# MiaRec

## Cisco Ucm-Integration-Guide

MiaRec, Inc.

# Table of contents

# 1. Cisco UCM Recording Integration Guide

This guide describes the configuration procedures required for call recording on Cisco Unified Communication Manager (UCM) platform and the phones that have the Built-in-Bridge (BiB) capability.

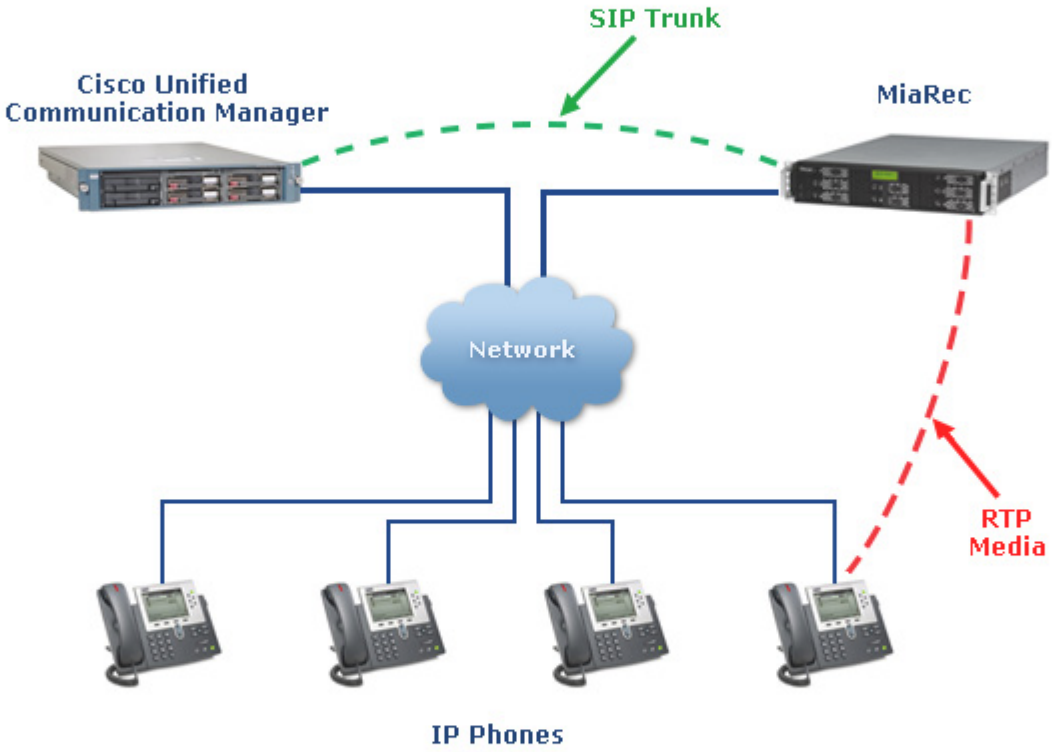
## 1.1 Requirements

The features utilized in this method of recording require the following:

- Cisco Unified Communications Manager v.8.5.1 or newer.
- 3-rd generation phones that have the built-in bridge capability (BIB).

# 2. How it Works

The MiaRec call recording system utilizes the Built-in-Bridge call monitoring and recording capability available in 3-rd generation of Cisco phones. Cisco UCM establishes SIP trunk connections to MiaRec recording server and notifies the latter when the call is started. Cisco IP phone relays RTP media directly to the recorder.



# 3. Cisco Phones Supporting Built-in-Bridge Feature

The following table lists Cisco IP phone models, which support the Built-in-Bridge feature for call recording and monitoring:

| Phone model | Supported protocols |
| --- | --- |
| Cisco 6901 | not supported |
| Cisco 12 S | not supported |
| Cisco 12 SP | not supported |
| Cisco 30 SP+ | not supported |
| Cisco 3905 | not supported |
| Cisco 3911 | not supported |
| Cisco 6901 | not supported |
| Cisco 6911 | SCCP, SIP |
| Cisco 6921 | SCCP, SIP |
| Cisco 6941 | SCCP, SIP |
| Cisco 6945 | SCCP, SIP |
| Cisco 6961 | SCCP, SIP |
| Cisco 7811 | SIP |
| Cisco 7821 | SIP |
| Cisco 7841 | SIP |
| Cisco 7861 | SIP |
| Cisco 7902 | not supported |
| Cisco 7905 | not supported |
| Cisco 7906 | SCCP, SIP |
| Cisco 7910 | not supported |
| Cisco 7911 | SCCP, SIP |
| Cisco 7912 | not supported |
| Cisco 7914 Sidecar | SCCP |
| Cisco 7915 Sidecar | SCCP, SIP |
| Cisco CKEM Sidecar | SIP |
| Cisco 7920 | not supported |
| Cisco 7921 | SCCP |
| Cisco 7925 | SCCP |
| Cisco 7926 | SCCP |
| Cisco 7931 | SCCP, SIP |
| Cisco 7935 | not supported |
| Cisco 7936 | not supported |
| Cisco 7937 | SCCP |
| Cisco 7940 | not supported |
| Cisco 7941 | SCCP, SIP |

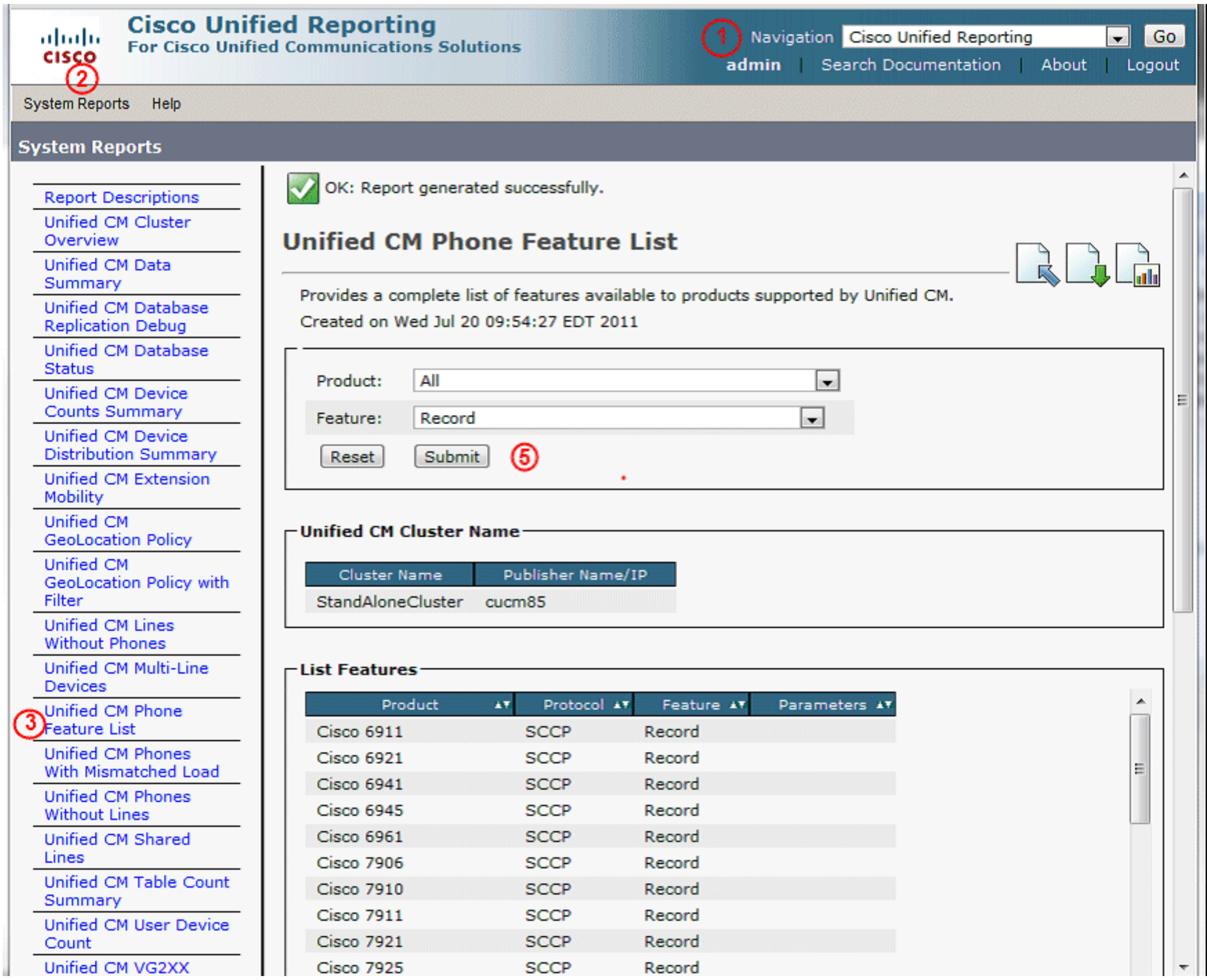
| Phone model | Supported protocols |
|---|---|
| Cisco 7941G-GE | SCCP, SIP |
| Cisco 7942 | SCCP, SIP |
| Cisco 7945 | SCCP, SIP |
| Cisco 7960 | not supported |
| Cisco 7961 | SCCP, SIP |
| Cisco 7961G-GE | SCCP, SIP |
| Cisco 7962 | SCCP, SIP |
| Cisco 7965 | SCCP, SIP |
| Cisco 7970 | SCCP, SIP |
| Cisco 7971 | SCCP, SIP |
| Cisco 7975 | SCCP, SIP |
| Cisco 7985 | SCCP, SIP |
| Cisco 8811 | SIP |
| Cisco 8831 | SIP |
| Cisco 8841 | SIP |
| Cisco 8845 | SIP |
| Cisco 8851 | SIP |
| Cisco 8861 | SIP |
| Cisco 8865 | SIP |
| Cisco 8941 | SCCP, SIP |
| Cisco 8945 | SCCP, SIP |
| Cisco 8961 | SIP |
| Cisco 9951 | SIP |
| Cisco 9971 | SIP |
| Cisco DX650 | SIP |
| Cisco E20 | not supported |
| Cisco EX60 | not supported |
| Cisco EX90 | not supported |
| Cisco CTS 500 | not supported |
| Cisco CTS 500-32 | not supported |
| Cisco ATA 186 | not supported |
| Cisco ATA 187 | not supported |
| Cisco ATA 188 | not supported |
| Cisco IP Communicator | SCCP, SIP |
| Cisco Jabber for Windows | SCCP, SIP |

| Phone model | Supported protocols |
|---|---|
| Cisco Jabber for Mac | SCCP, SIP |
| Cisco Jabber for iPad | not supported |
| Cisco Jabber for Android | not supported |
| Cisco Unified Personal Communicator | not supported |
| Cisco VGC Phone | not supported |
| VG224 | not supported |
| VG248 | not supported |
| CTI Port | not supported |
| CTI Remote Device | not supported |
| CTI Route Point | not supported |

## 3.1 Identify phones that support Built-in-Bridge recording

An up-to-date list of phone models that support the Built-in-Bridge recording may be received with the following instructions:

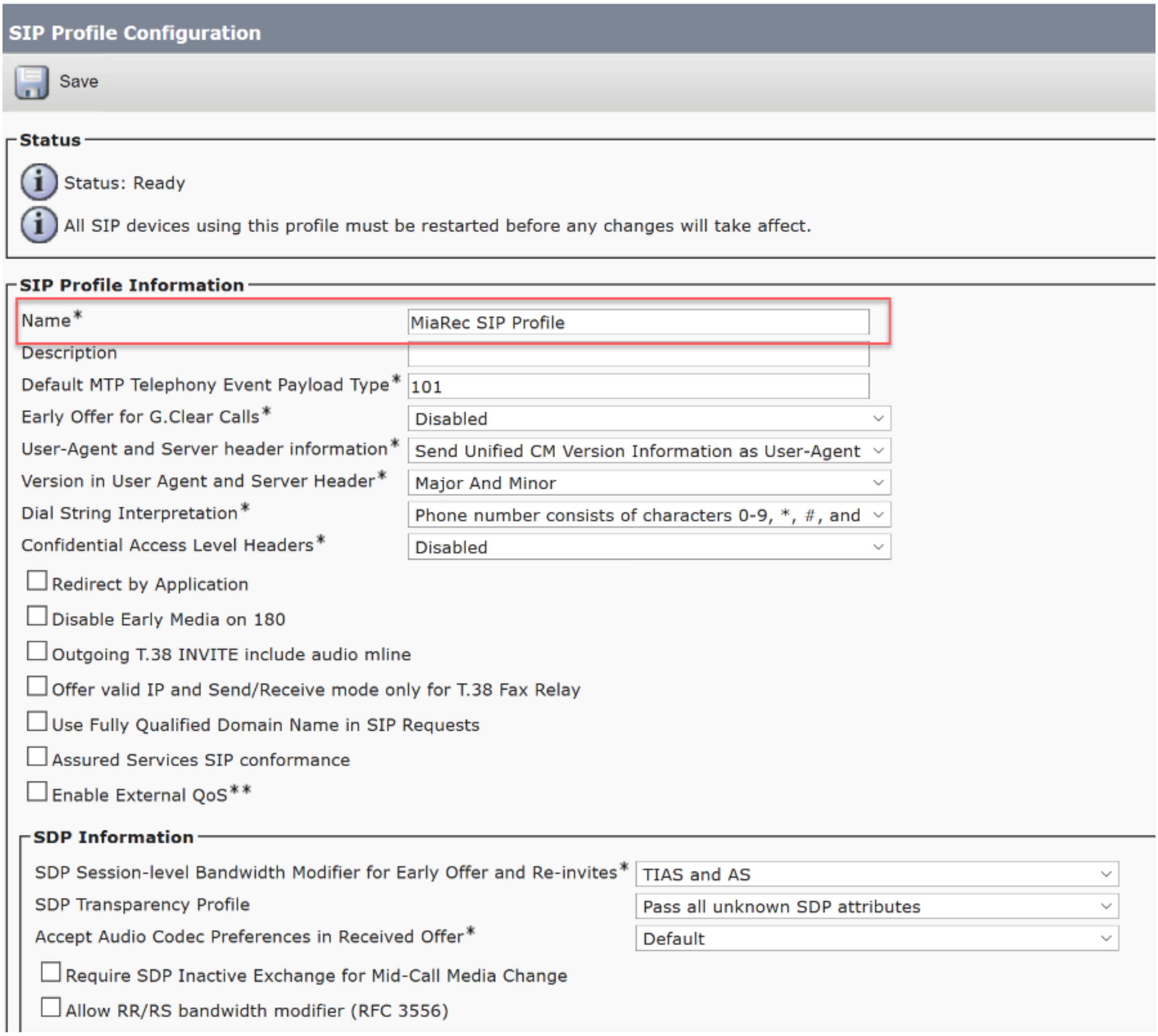
1. Start the **Cisco Unified Reporting Manager Administration** application. In the **Navigation** menu, select **Cisco Unified Reporting** and click **Go**.
2. In the navigation bar, click **System Reports**.
3. In the left-side panel with a list of reports, click **Unified CM Phone Feature List**.
4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if the report already exists.
5. To generate a report of all devices that support recording, choose the following settings and click the **Submit** button:
6. **Product**: *All*
7. **Feature**: *Record*
8. The **List Features** section will display a list of all devices that support the recording feature. You can click the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.


Cisco Unified Reporting
For Cisco Unified Communications Solutions
Navigation Cisco Unified Reporting Go
admin | Search Documentation | About | Logout
System Reports Help
System Reports
Report Descriptions
Unified CM Cluster Overview
Unified CM Data Summary
Unified CM Database Replication Debug
Unified CM Database Status
Unified CM Device Counts Summary
Unified CM Device Distribution Summary
Unified CM Extension Mobility
Unified CM GeoLocation Policy
Unified CM GeoLocation Policy with Filter
Unified CM Lines Without Phones
Unified CM Multi-Line Devices
Unified CM Phone Feature List
Unified CM Phones With Mismatched Load
Unified CM Phones Without Lines
Unified CM Shared Lines
Unified CM Table Count Summary
Unified CM User Device Count
Unified CM VG2XX
OK: Report generated successfully.
Unified CM Phone Feature List
Provides a complete list of features available to products supported by Unified CM.
Created on Wed Jul 20 09:54:27 EDT 2011
Product: All
Feature: Record
Reset Submit
Unified CM Cluster Name
Cluster Name Publisher Name/IP
StandAloneCluster cucm85
List Features
Product Protocol Feature Parameters
Cisco 6911 SCCP Record
Cisco 6921 SCCP Record
Cisco 6941 SCCP Record
Cisco 6945 SCCP Record
Cisco 6961 SCCP Record
Cisco 7906 SCCP Record
Cisco 7910 SCCP Record
Cisco 7911 SCCP Record
Cisco 7921 SCCP Record
Cisco 7925 SCCP Record
1
2
3
5

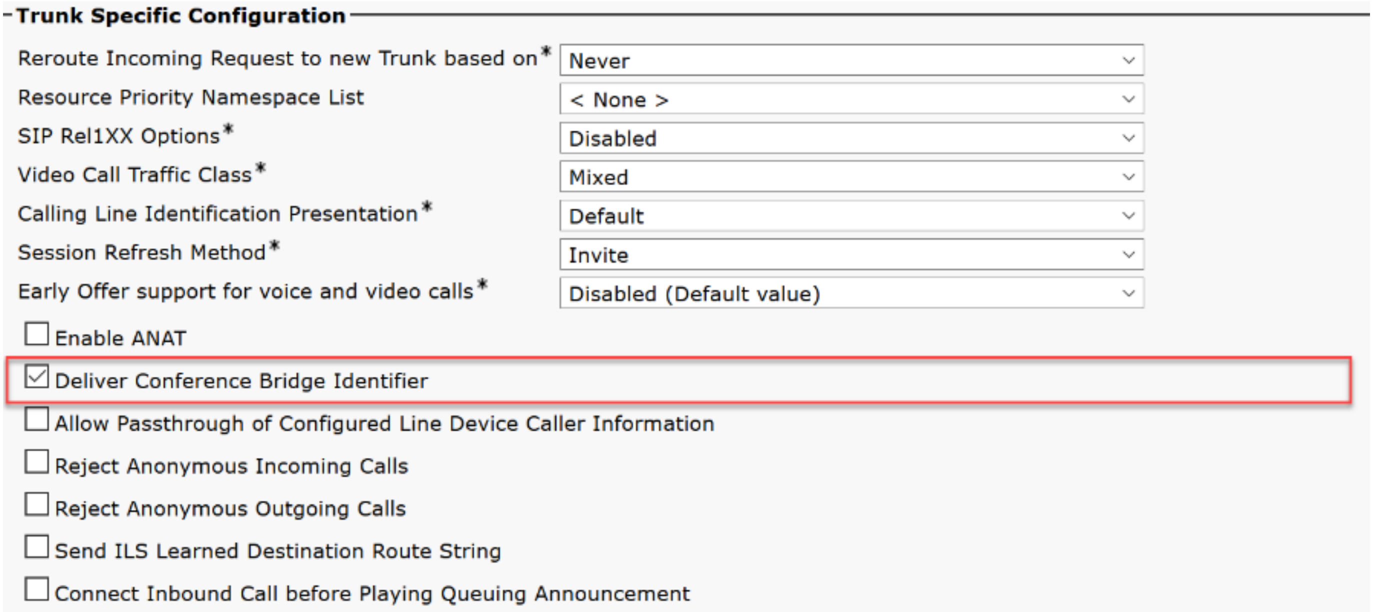
# 4. Configure CUCM

## 4.1 Step 1: Create the SIP Profile for Recorder

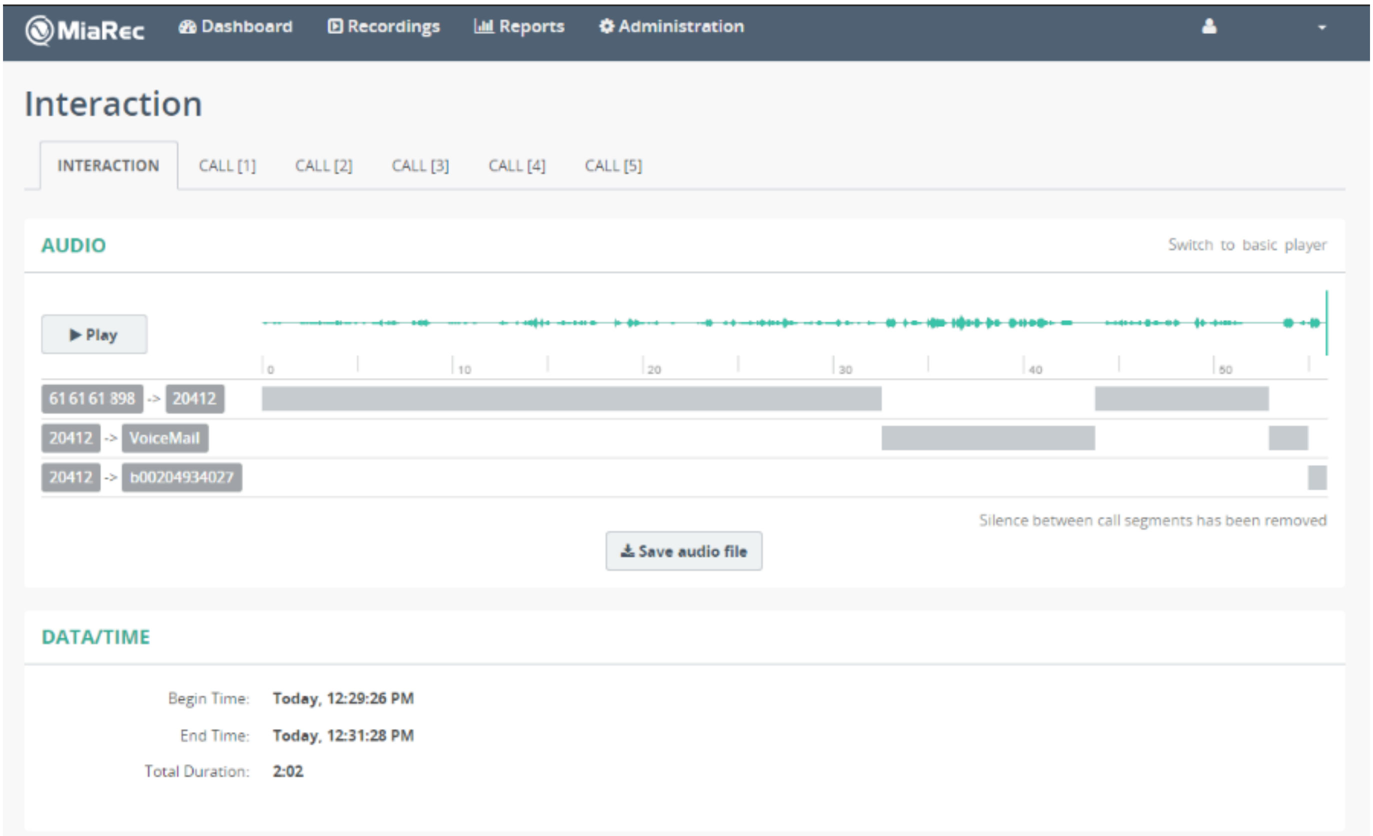
Use the **Device > Device Settings > SIP Profile** menu option in Cisco Unified Communications Manager Administration to create a SIP profile for recorder.




Make sure that the **Deliver Conference Bridge Identifier** option is checked. If enabled, it allows you to deliver additional information (specifically, the b-number that identifies a conference bridge) to the recorder across the SIP trunk. If the check box is left unchecked, the far-end information for the remote conference remains empty. Check the **Deliver Conference Bridge Identifier** check box on the remote cluster SIP profile as well.




Checking this check box is not required for recording, but the conference bridge identifier helps to group multiple call segments belonging to the same conference into one interaction, like shown in the screenshot below:



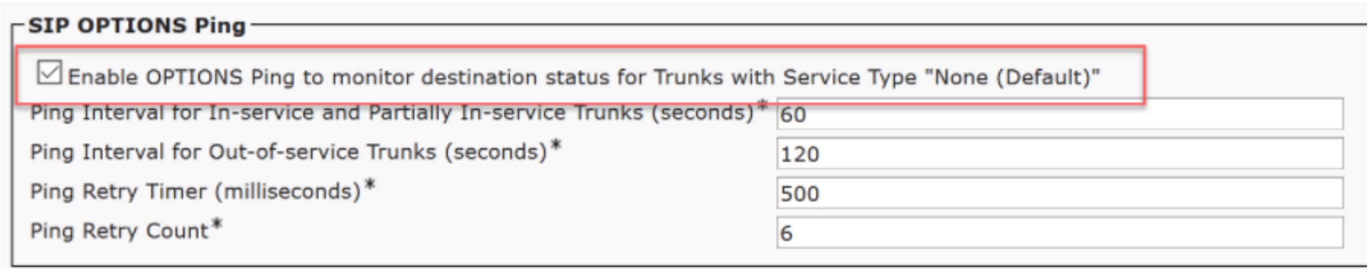

## 4.1.1 Configure SIP Options Ping

In multi-server setup, it is recommended to enable the SIP Options Ping feature for each recording server. In a single-server setup, this feature should be disabled (see details below).

- **Single-server setup** - disable SIP OPTIONS Ping
- **Multi-server setup** - enable SIP OPTIONS Ping

Cisco UCM starting from v.8.5(1) supports the SIP OPTIONS Ping feature. Cisco UCM periodically sends a SIP OPTIONS (ping) message to each recording server to detect its availability. If the recording server is unavailable – indicated by either no response, response of “408 Request Timeout” response of “503 Service Unavailable”, Cisco UCM marks this recording server as unavailable. It skips that server in the round-robin or sequential list of recording servers. The SIP Options Ping feature allows detecting availability of the recording server earlier, without having to wait until a call is ready to be recorded.

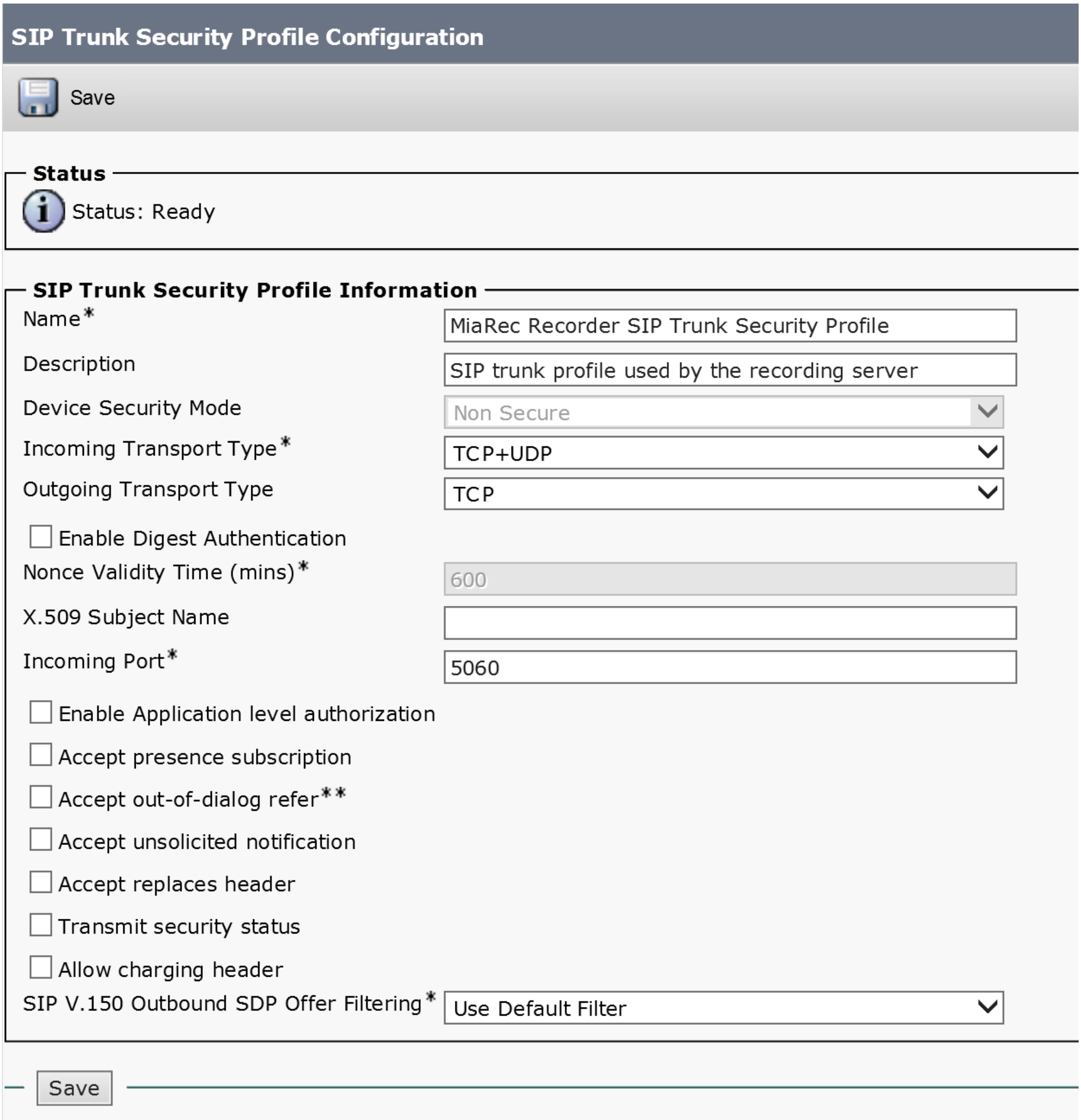
However, **in single-node deployments, SIP Options Ping is not recommended**. Not only it is not helpful, but it can result in unnecessary failure recovery delays.




## 4.2 Step 2: Create the SIP Trunk Security Profile

Use the **System > Security > SIP Trunk Security Profile** menu option in Cisco Unified Communications Manager Administration to create the SIP Trunk Security profile for each MiaRec recording server.

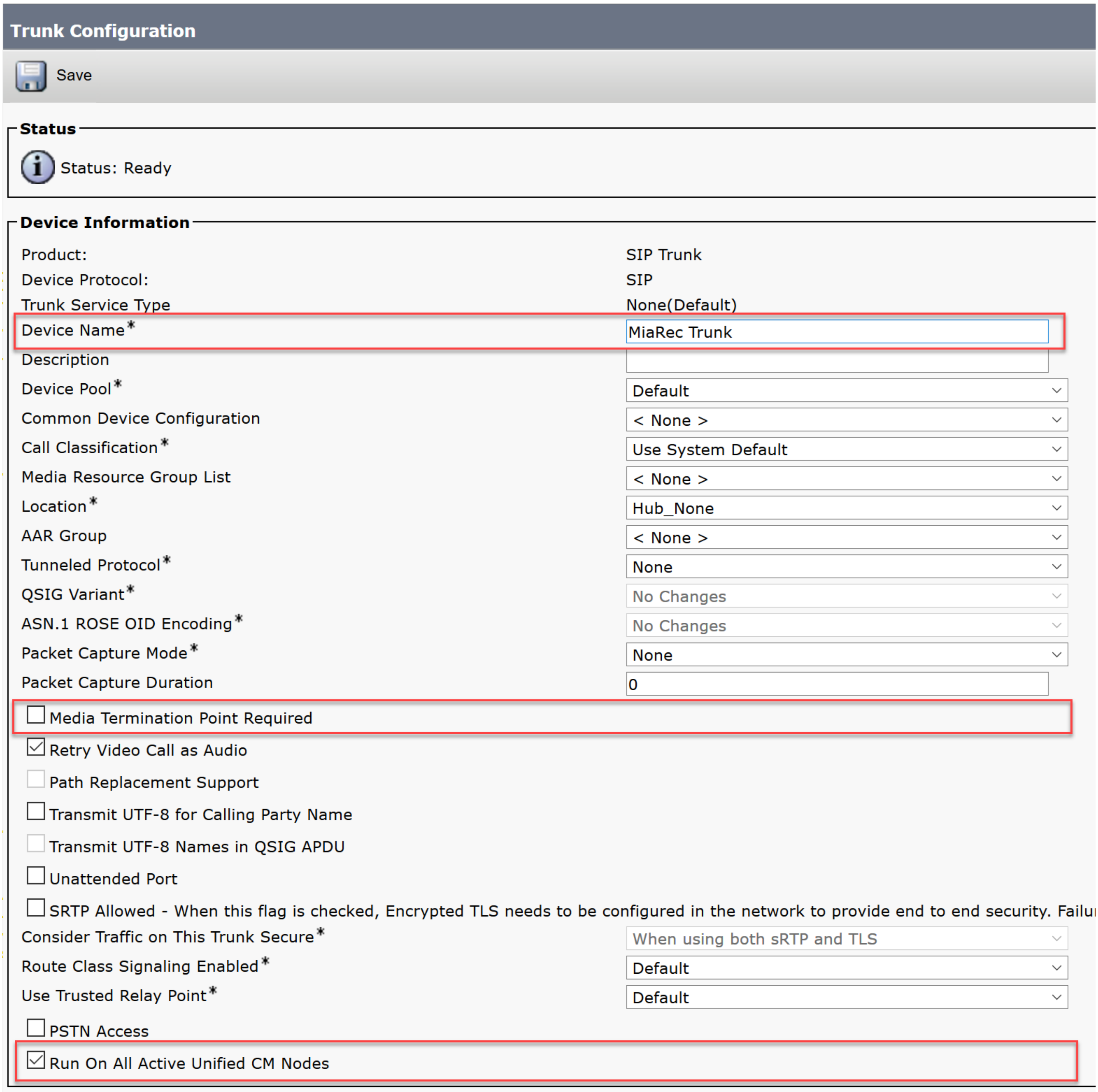
- In the **Incoming Transport Type** field, select **TCP+UDP**.
- In the **Outgoing Transport Type** field, select **TCP** (this setting has to match the configuration of MiaRec). **TCP** is recommended.
- Uncheck the **Enable Digest Authentication** option.
- Set the **Device Security Mode** parameter to **Non Secure**.



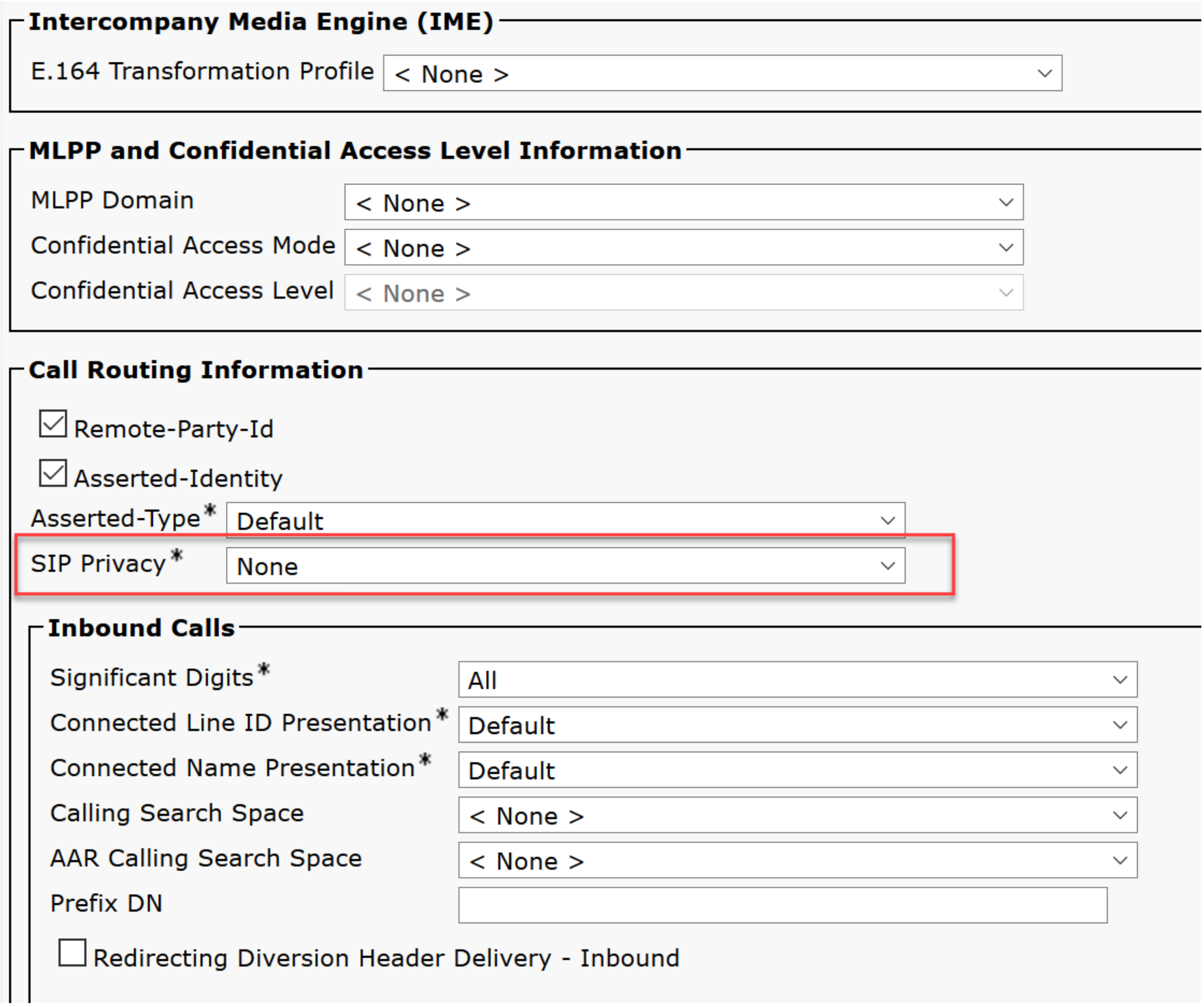

## 4.3 Step 3: Create the SIP Trunk that Points to the Recorder

Use the **Device > Trunk** menu option in Cisco Unified Communications Manager Administration to create the SIP trunk that points to the recorder.

- Ensure that the **Media Termination Point Required** check box is unchecked.
- Select the **Run On All Active Unified CM Nodes** check box.

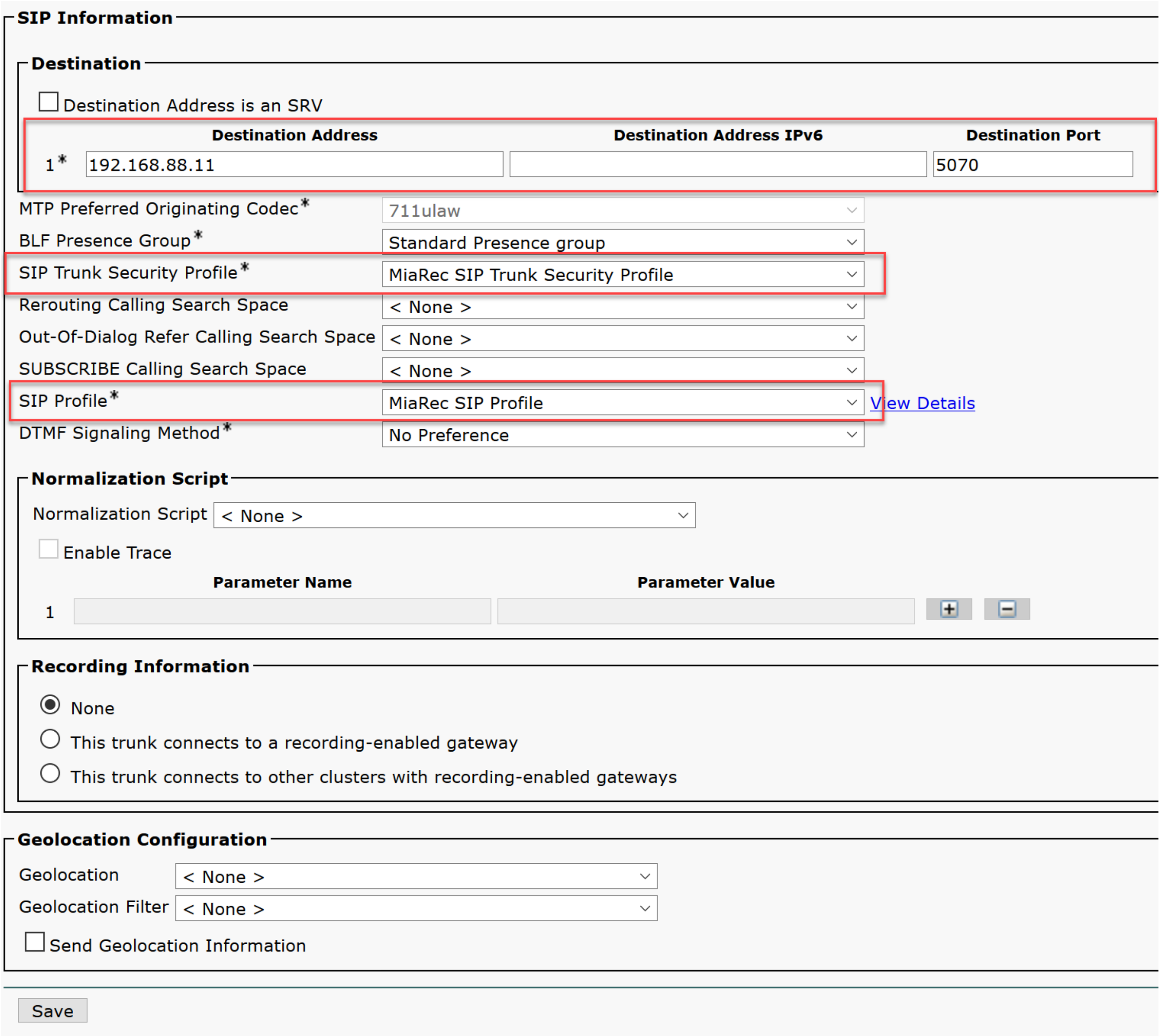



Make sure the **SIP Privacy** option is set to **None**. Otherwise, in call details, you will see the "Anonymous" text instead of the user's extension.



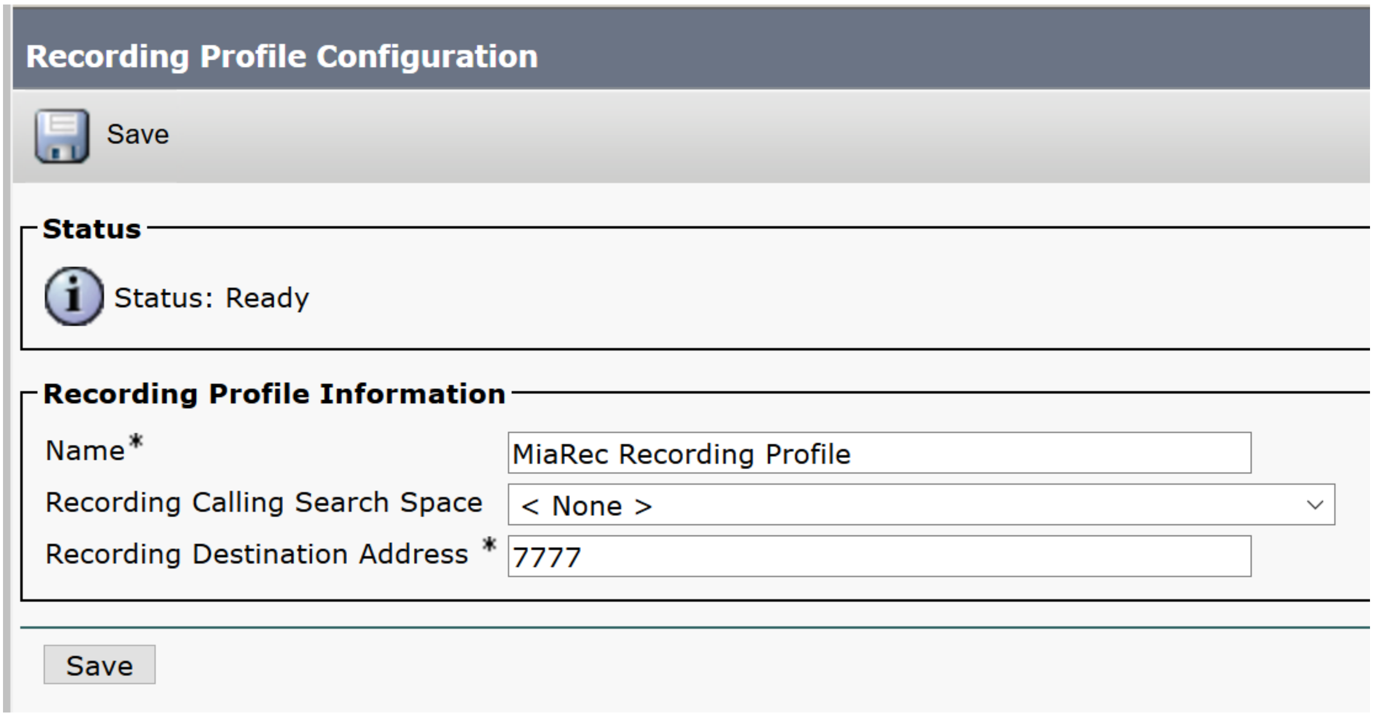

In the **SIP Information** section, provide the following configuraiton:

- The **Destination Address** field should point to the IP-address or DNS name of the recorder server.
- The **Destination Port** field should match the port on which MiaRec recorder is listening for the messages from CUCM (see the configuration of MiaRec below).
- In the **SIP Trunk Security Profile** field, select the previously created SIP trunk security profile for the recorder.
- In the **SIP Profile** field, select the previously created SIP profile for the recorder.




## 4.4 Step 4: Create a Recording Profile

Use the **Device > Device Settings > Recording Profile** menu option in Cisco Unified Communications Manager Administration to create a recording profile.




- Set **Recording Destination Address** to the directory number that associates the recorder with this recording profile. The only guideline for this number: it should be possible for UCM to route it to the SIP trunk where the recorder is defined. No user is going to directly call this number, this is internal to the system. Make sure it does not collide with your numbering plan. This is why the example shows '7777'
- Set **Recording Calling Search Space** to the CSS that includesthe partitions containing the user phones and the partition that you set up for the MiaRec SIP Trunk. **Important!** Recording will not work if CSS of the Recording Profile and phones do not match! The screenshot above shows the **None** value, but in most production configurations, it should be explicitly set to the correct CSS.

## 4.5 Step 5: Create a Route Pattern/Group for the Recorder

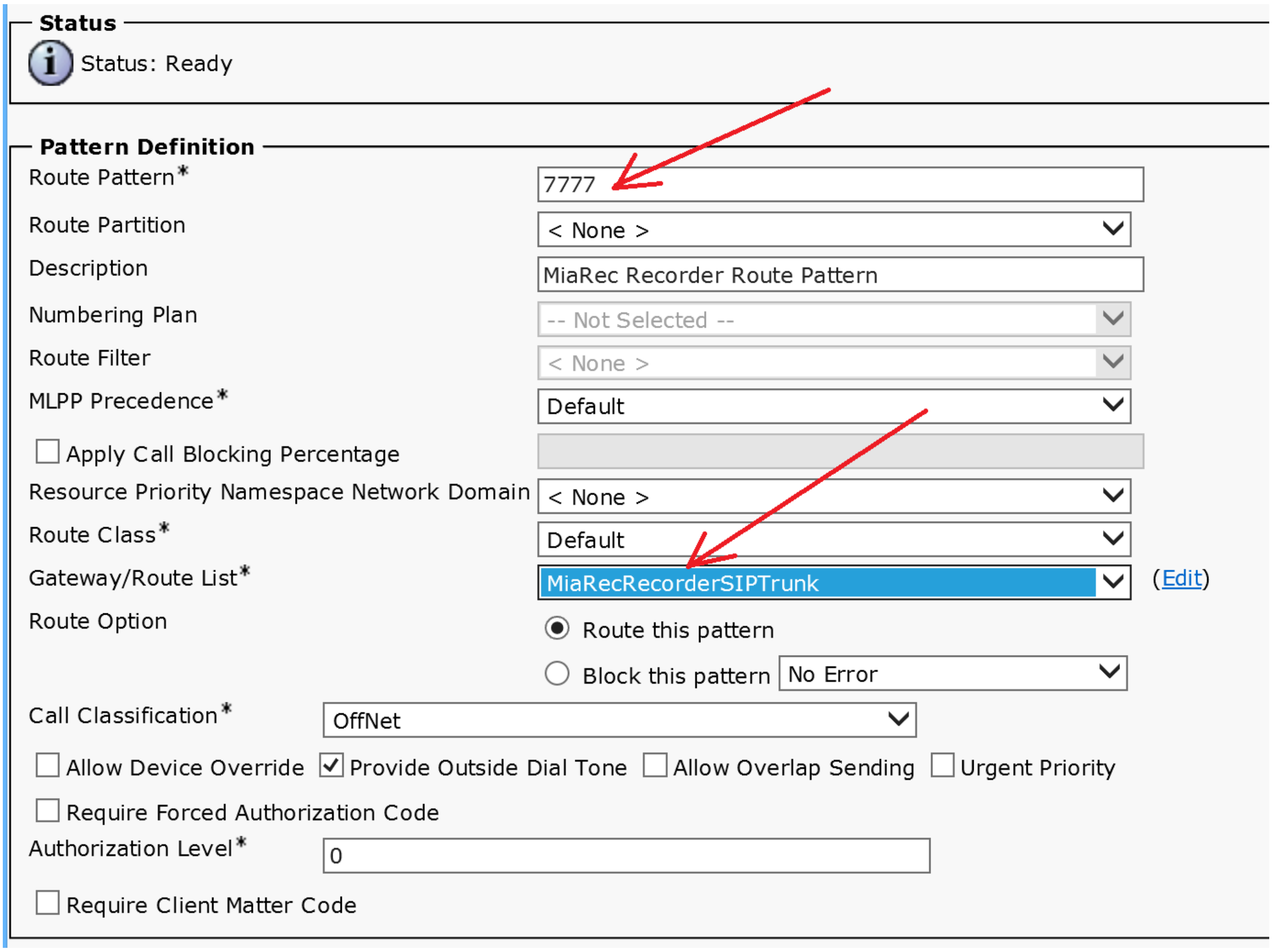
This configuration step depends on how many recorders are used in a cluster, one or multiple.

- For a single recorder, create a route pattern.
- For multiple recorders in HA configuration, create a route group.

### 4.5.1 Single server configuration

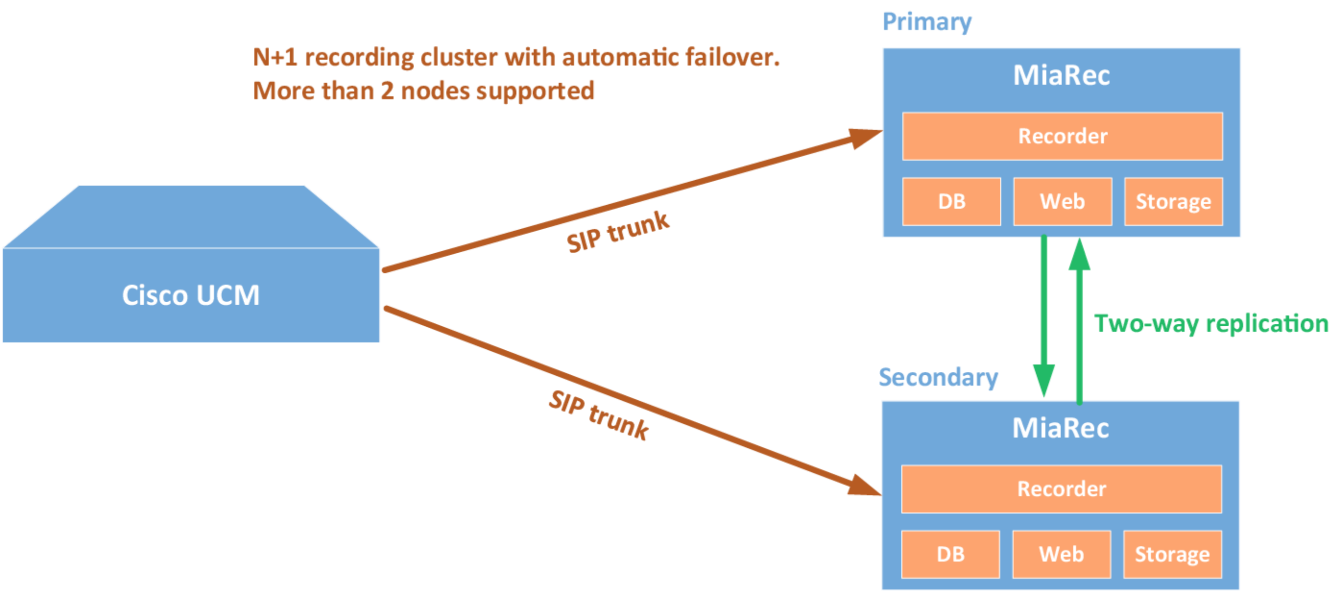
Use the **Call Routing > Route/Hunt > Route Pattern** menu option in Cisco Unified Communications Manager Administration to create a route pattern for the MiaRec recorder SIP trunk:

- The **Route Pattern** should match the directory number associated with the MiaRec recorder. This DN is used to reach the SIP Trunk of MiaRec recorder. No user is going to directly call this number manually. Make sure it does not collide with your numbering plan. This is why the example shows '7777'.
- Set **Route partition** to the partition that includes the user phones.
- In **Gateway/Route List** field, select the SIP trunk that points to the announcement player




### 4.5.2 Multiple servers configuraiton

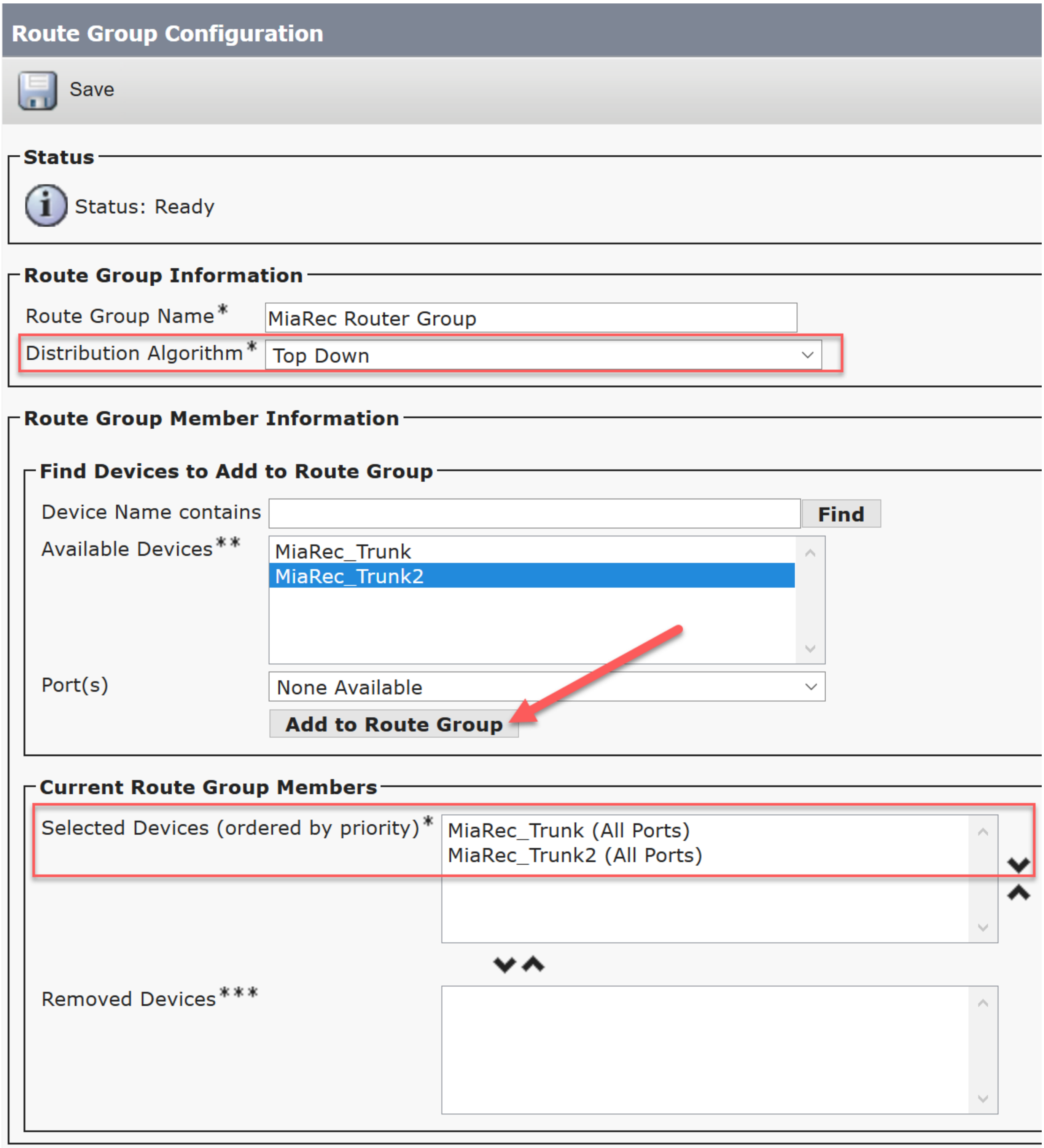
Each recording server in Cisco UCM is configured as a separate SIP Trunk. Cisco UCM will failover automatically from the primary recording server to the secondary in case of failure.



#### Create a new Route Group

Use the **Call Routing > Route/Hunt > Route Group** menu option in Cisco Unified Communications Manager Administration to create a route group for the MiaRec SIP trunk:

- Under the **Find Devices to Add to Route Group** section, assign the previously created SIP trunk(s) to this route group. Select the desired SIP trunk(s) and click the **Add to Route Group** button.
- Set the **Distribution Algorithm** setting to **Top Down**. Note, the Circular algorithm is not suitable for call recording SIP Trunk, because it causes CUCM to send one side of audio one recorder and another side to another recorder (during playback, you will hear one side of conversation).



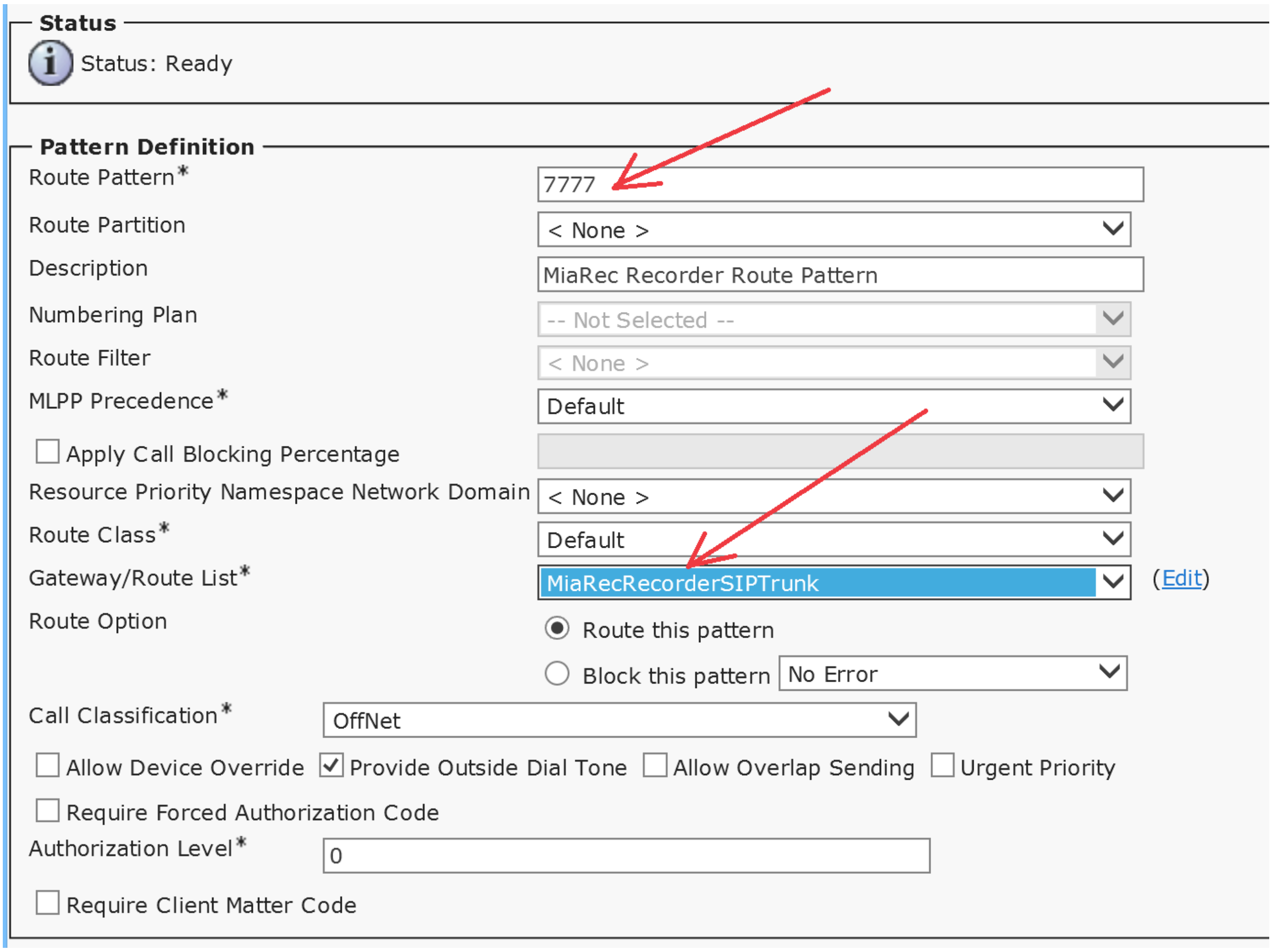
#### Create a new route list

Select **Call Routing > Route/Hunt > Route List** menu item and click the **Add New** button.

- Select the appropriate **Cisco Unified Communications Manager Group** and click the **Save** button.
- Under the **Route List Member Information** section, click the **Add Route Group** button.
- In the **Route Group** field, select the previously created route group, then click **Save**.
- On the **Route List Configuration** page, click the **Save** button.

#### Create a new route pattern

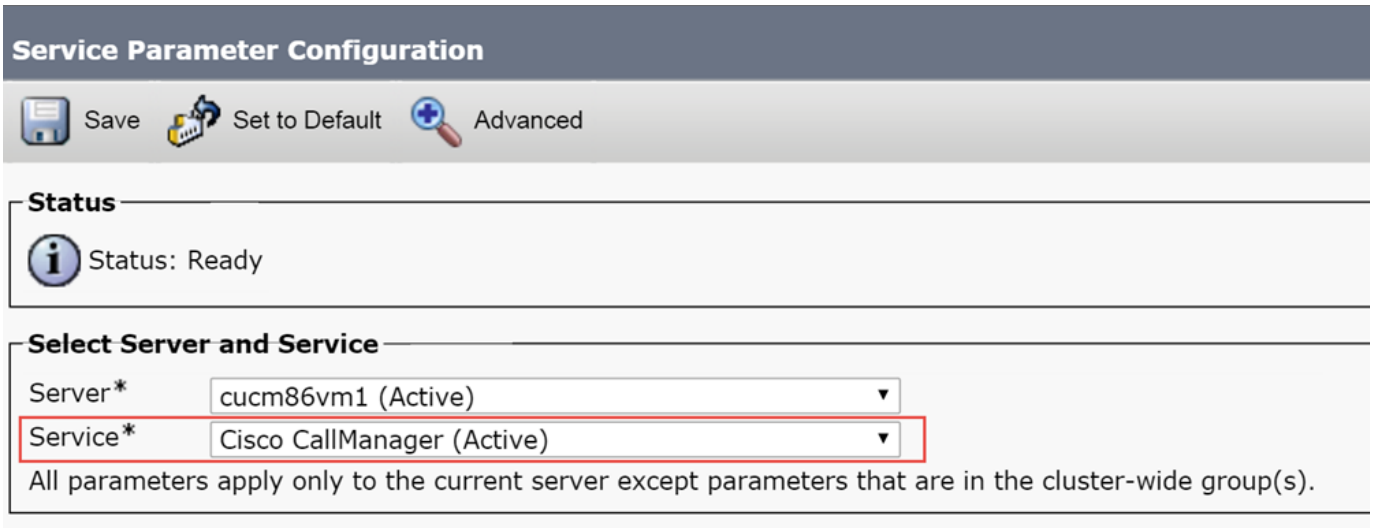
- The **Route Pattern** field should match the value specified in the **Recording Destination Address** in the previously created recording profile.
- In the **Route partition** field, select the partition that includes the user phones.
- In **Gateway/Route List** field, select the route list in which the recorder is a member.



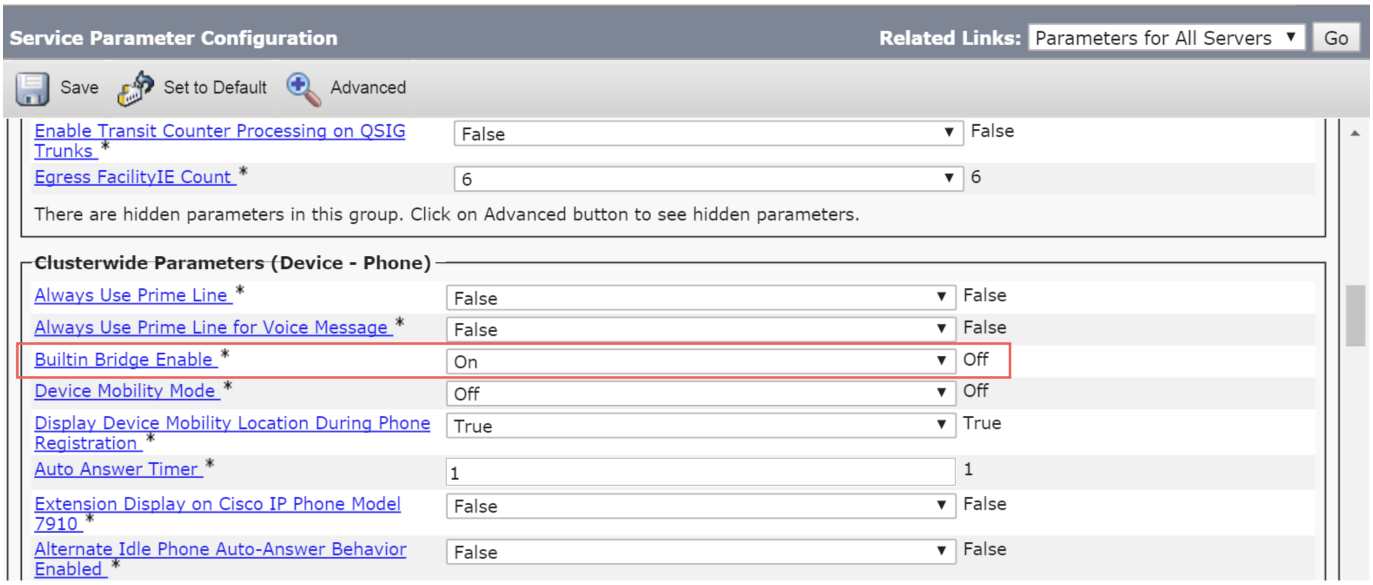

## 4.6 Step 6: Enable Built-in-Bridge for all Phones (optional)

The Built-in-Bridge option can be enabled on per-phone basis or on system level (default to all phones).

Access the **System > Service Parameters** menu option in Cisco Unified Communications Manager Administration, select your CUCM server from the **Server** list and **Cisco CallManager** from the **Service** list:




To enable the Built-in-Bridge option on system level, under the **Clusterwide Parameters (Device - Phone)** section, in the **Builtin Bridge Enable** field, select **On.**



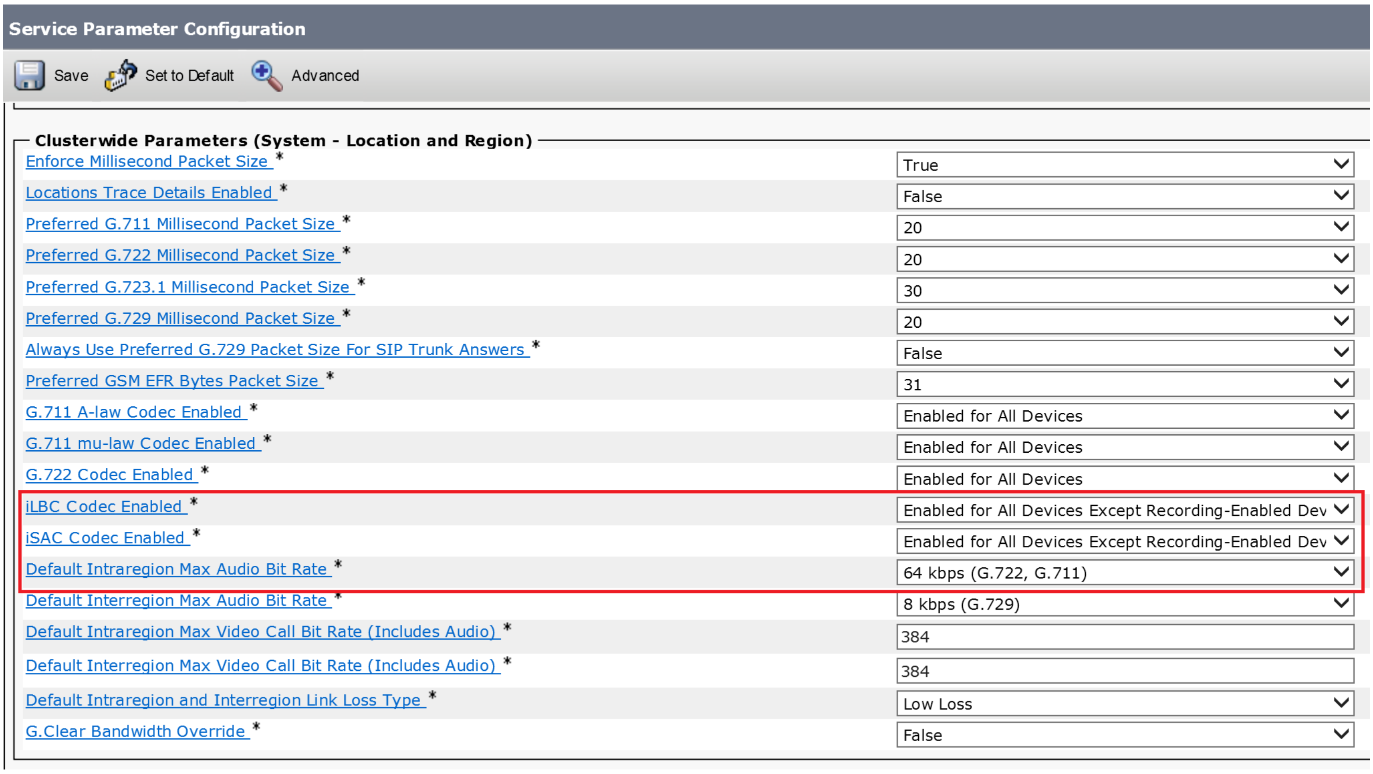

## 4.7 Codecs Configuration

The iLBC, iSAC, L16 and AAC-LD codecs should be disabled for Recording-Enabled devices as they are not supported by MiaRec recording system at the moment.

Use the **System > Service Parameters** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

In the **Clusterwide Parameters (System - Location and Region),** provide the following configuration:

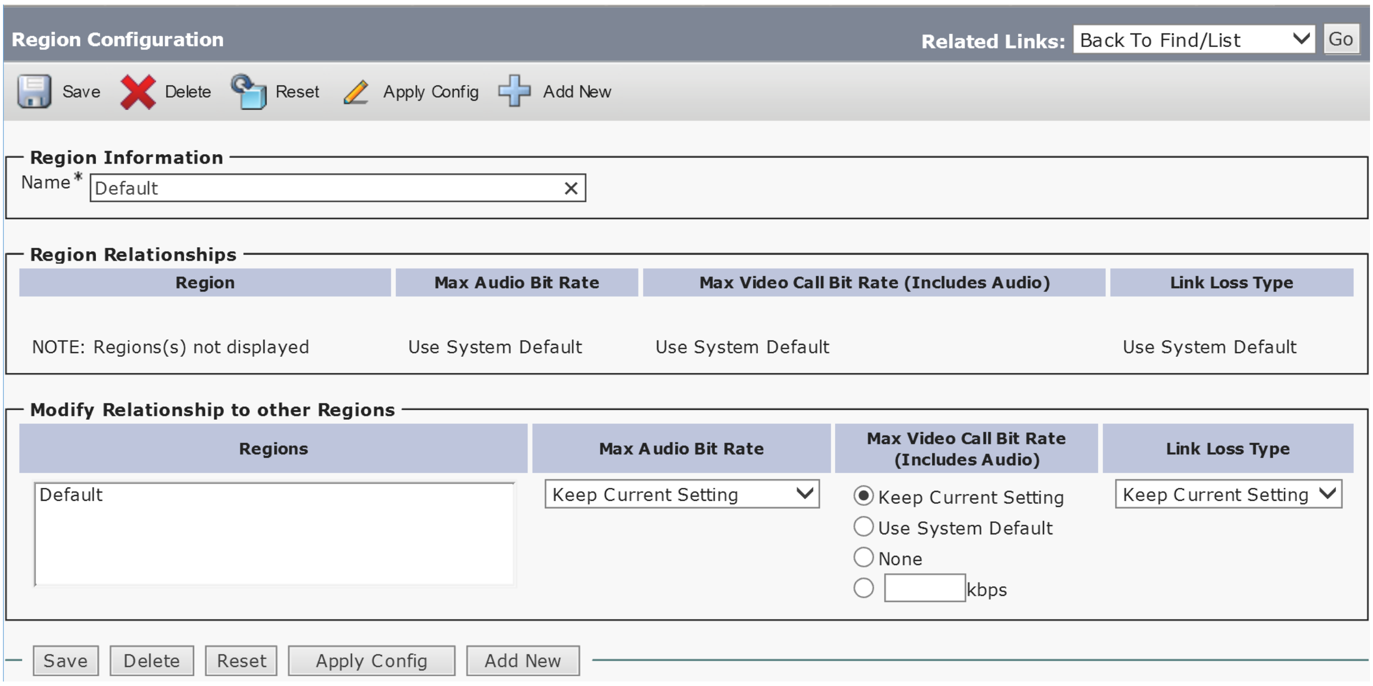
- In the **iLBC Codec Enabled** field, select **Enabled for All Devices Except Recording-Enabled Devices.**
- In the **iSAC Codec Enabled** field, select **Enabled for All Devices Except Recording-Enabled Devices**
- In the **Default Intraregion Max Audio Bit Rate** field, select **64 kbps (G.722, G.711)**




### Disable 256kpbs wideband codec

Latest models of Cisco phones support high quality 256kbps wideband codec for phone-to-phone communications withing the same region. Unfortunately, this codec is not supported by Cisco Built-in-Bridge recording method and it should be disabled. Otherwise, internal calls between users will not be recorded.

Navigate to the **System > Region** menu option in Cisco Unified Communications Manager Administration and change the **Max Audio Bit Rate** per-region resetting to either **Use System Default** or **64 kbps (G.722, G.711)** as shown in the screenshot below:



#### Recording of conference calls

Recording of conference calls on Cisco platform has the following limitations:

- Cisco UCM doesn't support re-negotiation of audio codecs for the calls, which are recorded with the Built-in-Bridge method.
- The Cisco Software Conference Bridge supports only G.711 and 256k wideband codecs.

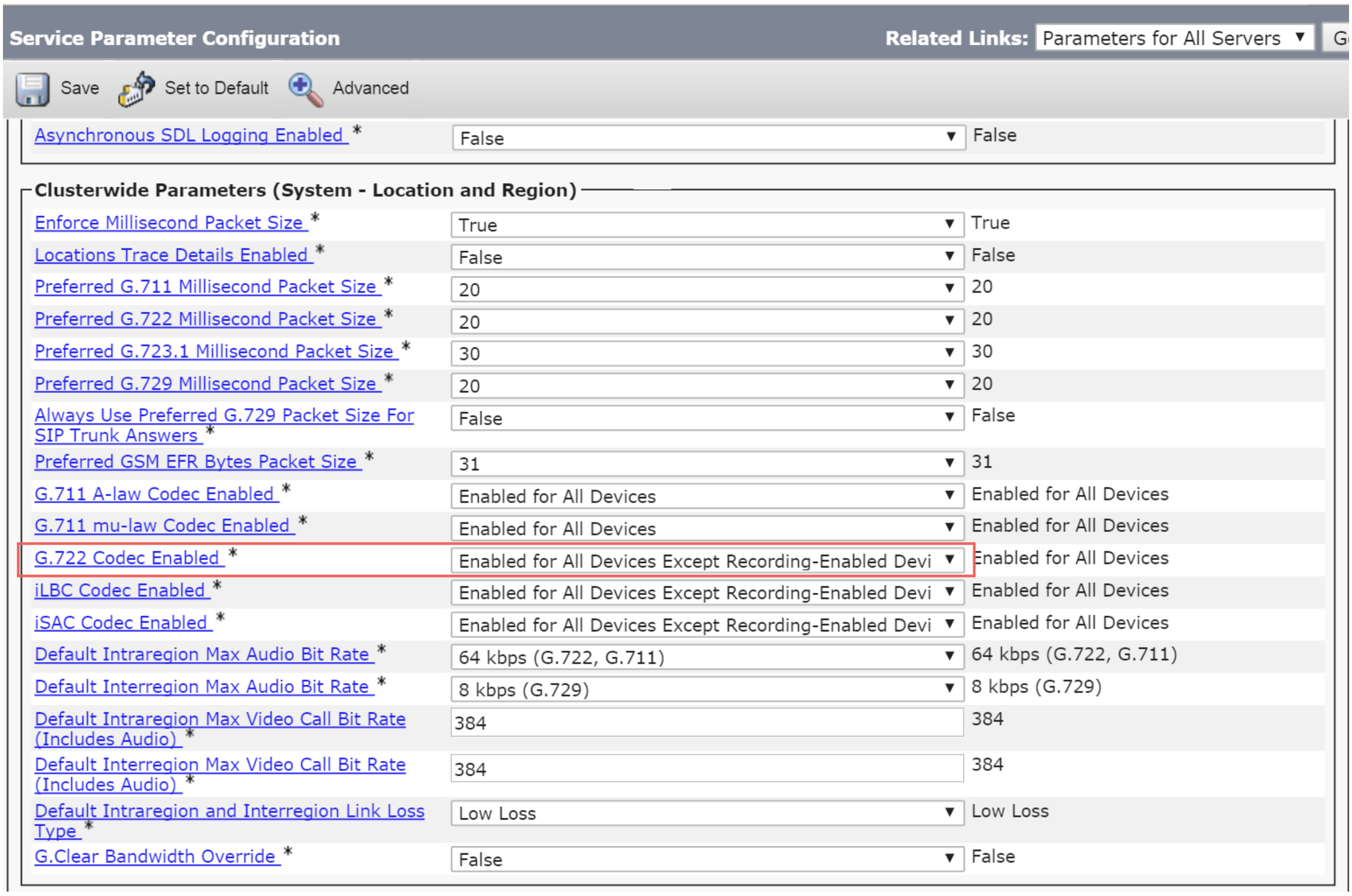
The following call scenario may occur:

- One user makes a call to another user. If these two users use Cisco phones, then G.722 wideband codec is chosen for such call.
- Then one of users tries to create a 3-way conference and adds the third user to the conference.
- CUCM creates a software-based conference to mix audio from three users. The software-based conference doesn't support G.722 codec.
- CUCM needs to re-negotiate the codec with each of users and change it from G.722 to G.711.
- But CUCM cannot do that, because such call is recorded with the BiB method and the codec is fixed for a such call.
- As a result, the user, who tries to create a conference is dropped from a conference.

There are two workarounds in this situation:

1. Disable G.722 codec for users, which are recorded with BiB method.
2. Allocate codec transcoding resources on Cisco platform to automatically convert audio from one codec to another on-flight.

To disable G.722 codec, change the **G.722 Codec Enabled** setting to **Enabled for All Devices Except Recording-Enabled Devices**.



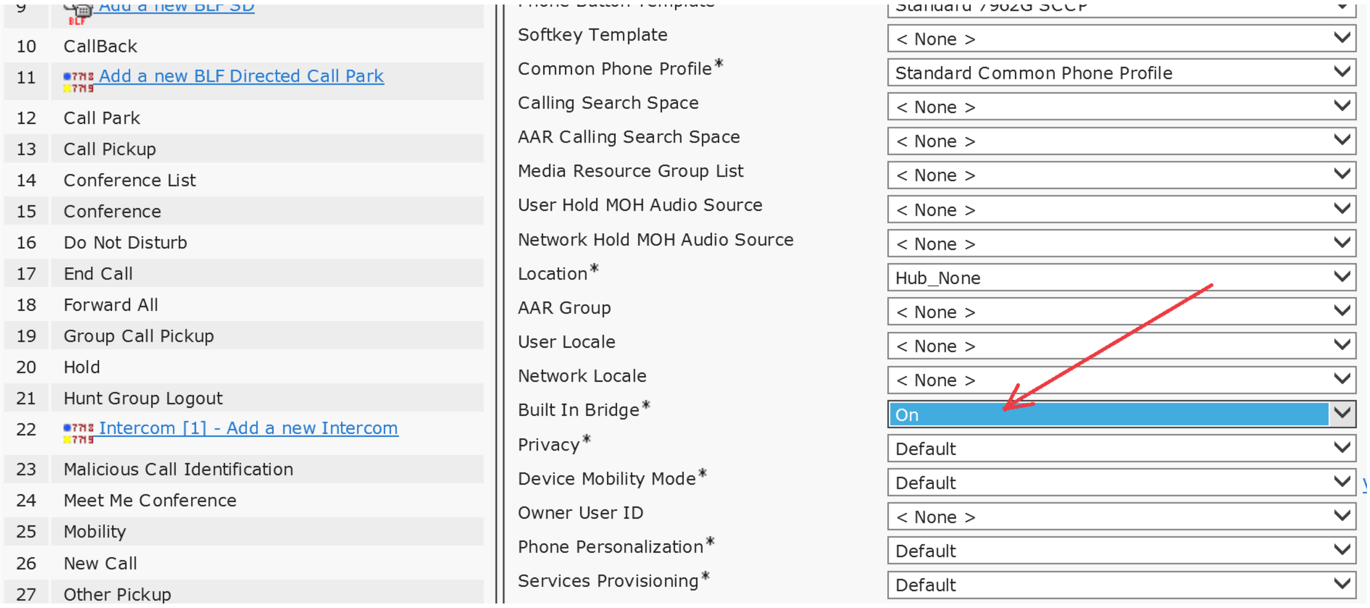
# 5. Configure Phones

## 5.1 Enable Built-in-Bridge on per-phone basis

**Info**

Built-in-Bridge option may be configured clusterwide for all phones.

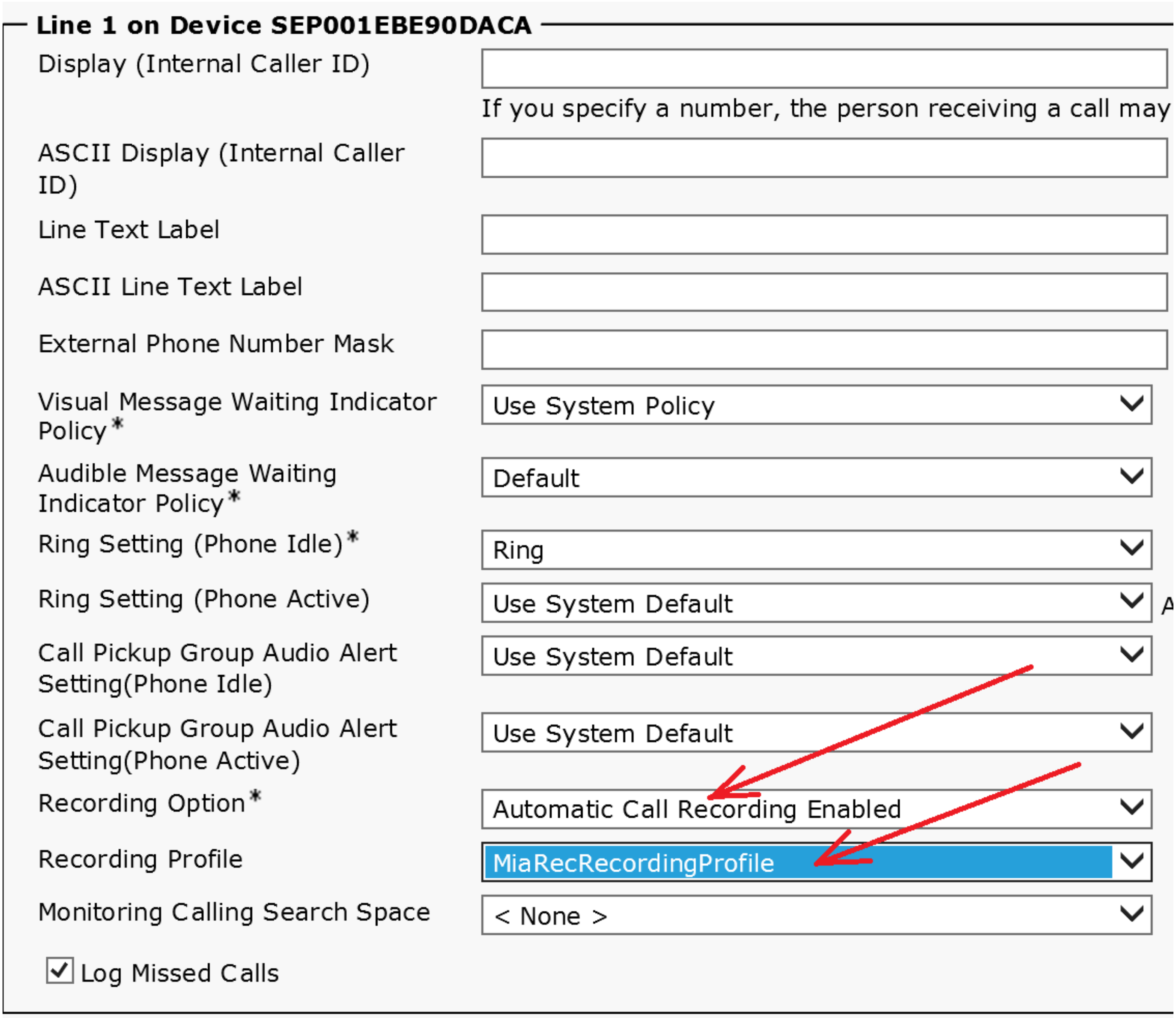
Use the **Device > Phone** menu option in Cisco Unified Communications Manager Administration to enable the **Built-in-Bridge** option.




## 5.2 Enable recording for a line appearance

Use the **Device > Phone** menu option in Cisco Unified Communications Manager Administration to configure the line appearance of a particular phone.

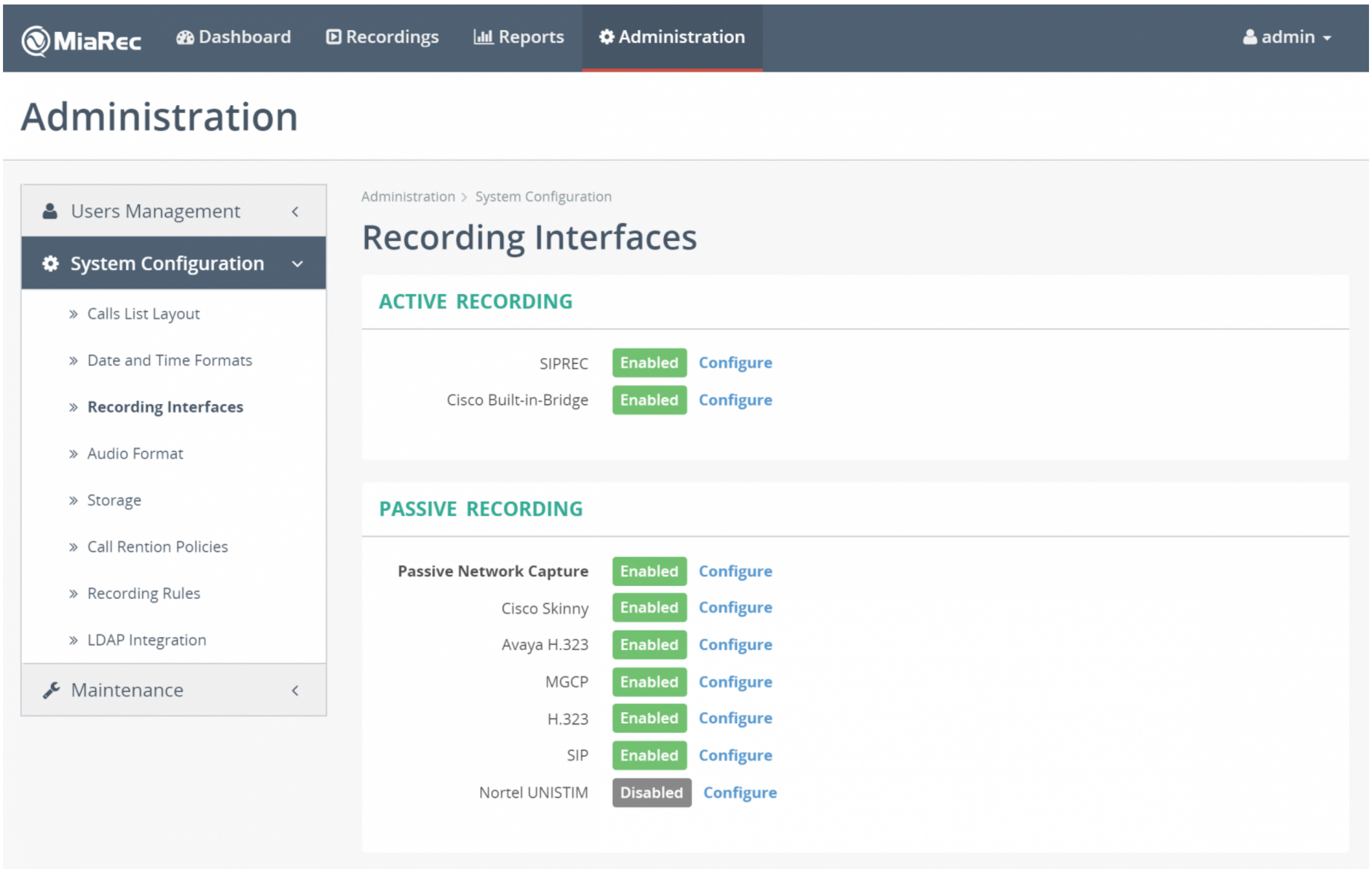
- To enable recording of an agent, in the **Recording Option** field, select one of the following options:
  - **Automatic Call Recording Enabled**
  - **Selective Call Recording Enabled**
- In the **Recording Profile** field, select the previously created recording profile.


Line 1 on Device SEP001EBE90DACA
Display (Internal Caller ID)
If you specify a number, the person receiving a call may
ASCII Display (Internal Caller ID)
Line Text Label
ASCII Line Text Label
External Phone Number Mask
Visual Message Waiting Indicator Policy*
Use System Policy
Audible Message Waiting Indicator Policy*
Default
Ring Setting (Phone Idle)*
Ring
Ring Setting (Phone Active)
Use System Default
Call Pickup Group Audio Alert Setting(Phone Idle)
Use System Default
Call Pickup Group Audio Alert Setting(Phone Active)
Use System Default
Recording Option*
Automatic Call Recording Enabled
Recording Profile
MiaRecRecordingProfile
Monitoring Calling Search Space
< None >
Log Missed Calls

# 6. Configure MiaRec

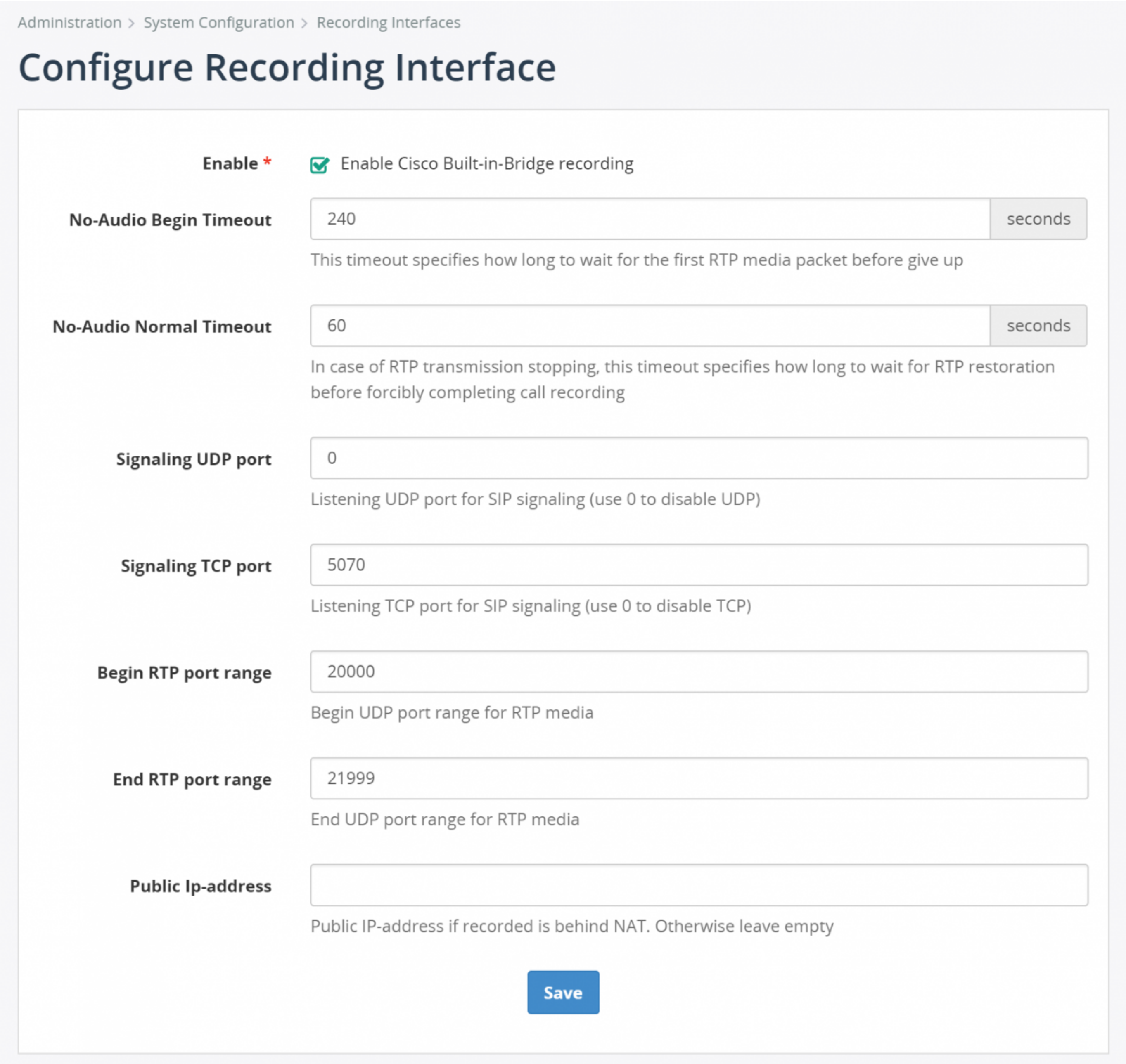
On the MiaRec web portal,navigate to the **Administration -> System Configuration -> Recording Interfaces** menu.

Next to **Cisco Built-in-Bridge** recording interface, click **Configure**.




On the **Configure Recording Interface** page, provide the following setting:

| Option | Description |
|---|---|
| **Signaling UDP port** and **Signaling TCP port** | These port values should be set to the same values as configured in step Create a SIP Trunk that points to the recorder |
| **Begin RTP port range** and **End RTP port range** | RTP port range should be set to the values that do not conflict with other recording interfaces or other networking applications running on the same host as MiaRec application. Make sure that the port range is large enough for anticipated number of concurrently recorded calls. One concurrent call requires two UDP ports to receive media streams from the agent's phone. |
| **Public Ip-address** | Public IP address if MiaRec server is located behind NAT. Make sure that port forwarding is configured properly on your NAT router. If MiaRec server is not behind NAT, then leave this parameter empty. |
| **No-Audio Begin Timeout** | This timeout value specifies how long to wait for the first RTP media packet before giving up. |
| **No-Audio Normal Timeout** | In case of RTP transmission stop, this timeout value specifies how long to wait for RTP restoration before forcibly completing the call recording. |


Administration > System Configuration > Recording Interfaces
Configure Recording Interface
Enable *
Enable Cisco Built-in-Bridge recording
No-Audio Begin Timeout
240
seconds
This timeout specifies how long to wait for the first RTP media packet before give up
No-Audio Normal Timeout
60
seconds
In case of RTP transmission stopping, this timeout specifies how long to wait for RTP restoration before forcibly completing call recording
Signaling UDP port
0
Listening UDP port for SIP signaling (use 0 to disable UDP)
Signaling TCP port
5070
Listening TCP port for SIP signaling (use 0 to disable TCP)
Begin RTP port range
20000
Begin UDP port range for RTP media
End RTP port range
21999
End UDP port range for RTP media
Public Ip-address
Public IP-address if recorded is behind NAT. Otherwise leave empty
Save

# 7. Configure Firewall

If the firewall is running on the MiaRec recording server, then add exclusion rules for the following ports as described here:

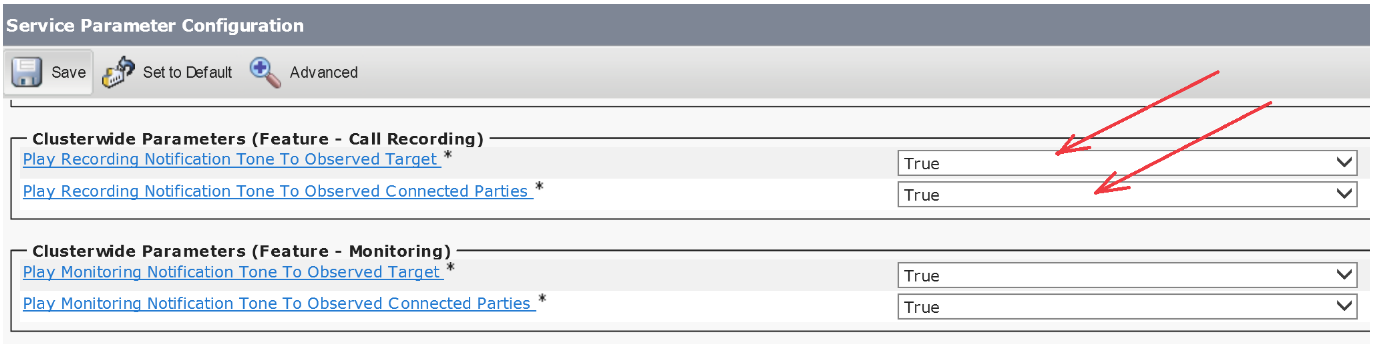
- **Signaling UDP Port** and **Signaling TCP Port**
- **Begin/End RTP port range** (UDP)

# 8. Optional Configuration

## 8.1 Configure notification tones for recording

The recording notification tones can be played either to the agent only, the customer only, or to both.

Use the **System > Service Parameters** menu option in Cisco Unified Communications Manager Administration and navigate to the **Clusterwide Parameters (Feature - Call Recording)** group to peform the nessessary configuration:



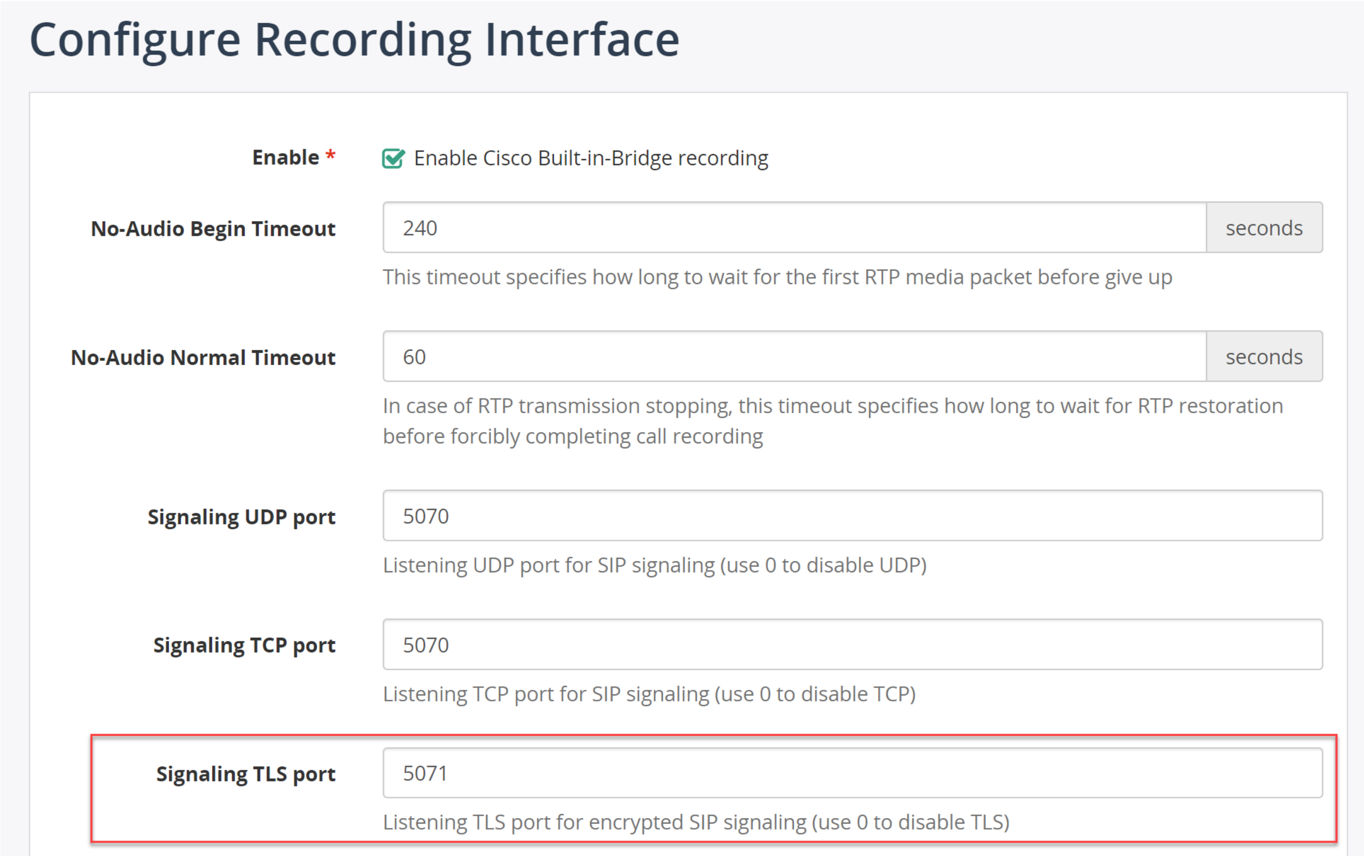

## 8.2 [How To] Configure SIP/TLS for SIP Trunk

This page describes how to configure a SIP/TLS encrypted connection for SIP Trunk towards MiaRec recorder in Cisco UCM.

### 8.2.1 Configure Signaling TLS port in MiaRec

Navigate in MiaRec web portal to **Administration -> Recording Interfaces -> Cisco BiB Configuration**.

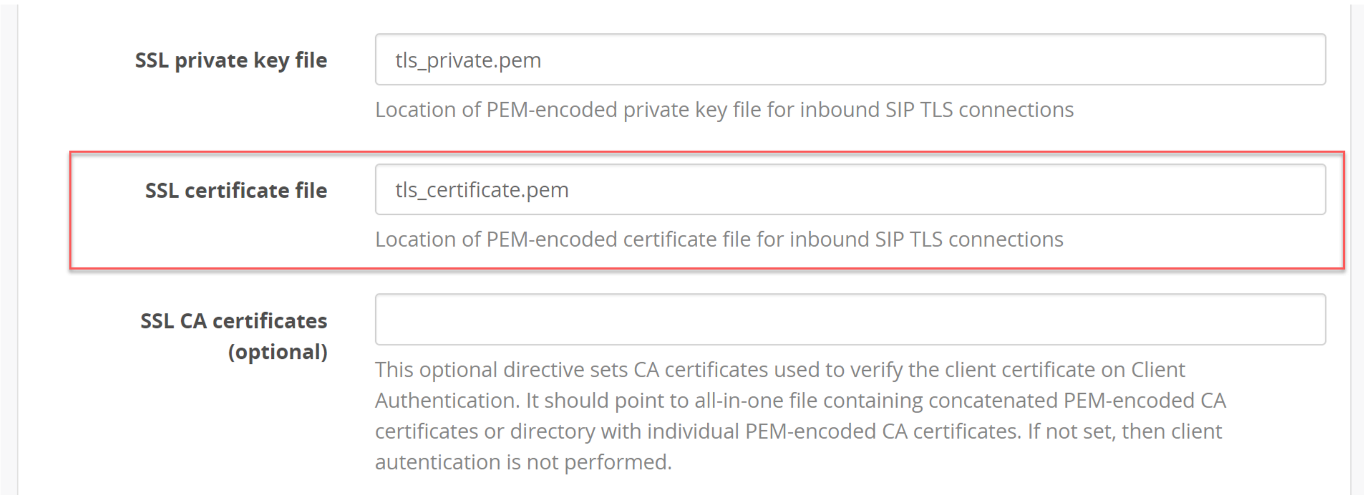
Configure the listening port in parameter **Signaling TLS port**, for example port 5071.




**Info**

If the firewall is enabled on the MiaRec server, make sure it allows an inbound connection to this port.

MiaRec application automatically generates the certificate. The location of the certificate file is configured in the same screen in the **SSL certificate file** parameter. By default, the value is `tls_certificate.pem`.




Locate this file on the MiaRec recording server. We will need to import this file into CUCM.

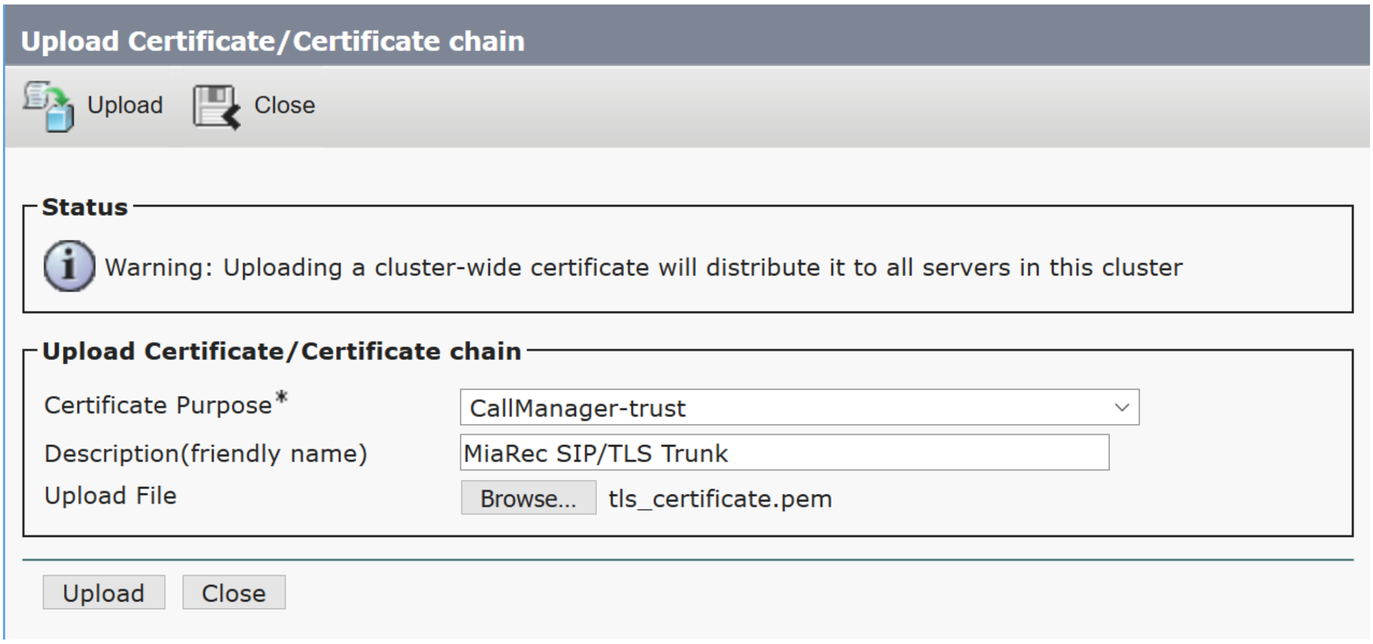
On Windows, the file is located in the same directory as **MiaRec.exe** file (by default, C:\Program Files (x86)\MiaRec Business\Bin).

On Linux, the file is located at `/opt/miarec/shared` or in older versions at `/var/lib/miarec`.

### 8.2.2 Import MiaRec SSL certificate into Cisco UCM

Login to **Cisco Unfied OS Administration** using Cisco UCM admin password. Navigate to **Security > Certificate Management** and click **Upload Certificate/Certificate Chain**.

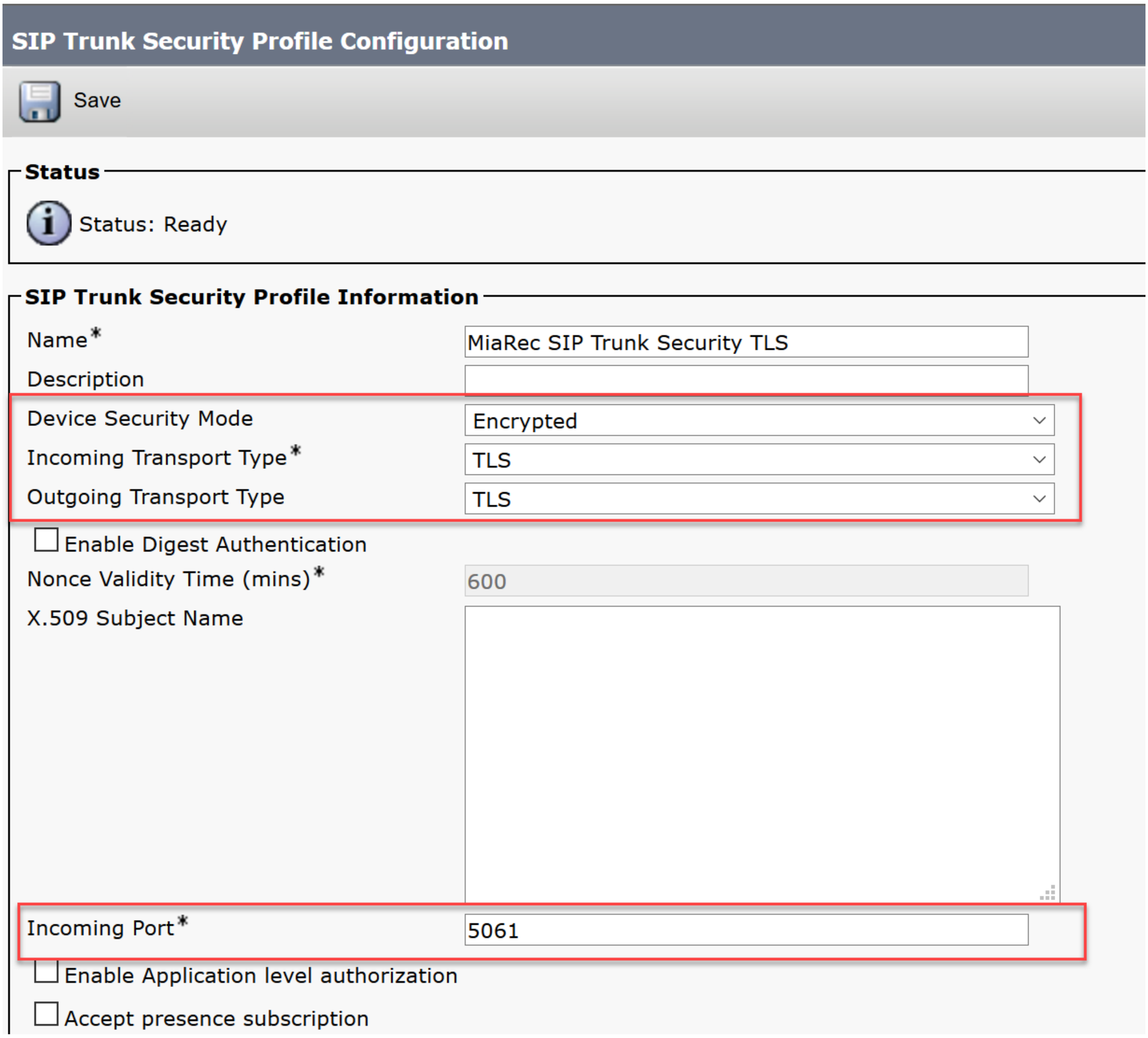
- In the **Certificate Purpose** field, select **CallManager-trust**
- Use the **Browse** button to upload the SSL certificate file from the MiaRec server




### 8.2.3 Configure SIP Trunk Security Profile

Use the **System > Security > SIP Trunk Security Profile** menu option in Cisco Unified Communications Manager Administration to create SIP Trunk Security profile for SIP/TLS connection to the MiaRec recording server.

- In the **Device Security Mode** field, select **Encrypted**.
- In the **Incoming Transport Type** field, select **TLS**.
- In the **Outgoing Transport Type** field, select **TLS** (this setting has to match the configuration of MiaRec).
- Uncheck the **Enable Digest Authentication** option.
- In the **Incoming Port** field, specify a unique port. CUCM will send SIP messages to MiaRec from this port. CUCM requires a unique port for each configured SIP Trunk. If the default port 5061 is busy, then try another port like 5062, 5063, etc.

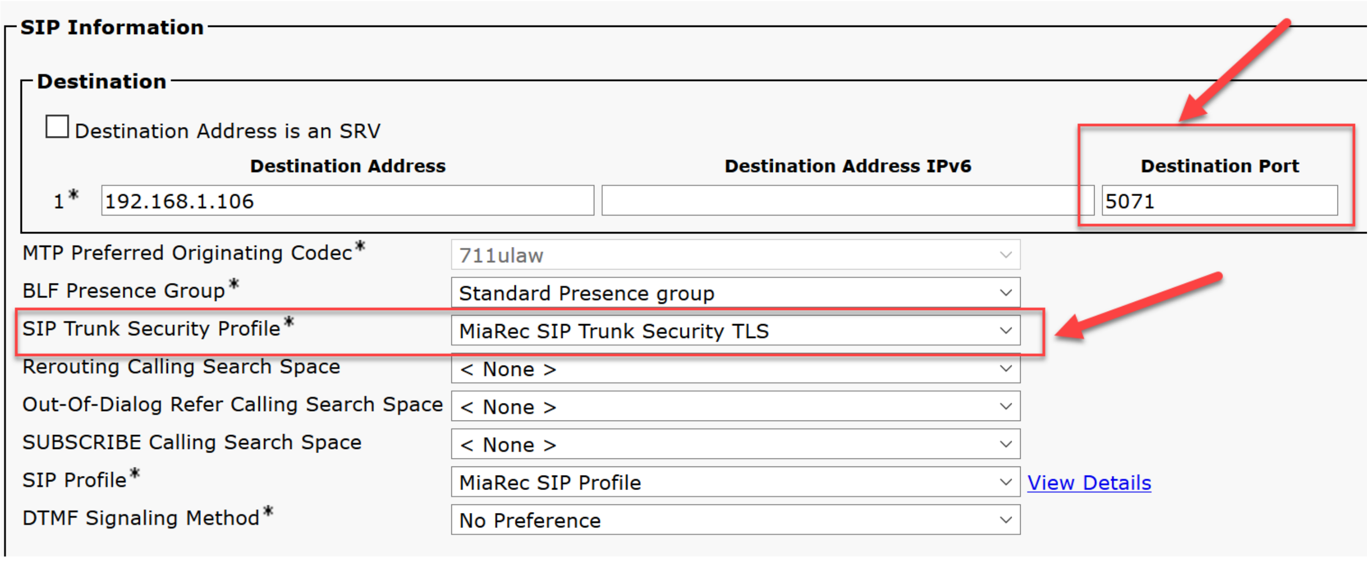



## 8.2.4 Configure SIP Trunk

Use the **Device > Trunk** menu option in Cisco Unified Communications Manager Administration to edit the previously created non-secure SIP trunk that points to the MiaRec recorder.

In the **SIP Information** section, provide the following configuration:

- **Destination Port** should match the port on which the MiaRec recorder is listening for the messages from CUCM (5071 in our example).
- Select the previously created **SIP Trunk Security Profile (TLS)** for the recorderz.




Click the **Reset** button for this trunk to reload CUCM configuration.

### 8.2.5 Troubleshooting

Enable trace logging in MiaRec (menu **Administration > Maintenance > Troubleshooting**) and look for any error messages related to TLS.

A successful establishment of the TLS connection produces the following output in the trace.log file:

```
2018/01/03 09:46:59.028 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(195)   Constructed context: method=SSLv23 ctx=09153A88
2018/01/03 09:46:59.028 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(510)   Constructed channel: ssl=09164AF8 method=SSLv23 context=00747C48
2018/01/03 09:46:59.028 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    General: state=before/accept initialization
2018/01/03 09:46:59.028 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=before/accept initialization
2018/01/03 09:46:59.082 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 read client hello A
2018/01/03 09:46:59.082 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write server hello A
2018/01/03 09:46:59.082 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write certificate A
2018/01/03 09:46:59.088 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write key exchange A
2018/01/03 09:46:59.088 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write server done A
2018/01/03 09:46:59.088 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 flush data
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 read client key exchange A
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 read finished A
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write session ticket A
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write change cipher spec A
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 write finished A
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSLv3 flush data
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    General: state=SSL negotiation finished successfully
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  PSSLChannel.cxx(22)    Accept: state=SSL negotiation finished successfully
2018/01/03 09:46:59.136 09:46:58.835    1        OpalListener:4b64 TransportTLS.cxx(144)   TLS         Started connection to 192.168.1.200:34226
(if=192.168.1.106:5071)
2018/01/03 09:46:59.136 09:46:58.835    4        OpalListener:4b64  ListenerTLS.cxx(49)    TLS Listen  Waiting on socket accept on tls$*:5071
2018/01/03 09:46:59.137 09:46:58.835    3     TransportHandler:467c      Listener.cxx(93)    Listen          Started handler thread on
tls$192.168.1.200:34226<if-read=tls$192.168.1.106:5071, if-write=tls$192.168.1.106:5071> 0x09160FC0
2018/01/03 09:46:59.137 09:46:58.835    3     TransportHandler:467c CiscoBiBManager.cpp(185)    CiscoBiB Listener thread started on
tls$192.168.1.200:34226<if-read=tls$192.168.1.106:5071, if-write=tls$192.168.1.106:5071> 0x09160FC0
2018/01/03 09:46:59.137 09:46:58.835    3     TransportHandler:467c       SipPdu.cpp(156)   SIP         PDU Created: <<Uninitialised>> CSeq=
2018/01/03 09:46:59.161 09:46:58.835    5     TransportHandler:467c       SipPdu.cpp(671)   SIP         PDU Parsed 399 bytes on tls$192.168.1.200:34226<if-
read=tls$192.168.1.106:5071, if-write=tls$192.168.1.106:5071> 0x09160FC0
2018/01/03 09:46:59.161 09:46:58.835    4     TransportHandler:467c       SipPdu.cpp(734)   SIP         PDU Received 399 bytes on tls$192.168.1.200:34226<if-
read=tls$192.168.1.106:5071, if-write=tls$192.168.1.106:5071> 0x09160FC0
OPTIONS sip:192.168.1.106:5071 SIP/2.0
Content-Length: 0
Contact: <sip:192.168.1.200:5061;transport=tls>
User-Agent: Cisco-CUCM11.5
Call-ID: 17095a80-a4d11712-19475-c801a8c0@192.168.1.200
CSeq: 101 OPTIONS
Date: Wed, 03 Jan 2018 17:46:58 GMT
Via: SIP/2.0/TLS 192.168.1.200:5061;branch=z9hG4bK1959e66d3ef22
From: <sip:192.168.1.200>;tag=275457321
Max-Forwards: 0
To: <sip:192.168.1.106>
```

Contact a MiaRec representative if you face any issues.\