CCS-UC-1

Secure SIP Endpoint with Cisco® Unified Communications Manager 11.0

Configuration Guide

Crestron Electronics, Inc.

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited non-exclusive, non-transferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

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, please visit www.crestron.com/opensource.

Crestron, the Crestron logo, AirMedia, Crestron Mercury, and Crestron Toolbox are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Bugzilla is either a trademark or registered trademark of the Mozilla Foundation in the United States and/or other countries. Cisco is either a trademark or registered trademark of Cisco Systems, Inc. in the United States and/or other countries. Microsoft is either a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

This document was written by the Technical Publications department at Crestron.
©2017 Crestron Electronics, Inc.

Contents

CCS-UC-1: Secure SIP Endpoint with Cisco Unified Communications Manager 11.0

Introduction

This configuration guide describes the necessary procedure to configure a Crestron Mercury™ device, in a secure mode, to register to the Cisco® Unified Communications Manager as a basic AS SIP endpoint.

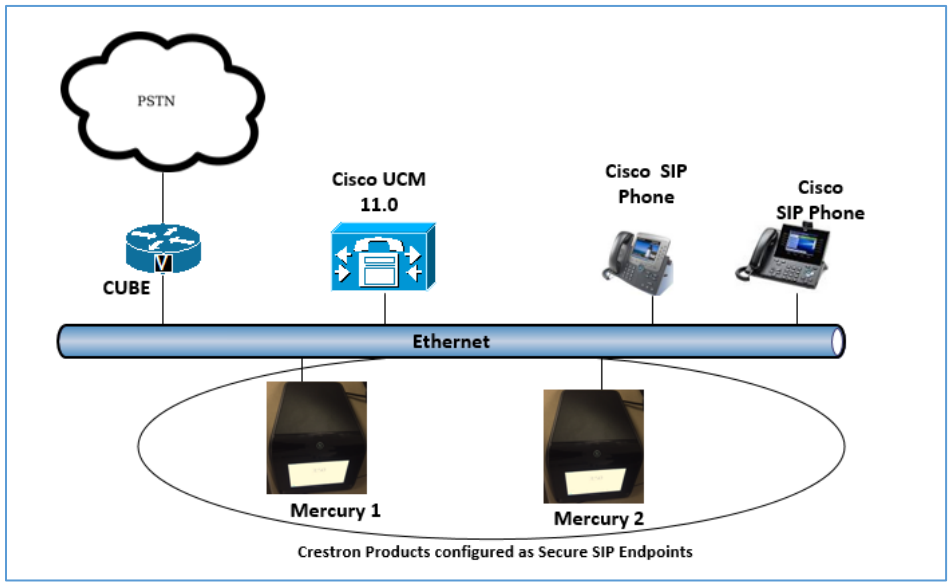
Audience

This document is intended for users attempting to configure and use the Crestron Mercury devices as secure SIP endpoints registering to the Cisco Unified Communications Manager (Cisco UCM).

Topology

The network topology for the Crestron Mercury endpoint to interop with the Cisco UCM is shown below.

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 Mercury as the secure SIP endpoints
- Cisco UBE (CUBE) to ensure secure signaling and media within the enterprise for PSTN calls

Software Requirements

- Cisco Unified Communications Manager v 11.0.1.20000-2
- Cisco UBE v 15.6
- Crestron Mercury devices v 1.3291.00019.001 or 1.3318.0002 (for G729 testing)

Hardware Requirements

- Cisco UCS-C240-M3S VMWare Host running ESXi 5.5
- Cisco 3845 as PSTN Gateway
- Cisco UBE as an SBC
- Cisco phone models: 8961 (SIP) and 8945 (SIP)
- Crestron Mercury devices (2)

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® product for conference rooms that integrate microphones and speakers into the user interface at the table.

Crestron Toolbox™ is used to discover and control all Crestron devices on the network.

The Crestron Mercury web interface is used to control the Crestron Mercury devices on the network.

Summary

The Crestron Mercury devices, in secure mode, are configured on the Cisco UCM as Assured Service (AS) SIP endpoints. The devices successfully register to the Cisco UCM with digest authentication.

The sections below describe supported and unsupported features on a Crestron Mercury device.

Features Supported

- Secure Mode: establishes a secure SIP and RTP session with the Cisco UCM
- Registration with digest authentication
- Basic calls with G729, G722, G711u, and G711a codecs
- Caller ID (limited to only calling number)

- DTMF support
- Early media support
- Retrieval of a parked call
- Transferee in a call transfer
- Conference participant
- Member of hunt group

Features Not Supported

- Caller ID presentation with name and number display
- Call hold and resume
- Call forwarding on the device (Forwarding can be configured on the PBX for the DN assigned to the endpoint.)
- Call waiting
- Conference
- Initiating attended call transfer
- Initiating semi-attended call transfer
- Initiating blind call transfer
- Configuration of shared line on device
- Initiating call park
- Do Not Disturb (DND)

Known Issues and Limitations

- Caller ID is not supported on the device. Currently only the calling party number is displayed as the caller ID. This issue is tracked via Crestron's Bugzilla™ software, Defect: 119006.
- The active call timer on the device does not reflect the correct call duration. The active call duration includes the time for which the unit was being alerted also. This issue is tracked via Crestron's Bugzilla software Defect: 124001.
- The first ringback heard on the device is stuttered – resembles a mix of local and remote ringback. This issue is tracked via Crestron's Bugzilla software Defect: 122421.
- On the Crestron Mercury web user interface, there is currently no notification provided to the user when certain mandatory configurations are missing. This issue is tracked via Crestron's Bugzilla software Defect: 125193.
- On the Crestron Mercury web user interface, a configuration of DHCP OFF on the Network configuration page mandates configuration of both the adapters. The user is unable to save changes unless both the adapters are configured and is notified of an invalid IP against the default of 0.0.0.0 for an unused adapter. This issue is tracked via Crestron's Bugzilla software Defect: 126236.

- On the Crestron Mercury web user interface, there is currently no check to validate whether a certificate that is being deleted is in use, i.e., whether it is on the trusted list or not. This issue is tracked via Crestron's Bugzilla software Defect: 126232.
- On the Crestron Mercury device, for certain called numbers that cannot be reached or are invalid, the user only hears a reorder tone and does not have the option to disconnect the call except by pressing the call button again. This issue is tracked via Crestron's Bugzilla software Defect: 122633.

Crestron Mercury Configuration

Setup

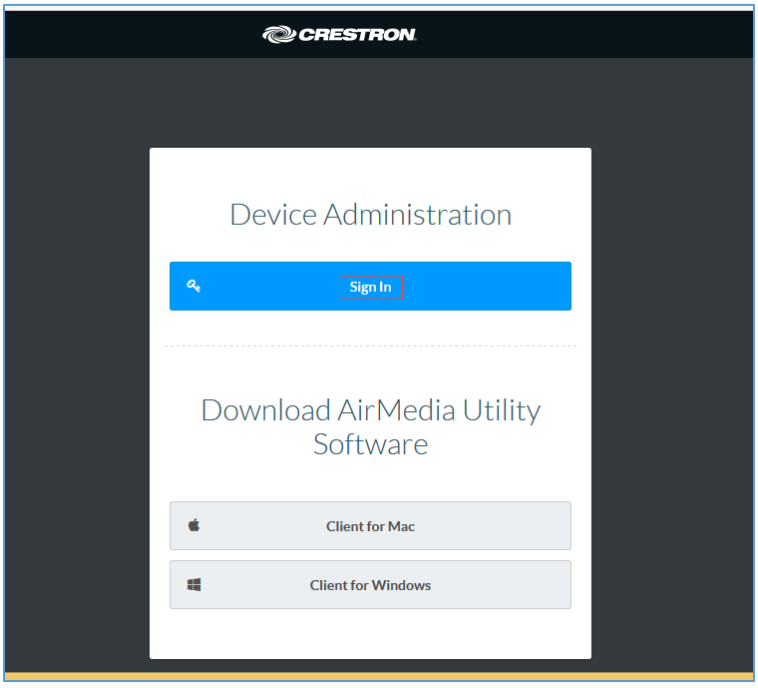
The LAN port of the Crestron Mercury device needs to be connected to one PoE+ port to power it up and network connectivity with the Cisco UCM. The PoE+ switch that is used should have the LLDP functionality enabled for the device to power up and be completely functional. By default, the "poeplus" configuration is set to Off on the device.

Configuring the device

To configure this device, follow this procedure:

1. Access the web GUI for the device by using an http session with the device's IP address. The device IP address *10.80.25.50* was used in this example. The initial page that displays is shown below.

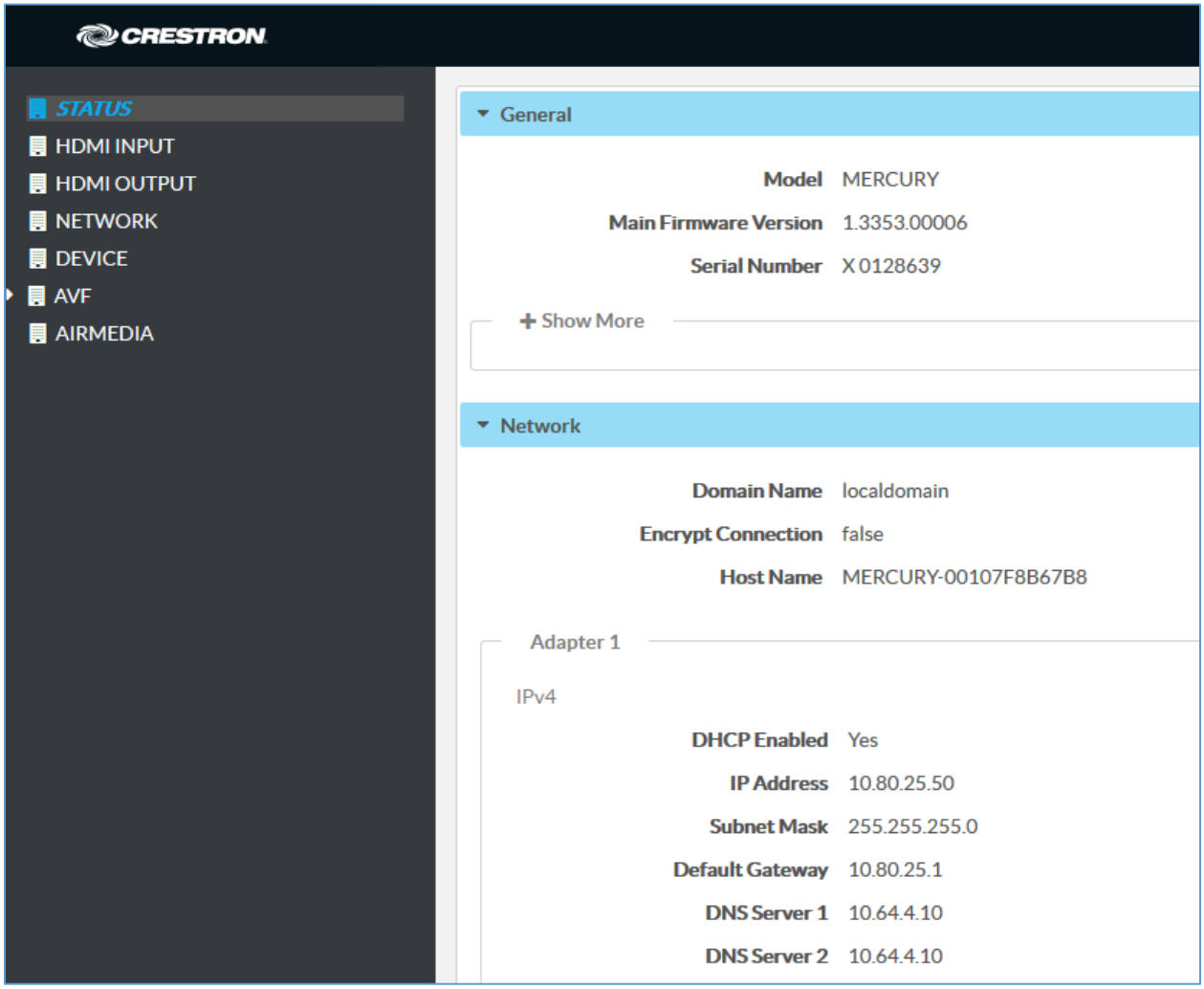
   Crestron Mercury: Login to Web GUI



2. Click **Sign In** and log in to the device. For information on device administration, refer to the CCS-UC-1 Supplemental Guide (Doc. 7844) at www.crestron.com/manuals.

   The Status screen that appears displays basic information on the device.

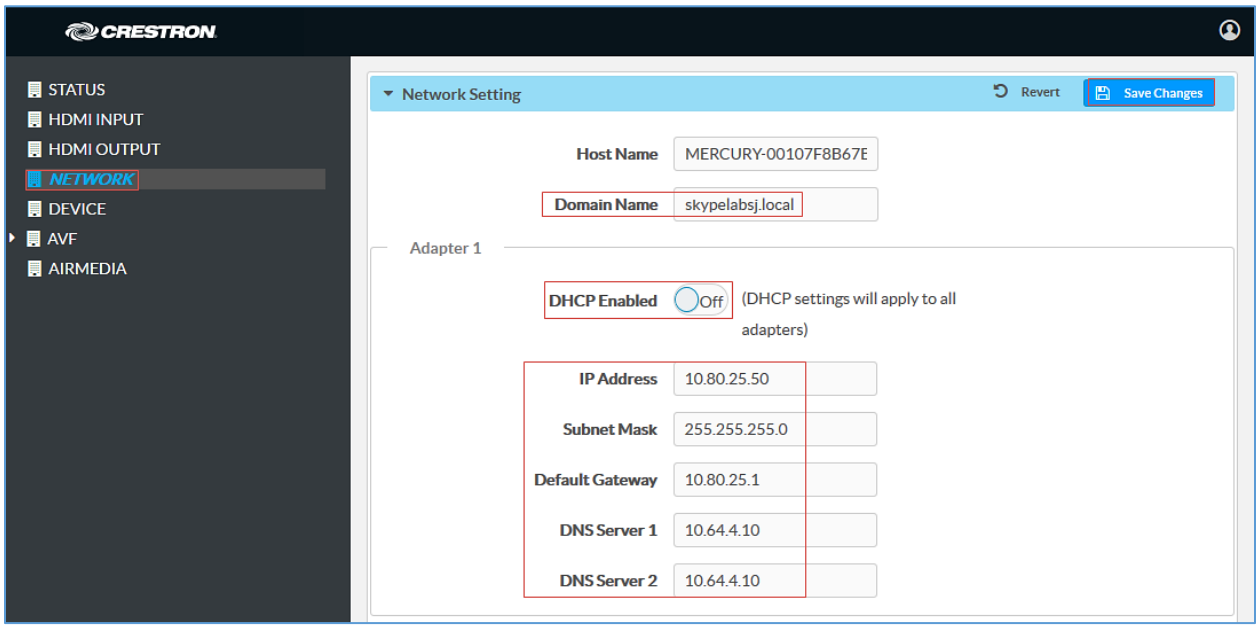
Crestron Mercury: Status



   The device can be configured from the **Network** page.

3. On the web GUI, navigate to **Network**.

Crestron Mercury: Network Setting: DHCP Off: Static IP Configured



4. Enter the following parameters in the **Adapter 1** section to configure the Crestron Mercury device.
   - **Domain Name**: *skypelabsj.local* was used in this test
   - **DHCP**: Choose either of the following:
     - Obtain an IP address automatically
     - Use the following IP address

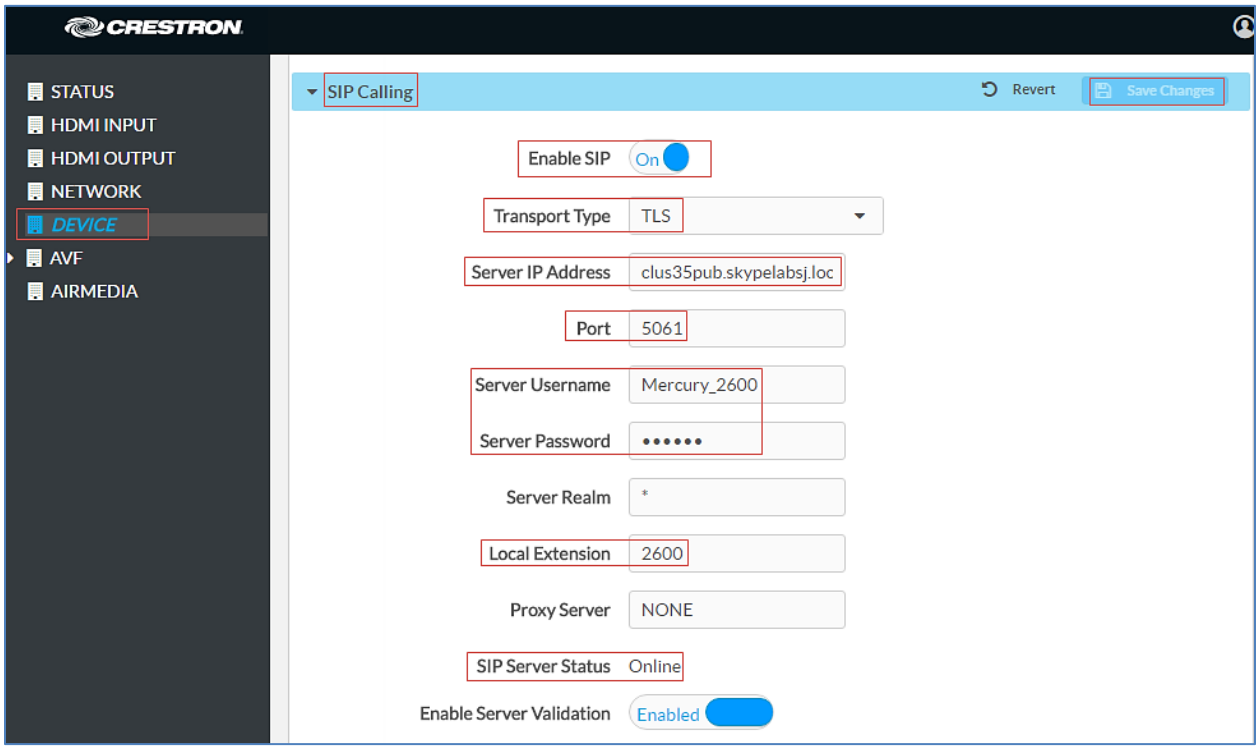
       For the test, a static IP was configured.
       - **IP address**: *10.80.25.50* was used in this example
       - **Subnet Mask**: *255.255.255.0* was used in this example
       - **Default Gateway**: *10.80.25.1* was used in this example
       - **DNS Servers**: *10.64.4.10* was used in this example
5. Click **Save Changes**.

Configuring the TLS SIP Parameters

To configure the TLS SIP parameters, follow this procedure:

1. On the web GUI, navigate to **Device** > **SIP Calling**.

Crestron Mercury: Device Configuration: SIP Parameters



2. Enable the check box for **Enable SIP**.
3. Configure the **Server IP Address**: Enter the FQDN of the primary Cisco UCM node. *clus35pub.skypelabsj.local* was used in this example.
4. Configure the **Port**: *5061*, used in this example.
5. Configure the **Server Username**: Enter the end user configured on Cisco UCM for this device. *Crestron Mercury_2600* was used in this example.
6. Configure the **Server Password**: Enter the password as configured on Cisco UCM for this end user.
7. Configure the **Local Extension**: Enter the directory number that was configured for this device on Cisco UCM. *2600* was used in this example.
8. Leave all other fields at their default values.
9. Click **Save Changes**.

Once the device successfully registers with the Cisco UCM, the **SIP Server Status** updates its status to show *Online.*

Add Certificates

For a successful TLS handshake between the Crestron Mercury device and the Cisco UCM, the following certificates need to be added to the Crestron Mercury:

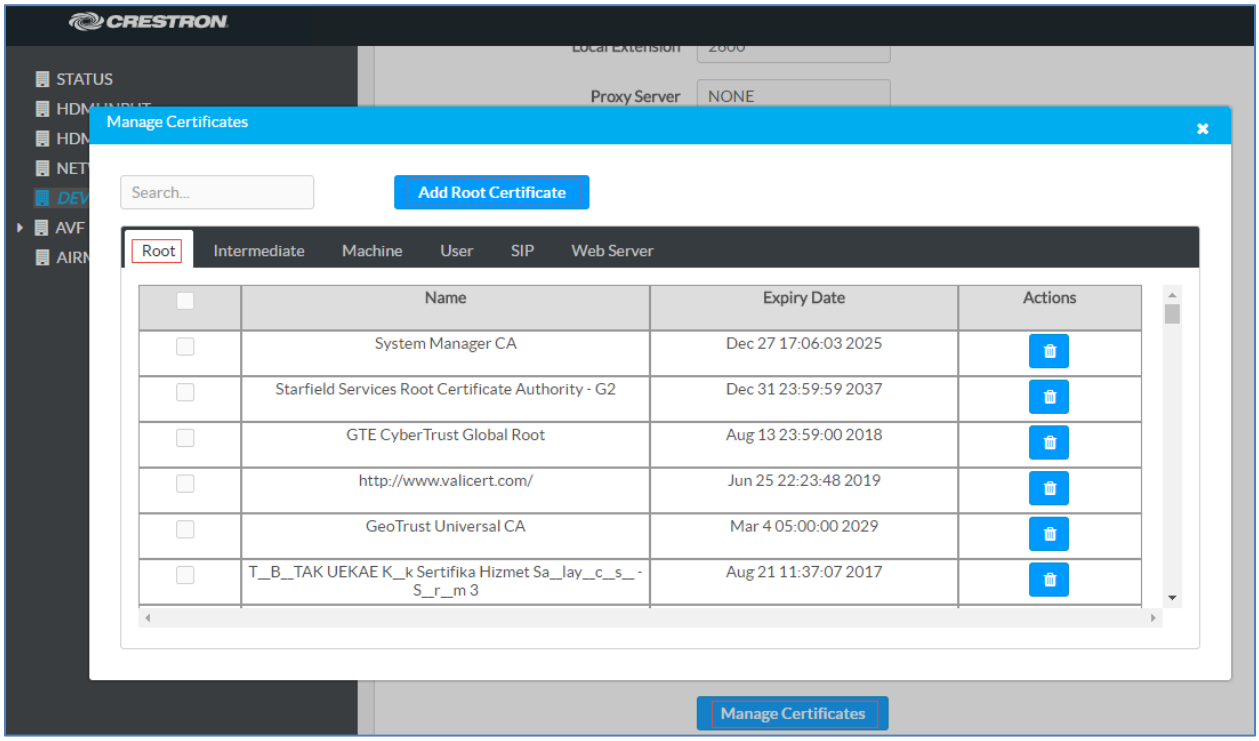
- RootCA certificate (*root_cer*). This is the certificate that is downloaded from the certificate authority that serves the Cisco UCM (the DNS IP configured on the CUCM and Crestron Mercury device). This certificate is required by the Crestron Mercury device to allow it to validate the Cisco UCM when Enable Server Validation is enabled in the **SIP Calling** configuration screen.
- SIP certificate (*sip-cert.pfx*). This is a specific device certificate that is downloaded from the same certificate authority that serves the Cisco UCM. This certificate contains information on the 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.

Add Root Certificate

To upload certificates to the device, follow this procedure:

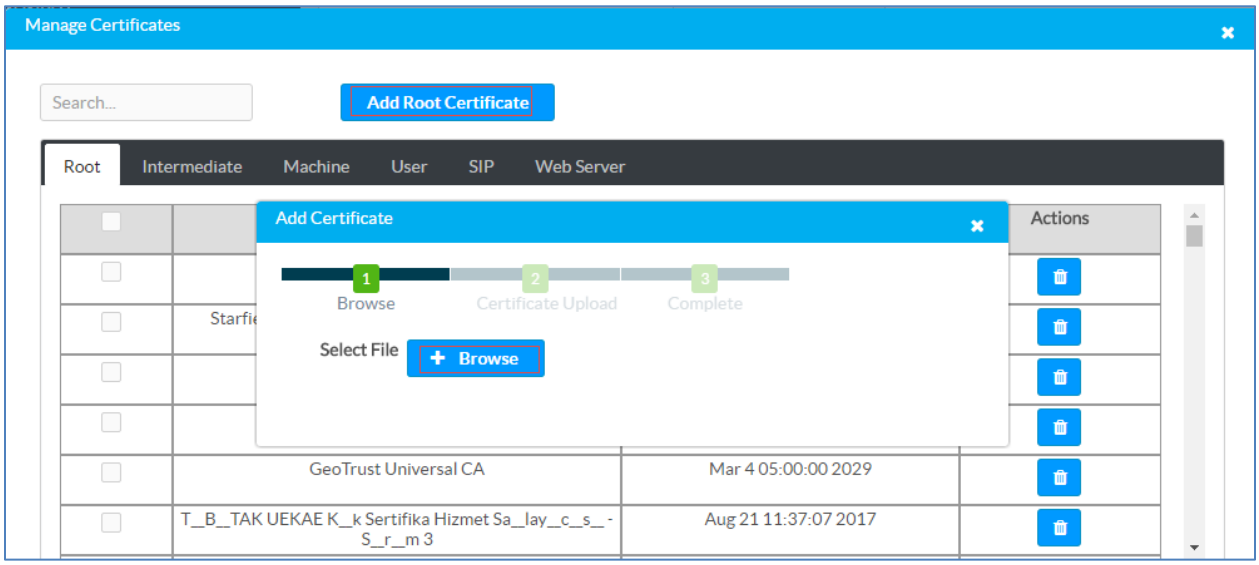
1. On the web GUI, navigate to **Device** > **SIP Calling**.
2. Click **Manage Certificates**.

Crestron Mercury Configuration: Manage Certificates: Add Root Certificate



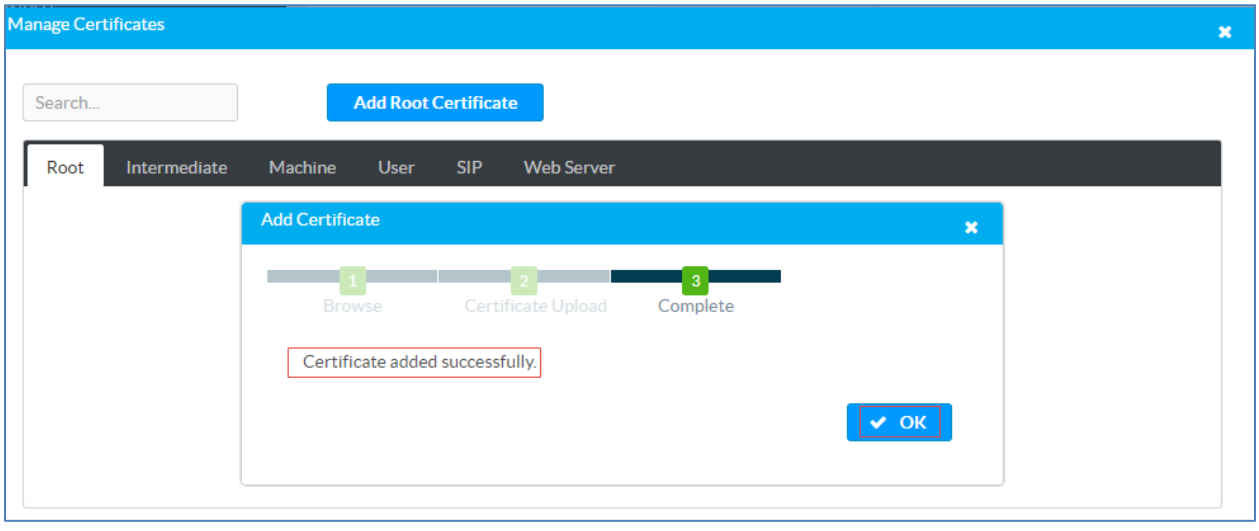
3. Click **Add Root Certificate**.

Crestron Mercury Configuration: Manage Certificates: Add Certificate: Browse



4. In the **Add Certificate** window, click **Browse**.
5. Select the *root_cer.cer* file that needs to be uploaded, and click **OK**.
6. On the screen that follows, click **Load**. The device indicates that the certificate was added successfully.

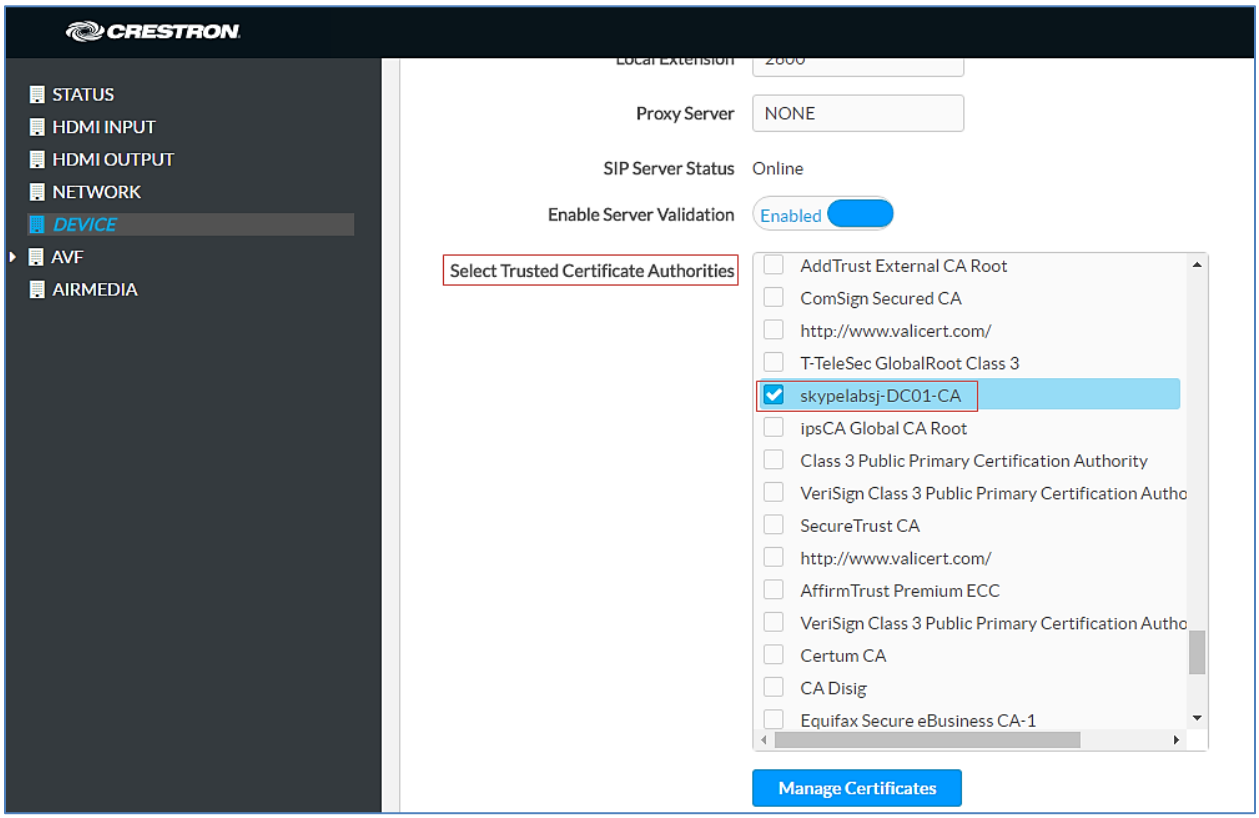
Crestron Mercury Configuration: Manage Certificates: Add Certificate: Add Complete



7. Click **OK** and close the **Manage Certificates** window.

   The certificate authority from where this root-cer certificate was downloaded appears in the list of trusted certificate authorities.
8. On the main **SIP Calling** screen, navigate to **Select Trusted Certificate Authorities**.

Crestron Mercury Configuration: SIP Calling: Select Trusted Certificate Authorities

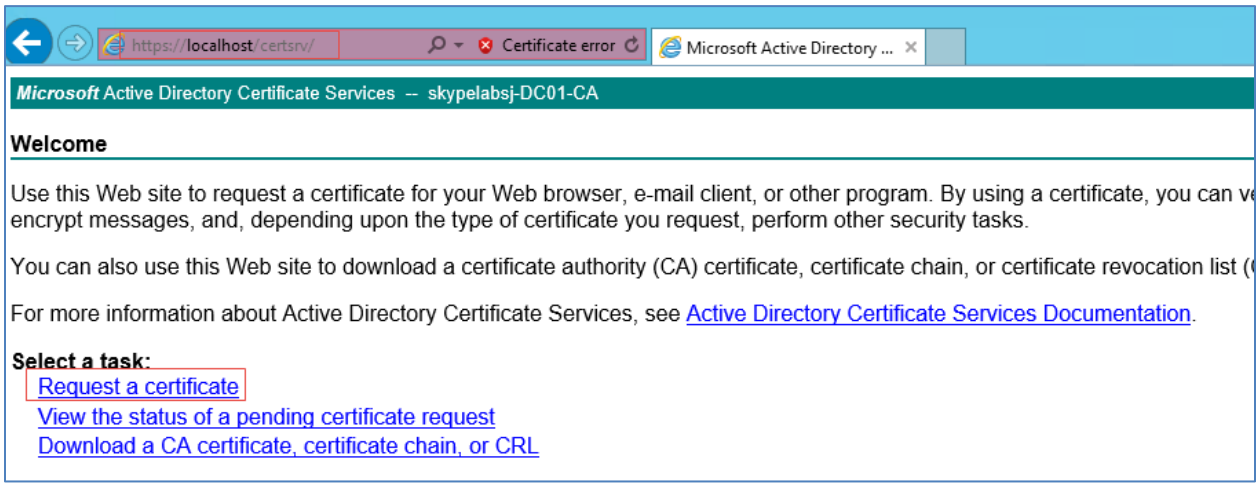


9. From the list of certificate authorities, select the certificate authority (from where the *root_cer.cer* certificate was downloaded).

Generate Device Certificate Request and Download Device Certificate from CA

On the CA, open a browser and access the Certificate Services. For this example, a Microsoft® Active Directory was used to generate a specific device certificate request.

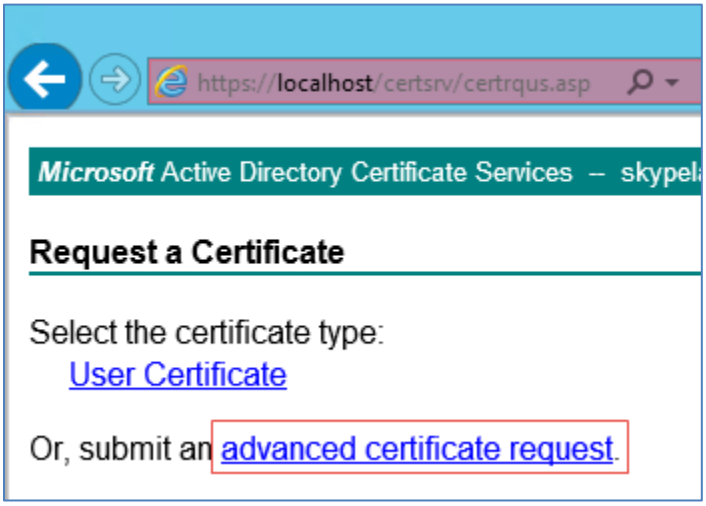
Certificate Authority: Request a Certificate



To generate and download a device certificate, follow this procedure:

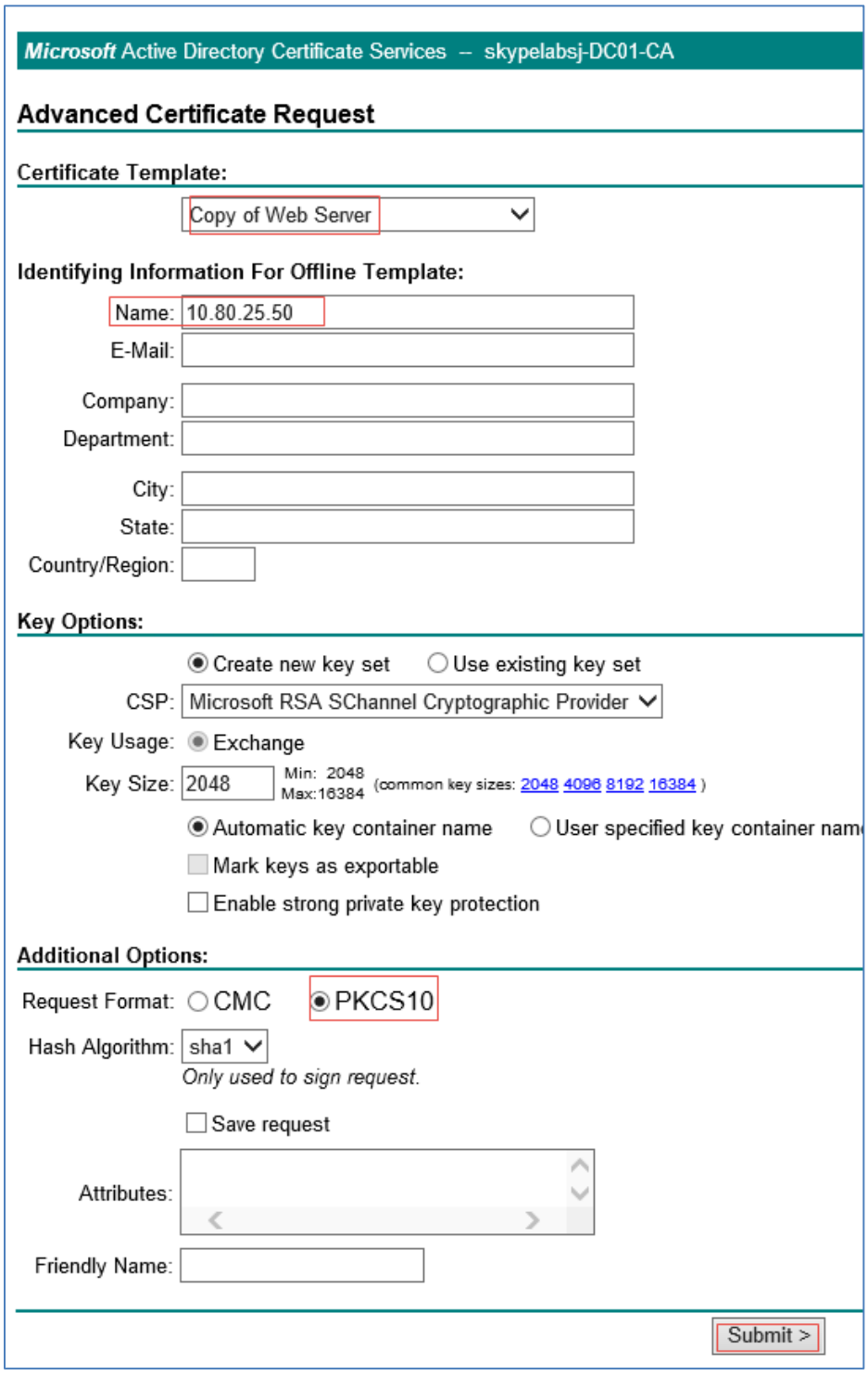
1. Click **Request a certificate**.

   Certificate Authority: advanced certificate request



2. Click **advanced certificate request**.
3. On the screen that follows, click **Create and Submit a request to this CA**.

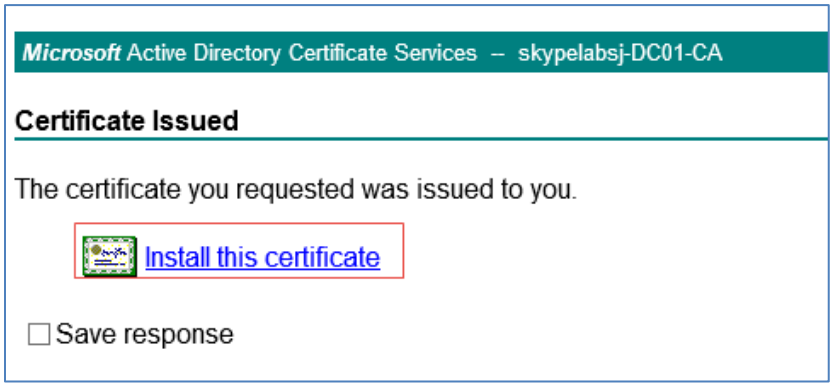
Certificate Authority: Submit Device-Specific Certificate Request



4. Select a **Certificate Template** that does client and server authentication. *Copy of Web Server* was used in this example.
5. Configure **Identifying Information for Offline Template**: **Name**: Assign the device IP to be the common name. The IP address used in this example is *10.80.25.50.*

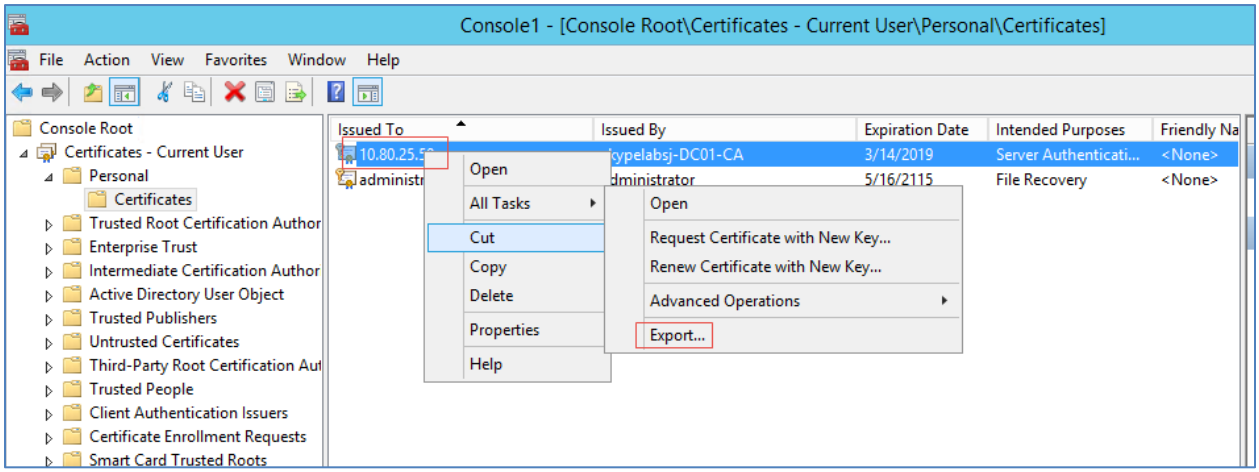
6. In the **Additional Options** section, configure the **Request Format**. *PKCS10* was used in this example.
7. Click **Submit**.

Certificate Authority: Install certificate



8. Click **Install this Certificate**.
9. Export this certificate from the certificate store

Certificate Authority: Export Device Certificate



The certificate should be exported as a ***sip_cert.pfx*** with the following parameters.

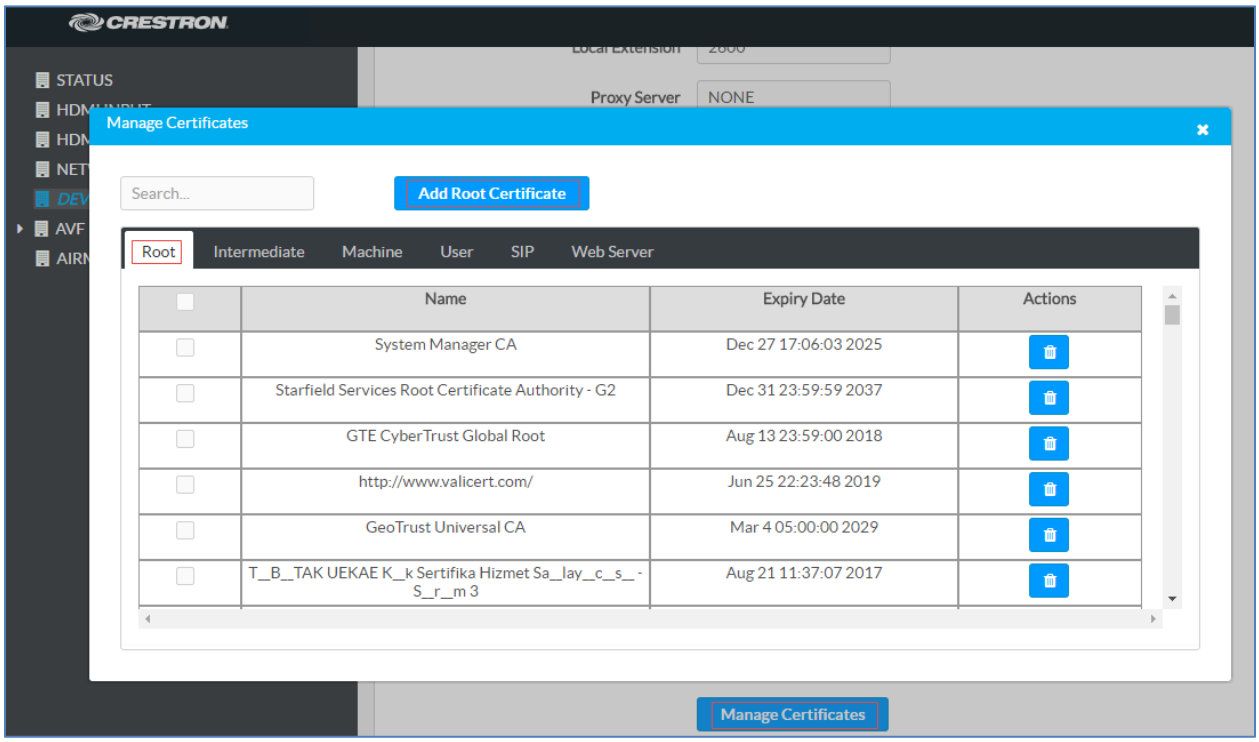
- The option to export the private key.
- The certificate should have a .PFX extension.
- A password. Enter this same password when importing this SIP certificate on the Crestron Mercury device.

Add SIP Certificate

To add a SIP certificate, follow this procedure:

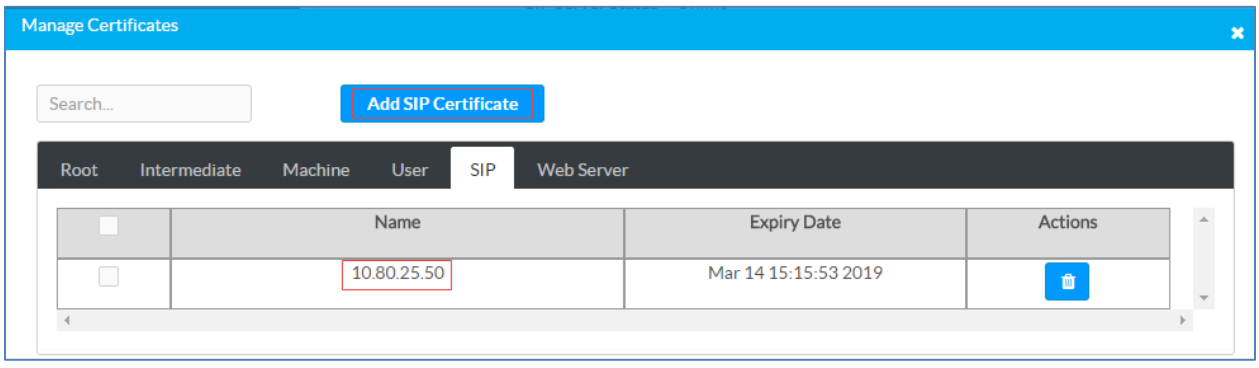
1. On the web GUI, navigate to **Device** > **SIP Calling**.
2. Click **Manage Certificates**.

Crestron Mercury Configuration: Manage Certificates



3. Click the **SIP** tab.

Crestron Mercury Configuration: Manage Certificates: Add SIP Certificate



4. Click **Add SIP Certificate**.
5. In the **Add Certificate** window, click **Browse**.
6. Select the sip_cert file that needs to be uploaded, and click **OK**.
7. Enter the password that was used when exporting this certificate on the CA.

The SIP certificate is now listed under the SIP tab. The name of the certificate is the common name provided when generating the device specific certificate request on the CA.

A typical TLS handshake consists of the following steps:

1. The Crestron Mercury device sends a Client Hello to the Cisco UCM server.
2. The Cisco UCM server sends a Server Hello.
3. The Cisco UCM server sends its certificate and a certificate request from the Crestron Mercury device.
4. The Crestron Mercury device sends its certificate.
5. The Crestron Mercury device verifies the server certificate.
6. The Cisco UCM Server changes the cipher spec and sends an encrypted handshake message.
7. Application data is exchanged between the the Cisco UCM and the Crestron Mercury device.

NOTE: The Crestron Mercury device supports TLS v1.0.

NOTE: The device itself uses SIP port 5060 (instead of 5061) to communicate to the Cisco UCM, even in a secure mode.

Cisco UCM Configuration

This section describes the Cisco UCM configuration necessary to integrate the Crestron Mercury device as a secure SIP endpoint.

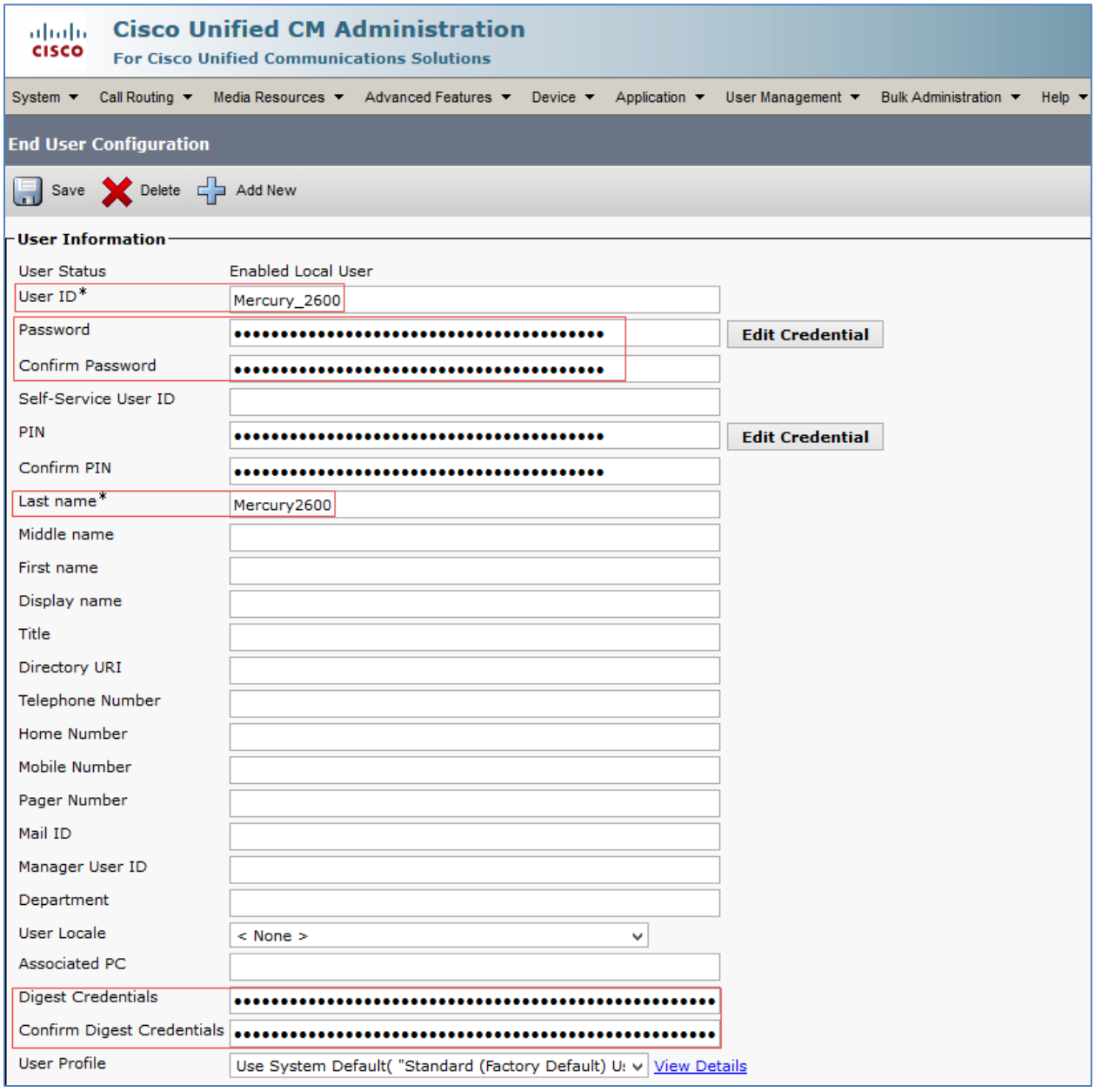
NOTE: It is assumed that the general installation and basic Cisco UCM configuration have already been administered.

Configure the End User

To configure the end user, follow this procedure:

1. Navigate to **User Management** > **End User**.
2. Click **Add New**. The End User configuration window appears.

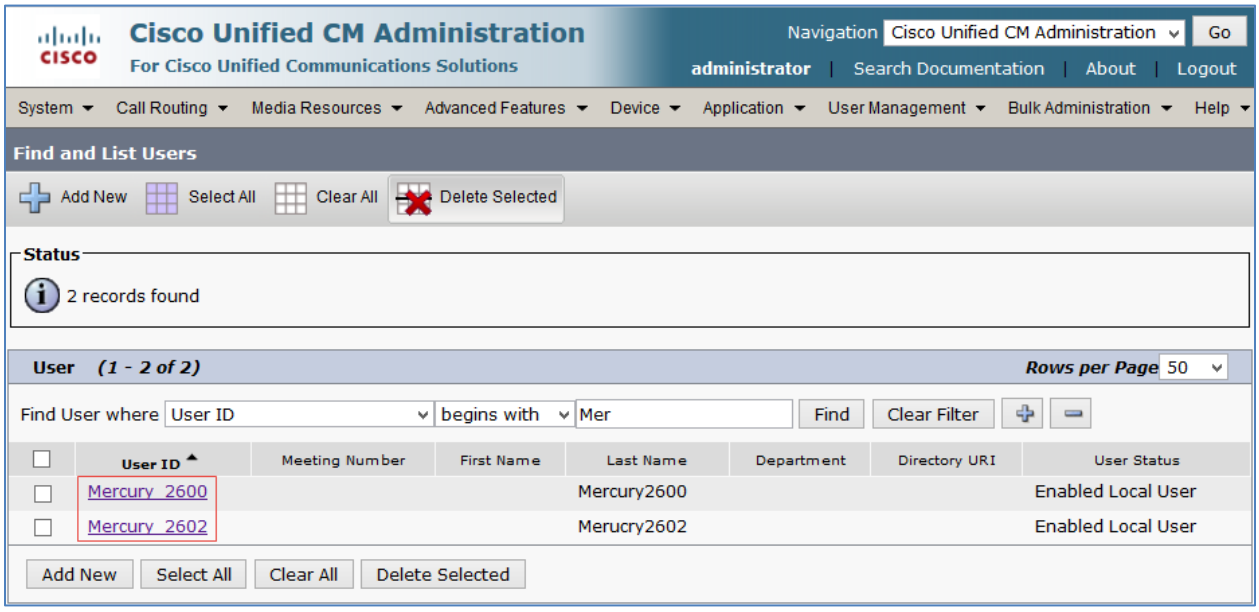
Cisco UCM: End User Configuration



3. Configure **User ID**: Enter a unique end user identification name. Two users were configured for this example for the Crestron Mercury devices: *Crestron Mercury_2600* and *Crestron Mercury_2602*.

4. Configure **Password**: Enter any password. This same password will be entered on the Crestron Mercury device against the SIP Server Password. The password in this example was *123456*.
5. **Confirm Password**: Re-enter the same password configured above.
6. Configure the **Last Name**: Enter the end user last name.
7. Configure the **Digest Credentials**: Enter a string of alphanumeric characters.
8. **Confirm Digest Credentials**: Re-enter the digest credentials entered above.
9. Click **Save**. All of the configured users are listed.

Cisco UCM: End Users Configured for All Crestron Mercury Devices



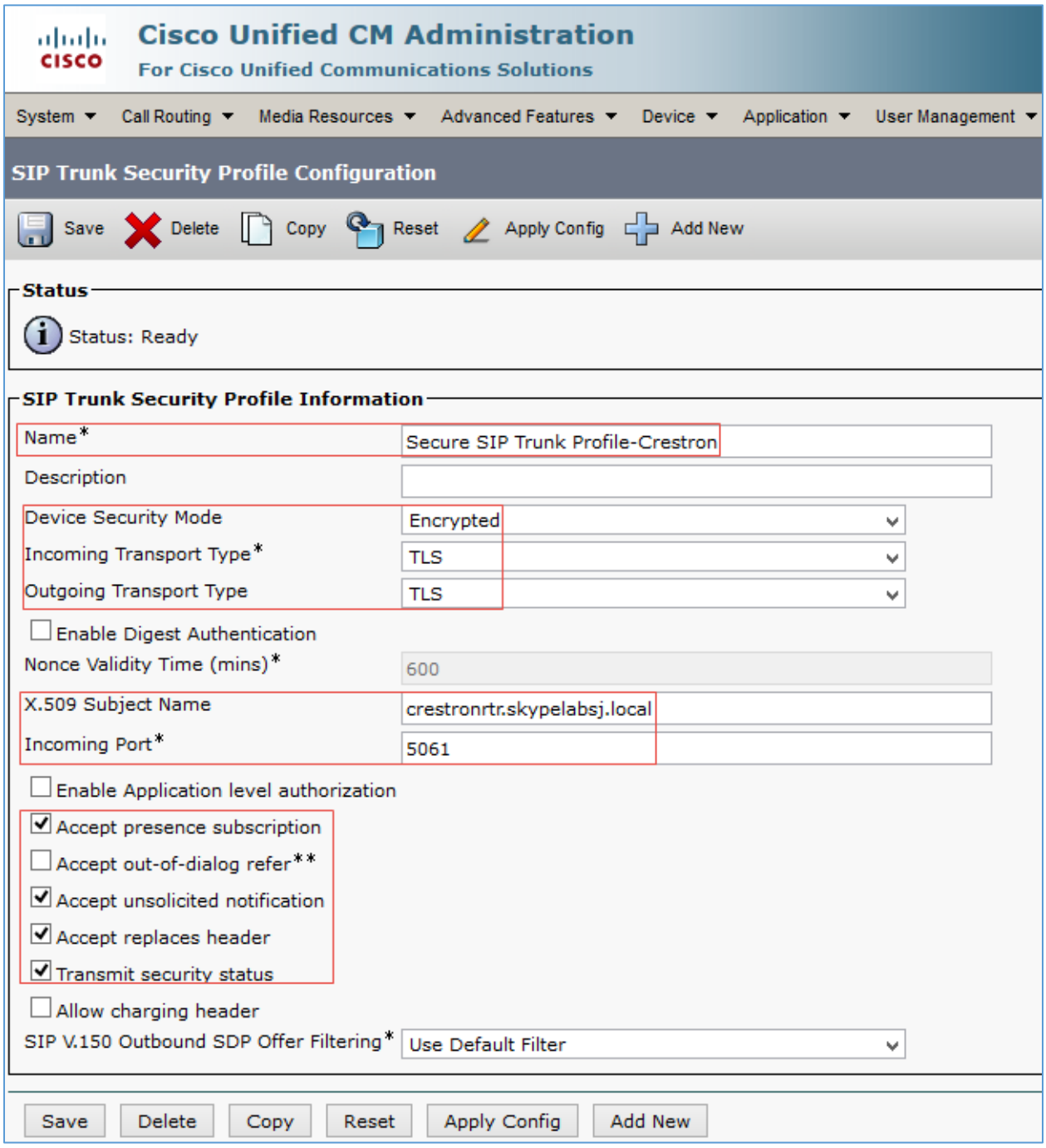
Configure a Secure SIP Trunk Security Profile

For the example, a new SIP Trunk Security Profile, **Secure SIP Trunk Profile-Crestron** was configured.

To add a new SIP Trunk Security Profile, follow this procedure:

1. Navigate to **System** > **Security** > **SIP Trunk Security Profile**.
2. Click **Add New**.

Cisco UCM: Secure SIP Trunk Security Profile Configuration



3. Configure a **Name:** *Secure SIP Trunk Profile-Crestron* was used in this example.
4. Configure **Device Security Mode**: *Encrypted*.
5. Configure **Incoming Transport Type**: *TLS*.
6. Configure **Outgoing Transport Type**: *TLS*.
7. Configure **X.509 Subject Name**: as the FQDN of the Cisco UBE. *crestronrtr.skypelabsj.local* was used in this example.
8. Configure **Incoming Port**: *5061* was used in the example.
9. Check the **Transmit security status** check box.

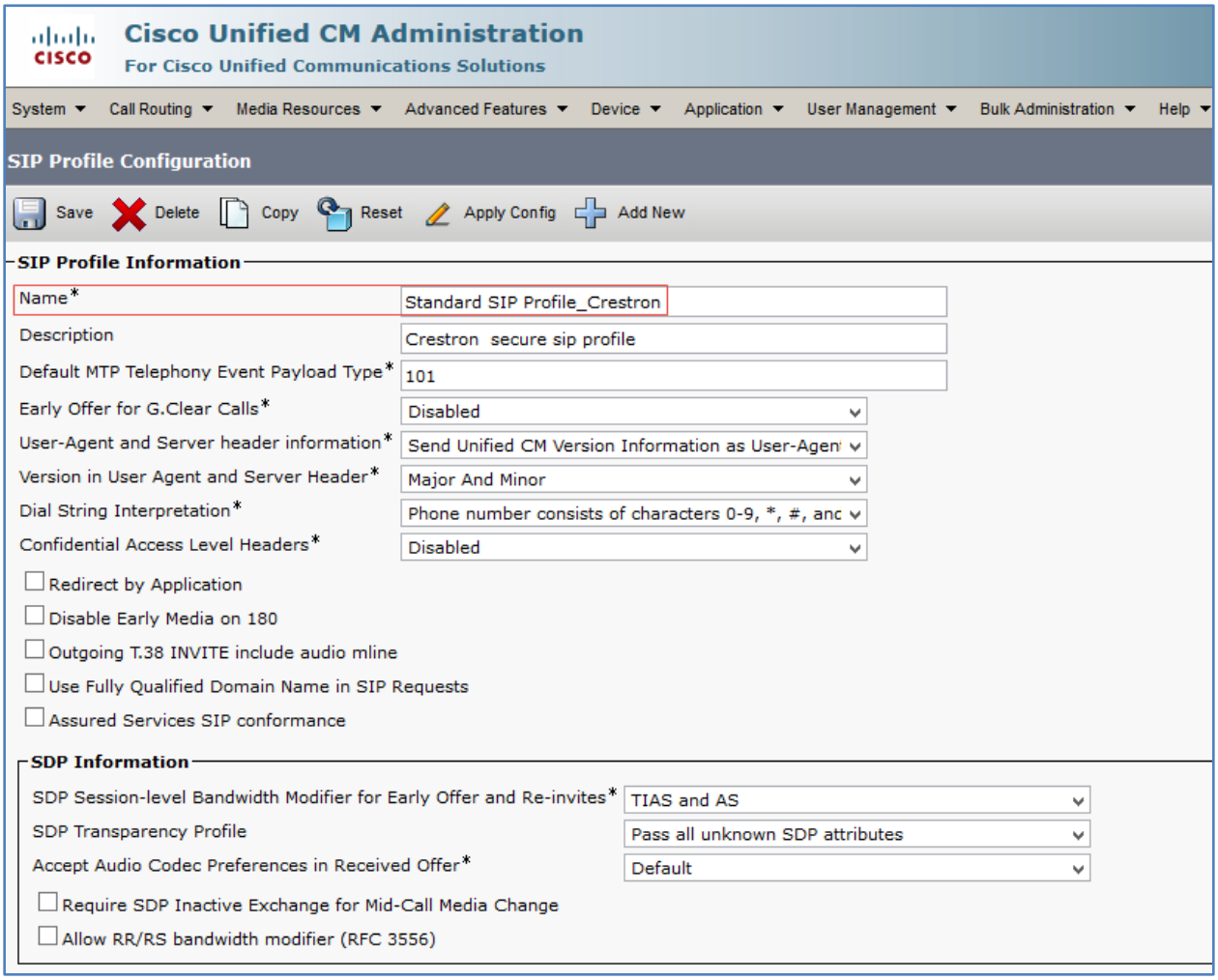
Configure a Secure SIP Profile for Trunk

For the example, a new SIP Profile **Standard SIP Profile_Crestron** was configured and assigned to the trunk used for PSTN calls.

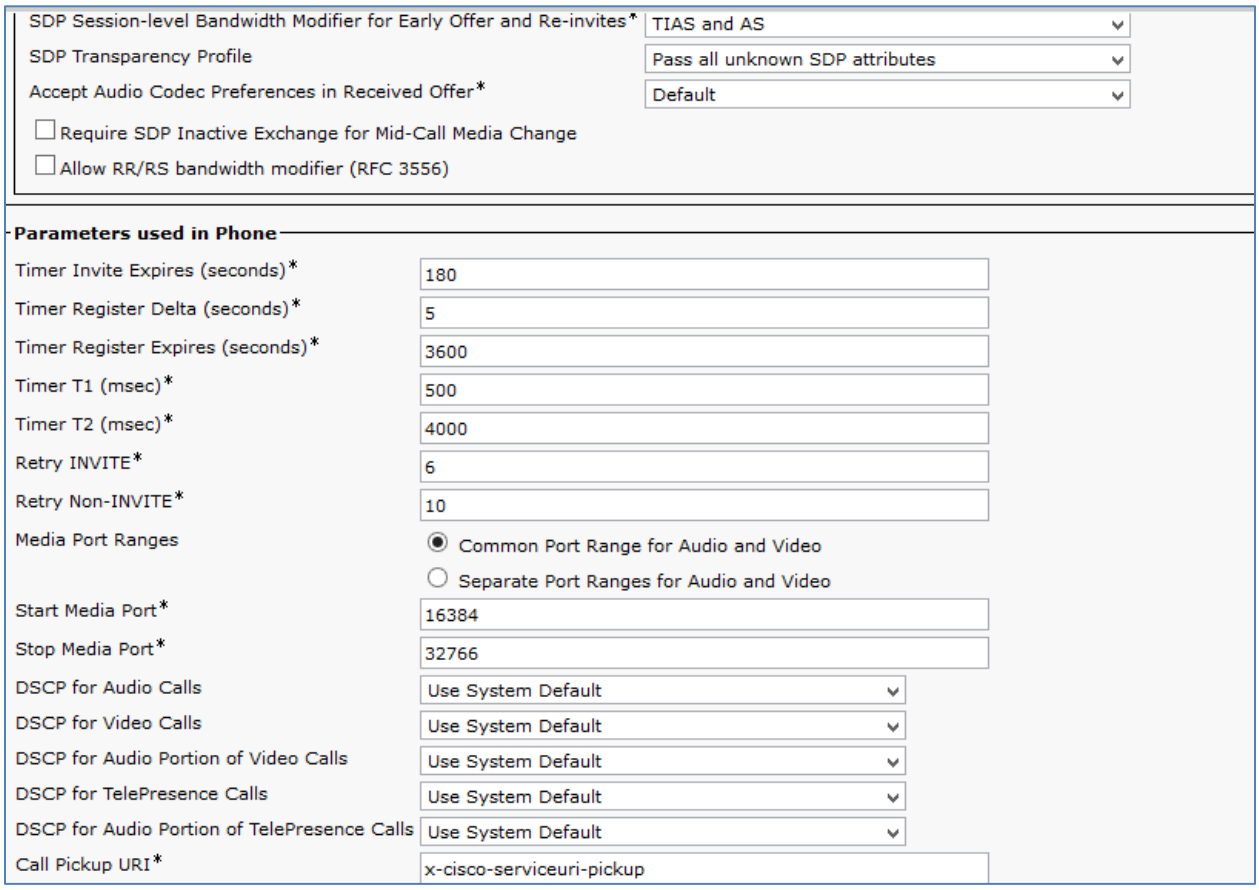
To add a new SIP Profile, follow this procedure:

1. Navigate to **Device** > **Device Settings** > **SIP Profile**.

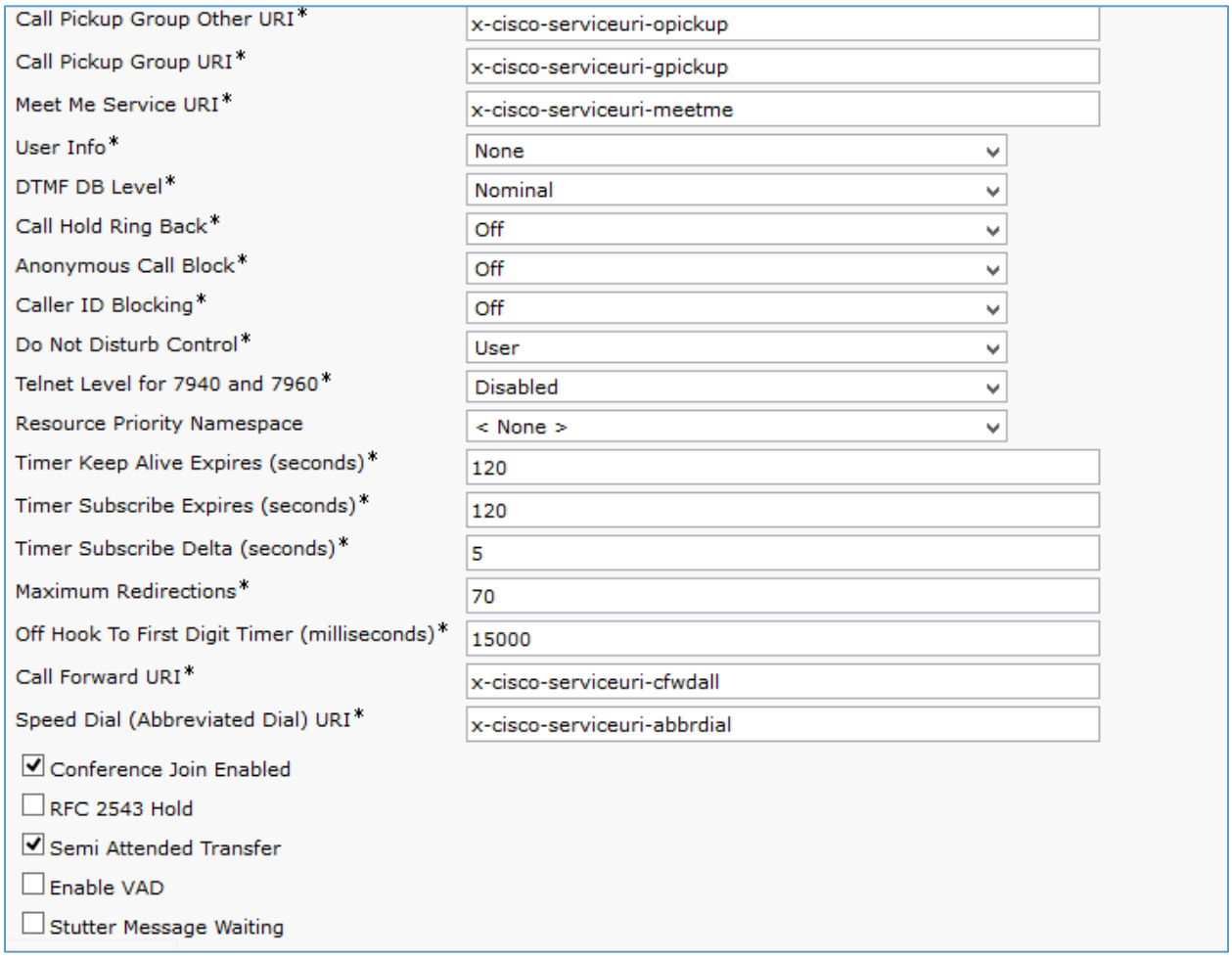
Cisco UCM: Trunk Secure SIP Profile Configuration (1/4)



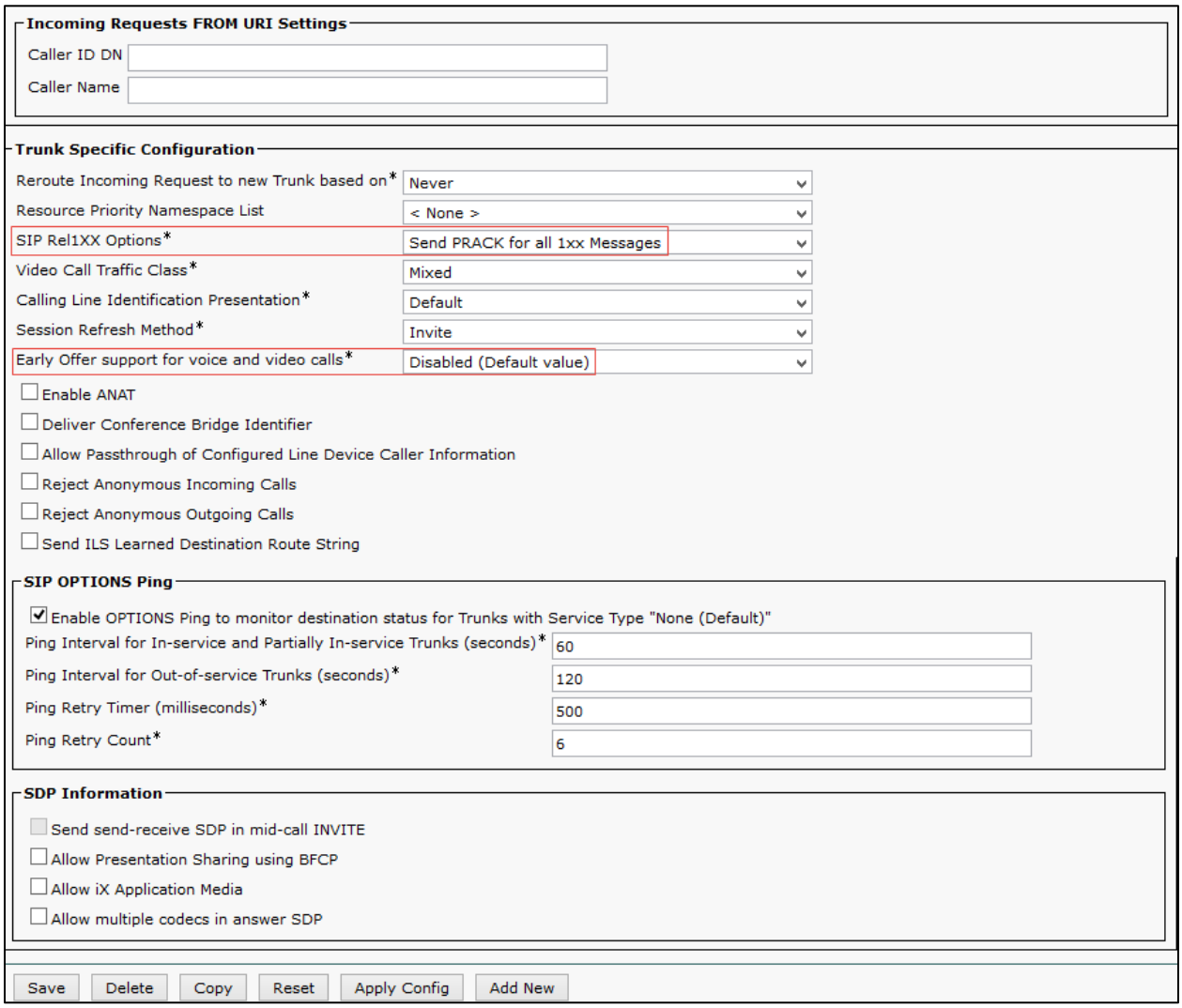
Cisco UCM: Trunk Secure SIP Profile Configuration (2/4)



Cisco UCM: Trunk Secure SIP Profile Configuration (3/4)



Cisco UCM: Trunk Secure SIP Profile Configuration (4/4)



2. On the screen that appears, click **Add New** and configure the SIP Profile:
   - Assign a **Name**: *Standard SIP Profile_Crestron* was used in this example.
   - Configure **SIP Rel1XX Options**: *Send PRACK for all 1xx Messages*
   - Configure **Early offer support for voice and video calls *** as *Disabled*
3. Retain all other default configurations.
4. Click **Save**, and then click **Apply Config**.

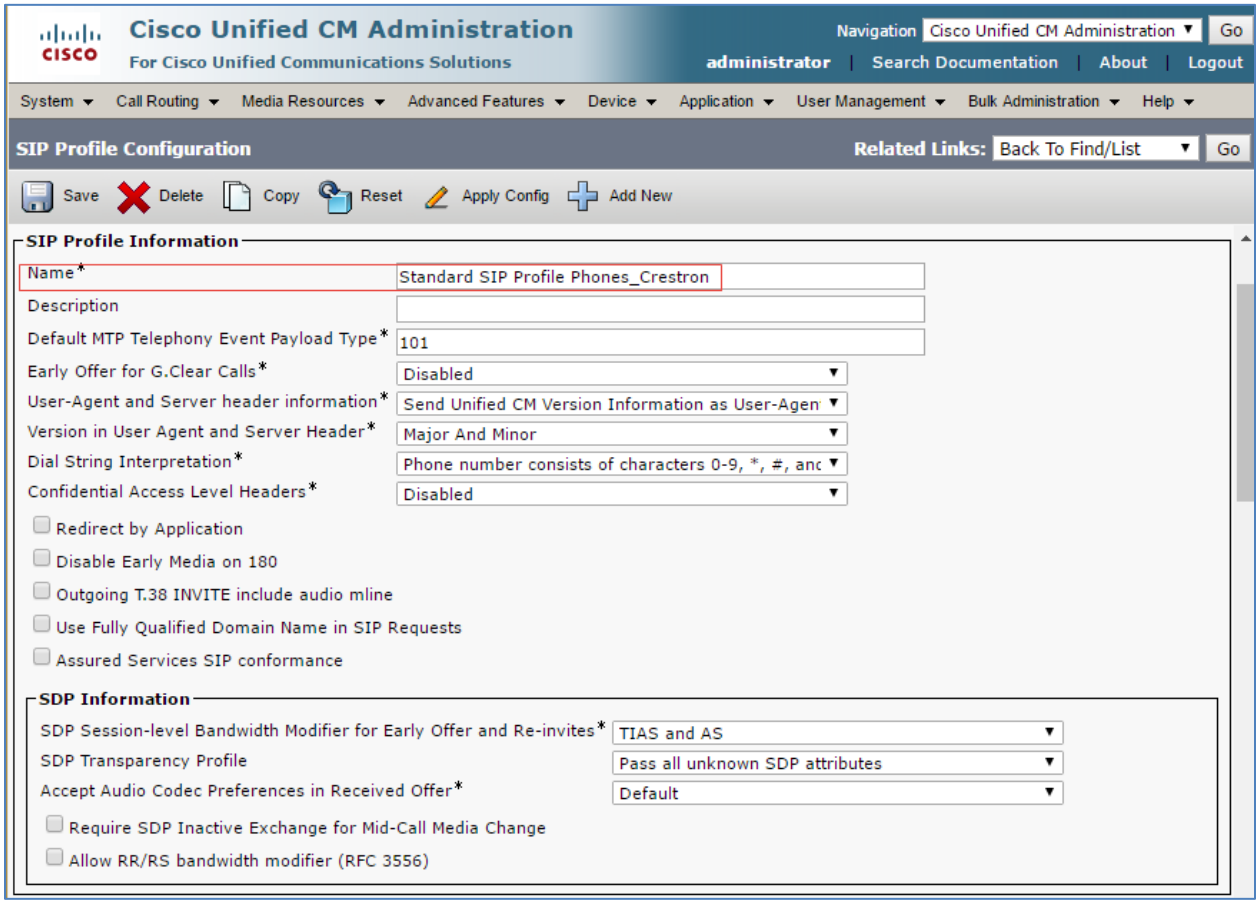
Configure a Secure SIP Profile for Phones

For the test, a new SIP Profile **Standard SIP Profile Phones_Crestron** was configured and assigned to the Crestron Mercury devices and phones registered to the Cisco UCM.

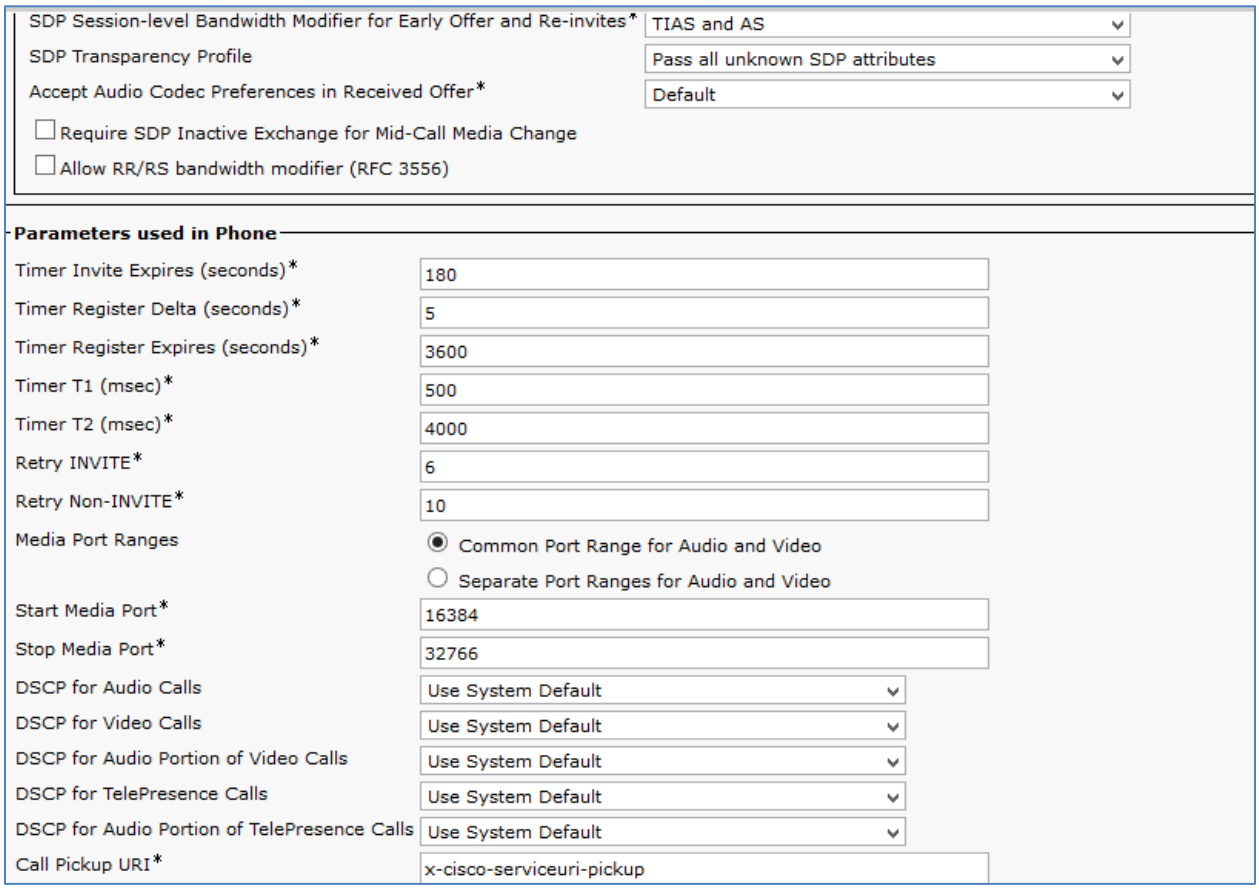
To add a new SIP Profile, follow this procedure:

1. Navigate to **Device** > **Device Settings** > **SIP Profile**.

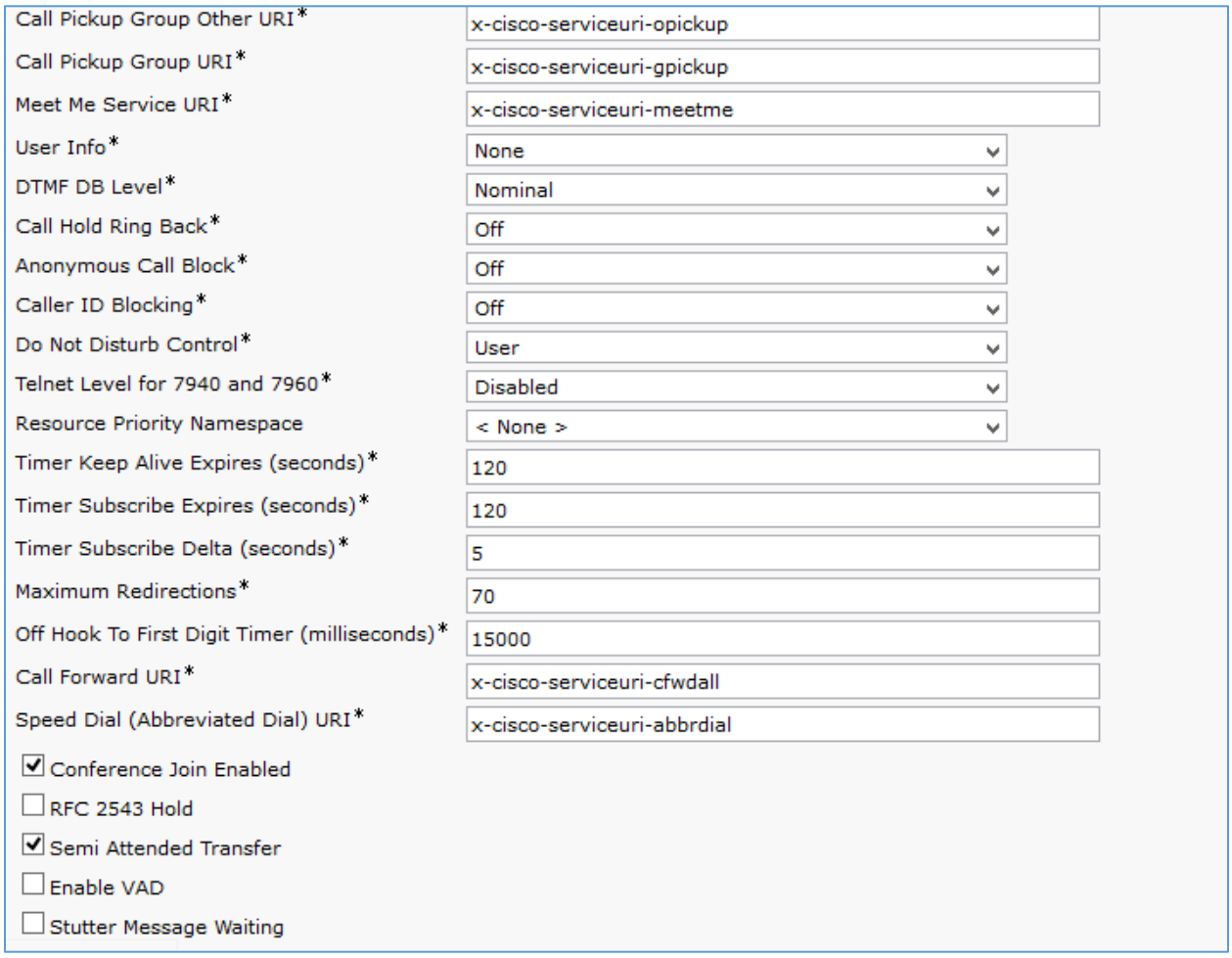
Cisco UCM: Secure SIP Profile Configuration (1/4)



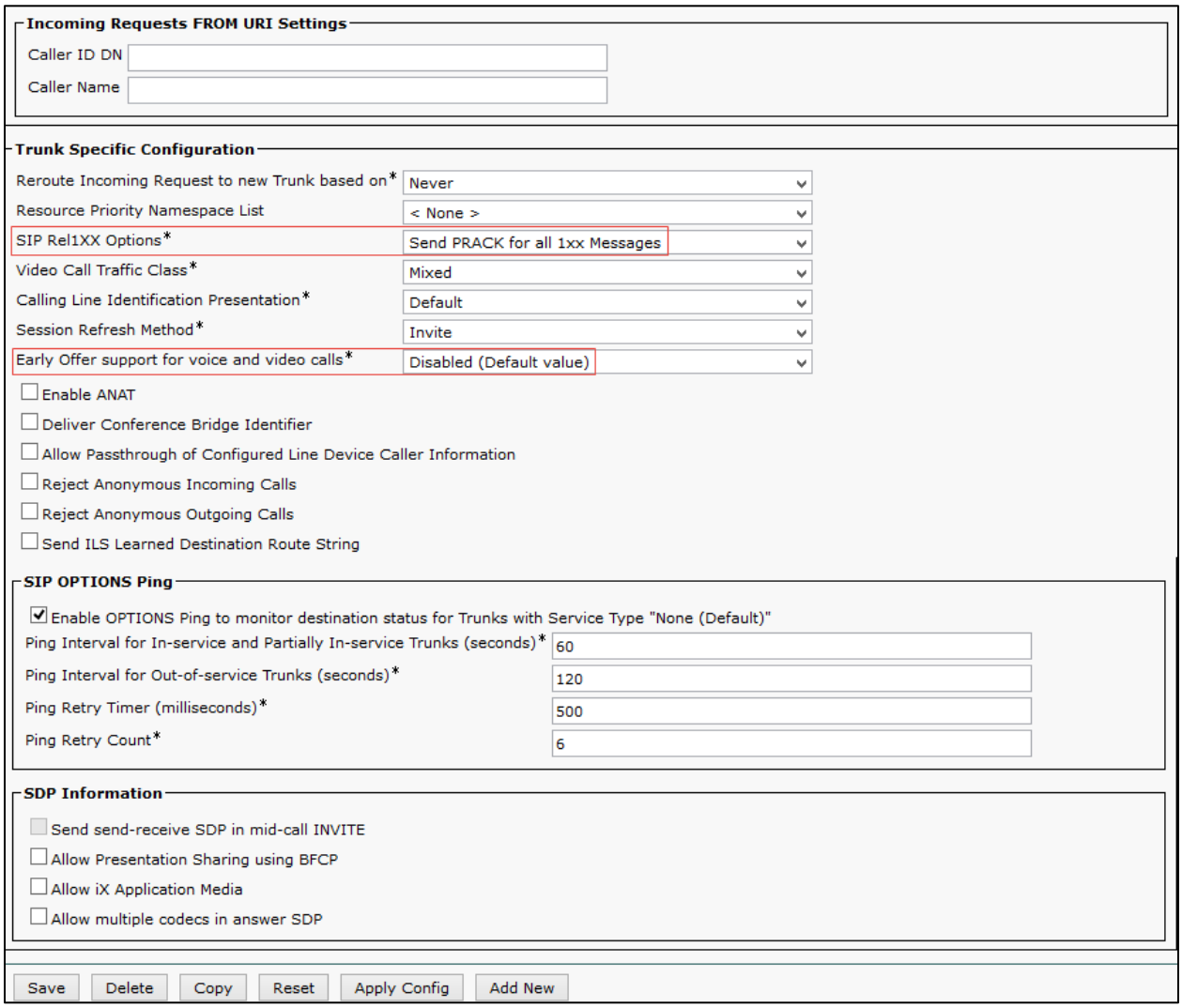
Cisco UCM: Secure SIP Profile Configuration (2/4)



Cisco UCM: Secure SIP Profile Configuration (3/4)



Cisco UCM: Secure SIP Profile Configuration (4/4)



2. On the screen that appears, click **Add New** and configure the SIP Profile:
    a. Assign a **Name**: *Standard SIP Profile Phones_Crestron* was used in the example.
    b. Configure **Early Offer support for voice and video calls*** as *Disabled*
3. Retain all other default configurations.
4. Click **Save**, and then click **Apply Config**.

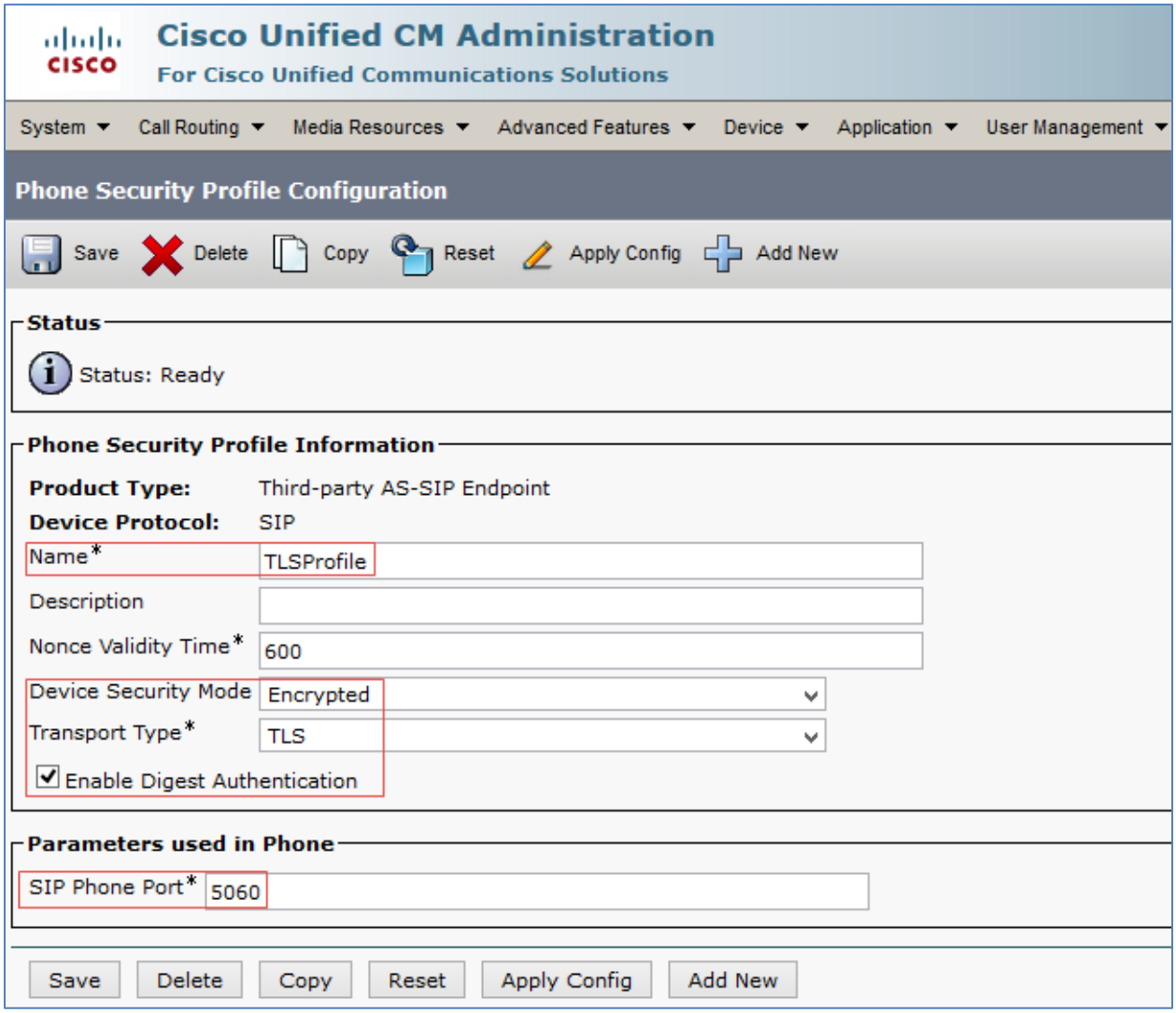
Configure Phone Security Profile

To configure phones on the Cisco UCM in secure mode, each phone type requires its own Phone Security Profile. For the example, separate phone security profiles were configured for the Crestron Mercury device, and the 8945 and 8961 phone-types used.

To configure the Phone Security Profile for the Crestron Mercury device, follow this procedure:

1. Navigate to **System** > **Security** > **Phone Security Profile**.

Cisco UCM: Phone Security Profile Configuration for Crestron Mercury



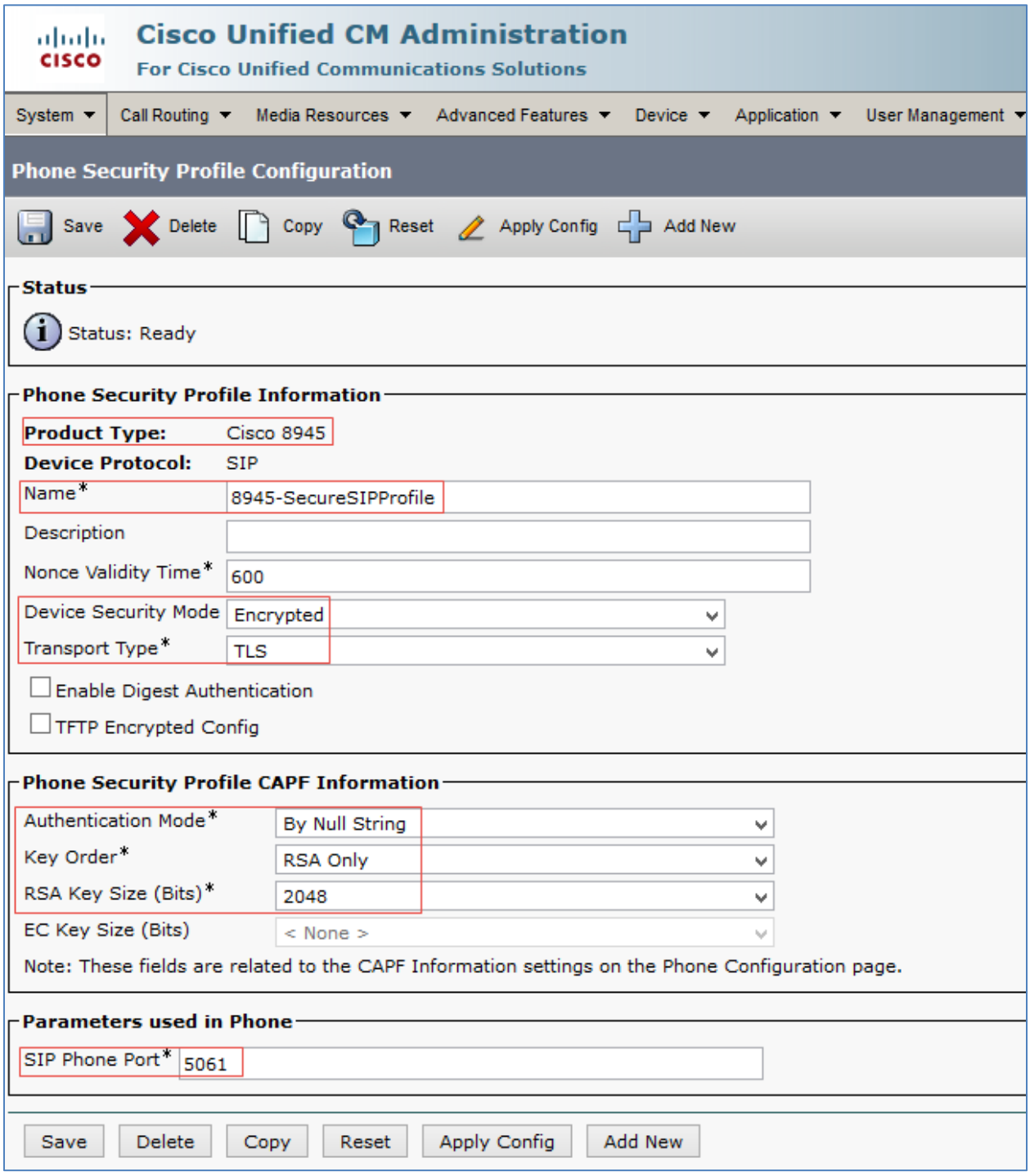
2. Click **Add New**.
3. Select **Product Type: Third party AS-SIP Endpoint**.
4. Configure a **Name**: *TLS profile* was used in this example.
5. Configure **Device Security Mode:** *Encrypted*
6. Configure **Transport Type**: *TLS*
7. Check the **Enable Digest Authentication** check box.

8. Configure **SIP Phone Port:** *5060*. The Crestron Mercury device used this port.
9. Click **Save**.

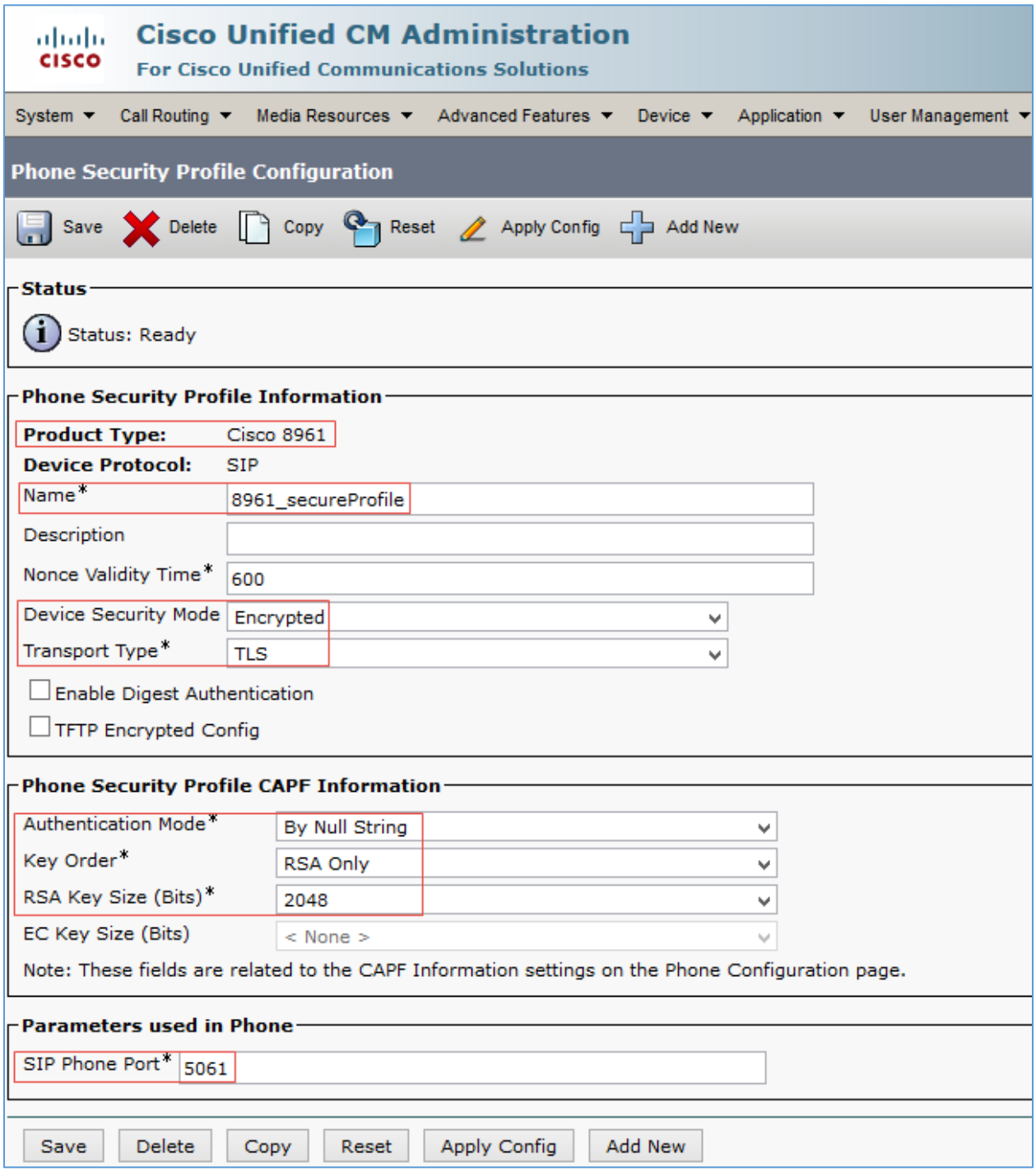
The 8945 and 8961 phone security profiles were configured by selecting the specific phone type as follows:

1. Navigate to **System** > **Security** > **Phone Security Profile**.
2. Click **Add New**.
3. Select **Product Type: Third party AS-SIP Endpoint**.
4. Configure a **Name**.
5. Configure **Device Security Mode**: *Encrypted*.
6. Configure **Transport Type**: *TLS*.
7. Configure **Phone Security CAPF Information**.
   - Authentication Mode: *By Null String*
   - Key Order: *RSA Only*
   - RSA Key Size: *2048*
8. Configure **SIP Phone Port**: *5061*.
9. Click **Save**, and then click **Apply Config**.

Cisco UCM: Phone Security Profile for 8945 Phone Type



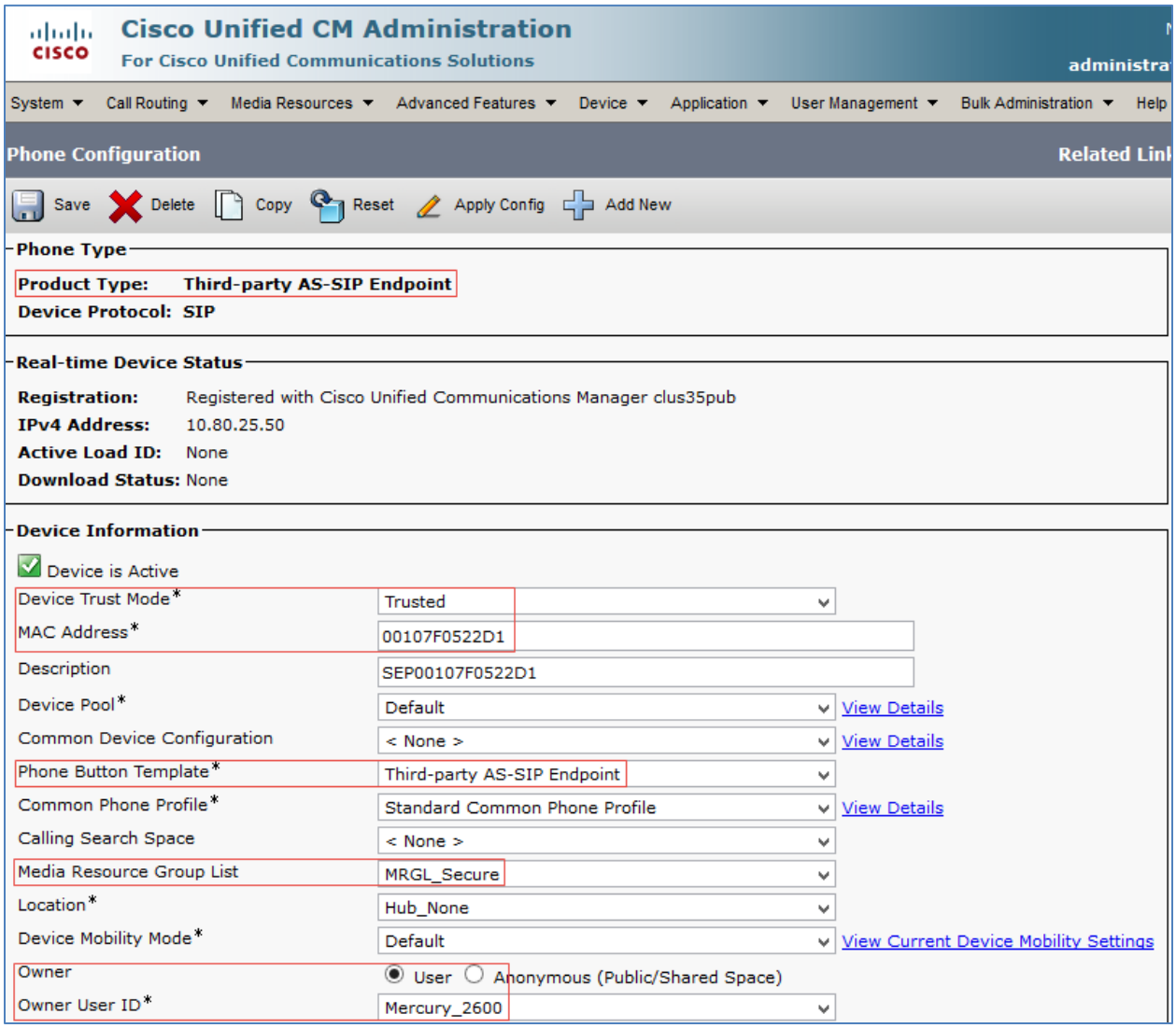
Cisco UCM: Phone Security Profile for 8961 Phone Type



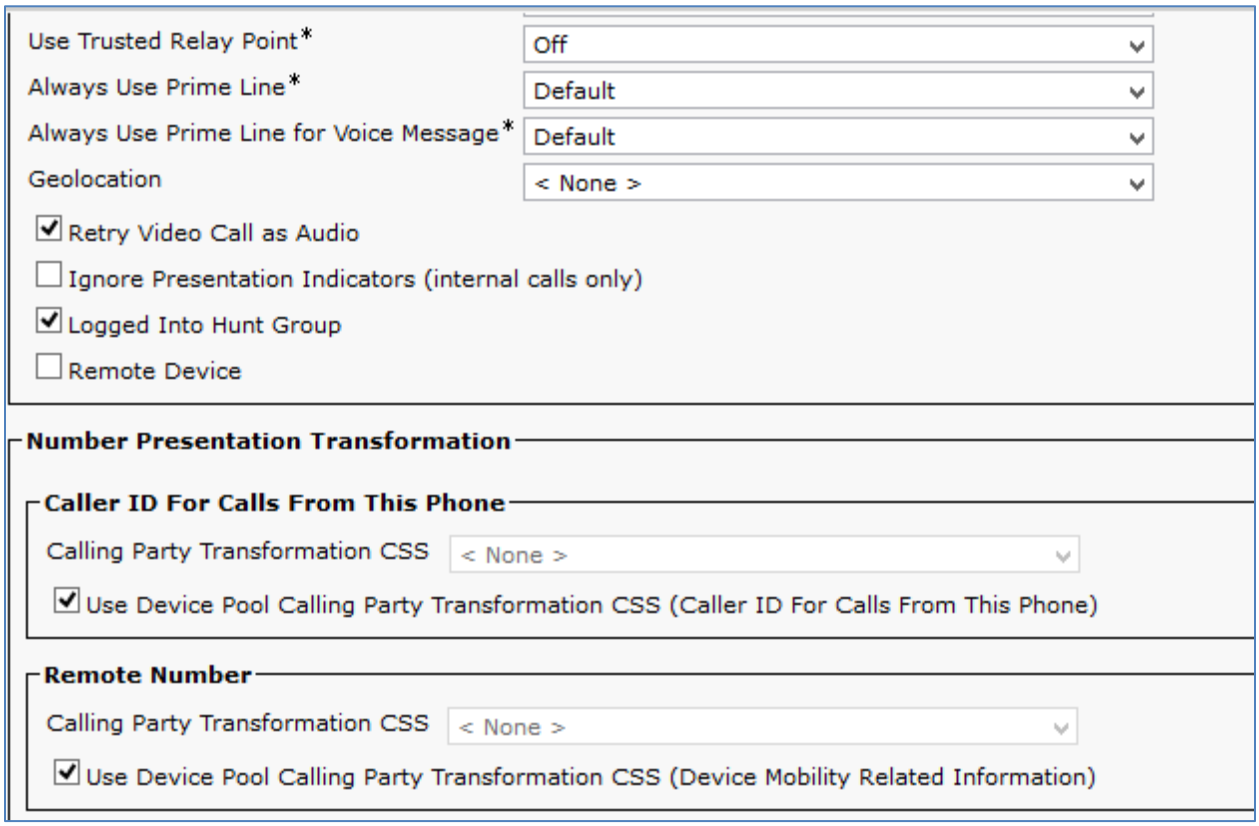
Configure the Crestron device as a Third-party SIP Device

1. Navigate to Device > Phone.
2. Click Add New.

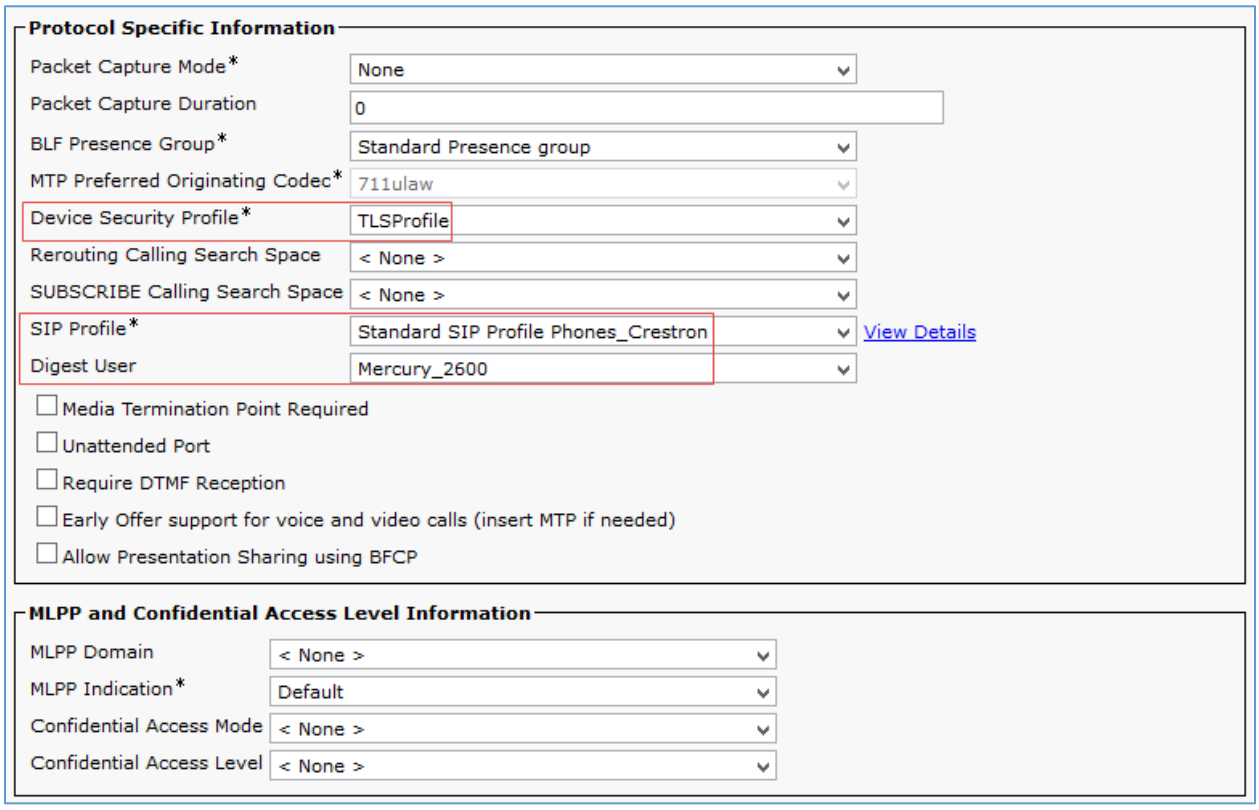
Cisco UCM: Add Crestron Device as Third-party SIP Device (1/3)



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

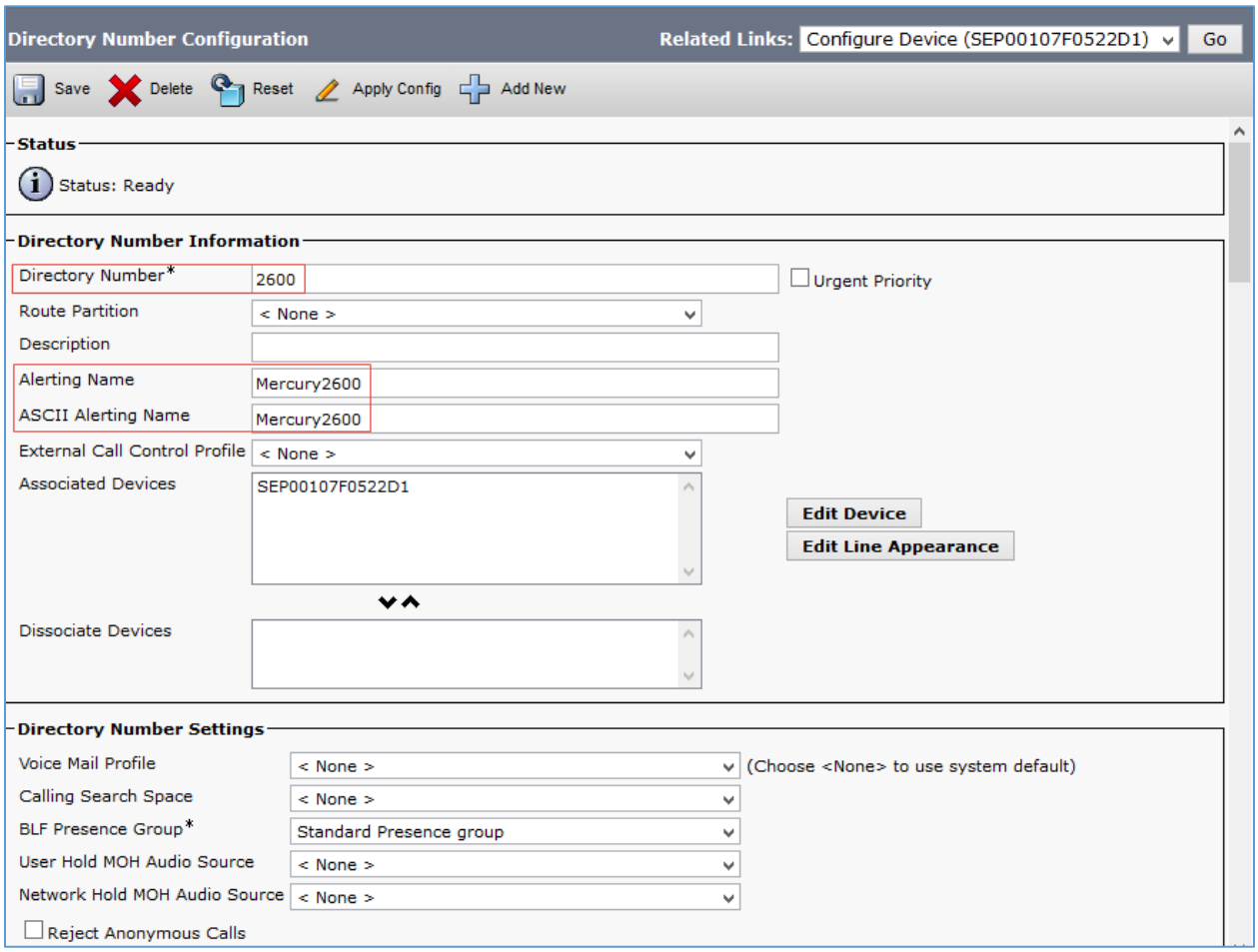


Cisco UCM: Add Crestron Device as Third-party SIP Device (3/3)

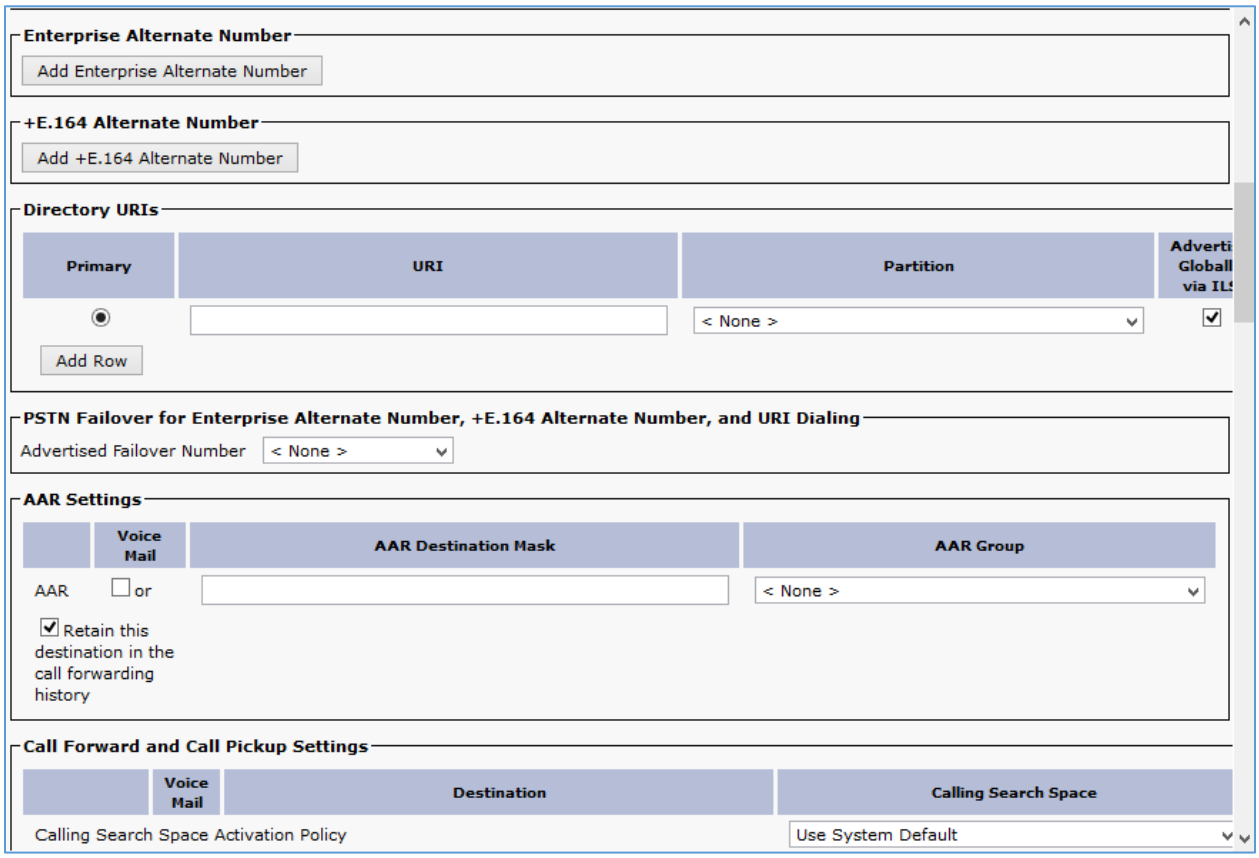


3. Select **Phone Type** as **Third-party AS-SIP Endpoint**.
4. Click **Next**.
5. Configure **MAC Address:** Enter the MAC Address of the Crestron Mercury device.
6. Select **Device Pool** as **Default**.
7. Select **Phone Button Template** as **Third-party AS-SIP Endpoint**.
8. Select **Media Resource Group List** *MRGL_Secure* as configured earlier was used in the example.
9. Select **Owner User ID** as configured earlier from the drop-down menu. *Crestron Mercury_2600* was selected in this test for the first Crestron Mercury device, and *Crestron Mercury_2602* for the second Crestron Mercury device.
10. Select **Device Security Profile** as configured earlier from the drop-down menu. *TLSProfile* was used in the example.
11. Select **SIP Profile** as configured earlier from the drop-down menu. *Standard SIP Profile Phones_Crestron* was used in the example.
12. Select **Digest User ID** as configured earlier from the drop-down. In this example, *Crestron Mercury_2600* was selected for the first Crestron Mercury device, *and Crestron Mercury_2602* was selected for the second Crestron Mercury device.
13. Click **Save**.
14. Add a **DN** to this phone. *DN 2600* was configured for one of the Crestron Mercury devices in this example. Similarly, *DN 2602* was added to the other Crestron Mercury device.

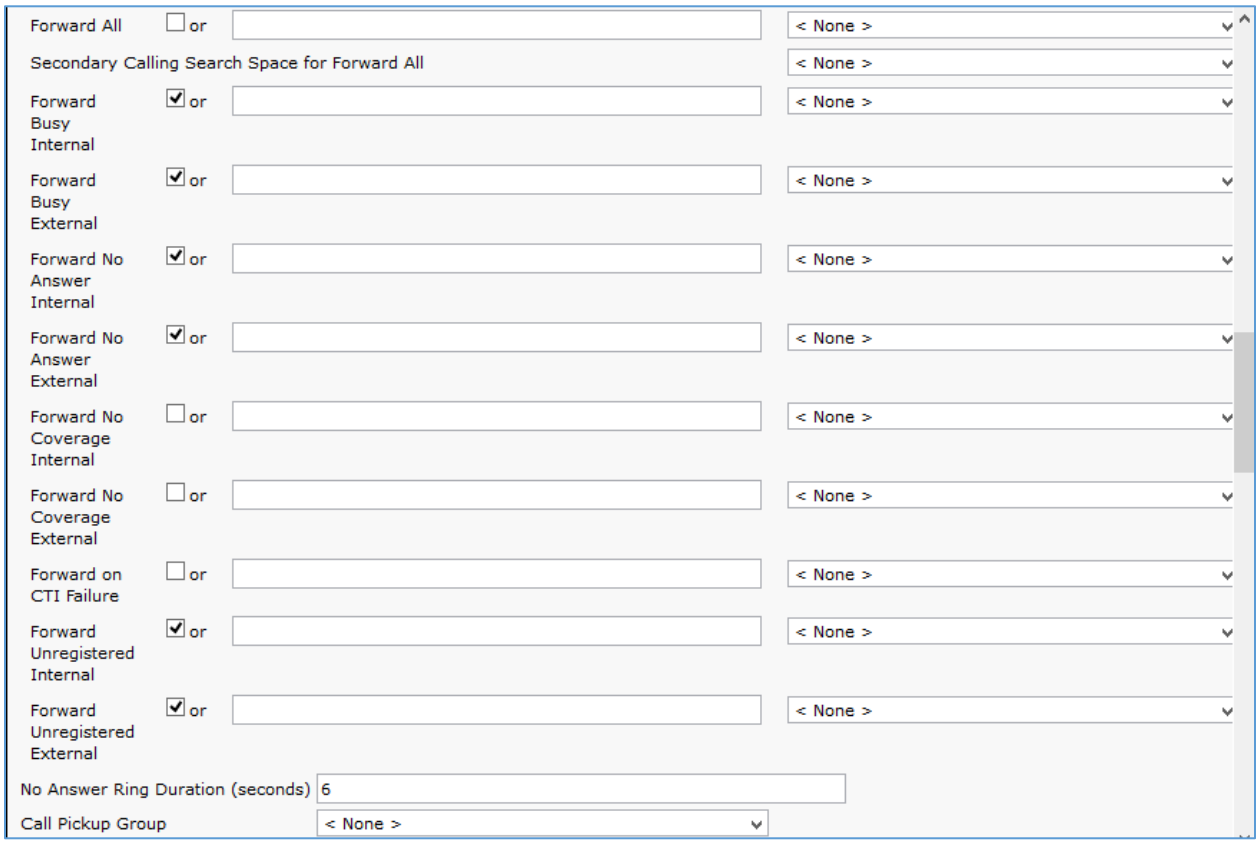
Cisco UCM: Add DN to Crestron Device: Third-party SIP Device (1/5)



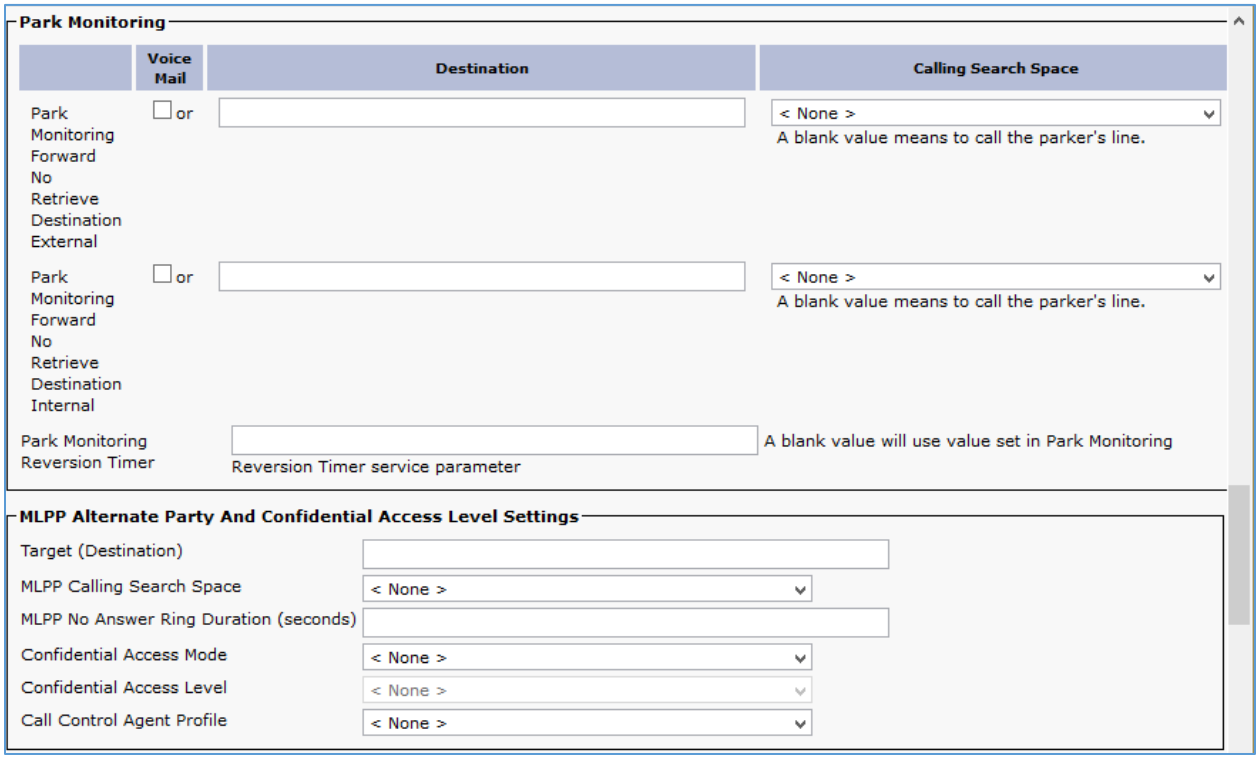
Cisco UCM: Add DN to Crestron Device: Third-party SIP Device (2/5)



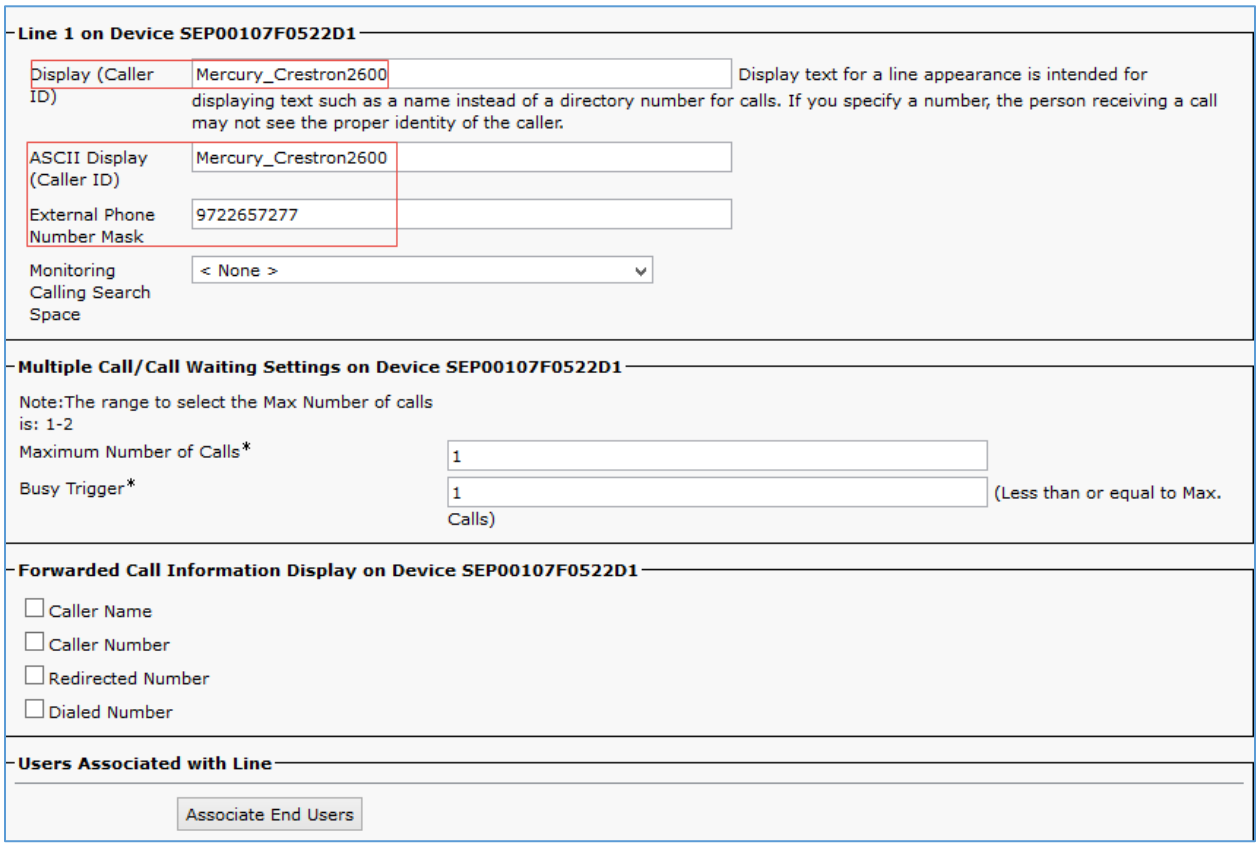
Cisco UCM: Add DN to Crestron Device: Third-party SIP Device (3/5)



Cisco UCM: Add DN to Crestron Device: Third-party SIP Device (4/5)



Cisco UCM: Add DN to Crestron Device: Third-party SIP Device (5/5)



Configure Media Resource Group and Media Resource Group List

A Media Resource Group (MRG) is required to include Music on Hold servers, Conference Bridges, and Media Termination Points that may be necessary to test the Cisco UCM or Service Provider features.

For secure SIP signaling and media for PSTN calls, and for secure G722 transfers and conferences, a Cisco UBE was used at the edge of the enterprise.

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

Cisco UBE configuration for MRG resources

The related Cisco UBE configuration is shown below:

```
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
 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
 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 2142425977
 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
```

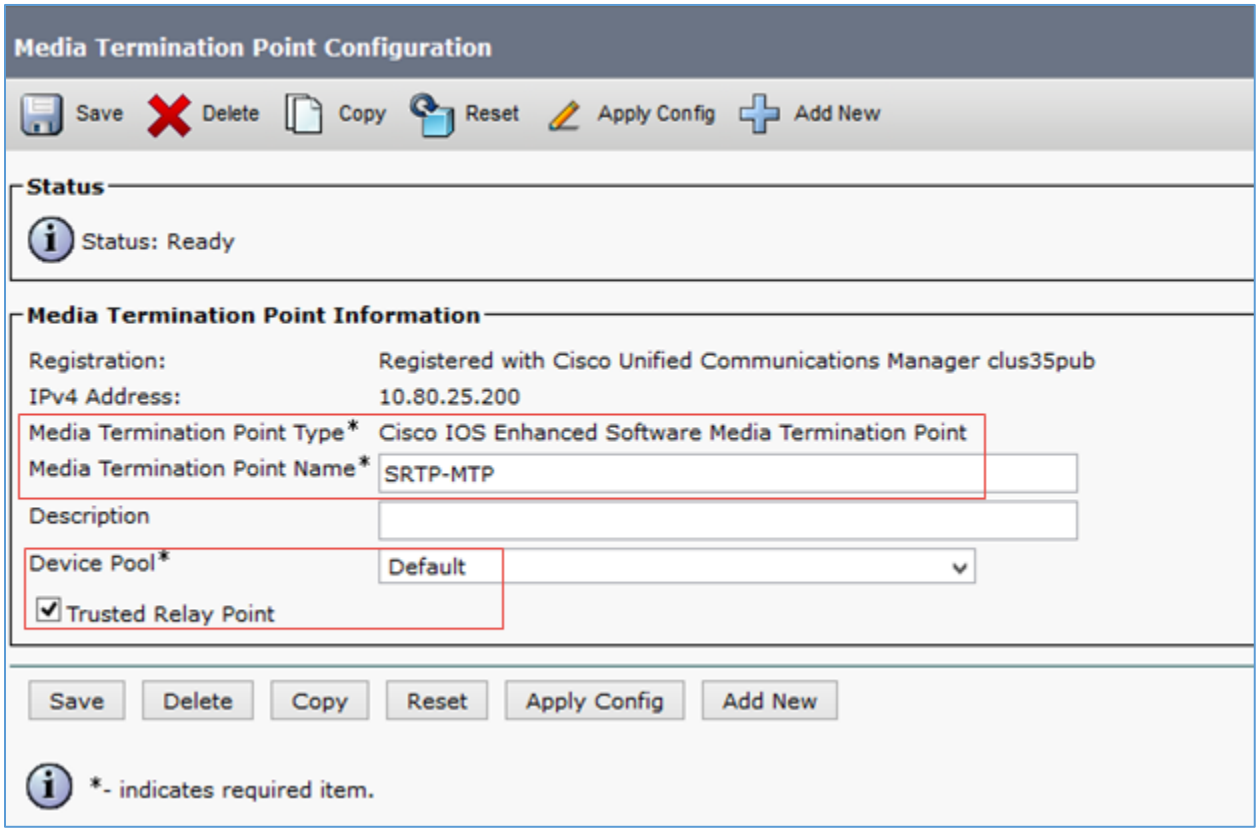
```
!
!
sip-ua
 crypto signaling remote-addr 10.80.25.2 255.255.255.255 trustpoint
CrestronCFB
!
!
!
gatekeeper
 shutdown
!
end
```

Cisco UCM Media Termination Point Configuration

A Media Termination Point utilizing the Cisco UBE resources was configured.

1. Select **Media Resources** > **Media Termination Point**.
2. Click **Add New**.

Cisco UCM: Add Cisco IOS Enhanced Software Media Termination Point



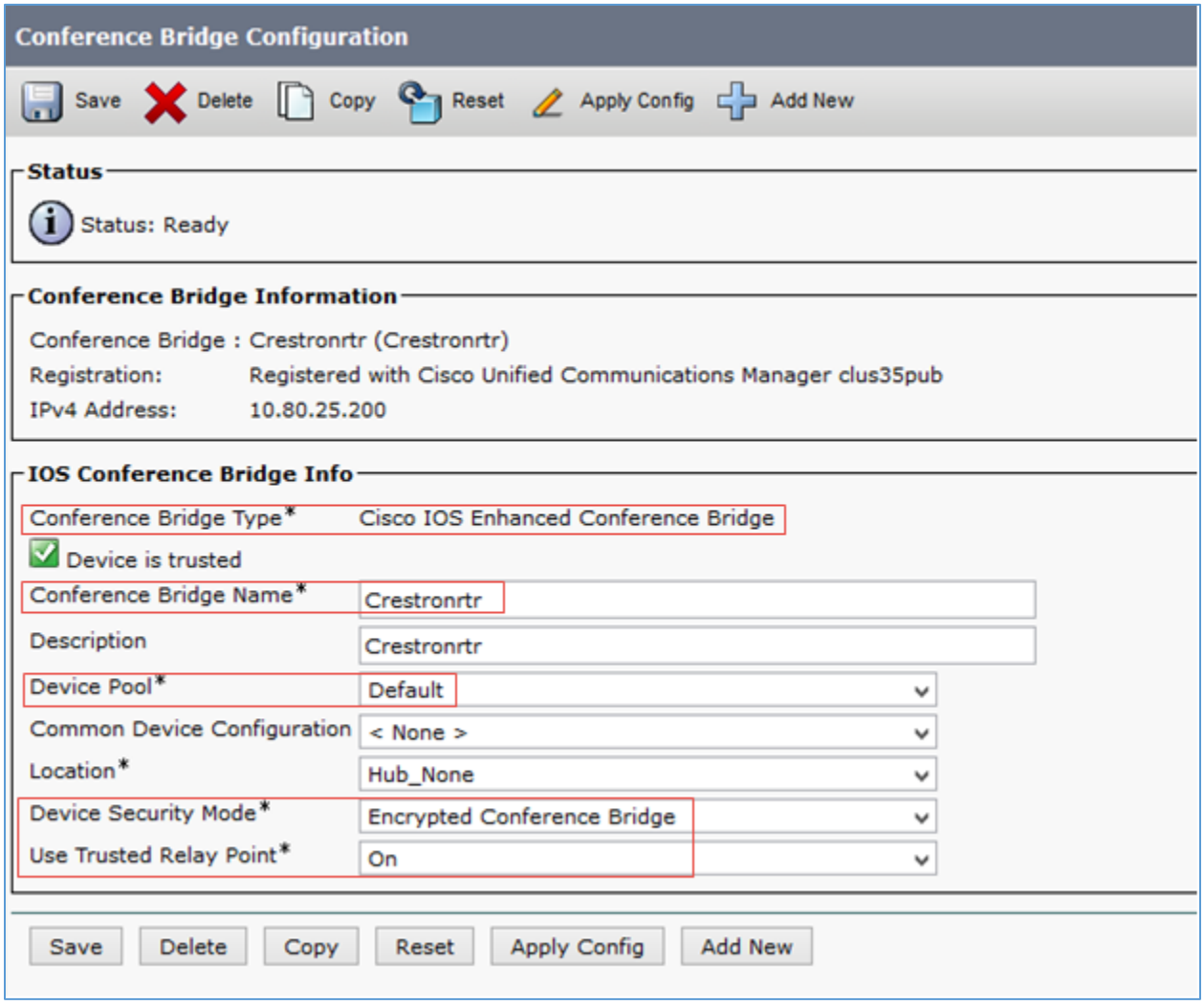
3. Select **Media Termination Point Type***: **Cisco IOS Enhanced Software Media Termination Point**
4. Configure **Media Termination Point Name*:** *SRTP-MTP* was used in this example. This is the same name as that configured on the Cisco UBE.
5. Configure **Device Pool**: *Default*.
6. Check the **Trusted Relay Point** check box.

Cisco UCM Conference Bridge Configuration

An IOS conference bridge utilizing the Cisco UBE resources was configured as shown below:

1. Select **Media Resources** > **Conference Bridge**.
2. Click **Add New**.

Cisco UCM: Conference Bridge Configuration



3. Select **Conference Bridge Type: Cisco IOS Enhanced Conference Bridge**.
4. Configure **Conference Bridge Name:** *Crestronrtr* was used in this example. This name is the same as that configured on the Cisco UBE.
5. Configure **Device Pool**: *Default*.
6. Select **Device Security Mode**: *Encrypted Conference Bridge.*
7. Select **Use Trusted Relay Point**: *On*.

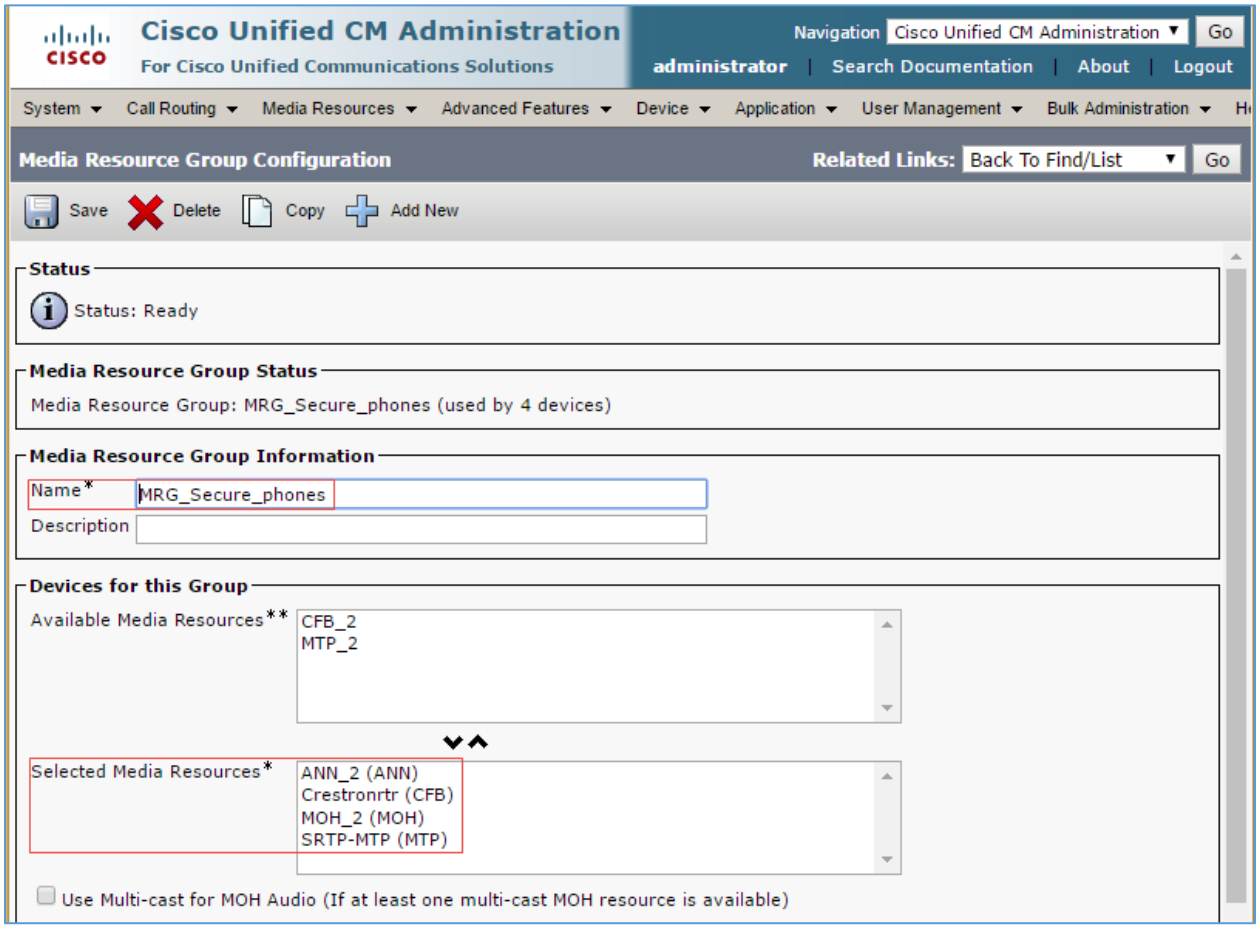
Cisco UCM MRG Configuration

Two Media Resource Groups were configured for this test. *MRG_Secure_trk* and *MRG_Secure_Phones* were assigned to the trunk and phones respectively.

The Media Resource Group *MRG_Secure_phones* was configured for this test.

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

Cisco UCM: Media Resource Group Configuration for Phones/Devices

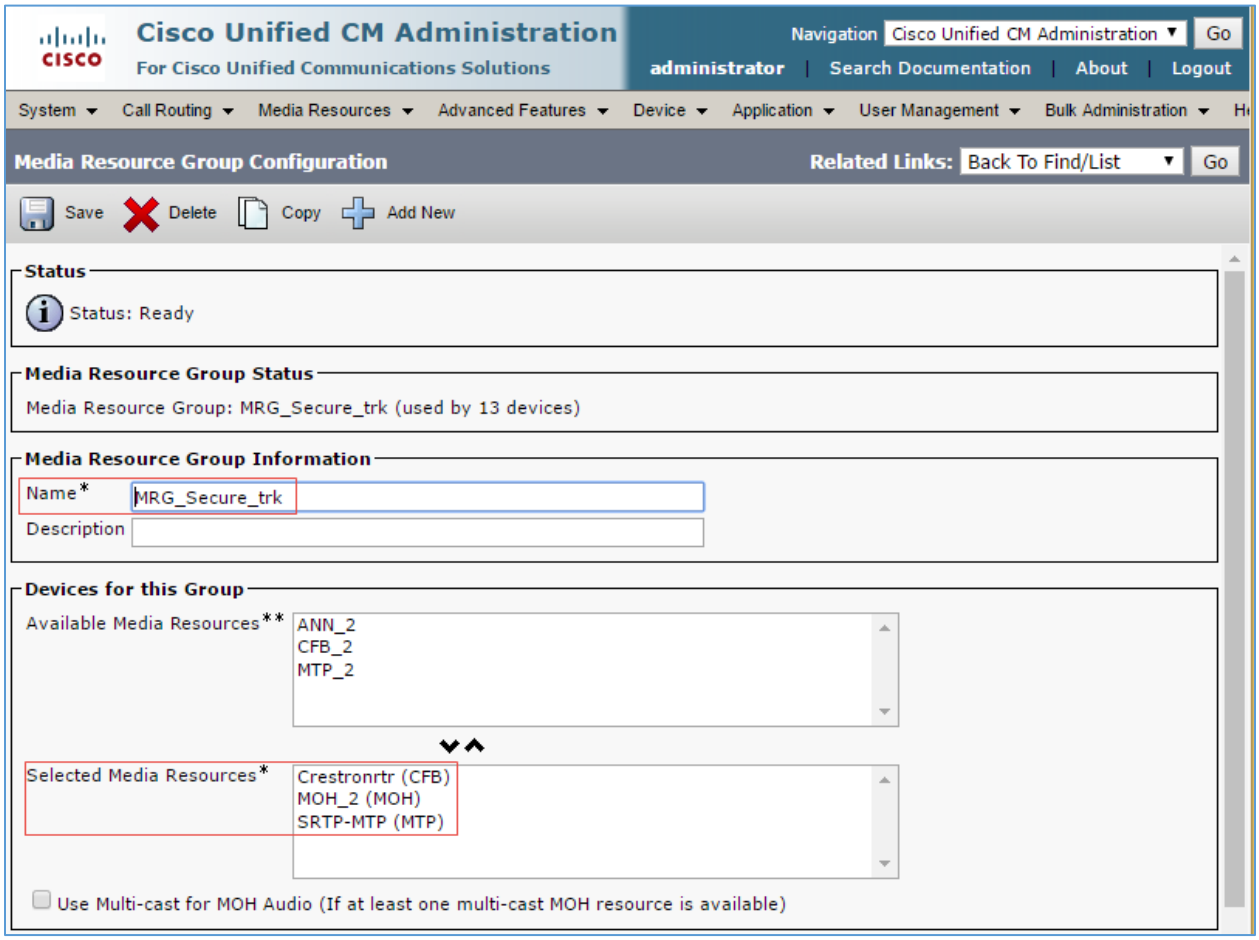


3. Provide a **Name**: *MRG_Secure_phones* was used in this example.
4. Select Media Resources from the **Available Media Resources**. For this example, the resources *MOH_2 (MOH) , ANN_2(ANN), Crestronrtr,* and *SRTP-MTP* were added.

Similarly, a Media Resource Group *MRG_Secure_trk* was configured for this example as follows.

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

Cisco UCM: Media Resource Group Configuration for Trunk

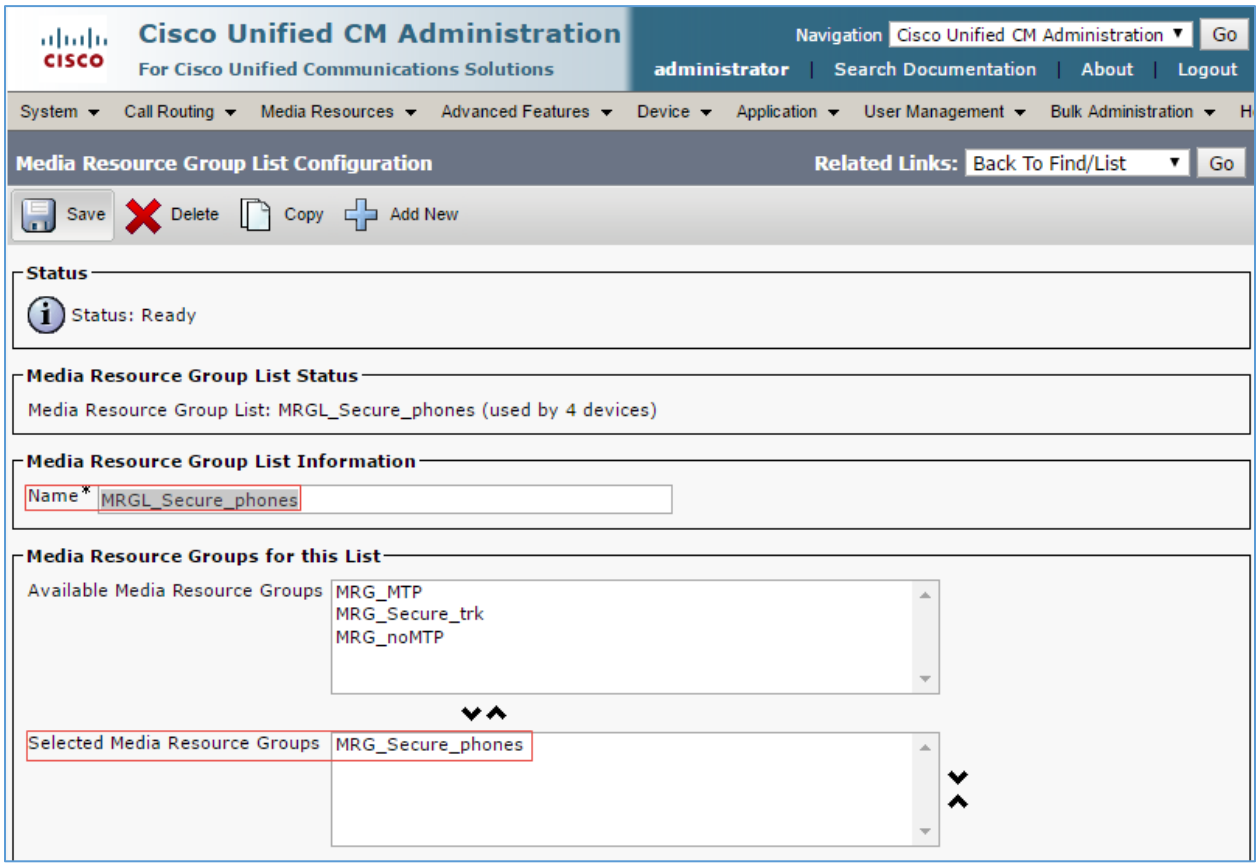


3. Provide a **Name**: *MRG_Secure_trk* was used in this example.
4. Select Media Resources from the **Available Media Resources**. For this example, the resources *MOH_2 (MOH), Crestronrtr*, and *SRTP-MTP* were added.

Configure the Media Resource Group List *MRGL_Secure_phones*.

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

Cisco UCM: Media Resource Group List Configuration-MRG_Secure_phones

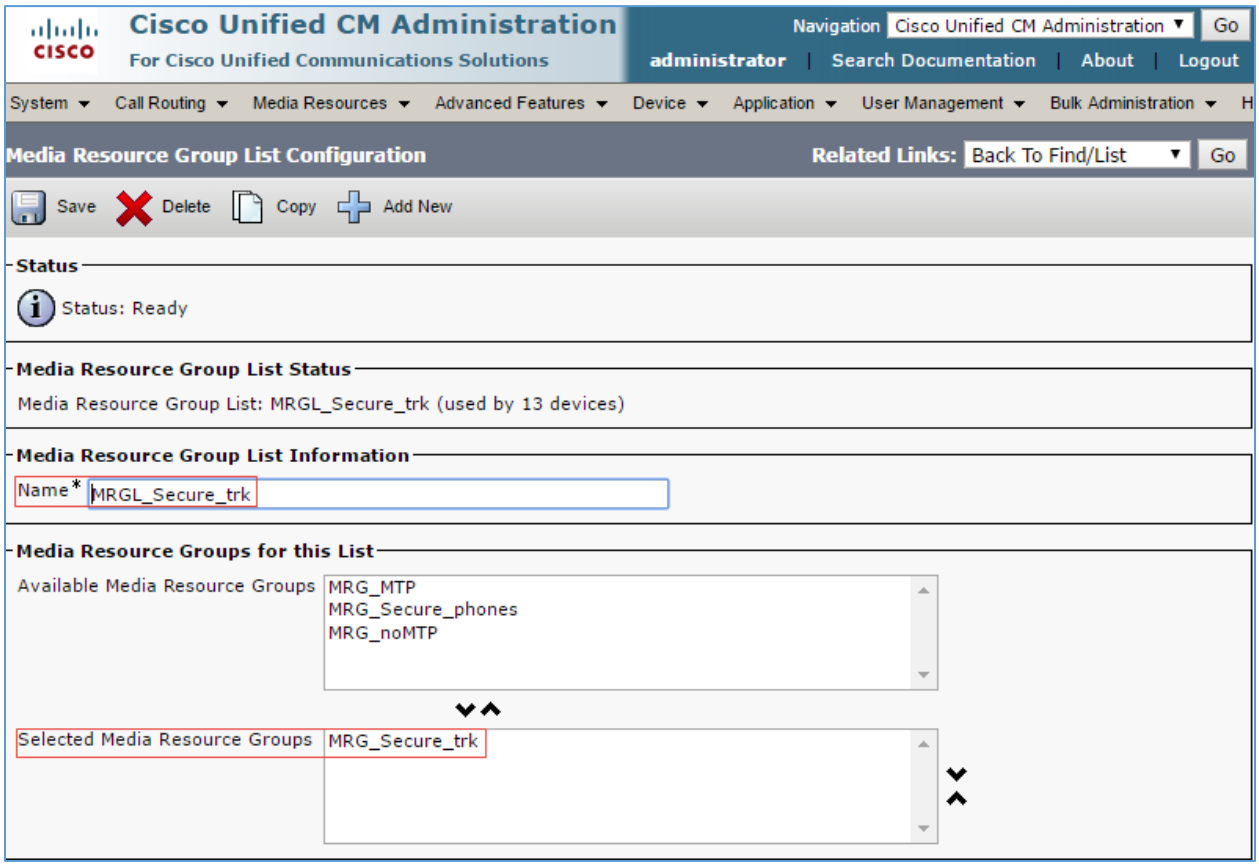


3. Provide a **Name:** *MRGL_Secure_phones* was used in this example.
4. Select the desired media resource groups from the **Available Media Resource Groups.** *MRG_Secure_phones* resource group was added to the list.

Similarly, configure the Media Resource Group List **MRGL_Secure_trk**

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

Cisco UCM: Media Resource Group List Configuration-MRG_Secure_trk



3. Provide a **Name:** *MRGL_Secure_trk* was used in this example.
4. Select the desired media resource groups from the **Available Media Resource Groups:** *MRG_Secure_trk* resource group was added to the list.

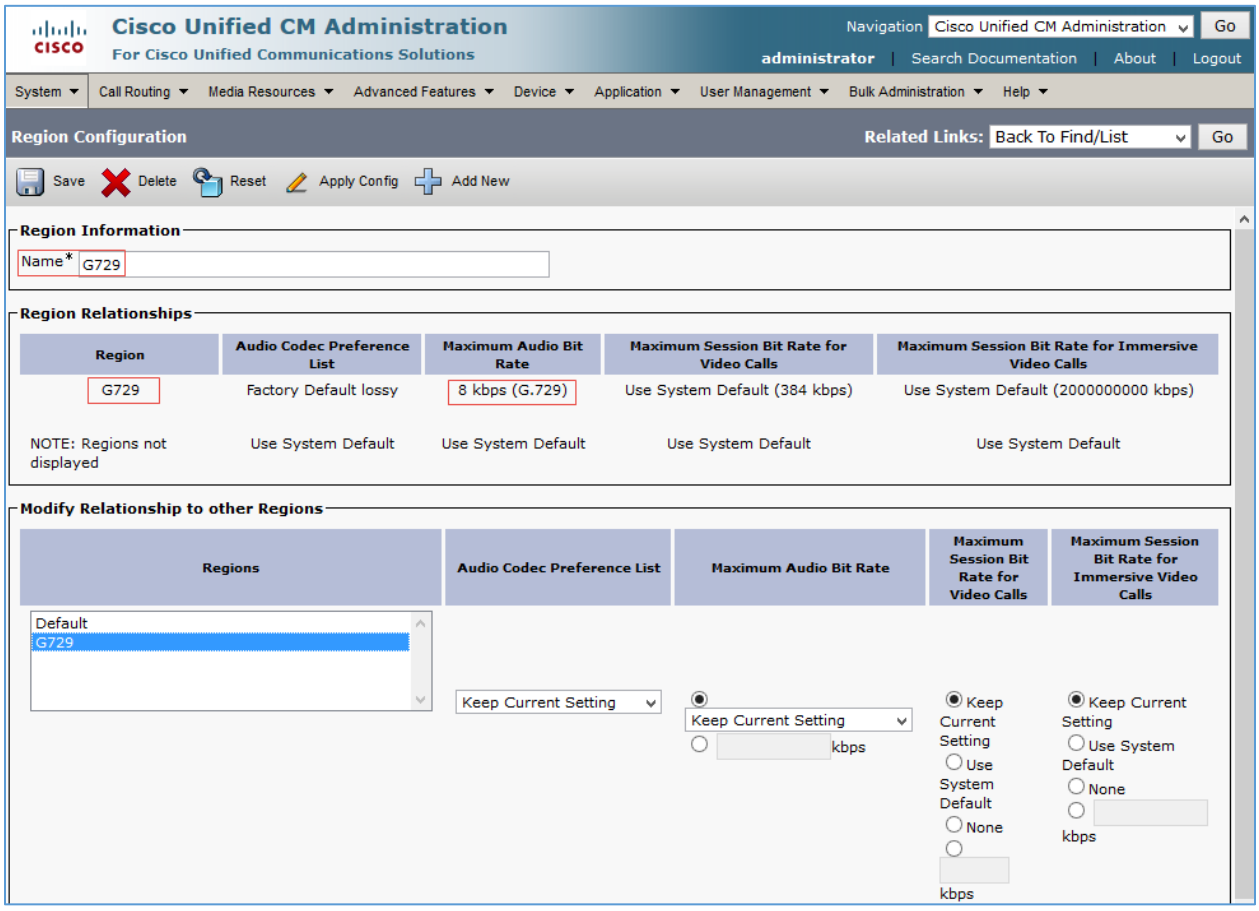
Configure Region for G729

To test the device capabilities with G729, a separate region with the G729 codec as preference needs to be configured. This new region needs to be assigned to the default device pool.

To configure a new region, perform the following procedure.

1. Navigate to **System** > **Region Information** > **Region**.
2. Click **Add New**.

Cisco UCM: Region Configuration



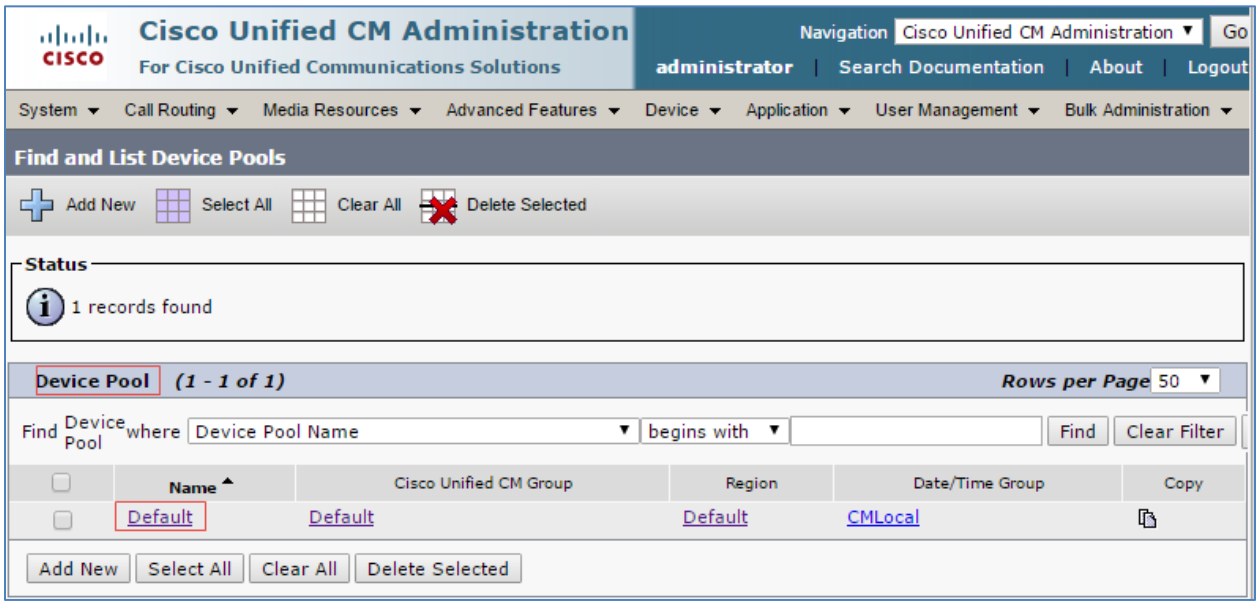
3. Configure a **Name:** *G729* was used in this example.
4. Click **Save**.
5. On the screen that follows, select the newly added region in the lower pane and select the ***Maximum Audio Bit Rate*** from the drop-down menu as *8kbps (G729).*
6. Click **Save**.

Modify Device Pool Configuration

For the test, the default device pool configuration was updated with the MRGL configured above.

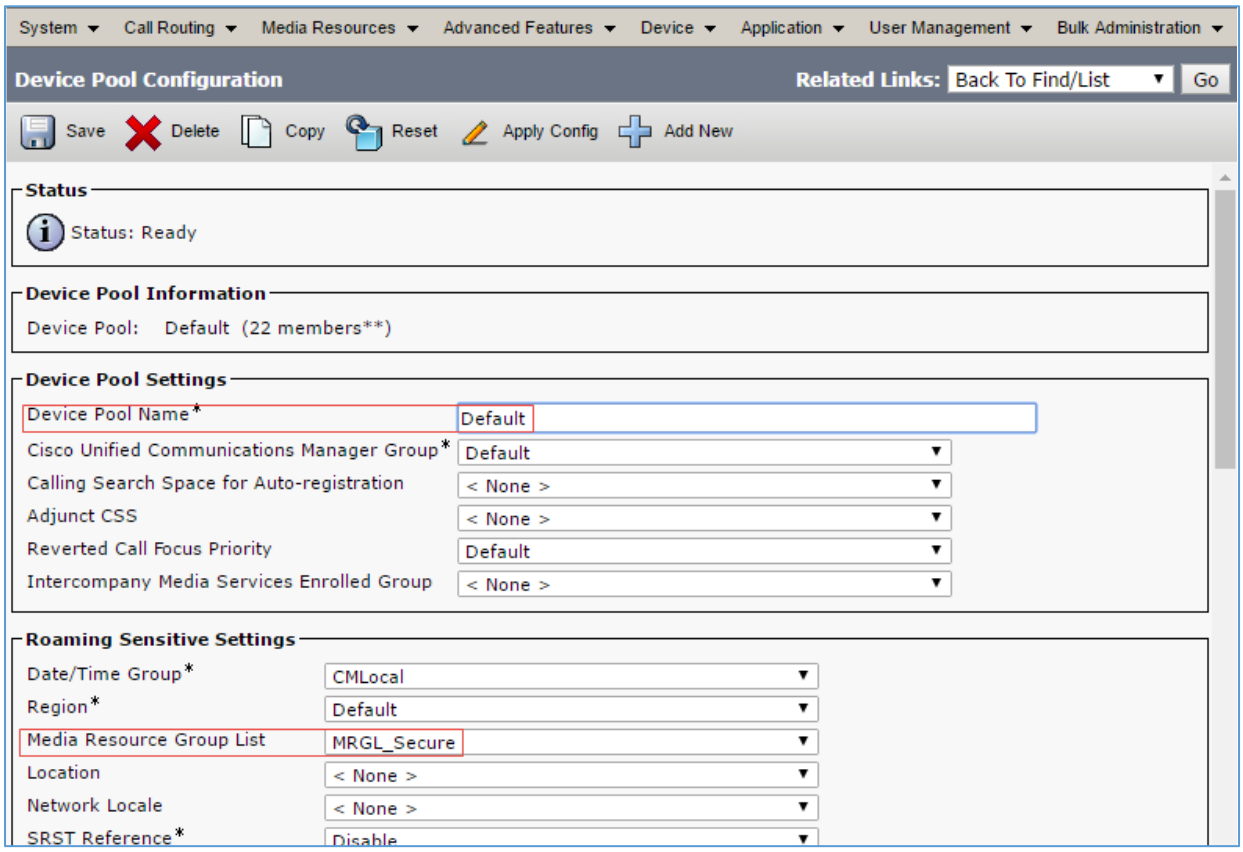
1. Navigate to **System** > **Device Pool**.

Cisco UCM: Find and List Device Pools



2. Click **Default**.
3. **Media Resource Group List**: Select the *MRGL_Secure* from the drop-down menu.

Cisco UCM: Device Pool Configuration

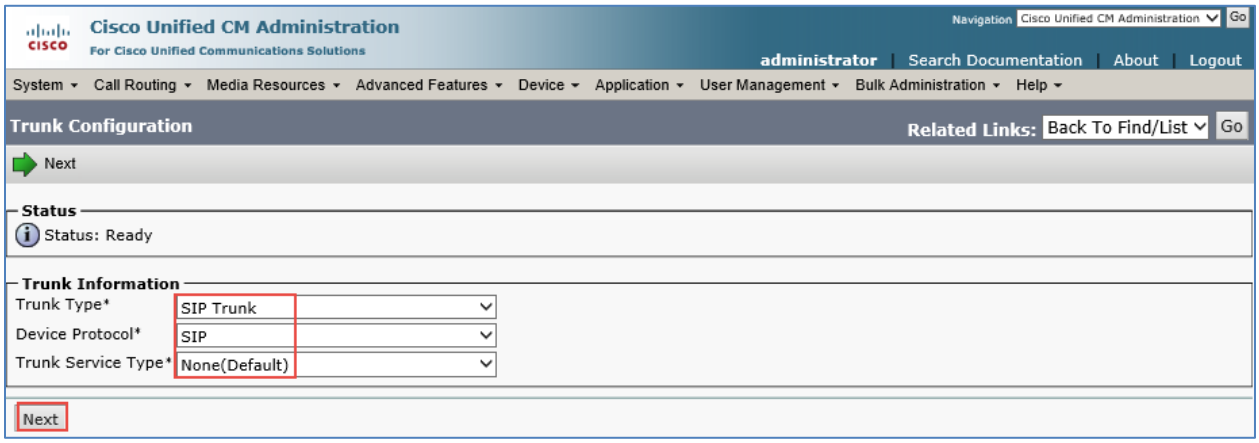


Configure Trunk

A trunk between the Cisco UCM and the Cisco UBE was configured to route PSTN calls. To create a new trunk, perform the following procedure.

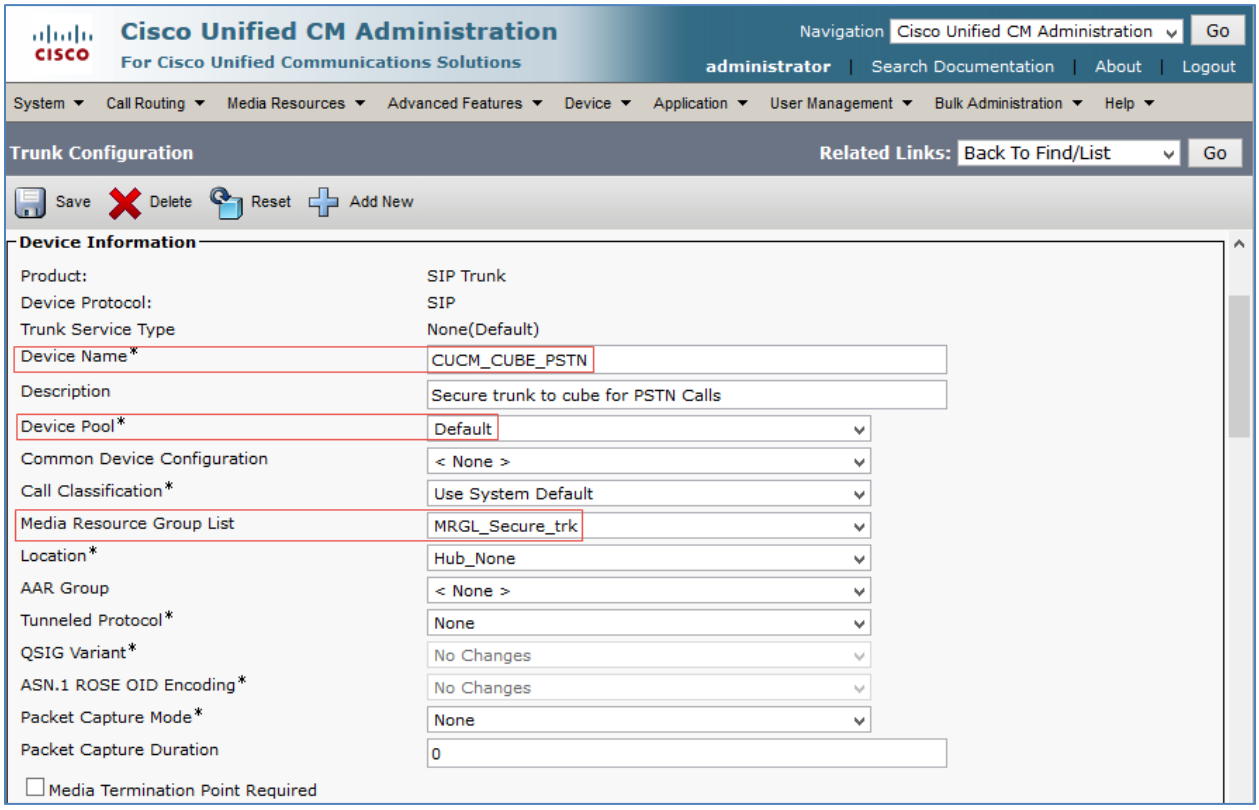
1. From the **Device** menu drop-down menu, select **Trunk**.
2. Click **Add New**.

Cisco UCM: Trunk Configuration



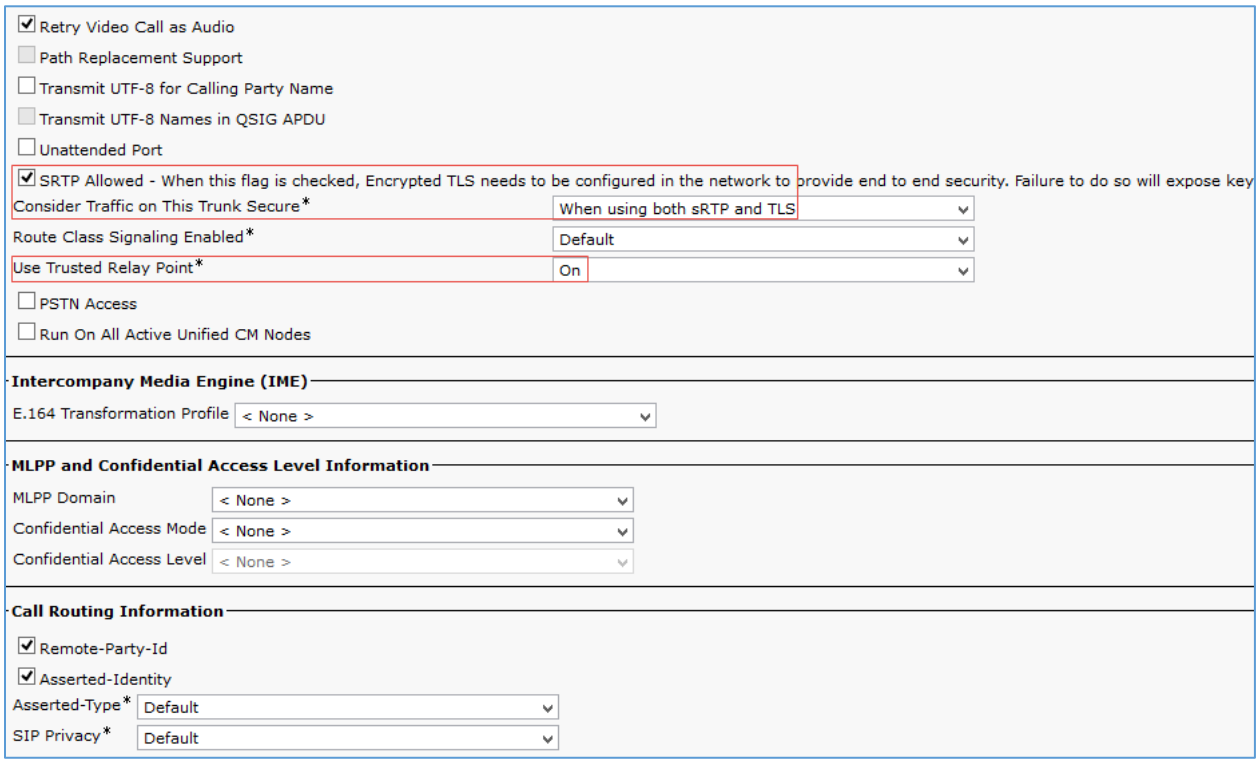
3. Select **Trunk Type*: SIP Trunk**, **Device Protocol*: SIP** and **Trunk Service Type*: None (Default)**
4. Click **Next**.

Cisco UCM: Trunk Configuration Parameters (1/5)



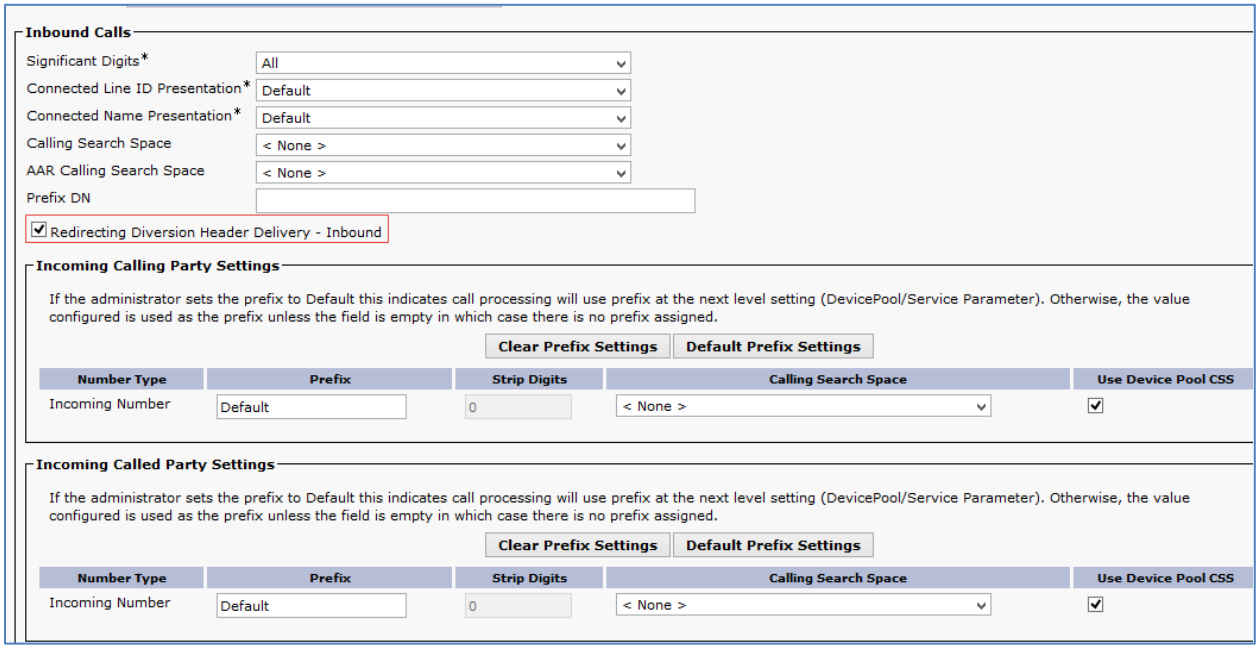
5. In the **Device Name** field, enter a unique SIP Trunk name and optionally, provide a description. *CUCM_CUBE_PSTN* was configured in this example.
6. From the **Device Pool** drop-down list, select a device pool. *Default* was used in this example.
7. From the **Media Resource Group List**, select *MRGL_Secure_trk* from the drop-down menu.
8. Ensure that the **Media Termination Point Required** check box is unchecked.

Cisco UCM: Trunk Configuration Parameters (2/5)



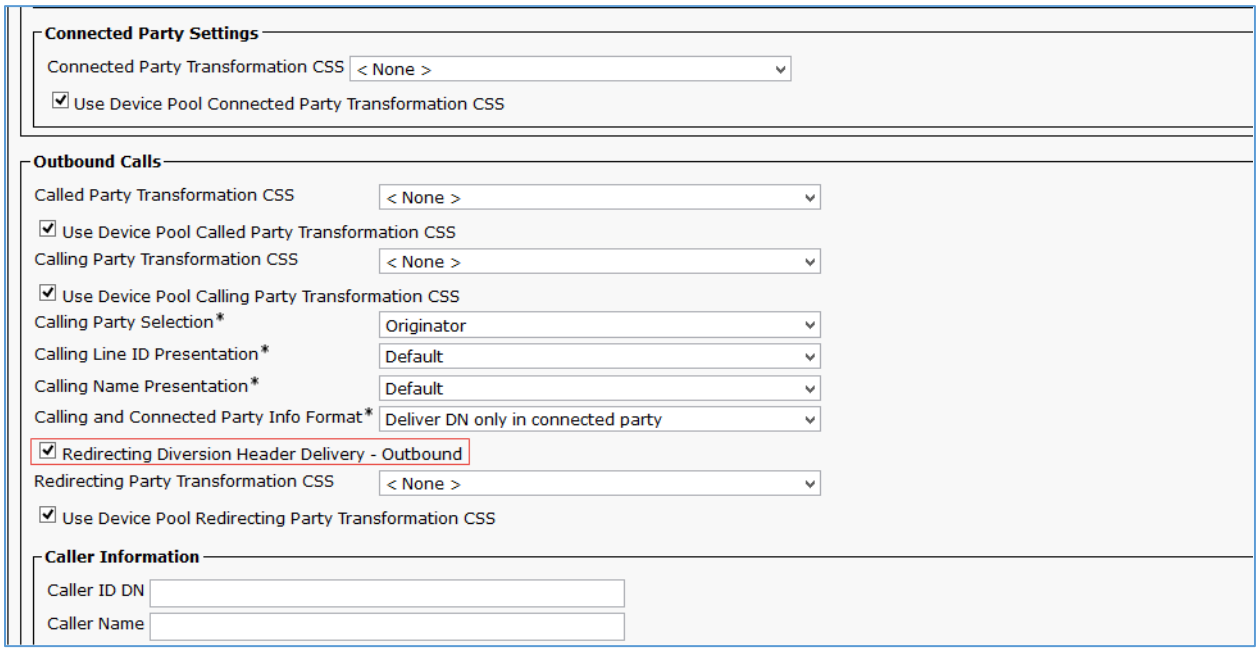
9. Check the **SRTP Allowed** check box.
10. Configure **Consider Traffic on This Trunk Secure:** *When using both sRTP and TLS.*
11. Configure **Use Trusted Relay Point:** *On*.

Cisco UCM: Trunk Configuration Parameters (3/5)



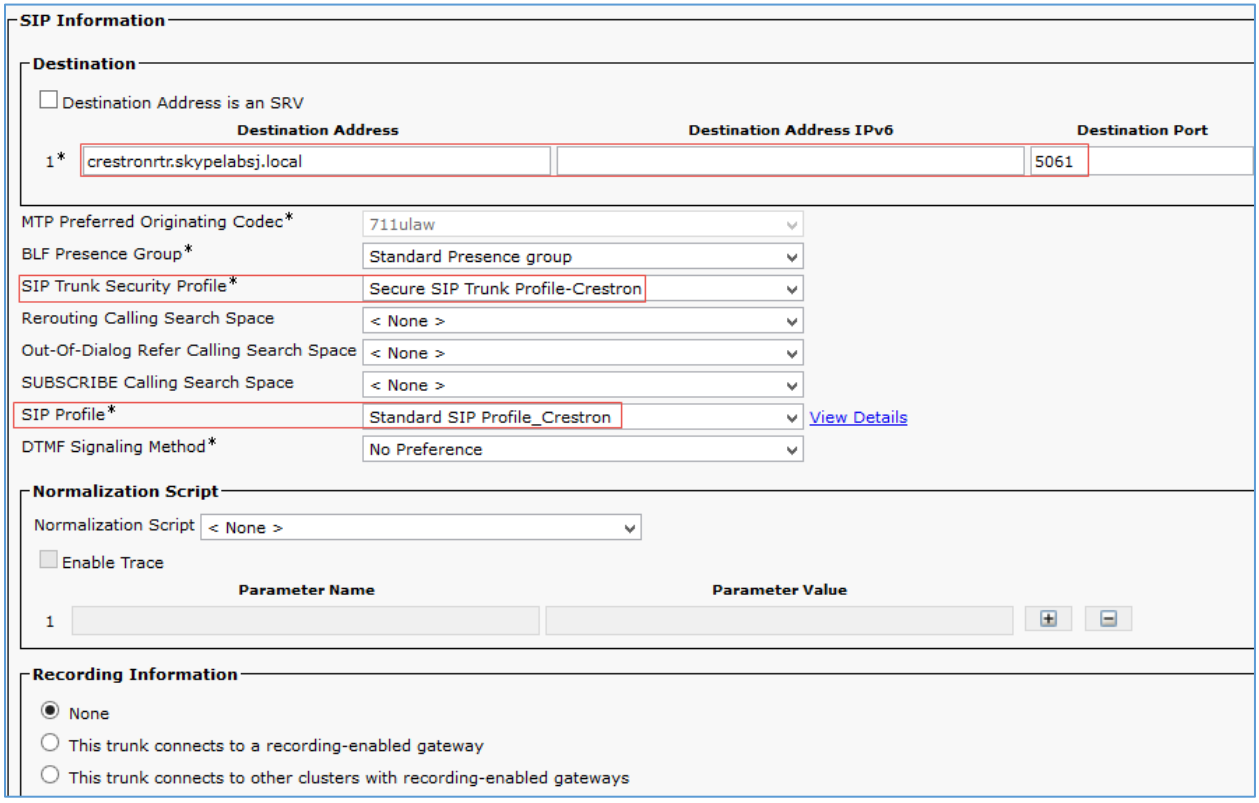
12. Select the **Redirecting Diversion Header Delivery – Inbound** check box.

Cisco UCM: Trunk Configuration Parameters (4/5)



13. Select the **Redirecting Diversion Header Delivery – Outbound** check box.

Cisco UCM: Trunk Configuration Parameters (5/5)



14. Under the **SIP Information**, perform the following procedure.
    a. Enter the FQDN of the Cisco UBE and port of the Cisco UBE LAN interface.
    b. Select the **Secure SIP Trunk Profile_Crestron** as the SIP Trunk Security Profile.
    c. Select the configured *Standard SIP Profile_Crestron* SIP Profile.
15. Click **Save**.

Configure Route Patterns

Route patterns were configured for the following actions.

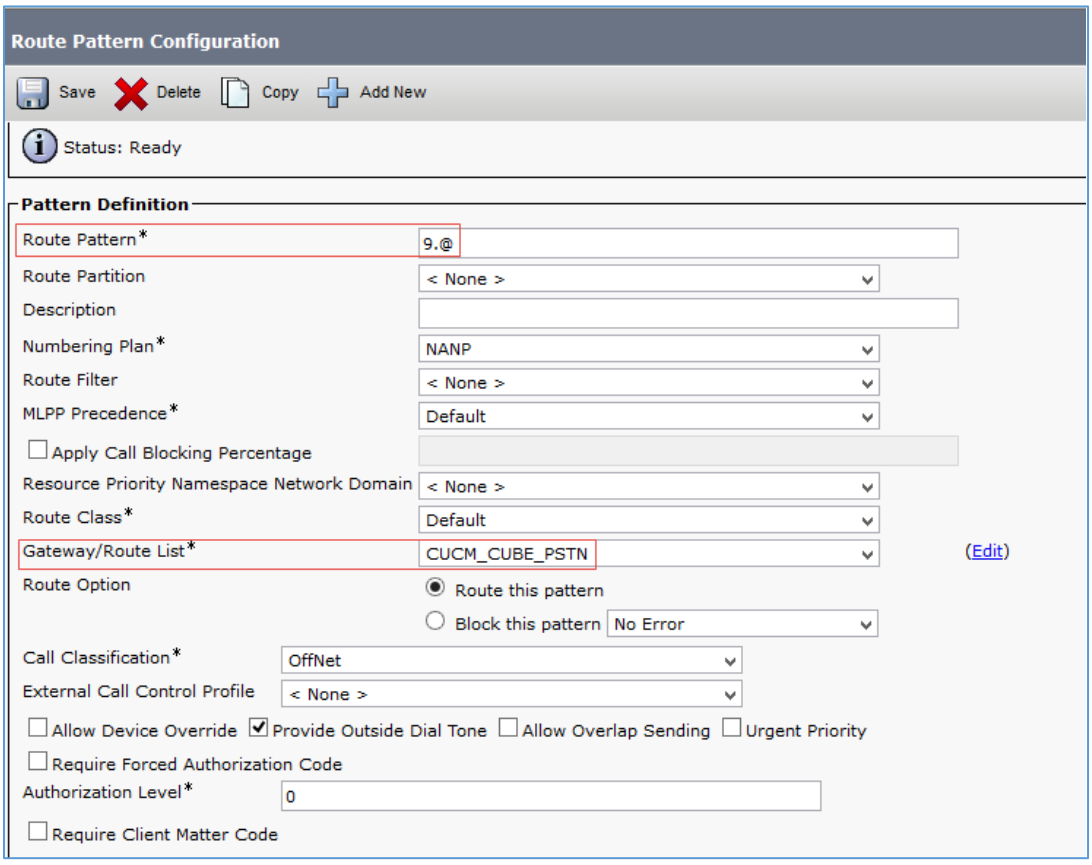
- To route calls from the Cisco UCM to the Cisco UBE towards PSTN GW
- To restrict caller ID on outgoing calls

To configure route patterns, perform the following procedure.

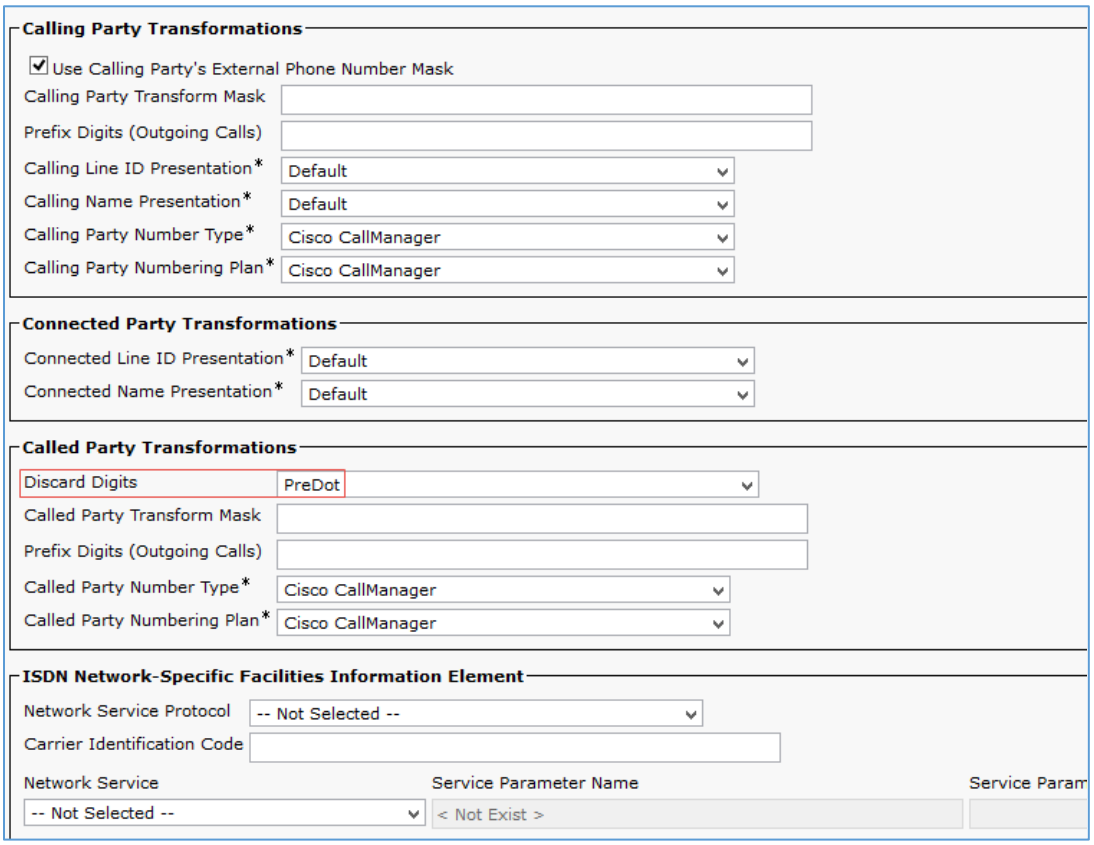
1. Navigate to **Call Routing** > **Route/Hunt** > **Route Pattern**.
2. Click **Add New.**
3. Enter the details desired and then click **Save**.

The route patterns **9.@** and **\+*** were configured to enable outbound dialing from Cisco UCM to Cisco UBE using the access code "9" and using the "+".

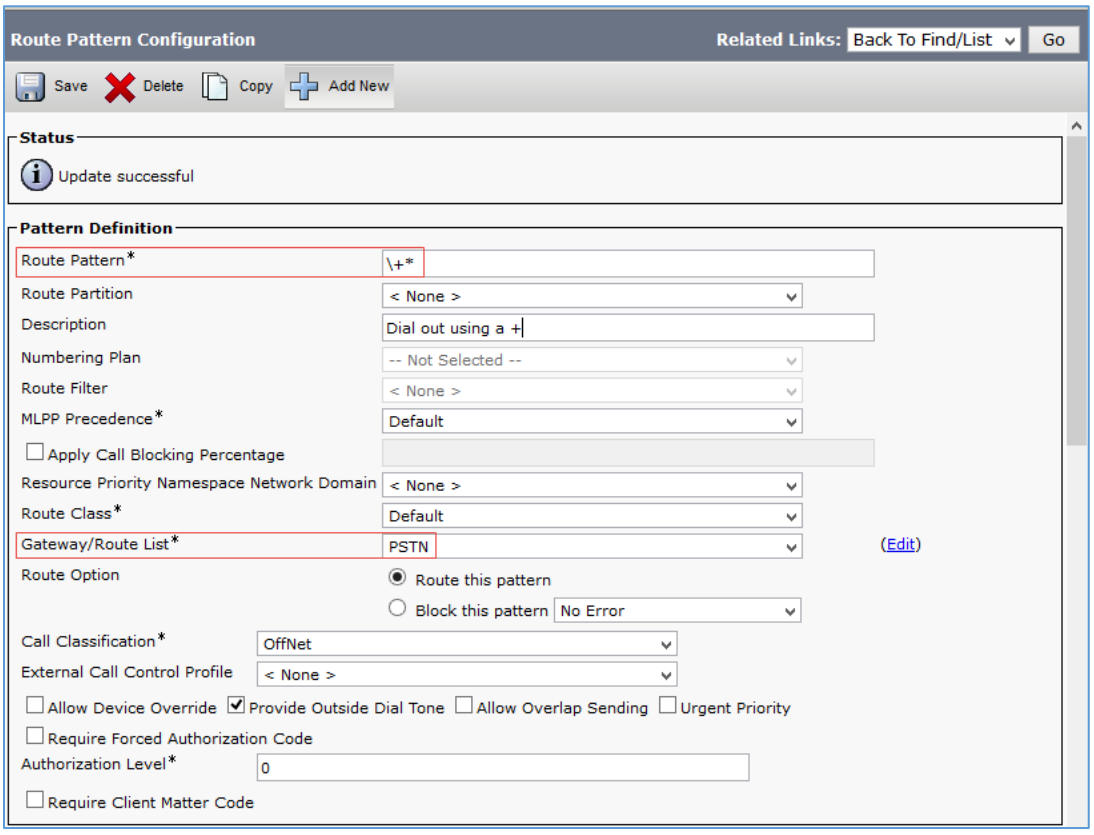
Cisco UCM: Route Pattern Configuration: Outbound Dialing Using Access Code 9 (1/2)



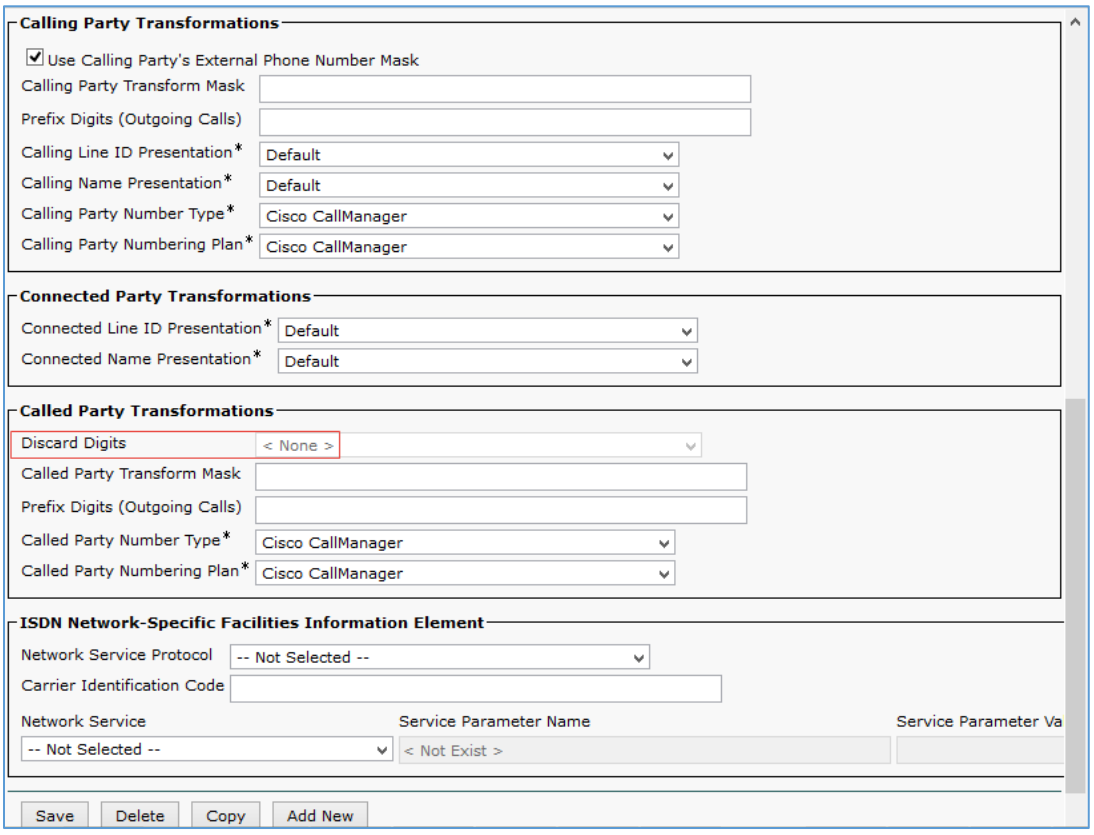
Cisco UCM: Route Pattern Configuration: Outbound Dialing Using Access Code 9 (2/2)



Cisco UCM: Route Pattern Configuration: Outbound Dialing Using a + (1/2)

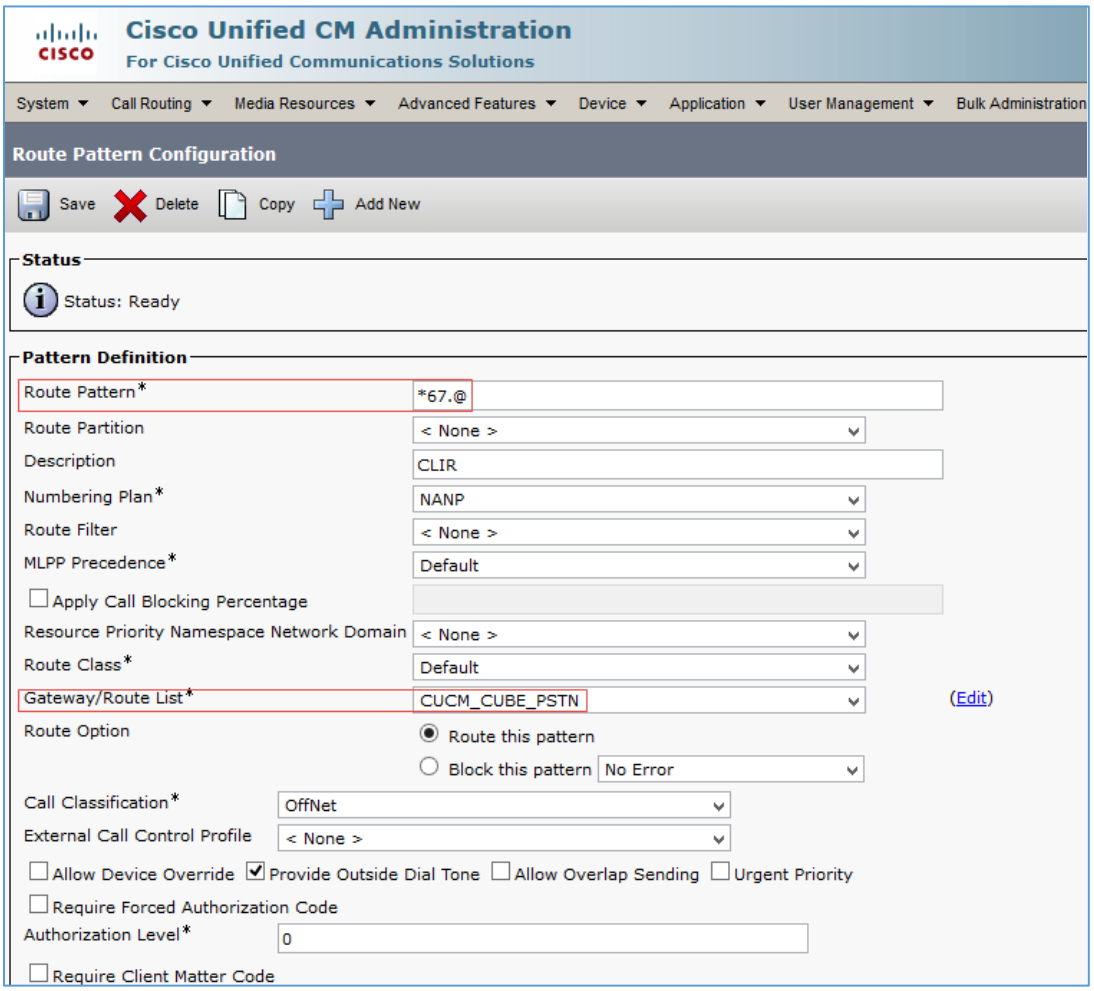


Cisco UCM: Route Pattern Configuration: Outbound Dialing Using a + (2/2)

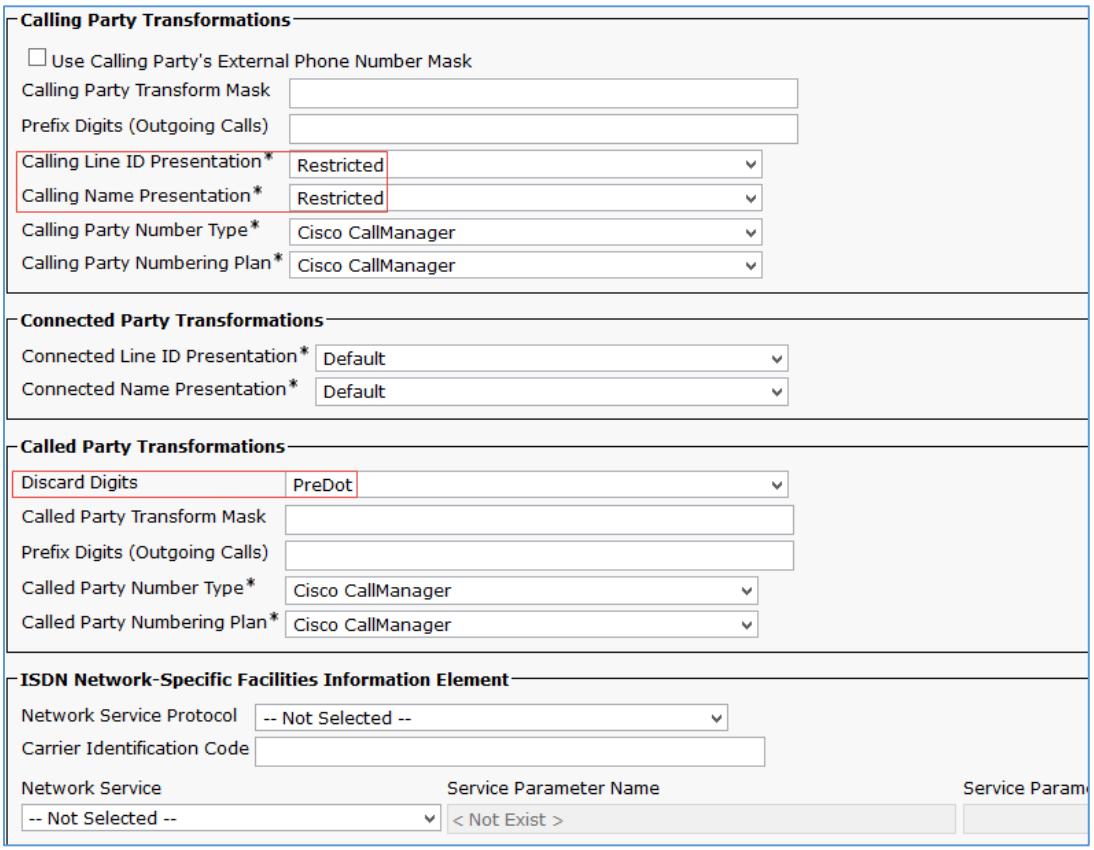


Similarly, the route pattern of ***67.@** was configured to restrict caller ID on outbound calls.

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



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



Crestron Electronics, Inc.
15 Volvo Drive Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

Supplemental Guide – DOC. 7991A
(2048877)
05.17
Specifications subject to
change without notice.