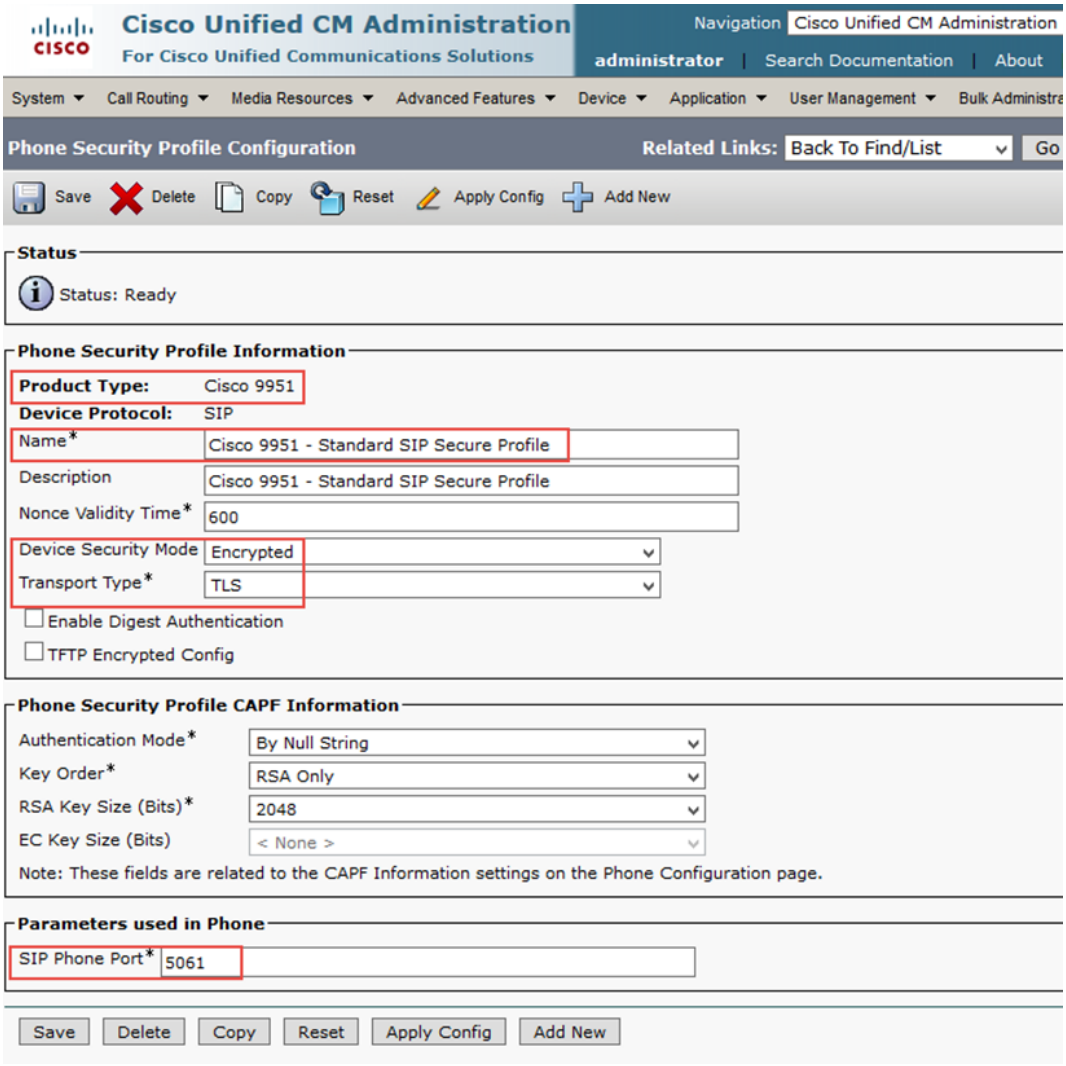


3. Select **Third-party AS-SIP Endpoint** for the **Product Type**.
4. Enter **TLSProfile** for the **Name** (for this example).
5. Select **Encrypted** for the **Device Security Mode**.
6. Select **TLS** for the **Transport Type**.
7. Check **Enable Digest Authentication**.
8. Enter **5061** (the DSP device used this port) for the **SIP Phone Port**.
9. Click **Save**.

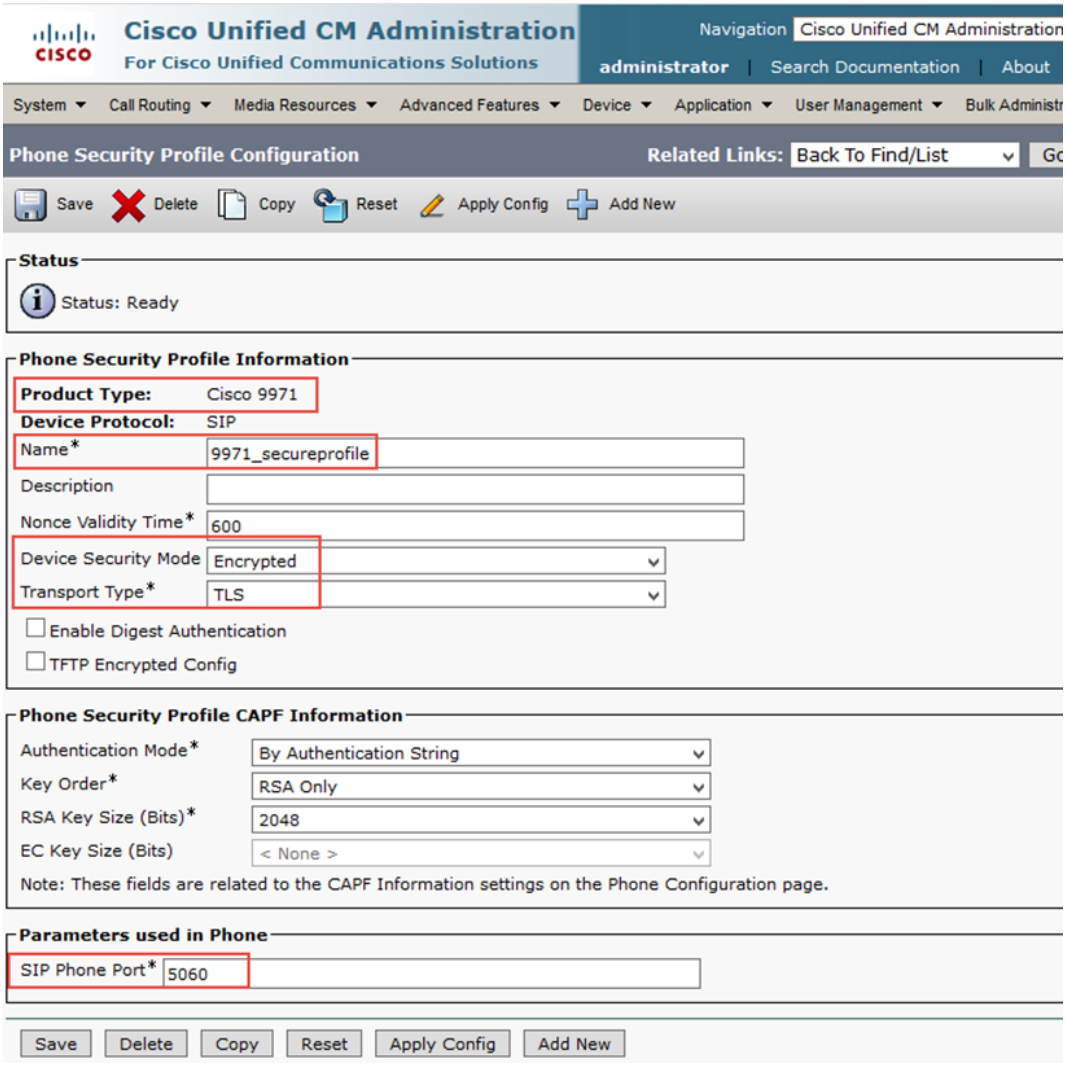
To configure the Phone Security Profile for the 9951 and 9971 phone types:

1. Click **System** > **Security** > **Phone Security Profile**.
2. Click **Add New**.

Cisco UCM: Phone Security Profile for 9951 Phone Type



Cisco UCM: Phone Security Profile for 9971 Phone Type

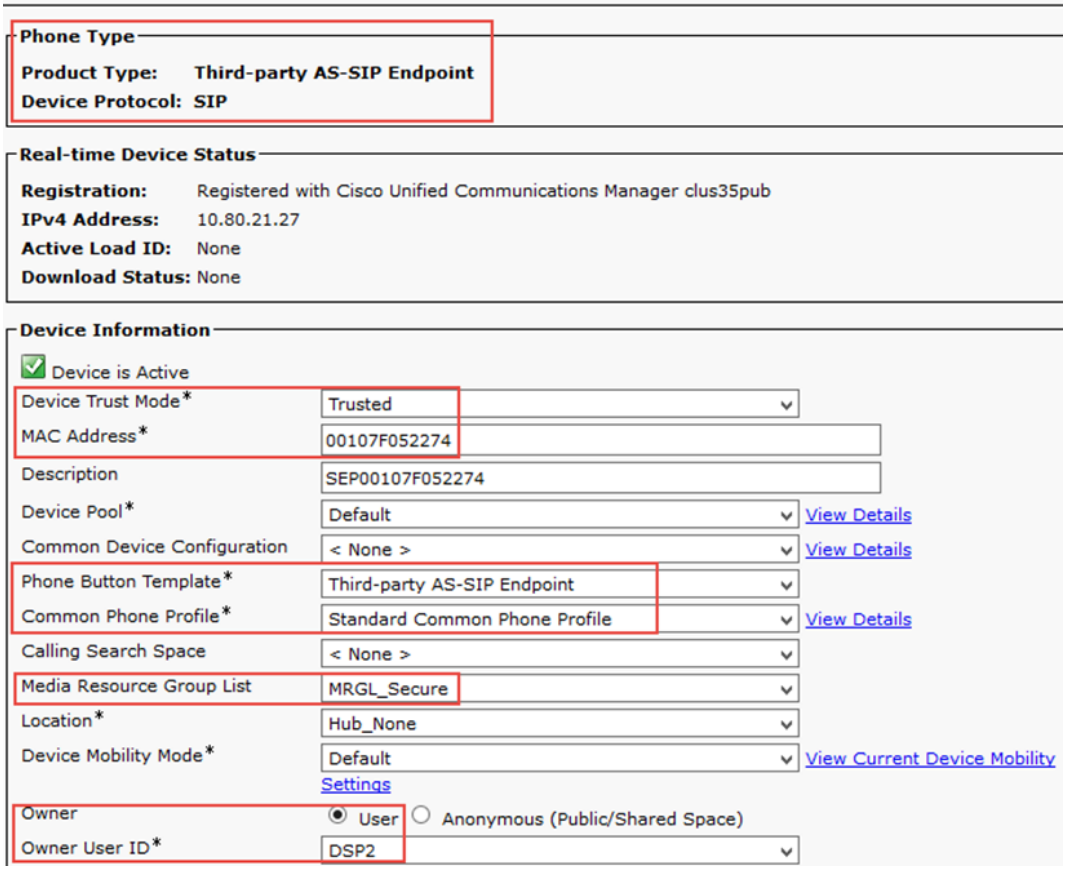


3. Select **Cisco 9951** (for the 9951 device), or **Cisco 9971** (for the 9971 device) for the **Product Type**.
4. Enter **Cisco 9951 - Standard SIP Secure Profile** (for the 9951 device) or **9971_secureprofile** (for the 9971 device) for the **Name**.
5. Select **Encrypted** for the **Device Security Mode**.
6. Select **TLS** for the **Transport Type**.
7. In the **Phone Security Profile CAPF Information** section:
    a. Select **By Null String** (for the 9951 device) or **By Authentication String** (for the 9971 device) for the **Authentication Mode**.
    b. Select **RSA Only** for the **Key Order**.
    c. Select **2048** for the **RSA Key Size (Bits)**.
8. Enter **5061** (fir the 9951 device) or **5060** (for the 9971 device) for the **SIP Phone Port**.
9. Click **Save**.

Configure the Crestron Device as a Third-party SIP Device

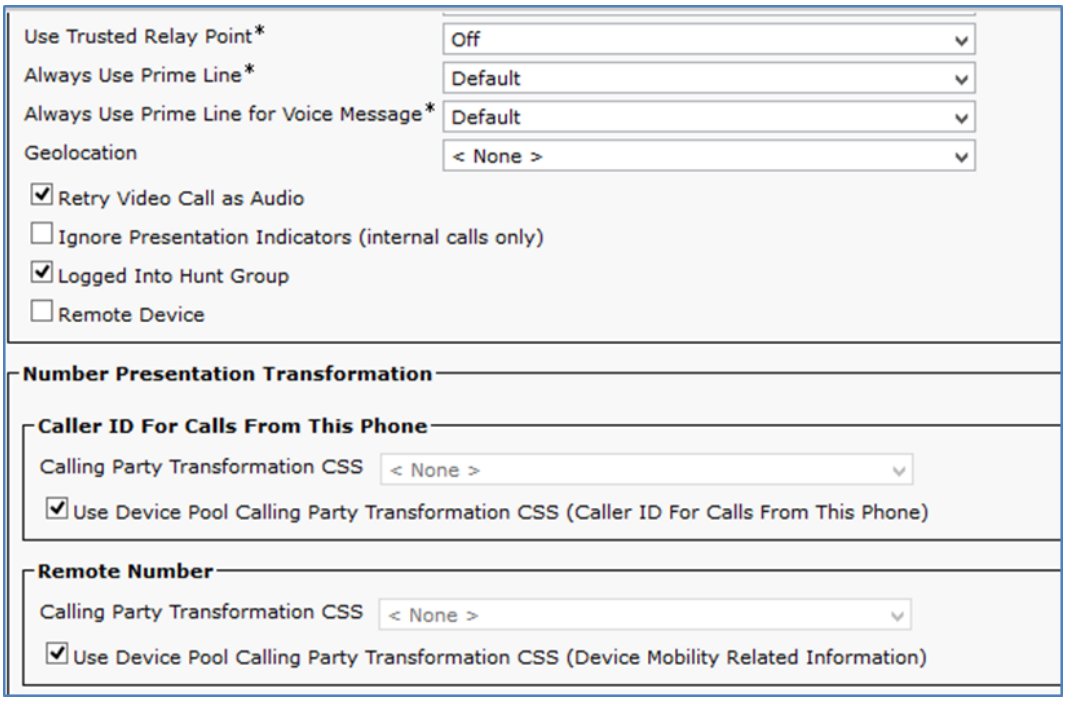
To configure the DSP device as a third-party SIP device:

1. Click **Device** > **Phone**.
2. Click **Add New**.
   Cisco UCM: Add Crestron Device as Third-party SIP Device (1/3)

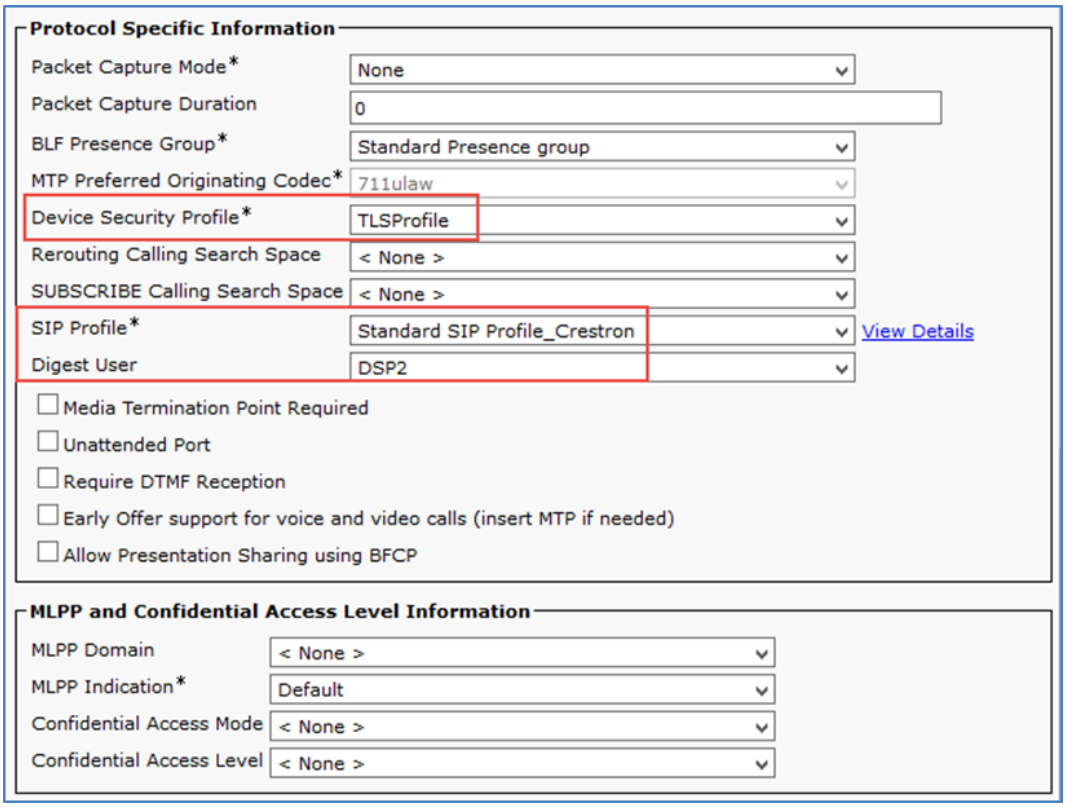


3. In the **Phone Type** section, select **Third-party AS-SIP Endpoint** for the **Product Type**.
4. Click **Next**.
5. Enter the MAC address of the DSP for the **MAC Address**.
6. Select **Default** for the **Device Pool**.
7. Select **Third-party AS-SIP Endpoint** for the **Phone Button Template**.
8. Click **User** for the **Owner**.
9. Select the End User configured earlier for the **Owner User ID**. This example selects **DSP1** for the first Crestron Avia DSP device and **DSP2** for the second Crestron Avia DSP device.
10. Select **MRGL_Secure** (configured earlier for this example) for the **Media Resource Group List**.

Cisco UCM: Add Crestron Device as Third-party SIP Device (2/3)



Cisco UCM: Add Crestron Device as Third-party SIP Device (3/3)



11. Select **TLSProfile** (configured earlier for this example) for the **Device Security Profile**.

12. Select **Standard SIP Profile_Crestron** (configured earlier for this example) for the **SIP Profile**.
13. Select **DSP1** for the first Crestron Avia DSP device and **DSP2** for the second (configured earlier for this example) for the **Digest User**.
14. Click **Save**.
15. Add a DN to this phone. This example configures DN 2500 for one of the Crestron Avia DSP devices and DN 2501 for the other.

Configure Media Resource Group and Media Resource Group List

A Media Resource Group (MRG) includes Music on Hold servers, conference bridges, and media termination points that may test the Cisco UCM or service provider features.

Use a Cisco UBE at the edge of the enterprise to ensure secure SIP signaling and media for PSTN calls, and establish secure transfers and conferences.

This Cisco UBE provided the DSP resources required by the Cisco UCM for transcoding, media termination points, and a conference bridge.

Configure the Cisco UBE for MRG Resources

The related Cisco UBE configuration is as follows:

```
crypto pki trustpoint TP-self-signed-3690608021
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3690608021
 revocation-check none
 rsakeypair TP-self-signed-3690608021
 !
crypto pki trustpoint CrestronCFB
 enrollment terminal
 fqdn crestronrtr.skypelabsj.local
 subject-name CN=crestronrtr.skypelabsj.local
 revocation-check none
 rsakeypair SFBCAKey
 !
 !
crypto pki certificate chain TP-self-signed-3690608021
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 33363930 36303830 3231301E 170D3135 30373038 31363138
 34375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 36393036
 30383032 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 81008CC1 308B5D7D 736C3A2F FE0DEF4D A0AEEDB6 B5755148 8CEF1F2D 4BC575EF
 DD00183A 10902D4F A647A3E2 B5E87A77 DB5A1721 DE7633CE D5D35A0A A48EC7BE
 ABBA6FB9 8F10A203 AAFE9A3F 4436B8AF 5556FA79 94AC3853 5B1CD9F8 D505FA2F
 56ED38E4 6C4B8F5E 810137FF DDED832F AC8CEC4B 7092CCA9 B22F73AC 8D90906A
 69BF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 144C60DF 878847B7 FCB4602A 430D4FFD D2DBECD0 27301D06
```

```
 03551D0E 04160414 4C60DF87 8847B7FC B4602A43 0D4FFDD2 DBECD027 300D0609
 2A864886 F70D0101 05050003 81810054 D4045CB8 1F1F5F76 3428D60B A23463AE
 0DF8523F 4403BCD8 158B5D65 BB155518 8843B518 FA2E5E81 8908E661 61A7C647
 D4422E9C F8E4E8D1 8223DAD0 4B05D719 9E1E9226 A50AACD2 7CD5C859 CD80D777
 38A3AB17 ADC68299 694086FF 03D0D931 39A66564 F9360751 7DD62FE2 CEFC8CEA
 C4C0E406 559791D2 6193CD67 0D3839
 quit
crypto pki certificate chain CrestronCFB
 certificate 50000000837EE13E3436DC23C6000000000083
 30820582 3082046A A0030201 02021350 00000083 7EE13E34 36DC23C6 00000000
 0083300D 06092A86 4886F70D 01010505 00305031 15301306 0A099226 8993F22C
 64011916 056C6F63 616C311A 3018060A 09922689 93F22C64 0119160A 736B7970
 656C6162 736A311B 30190603 55040313 12736B79 70656C61 62736A2D 44433031
 2D434130 1E170D31 37303230 37303033 3334335A 170D3139 30323037 30303333
 34335A30 27312530 23060355 0403131C 63726573 74726F6E 7274722E 736B7970
 656C6162 736A2E6C 6F63616C 30820122 300D0609 2A864886 F70D0101 01050003
 82010F00 3082010A 02820101 00BC58F7 5313EFC6 93E06237 89A4BA5D F94209AD
 D9C94161 DD6D4620 32EC47E2 7D88FC96 CCBFE1B5 AD6E2714 9ED0A9AB 58F77BA4
 B60A7642 3E3933C5 C95EBB14 0A6CCC58 223CF261 0C67BAC1 6C6CA462 FAC47AF2
 13246559 BE908F1B 338758A2 EEC0AE13 AFD04DCF 0DD072D5 1F259947 9899274F
 C81A1B70 81201496 AC76C35A 6E79C4CE 3B1FBA39 F009A2CE 1A991F03 4CD97CC3
 8E22AD52 94727101 570A8A1E 7B3D09A5 BFDDD75E 80A06C3C 829AD88F A3B5AEBB
 59E7993F 7BF62605 E094652D 0D53145B 52B17709 E393DA2A C76F2AB6 8DE683E1
 60F05DCB 7E22ACBB 7440EDA7 16C12FD0 96295FC4 30FBB97F 185F9242 B44A15EB
 AE2C6FF1 26C7DF40 CCE13636 E1020301 0001A382 027C3082 0278300E 0603551D
 0F0101FF 04040302 04F0301D 0603551D 0E041604 14F019A0 15E61282 A4AF76AE
 1C7C7E0C 75872C55 64301F06 03551D23 04183016 8014D17C 5CD92CCB D22D8BFC
 99ABAF07 D1944522 C0183081 D2060355 1D1F0481 CA3081C7 3081C4A0 81C1A081
 BE8681BB 6C646170 3A2F2F2F 434E3D73 6B797065 6C616273 6A2D4443 30312D43
 412C434E 3D444330 312C434E 3D434450 2C434E3D 5075626C 69632532 304B6579
 25323053 65727669 6365732C 434E3D53 65727669 6365732C 434E3D43 6F6E6669
 67757261 74696F6E 2C44433D 736B7970 656C6162 736A2C44 433D6C6F 63616C3F
 63657274 69666963 61746552 65766F63 6174696F 6E4C6973 743F6261 73653F6F
 626A6563 74436C61 73733D63 524C4469 73747269 62757469 6F6E506F 696E7430
 81C90608 2B060105 05070101 0481BC30 81B93081 B606082B 06010505 07300286
 81A96C64 61703A2F 2F2F434E 3D736B79 70656C61 62736A2D 44433031 2D43412C
 434E3D41 49412C43 4E3D5075 626C6963 2532304B 65792532 30536572 76696365
 732C434E 3D536572 76696365 732C434E 3D436F6E 66696775 72617469 6F6E2C44
 433D736B 7970656C 6162736A 2C44433D 6C6F6361 6C3F6341 43657274 69666963
 6174653F 62617365 3F6F626A 65637443 6C617373 3D636572 74696669 63617469
 6F6E4175 74686F72 69747930 3D06092B 06010401 82371507 0430302E 06262B06
 01040182 37150887 C8825984 899B7682 81873786 D0B27386 C9D70F6B 879CB26A
 82DBCD03 02016402 010A301D 0603551D 25041630 1406082B 06010505 07030106
 082B0601 05050703 02302706 092B0601 04018237 150A041A 3018300A 06082B06
 01050507 0301300A 06082B06 01050507 0302300D 06092A86 4886F70D 01010505
 00038201 010000DE 2572CE59 4DA3B950 CB7678B7 2F9E1688 6F0CFF6F E2082BD2
 743F2CB3 B7FB3D11 3102D9EE 4A39040B 93231018 80DDB05E A579A173 2305A856
 92AA9D77 43AEEB5C 1709092E 8BB3D027 AEE95023 D135DE3D 62F28752 E23BEA7C
 7E0708E7 8726ED59 25A95D3B 68ABB3AA CA96D5CA E4C7A87B 489284DE 6E5976D1
 D63CED20 D97C8C9F 17F08794 A80D369B AD6A2E75 1EDEEADD 57F39B27 6C3BAE8F
```

```
82B8DAF2 5D2A69F8 37C61A0B 638C43F9 5E2AFBD5 F3100F3D 8BF8F2F1 956D330A
137DA5D7 95AE7629 38C5212D 4CD5411C A4A0976B 2987A433 AC62D453 5EC0A9F4
8427E116 EDD471E0 3FC198A9 5DEBB321 4C655E3F B77A1F68 CCA38749 86C424EC
9F31DEA8 D734
quit
certificate ca 2C0BFAFACCBD24A1420DEF837B9FBC8F
3082037B 30820263 A0030201 0202102C 0BFAFACC BD24A142 0DEF837B 9FBC8F30
0D06092A 864886F7 0D010105 05003050 31153013 060A0992 268993F2 2C640119
16056C6F 63616C31 1A301806 0A099226 8993F22C 64011916 0A736B79 70656C61
62736A31 1B301906 03550403 1312736B 7970656C 6162736A 2D444330 312D4341
301E170D 31353036 30393138 35383534 5A170D32 30303630 39313930 3835325A
30503115 3013060A 09922689 93F22C64 01191605 6C6F6361 6C311A30 18060A09
92268993 F22C6401 19160A73 6B797065 6C616273 6A311B30 19060355 04031312
736B7970 656C6162 736A2D44 4330312D 43413082 0122300D 06092A86 4886F70D
01010105 00038201 0F003082 010A0282 010100A4 65F31045 74F51718 C32E37E1
7EE69305 B93C6A07 7DEA2BAD EB854545 2C2A4569 AF0CF2A7 DD525288 7FA9F0BB
7F7B9DFE E05C0A19 9C205F1E E3C913EF 753B5A88 A2B9CE4B B184E265 EEEDD894
BFA4FE27 AC778CD4 5D76A2EF 43F2DB10 12470BF8 0807EC2F EA64D0DC 386B38EC
0A46454A A456DBD8 FB0AE0B5 B9AFD285 38F818C9 8E3BCD39 47CE2905 378A9128
1836C101 7C368D89 8509281F 6F12920A 971257DD CCC23BE9 92860C8C CD47B52C
17887B9F A20B2995 FA26D0F9 6C34B64D 672C6B76 85AEA657 C61141CF 3382836E
6392C6EE 66F62BAB 2E72A77B 24A7A14E C34A7439 F7C460D3 DA0FB17C 9D9DC25A
DAFB62EE 850CF72F FC069549 773D503B 44D3B102 03010001 A351304F 300B0603
551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
0E041604 14D17C5C D92CCBD2 2D8BFC99 ABAF07D1 944522C0 18301006 092B0601
04018237 15010403 02010030 0D06092A 864886F7 0D010105 05000382 01010030
7404A98F 9B790586 F4A8D827 5CB8BD58 E692E9CF 2C79D897 768E7F85 FF1A717D
B2214917 5B2C8417 00787E4F EA21E1D3 F8B303DB CBB8A955 7314B955 959B47FD
48FBD08F 79038EE7 AC560B06 4612D894 B01E573B 4D76A02F D0B4C9C0 2D289F8A
A49C8A68 F2CAA915 B440384A BB459345 99A901F1 241A8DF4 6A2274D8 C902B806
A9F658BA 76086857 3ED1AA3E 4CA79EE9 D2255E06 92E464C9 18764495 F753EB53
5A60EB7F 4A8E58D7 B32A3563 AE8F90F7 E52D3B46 47F25409 4DAFE214 808D6F2C
FA79E6FF AA11F81E 14C8D6F9 B5DCC86B DBD9216C D6557FF9 D0D0F83F E0F0E004
33974FFF B212C328 49740D12 E96AA1CB 626BBCBC 8E786743 305F0DFB 3F3883
quit
voice-card 0
dspfarm
dsp services dspfarm
!
voice service voip
ip address trusted list
ipv4 0.0.0.0 0.0.0.0
no ip address trusted authenticate
address-hiding
mode border-element license capacity 100
srtp fallback
allow-connections sip to sip
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
supplementary-service media-renegotiate
```

```
 redirect ip2ip
 sip
 min-se 90
 session refresh
 header-passing
 registrar server expires max 120 min 60
 early-offer forced
 midcall-signaling passthru
 !
 voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g722-64
 codec preference 3 g711alaw
 !
 interface GigabitEthernet0/0
 ip address 10.64.4.246 255.255.0.0
 duplex auto
 speed auto
 !
 interface GigabitEthernet0/1
 description CUBE LAN facing Clus35pub
 ip address 10.80.25.200 255.255.255.0
 duplex auto
 speed auto
 !
 ip route 10.70.26.4 255.255.255.255 ISM0/0
 ip route 10.80.0.0 255.255.0.0 10.80.25.1
 ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
 ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
 !
 sccp local GigabitEthernet0/1
 sccp ccm 10.80.25.2 identifier 1 priority 1 version 7.0 trustpoint
CrestronCFB
 sccp
 !
 sccp ccm group 3
 bind interface GigabitEthernet0/1
 associate ccm 1 priority 1
 associate profile 3 register Crestronrtr
 associate profile 4 register SRTP-MTP
 !
 !
 !
 dspfarm profile 2 transcode universal security
 codec g711ulaw
 codec g722-64
 maximum sessions 4
 associate application CUBE
 !
 dspfarm profile 3 conference security
```

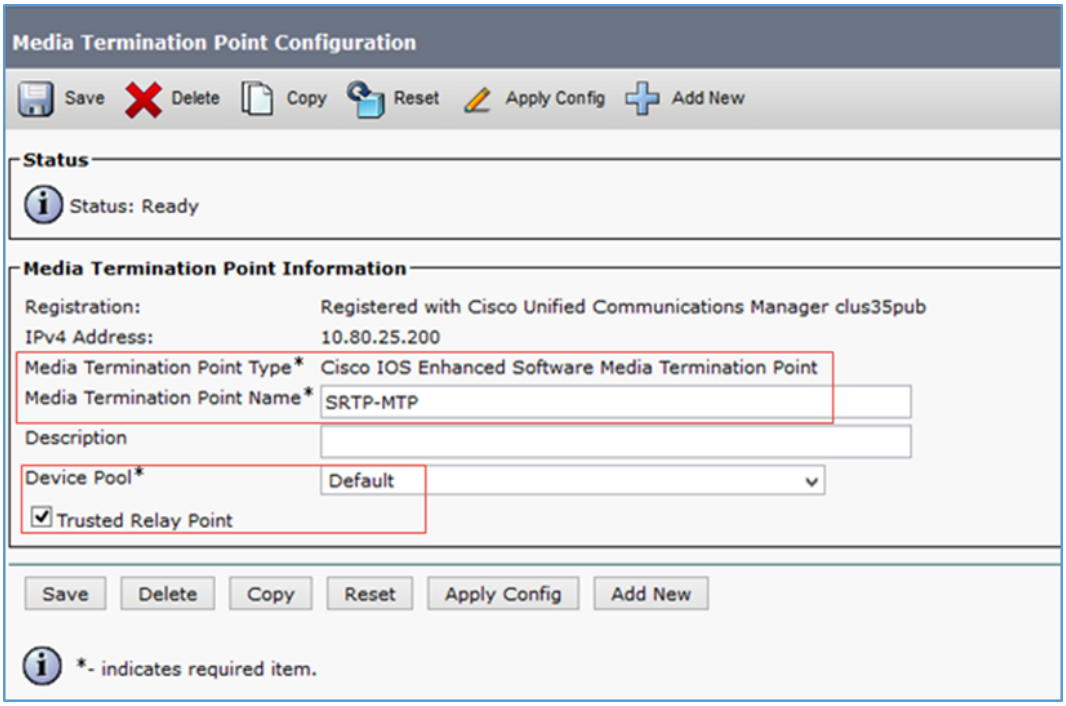
```
trustpoint CrestronCFB
codec g711alaw
codec g711ulaw
codec g722-64
maximum sessions 1
associate application SCCP
!
dspfarm profile 4 mtp security
trustpoint CrestronCFB
codec pass-through
maximum sessions software 10
associate application SCCP
!
dial-peer voice 201 voip
description incoming dial plan from PSTN GW
huntstop
session protocol sipv2
session transport udp
incoming called-number 972265727[7-9]
voice-class codec 1
voice-class sip bind control source-interface GigabitEthernet0/0
voice-class sip bind media source-interface GigabitEthernet0/0
dtmf-relay rtp-nte
no vad
!
dial-peer voice 300 voip
description outgoing dialplan towards PSTN GW for 18xx
huntstop
shutdown
destination-pattern 18.........
session protocol sipv2
session target ipv4:10.64.1.72
session transport udp
voice-class codec 1
voice-class sip bind control source-interface GigabitEthernet0/0
voice-class sip bind media source-interface GigabitEthernet0/0
dtmf-relay rtp-nte
!
dial-peer voice 401 voip
description incoming 18xx number from pbx
huntstop
shutdown
session protocol sipv2
session transport tcp tls
incoming called-number 18.........
voice-class codec 1
voice-class sip bind control source-interface GigabitEthernet0/1
voice-class sip bind media source-interface GigabitEthernet0/1
dtmf-relay rtp-nte
!
```

```
 dial-peer voice 100 voip
 description outgoing dialplan on LAN towards clus35pub
 huntstop
 destination-pattern 972265....
 session protocol sipv2
 session target ipv4:10.80.25.2:5061
 session transport tcp tls
 voice-class codec 1
 voice-class sip srtp-auth sha1-32 sha1-80
 voice-class sip bind control source-interface GigabitEthernet0/1
 voice-class sip bind media source-interface GigabitEthernet0/1
 dtmf-relay rtp-nte
 srtp
 !
 dial-peer voice 101 voip
 description incomign dialplan from clus35pub
 huntstop
 session protocol sipv2
 session transport tcp tls
 incoming called-number 21424259777
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet0/1
 voice-class sip bind media source-interface GigabitEthernet0/1
 dtmf-relay rtp-nte
 !
 dial-peer voice 200 voip
 description outgoing dialplan towards PSTN GW
 huntstop
 destination-pattern 2142425977
 session protocol sipv2
 session target ipv4:10.64.1.72
 session transport udp
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet0/0
 voice-class sip bind media source-interface GigabitEthernet0/0
 dtmf-relay rtp-nte
 no srtp
 !
 !
 sip-ua
 crypto signaling remote-addr 10.80.25.2 255.255.255.255 trustpoint
CrestronCFB
 !
 !
 !
 gatekeeper
 shutdown
 !
 end
```

Configure the Cisco UCM Media Termination Point

To configure a Media Termination Point utilizing Cisco UBE resources:

1. Click **Media Resources** > **Media Termination Point**.
2. Click **Add New**.
   Cisco UCM: Add Cisco IOS Enhanced Software Media Termination Point

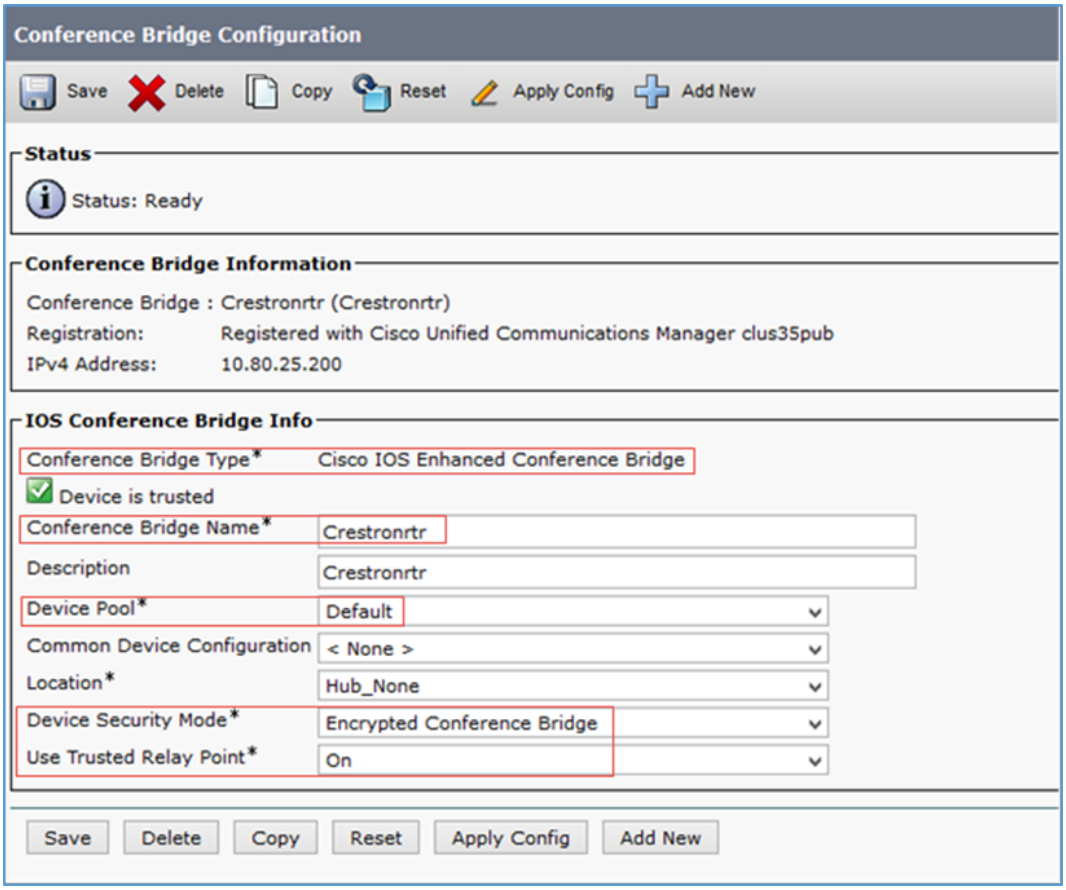


3. Select **Cisco IOS Enhanced Software Media Termination Point** for the **Media Termination Point Type**.
4. Enter **SRTP-MTP** for the **Media Termination Point Name** (for this example). It is the same name configured on the Cisco UBE.
5. Select **Default** for the **Device Pool**.
6. Check **Trusted Relay Point**.

Configure the Cisco UCM Conference Bridge

To configure an iOS® conference bridge utilizing Cisco UBE resources:

1. Click **Media Resources** > **Conference Bridge**.
2. Click **Add New**.
   Cisco UCM: Add Cisco IOS Enhanced Conference Bridge



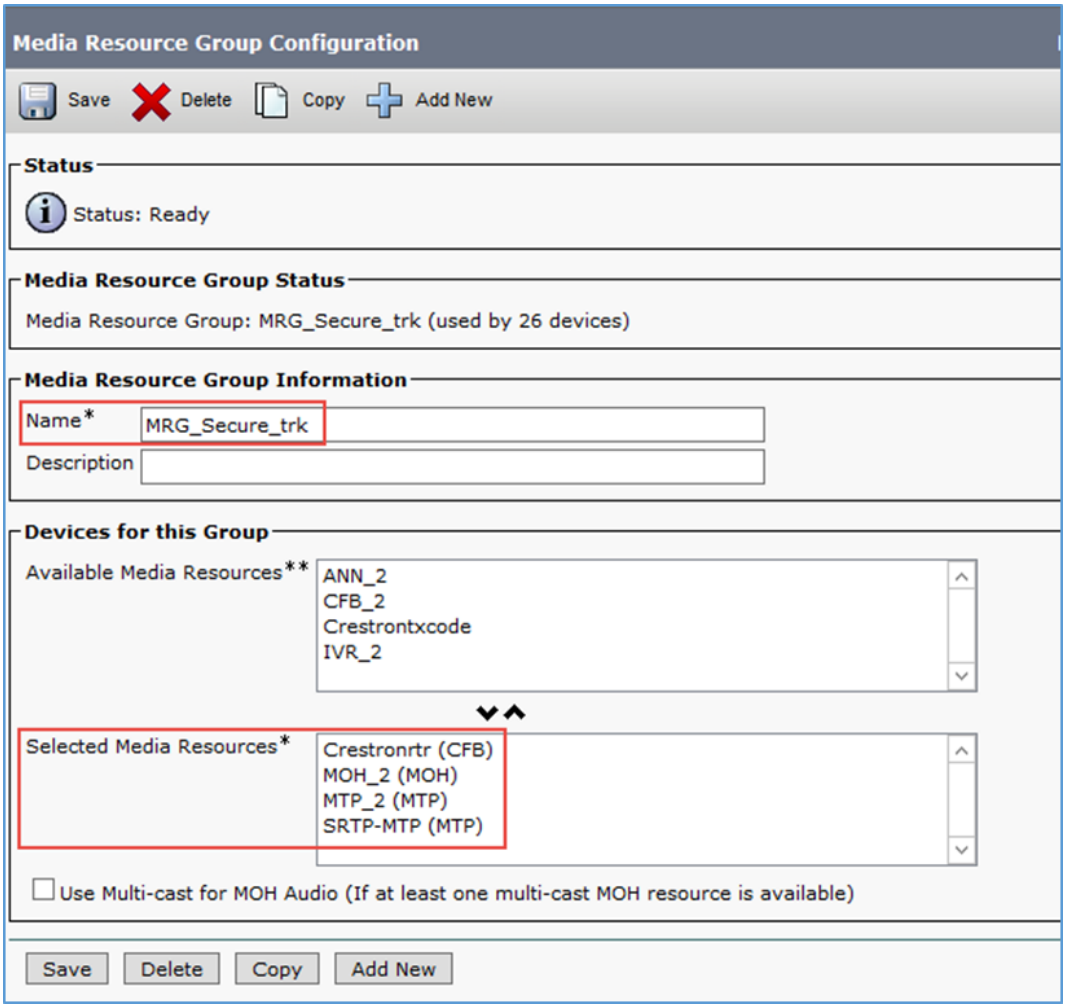
3. Select **Cisco IOS Enhanced Conference Bridge** for the **Conference Bridge Type**.
4. Enter **Crestronrtr** for the **Conference Bridge Name** (for this example). It is the same name configured on the Cisco UBE.
5. Select **Default** for the **Device Pool**.
6. Select **Encrypted Conference Bridge** for the **Device Security Mode**.
7. Select **On** for **Use Trusted Relay Point**.

Configure the Cisco UCM Conference MRG

To configure the **MRG_Secure** Media Resource Group (for this example):

1. Click **Media Resources** > **Media Resource Group**.
2. Click **Add New**.

Cisco UCM: Media Resource Group Configuration



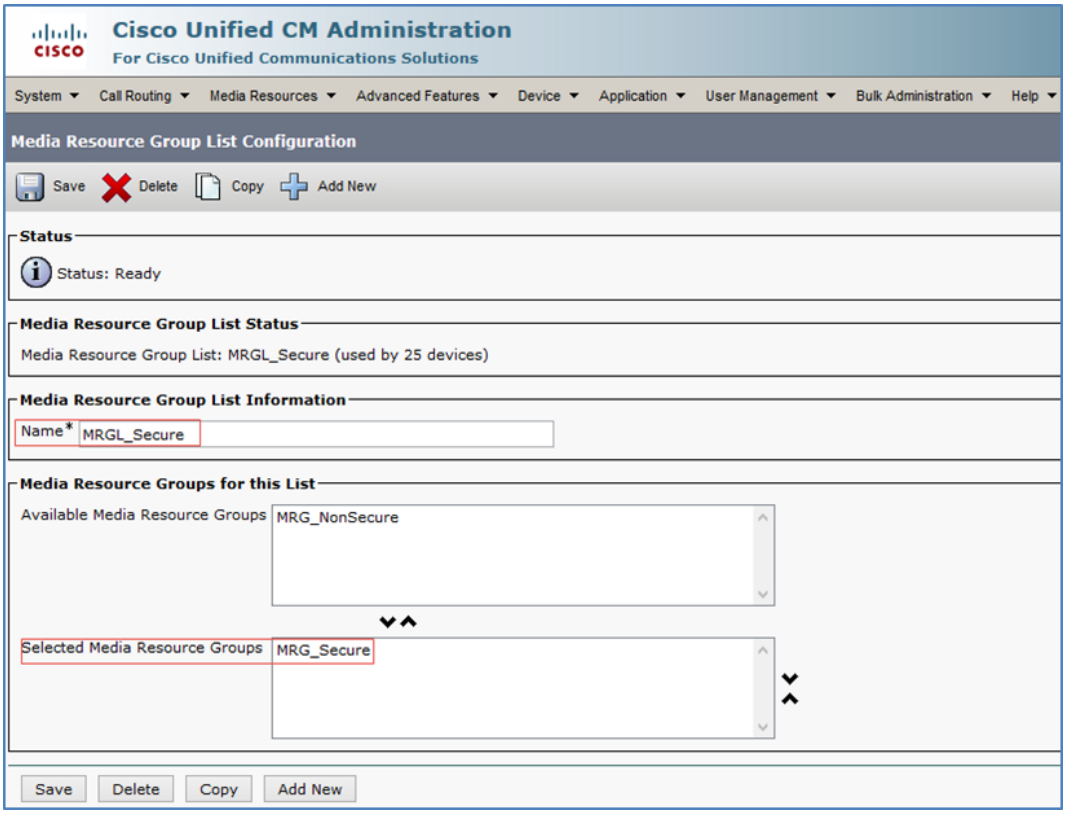
3. Enter **MRG_Secure_trk** for the **Name** (for this example).
4. Transfer media resources between the two lists.
    a. In the **Devices for this Group** section, select **Crestronrtr (CFB)** and **SRTP-MTP** from the **Available Media Resources** list.
    b. Click **V** (between the two lists) to move the selected resource to **Selected Media Resources** (for this example).

Configure the Cisco UCM Conference MRG List

To configure the **MRGL_Secure** Media Resource Group List (for this example):

1. Click **Media Resources** > **Media Resource Group List.**
2. Click **Add New**.

Cisco UCM: Media Resource Group List Configuration



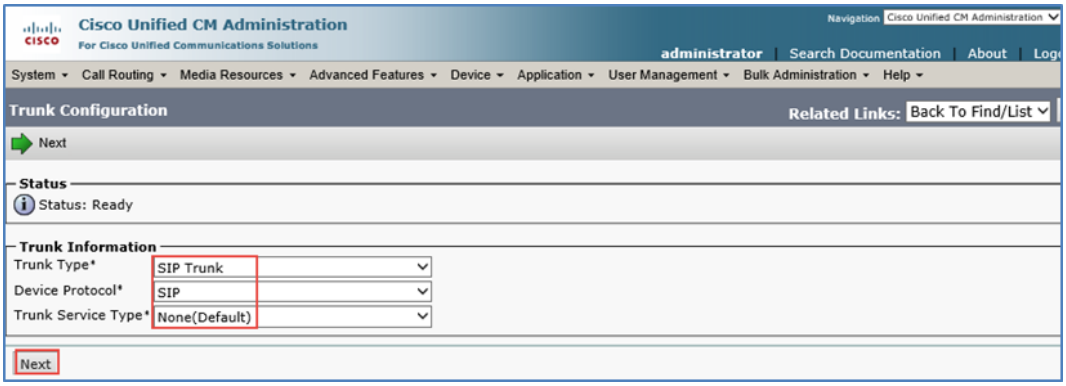
3. Enter **MRGL_Secure** for the **Name** (for this example).
4. Transfer media resource groups between the two lists.
    a. In the **Media Resource Groups for this List** section, select **MRG_Secure** from the **Available Media Resource Groups** list.
    b. Click **V** (between the two lists) to move the selected resource to **Selected Media Resource Groups** (for this example).

Configure the Cisco UCM - PSTN Gateway Trunk

This example configures a trunk between the Cisco UCM and the Cisco UBE to route PSTN calls.

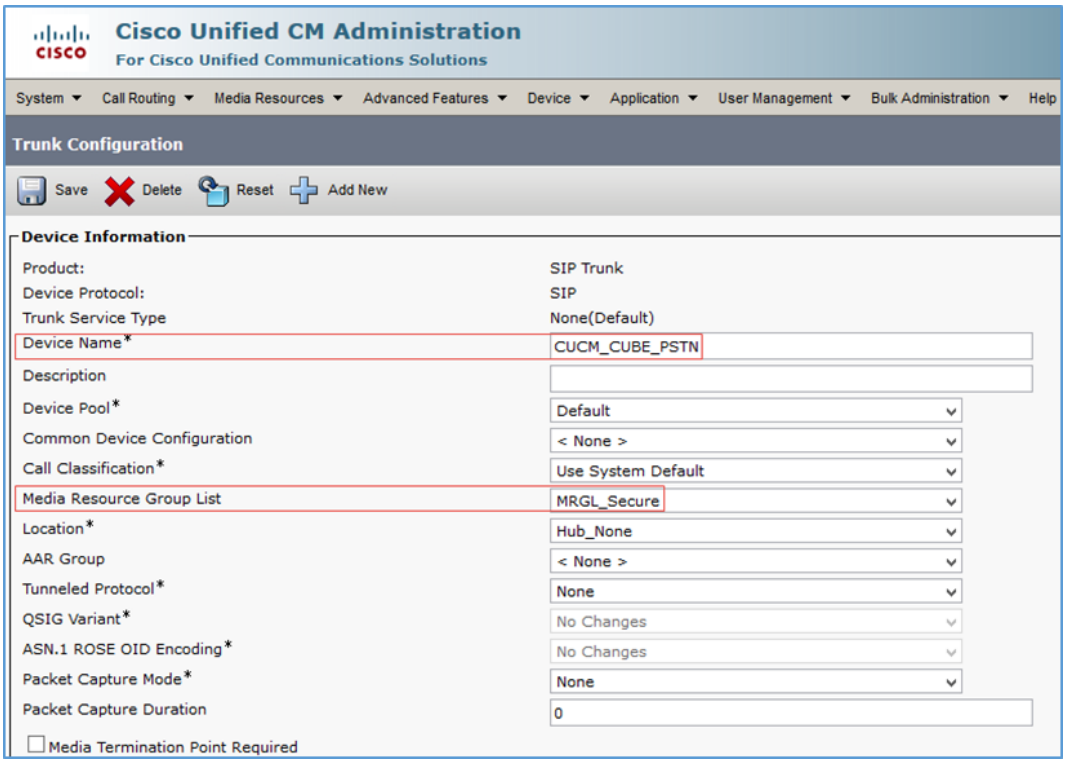
To create a new trunk:

1. Click **Device** > **Trunk**.
2. Click **Add New**.
   Cisco UCM: Add New Trunk



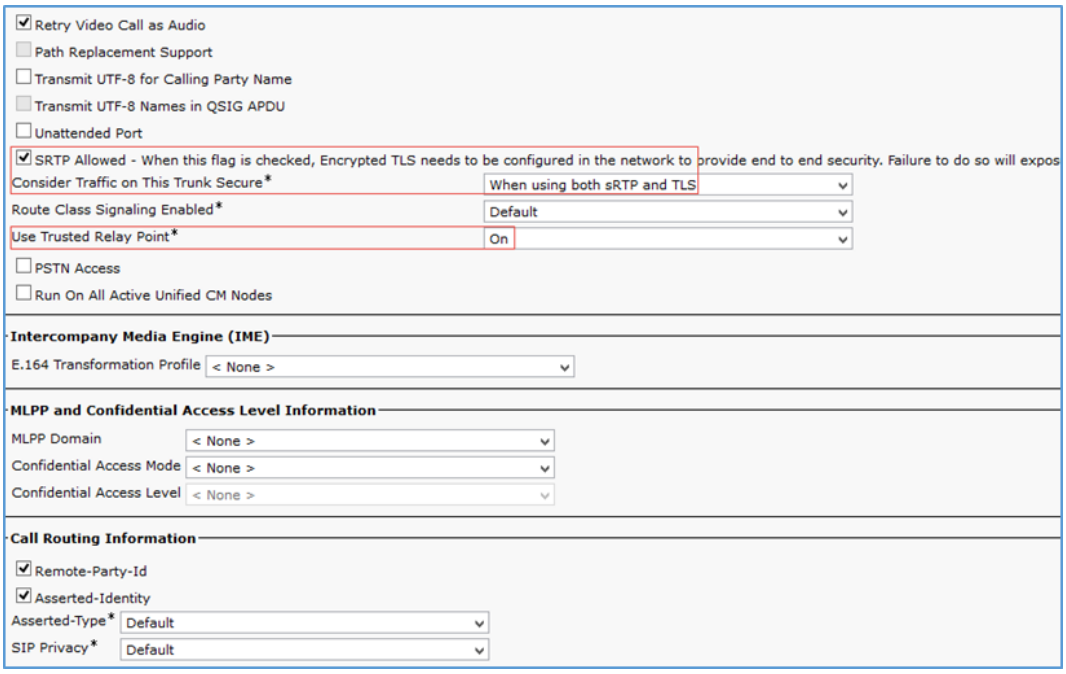
3. In the **Trunk Information** section, do the following:
   a. Select **SIP Trunk** for the **Trunk Type**.
   b. Select **SIP** for the **Device Protocol**.
   c. Select **None(Default)** for the **Trunk Service Type**.
4. Click **Next**.

Cisco UCM: Configure Cisco UCM-PSTN Trunk Parameters (1/5)



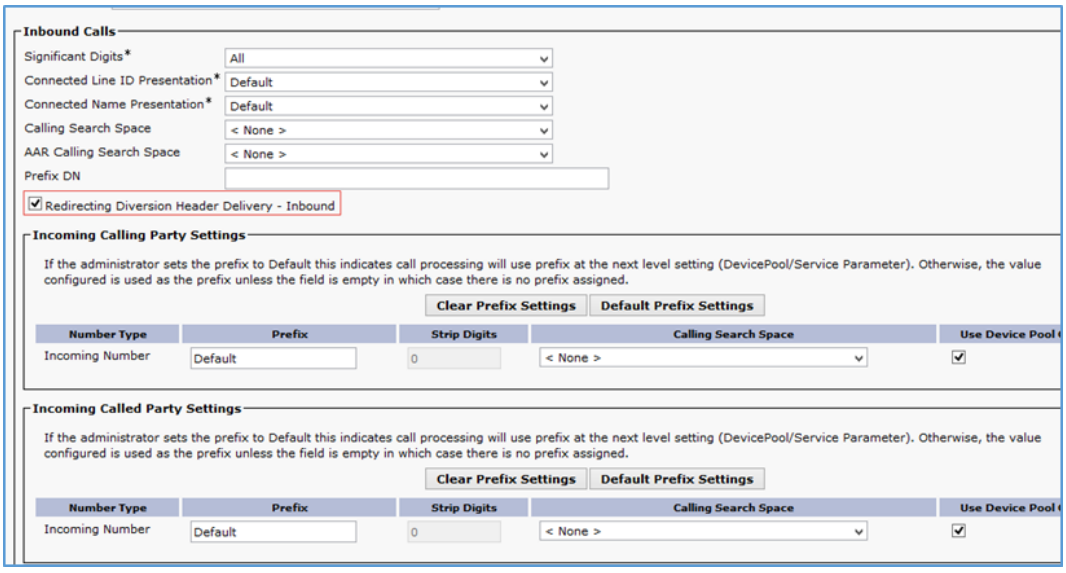
5. Enter a unique SIP Trunk name for the **Device Name**. This example uses **CUCM_CUBE_PSTN**. A **Description** is optional.
6. Select **Default** for the **Device Pool** (for this example).
7. Select **MRGL_Secure** for the **Media Resource Group List**.
8. Uncheck **Media Termination Point Required**.

Cisco UCM: Configure Cisco UCM-PSTN Trunk Parameters (2/5)



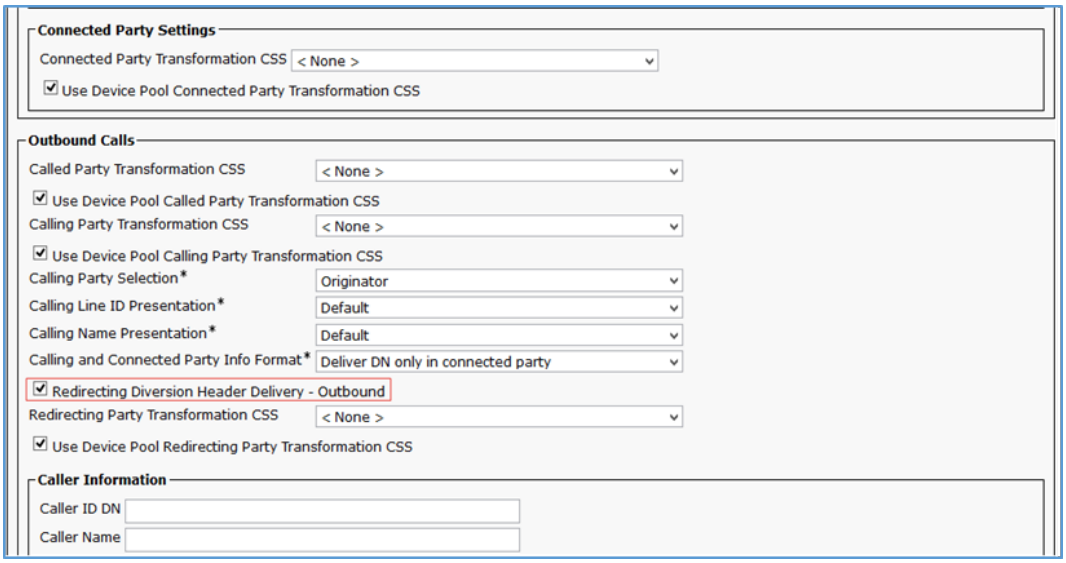
9. Check **SRTP Allowed**.
10. Select **When using both sRTP and TLS** for **Consider Traffic on This Trunk Secure**.
11. **Select On for Use Trusted Relay Point.**

Cisco UCM: Configure Cisco UCM-PSTN Trunk Parameters (3/5)



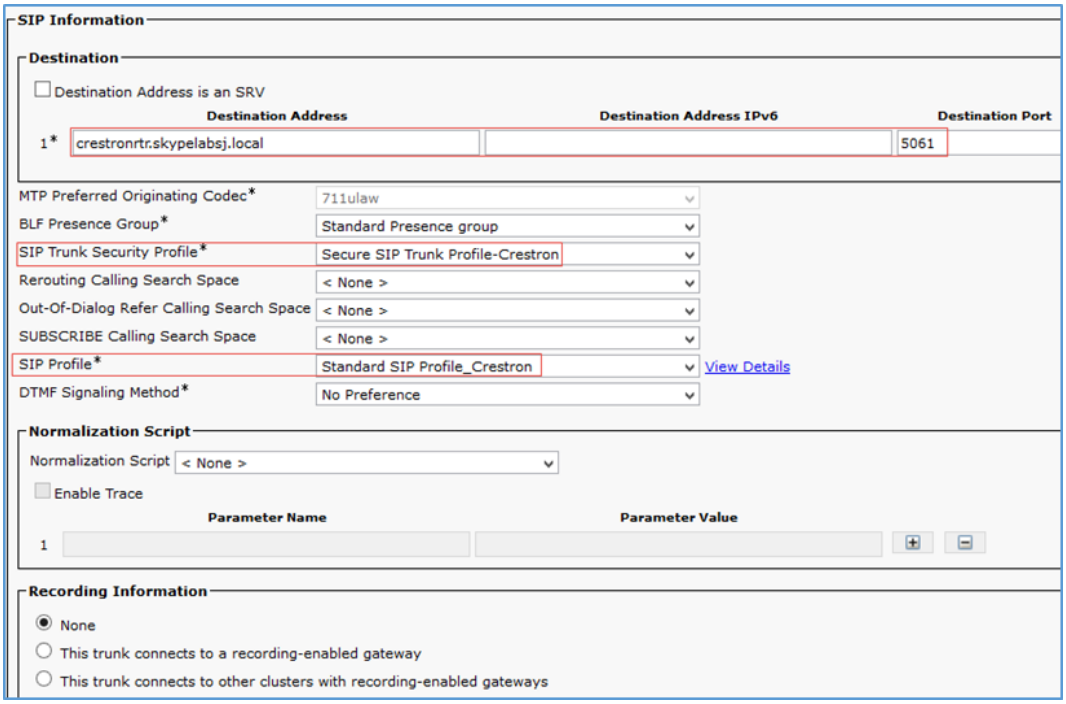
12. Check **Redirecting Diversion Header Delivery - Inbound**.

Cisco UCM: Configure Cisco UCM-PSTN Trunk Parameters (4/5)



13. Check **Redirecting Diversion Header Delivery - Outbound**.

Cisco UCM: Configure Cisco UCM-PSTN Trunk Parameters (5/5)



14. In the **SIP Information** section:
    a. Enter the FQDN of the Cisco UBE and port of the Cisco UBE LAN interfacefor the **Destination Address** and **Destination Port**, respectively.
    b. Select **Secure SIP Trunk Profile-Crestron** for the **SIP Trunk Security Profile**.
    c. Select **Standard SIP Profile_Crestron** for the **SIP Profile**.
15. Click **Save**.

Configure Route Patterns

Configure the following route patterns.

- Route calls from the Cisco UCM to the Cisco UBE toward PSTN gateway.
- Restrict Caller ID on outgoing calls.

To configure route patterns:

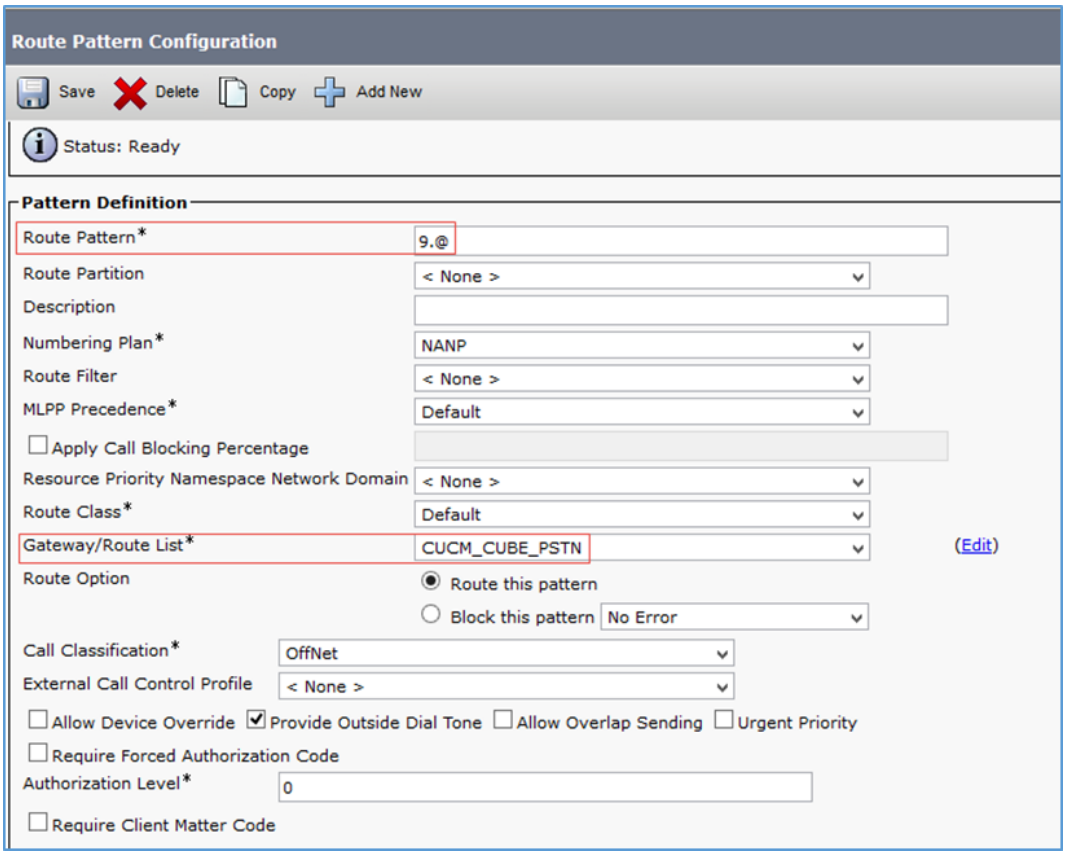
1. Click **Call Routing** > **Route/Hunt** > **Route Pattern**.
2. Click **Add New**.
3. Enter the desired information and then click **Save**.

PSTN Route Pattern

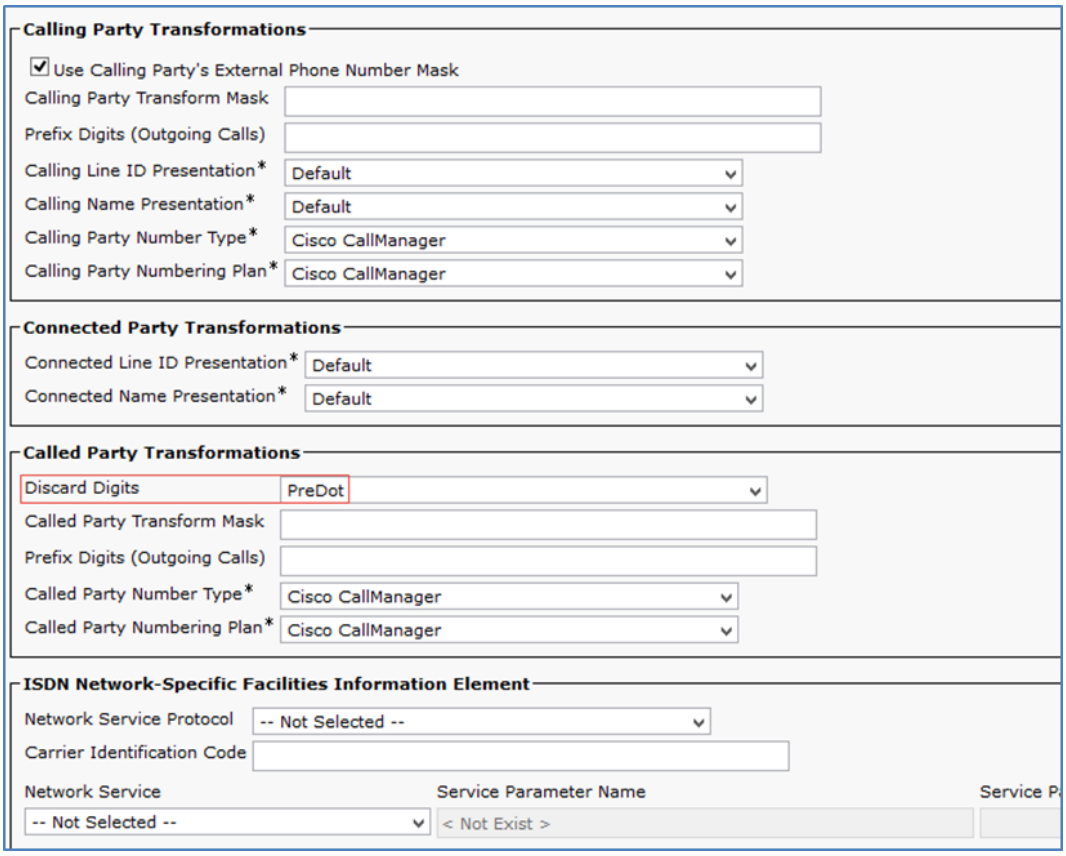
Configure the **9.@** route pattern to enable outbound calling from Cisco UCM to Cisco UBE using 9 as the access code.

The screenshots that follow show the configuration.

Cisco UCM: Route Pattern - Outbound Dialing Using Access Code 9 (1/2)



Cisco UCM: Route Pattern - Outbound Dialing Using Access Code 9 (2/2)

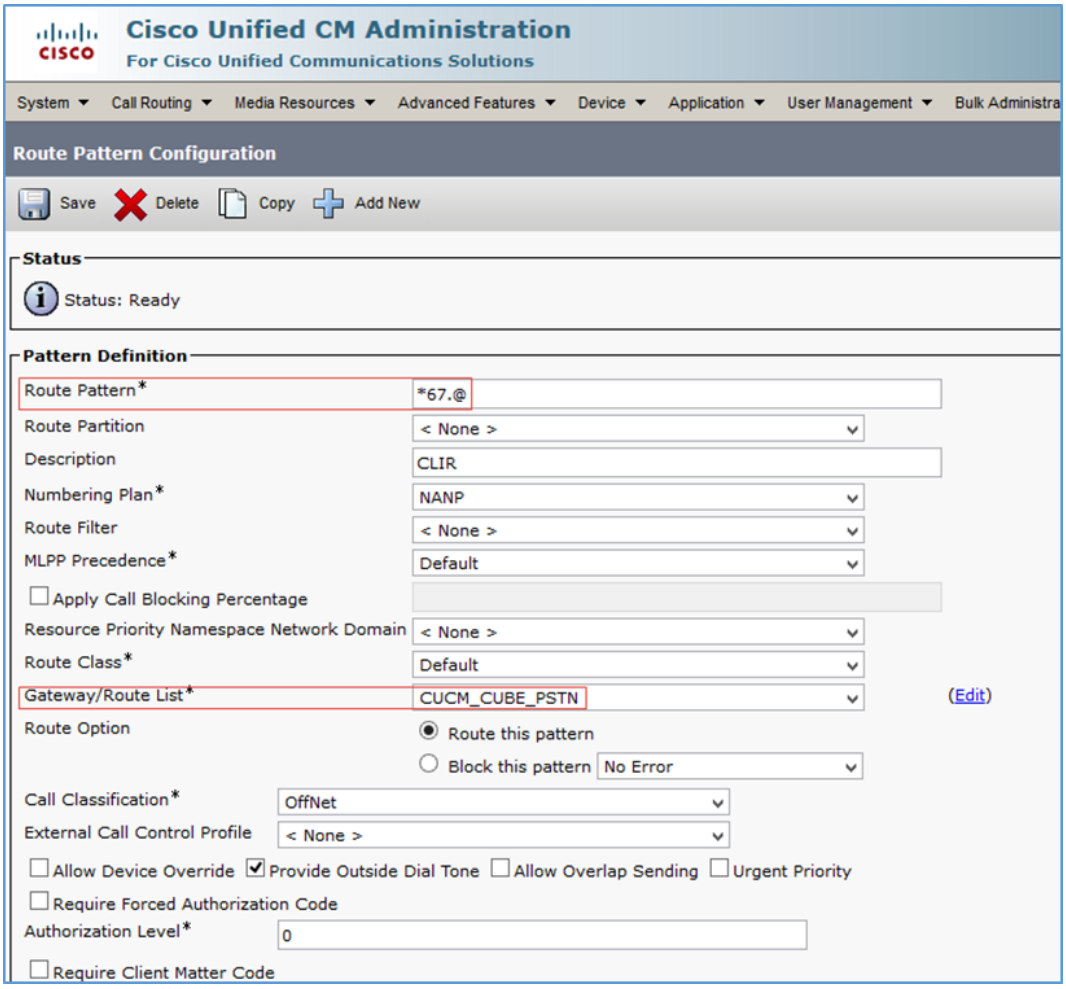


Restricted Caller ID Route Pattern

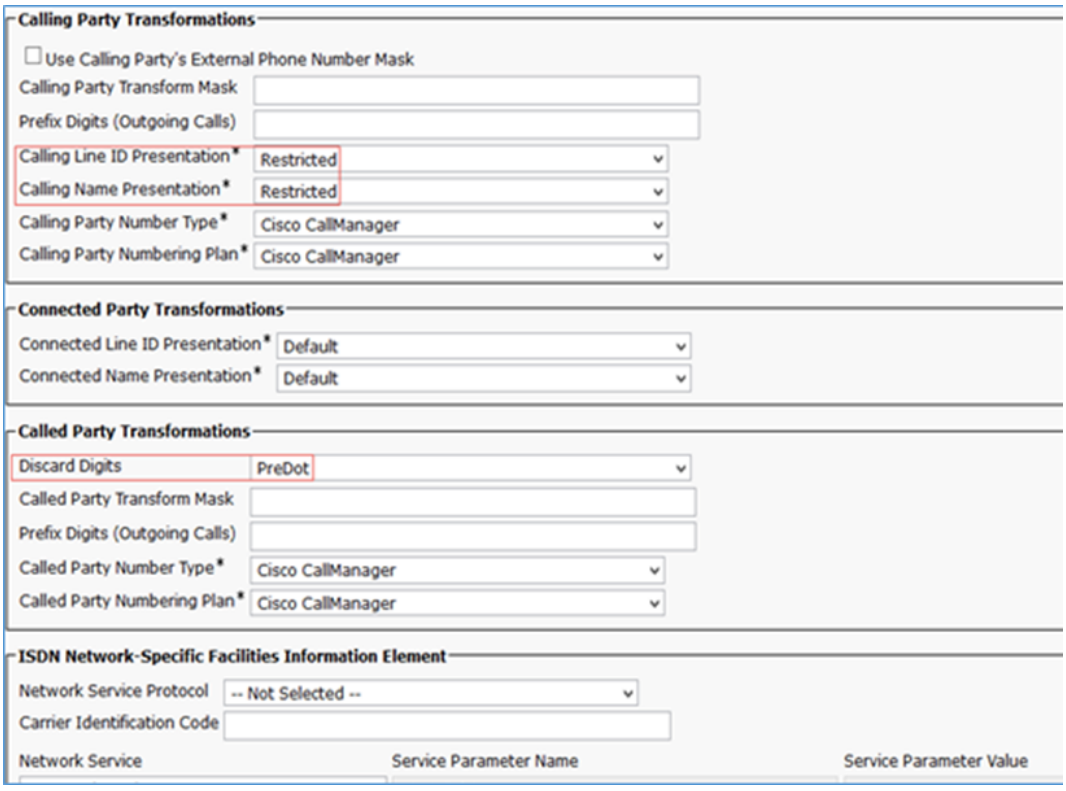
Configure the ***67.@** route pattern to restrict Caller ID on outbound calls.

The screenshots that follow show the configuration.

Cisco UCM: Route Pattern - Restrict Caller ID (1/2)



Cisco UCM: Route Pattern - Restrict Caller ID (2/2)



Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7656
www.crestron.com

Configuration Guide — 8336B
2052156
10.18
Specifications subject to
change without notice.