Ribbon SBC Edge SWe Lite R9.0 Interop with NICE Engage : Interoperability Guide

Table of Contents

Interoperable Vendors

Copyright

Document Overview

This document outlines the best practices for configuring Ribbon SBC SWe Lite for SIPREC feature verification.

About Ribbon SBC SWe Lite

The Ribbon Session Border Controller Software Edition Lite (SBC SWe Lite) provides best-in-class communications security. Microservices design to optimize resource allocation, dynamic scaling, automated lifecycle management are all attributes of the SBC SWe Lite, delivering edge SBC capabilities, such as robust network security, overload controls, SIP normalization, SIP Recording, IPv4-IPv6 interworking, and audio transcoding.

About NICE Engage platform

The NICE Engage Platform provides comprehensive omnichannel interaction recording. Omnichannel recording helps organizations provide customers a coherent experience by providing a single place to define and implement compliance and quality practices across all channels.

About SIP Recording

SIP Recording (SIPREC) is a recording capability that helps users to comply with regulations, to monitor the quality of service of representatives, to store call information for quality analysis, and so on. The Ribbon SBC SWe Lite supports SIPREC towards multiple recorders based on the Internet Engineering Task Force (IETF) standard.

The Ribbon SBC SWe Lite SIPREC supports the RFC standard for a SIP recording interface. To support SIPREC, the SBC SWe Lite acts as a Session Recording Client (SRC) initiating a Recording Session (RS) towards a Session Recording Server (SRS). The SBC SWe Lite initiates a recording session for all the Communication Sessions (CS) to record over SIP towards the SRS. The CS output is based on the SBC SWe Lite's Web UI configuration for enabling recording.

SIP Recording is supported on the SBC SWe Lite for the following purposes:

- Storing call information for quality analysis.
- Recording call and media sessions on a third-party recording server.
- Checking the call detail records and determining if a call is recording or not.
- Providing call detail records for recorded calls.

Table 1 : Terminology

Term	Definition
CS	Communication Session
RS	Recording Session
SRC	Session Recording Client
SRS	Session Recording Server

Scope

This document provides configuration best practices for deploying Ribbon's SBC SWe Lite for SIPREC interop. Note that these are configuration best practices, and each customer may have unique needs and networks. Ribbon recommends that customers work with network design and deployment engineers to establish the network design that best meets their requirements.

Non-Goals

It is not the goal of this guide to provide detailed configurations that meets the requirements of every customer. Use this guide as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers to configure both the Ribbon SBC and the third-party product. Navigating the third-party product as well as the Ribbon SBC SWe Lite GUI is required. Understanding the basic concepts of TLS/TCP/UDP, IP/Routing, and SIP /SRTP is also necessary to complete the configuration and for any required troubleshooting.

Prerequisites

Before proceeding with the interop, make sure you have the following:

- Ribbon SBC SWe Lite
- SBC SWe Lite License
    - This interop requires the acquisition and application of SIP sessions. Refer to Working with Licenses for more information.
- NICE Engage Platform
    - NICE Engage platform SIPREC server running on 4.1 version or above.
    - Licenses for the required number of recording sessions.
    - NICE Dispatch Integration Services running on the SIPREC server.

Product and Device Details

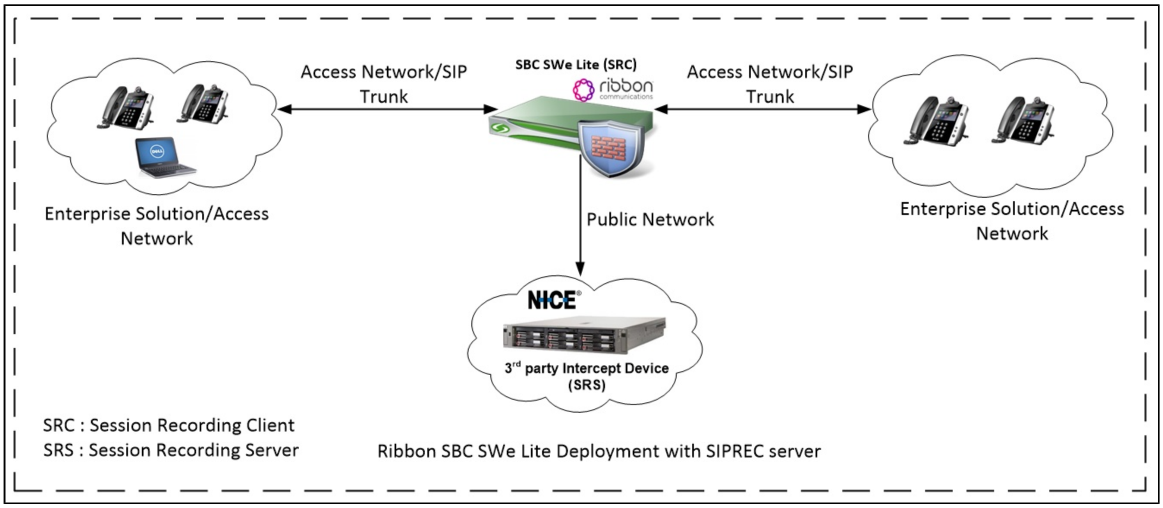
The configuration uses the following equipment and software:

Table 2 : Requirements

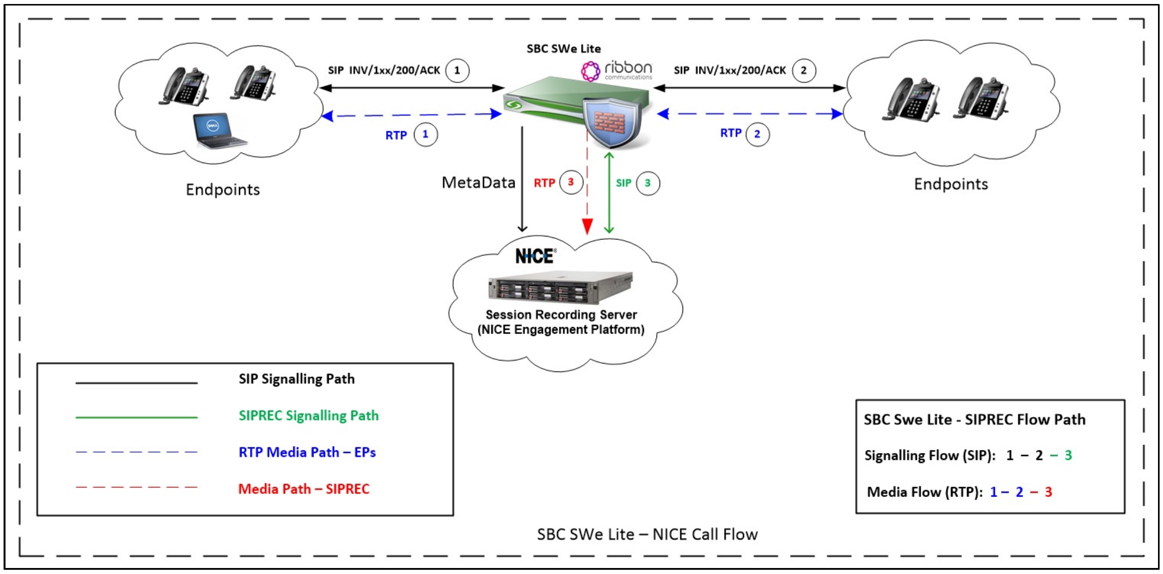
Product	Equipment	Software Version
Ribbon Networks	Ribbon SBC SWe Lite	9.0.1
Third-party Equipment	NICE Engage platform	4.1
Administration and Debugging Tools	Wireshark LX Tool	3.2.7 2.1.0.6

Network Topology and E2E Flow Diagrams

SBC SWe Lite - NICE Engage Deployment Topology



Interoperability Test Lab Topology and Call Flow Diagram



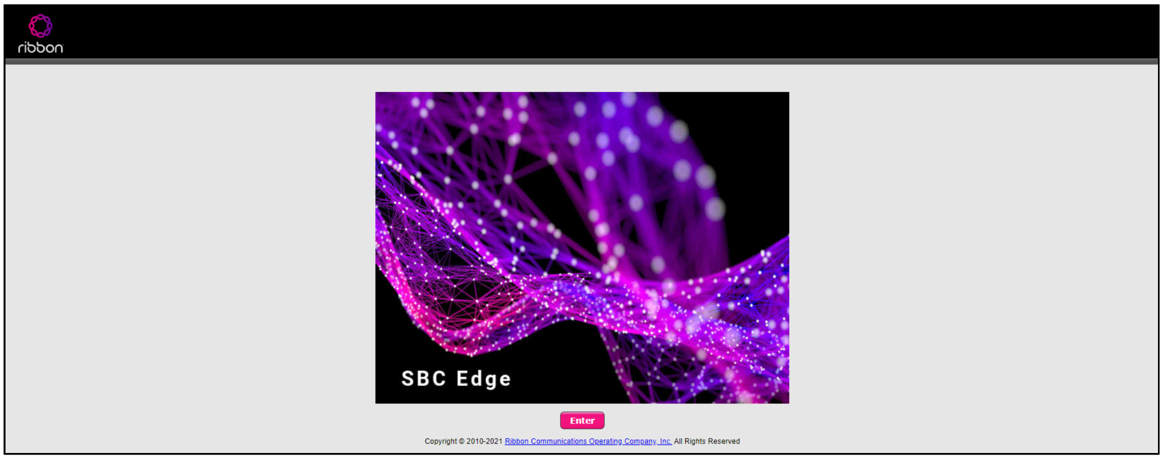
Installing the SBC SWe Lite

To install and run the SBC SWe Lite on the VMware ESXi, refer to Installing SBC SWe Lite on VMware ESXi.

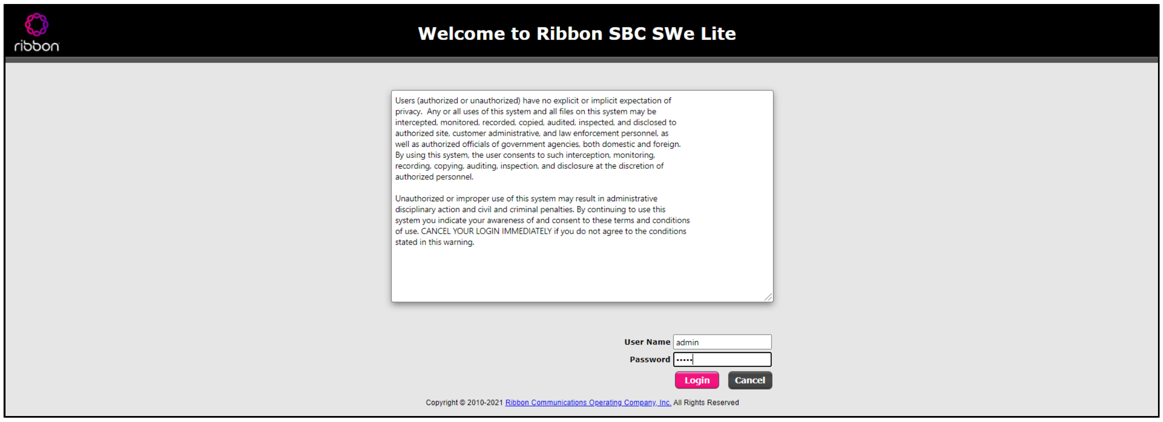
SBC SWe Lite Configuration

Accessing the SBC SWe Lite

Open any browser and enter the SBC SWe Lite IP address.

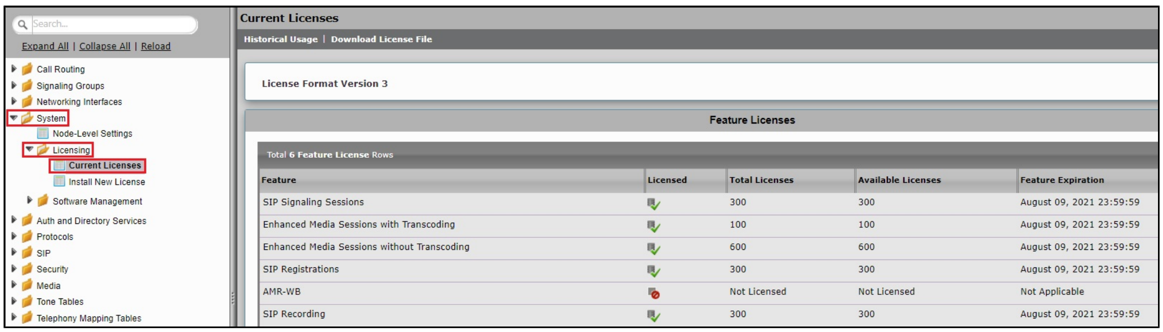


Click **Enter** and log in with a valid User ID and Password.



License and TLS Certificates

View License



For more details on Licenses, refer to Working with Licenses.

Import Trusted Root CA Certificates

A trusted certificate authority issues a Trusted CA Certificate. Trusted CA Certificates are imported to the SBC SWe Lite to establish its authenticity on the network.

From the **Settings** tab, navigate to **Security > SBC Certificates > Trusted CA Certificates.**

The following procedure shows you how to import Trusted Root CA Certificates, using either the File Upload or Copy and Paste method.

1. To import a Trusted CA Certificate, click the Import Trusted CA Certificate ( ) Icon.
2. Select either Copy and Paste or File Upload from the **Mode** menu.

3. If you choose **File Upload**, use the **Select File** button to find the file.
4. Click **OK**.

> **Note**
> Follow the above steps to import the SIPREC App Server certificates.

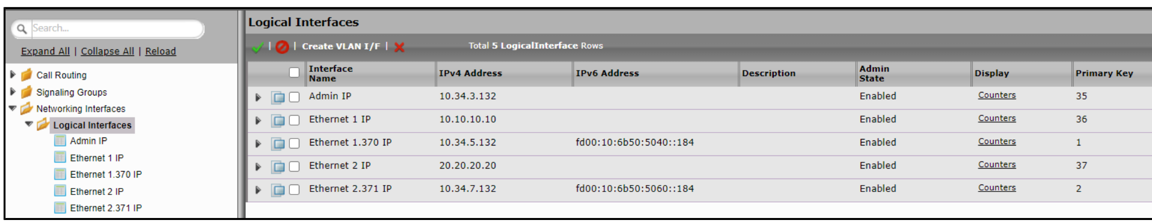
View Networking Interfaces

This section describes how to manage the way Ribbon SBC SWe Lite interfaces with the network. The SBC SWe Lite supports five system-created logical interfaces known as **Administrative IP**, **Ethernet 1 IP**, **Ethernet 2 IP**, **Ethernet 3 IP**, and **Ethernet 4 IP**. In addition to the system-created logical interfaces, the SBC SWe Lite supports user-created VLAN logical sub-interfaces.

From the **Settings** tab, navigate to **Networking Interfaces > Logical Interfaces.**

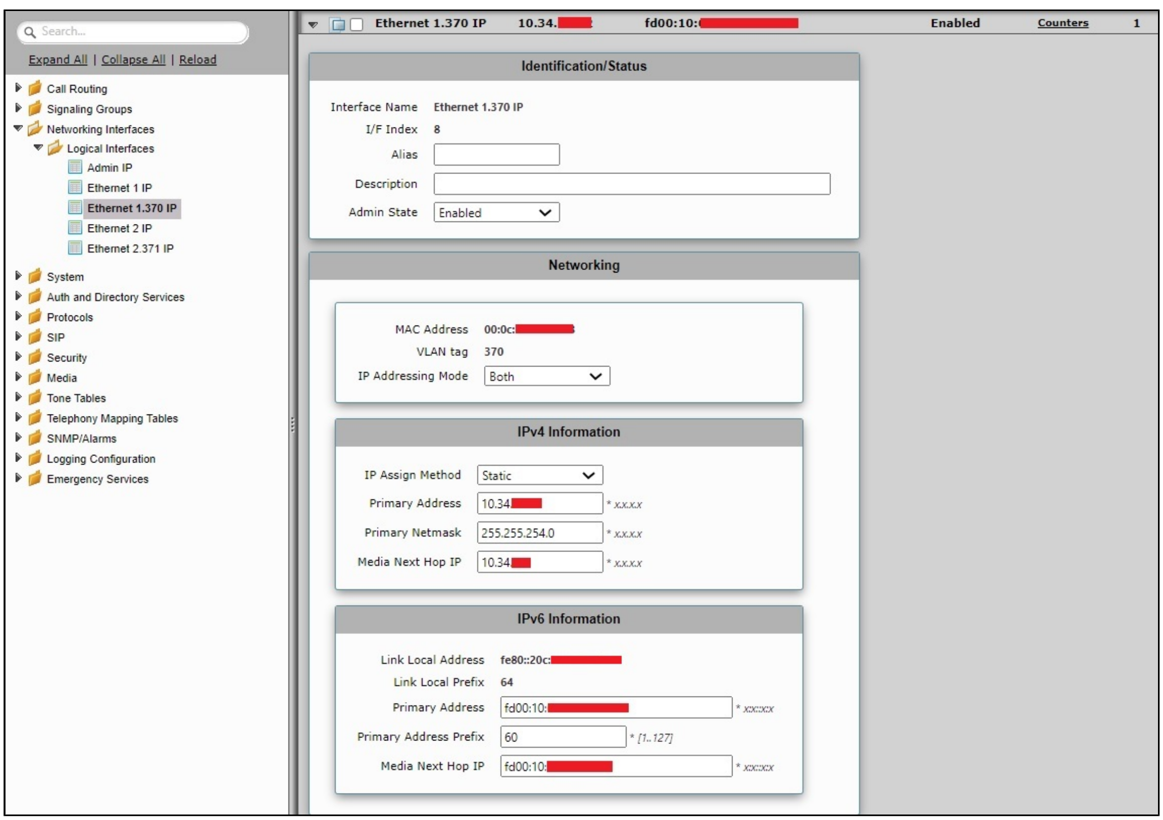
Administrative IP

The SBC SWe Lite system supports a logical interface called the Admin IP (Administrative IP, also known as the Management IP). A Static IP or DHCP is used for running the initial setup of the SBC SWe Lite system.

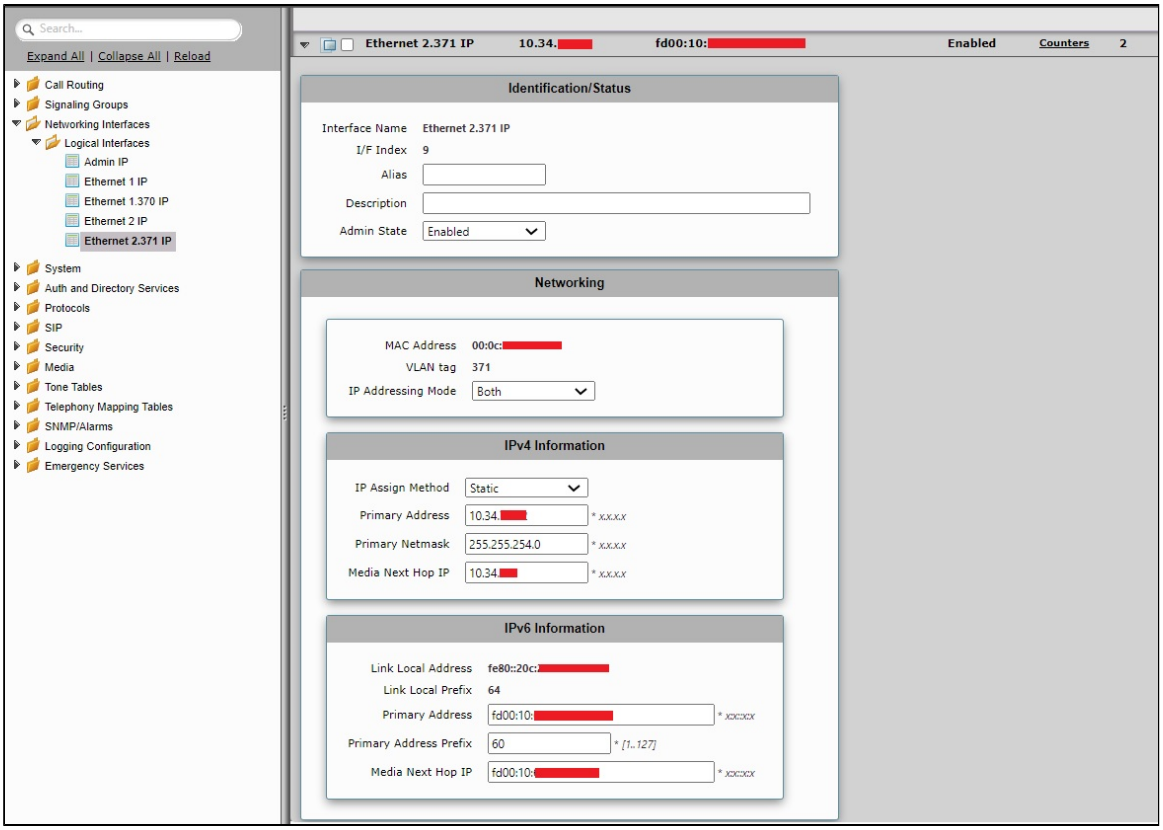


s

Ethernet 1 IP



Ethernet 2 IP



Configure Static Routes

Static routes communicate with remote networks. In a production environment, static routes are mainly configured for routing from a specific network to another network and accessed through one point or one interface (that is, single path access or default route).

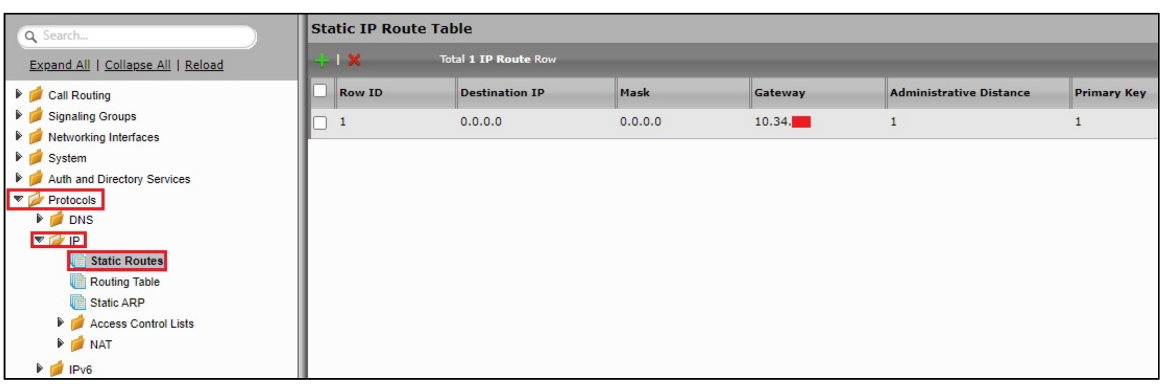
- Configure static routes for smaller networks with just one or two routes, so that a link is not wasted for exchanging dynamic routing information.
- You do not require static routes for networks that have a LAN-side gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with voice VLAN towards the SBC Edge,

Destination IP
Specifies the destination IP address.

Mask
Specifies the network mask of the destination host or subnet. If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called the 'default static route'.

Gateway
Specifies the IP address of the next-hop router to use for this static route.

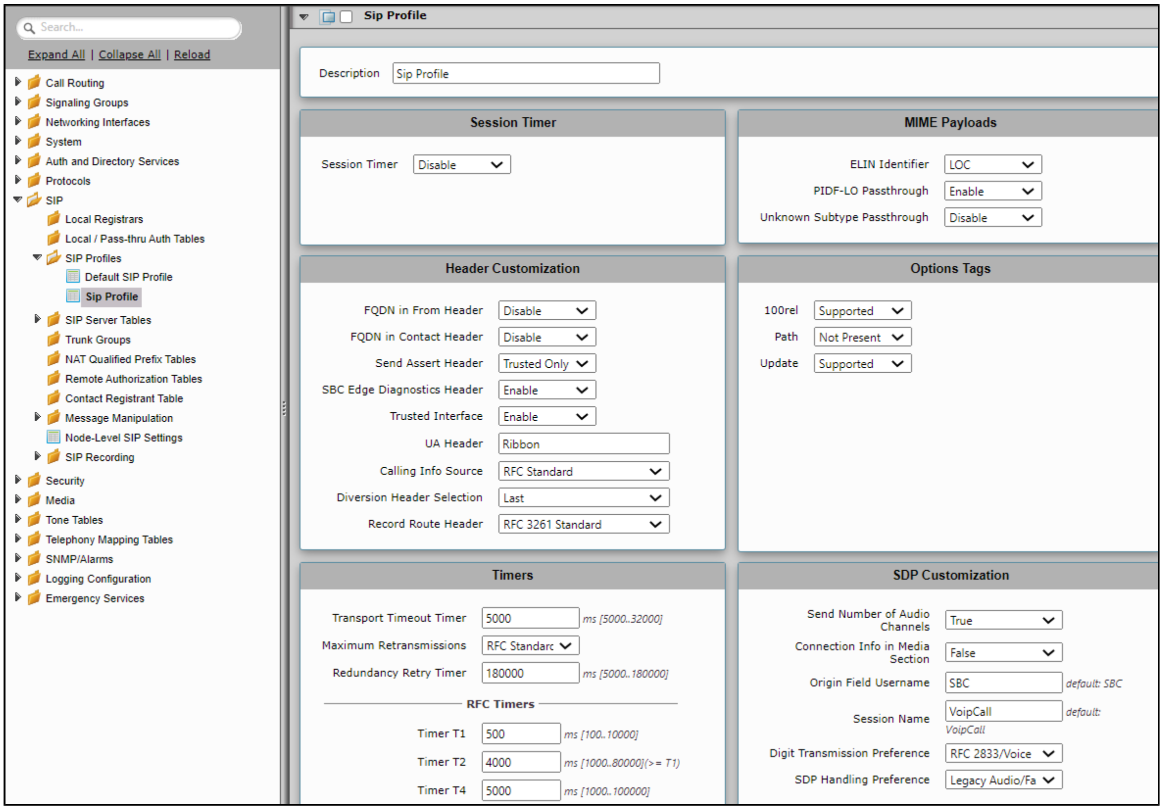
Metric
Specifies the cost of this route, hence indirectly specifying the preference of the route. Lower values indicate more preferred routes. The typical value is 1 for most static routes, indicating that static routes are preferred over dynamic routes.



Configure SIP Profile

SIP Profiles control how the SBC Edge communicates with SIP devices. They control important characteristics, such as session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

From the **Settings** tab, navigate to**SIP > SIP Profiles**.



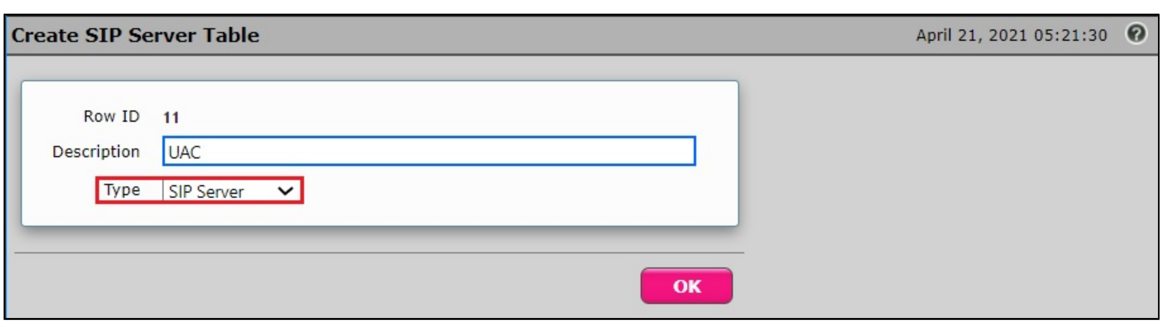
SIP Server Tables

SIP Server

SIP Server Tables contain information about the SIP devices connected to the SBC Edge. The entries in the tables provide information about the IP Addresses, ports, and protocols used for communicating with each server.

From the **Settings** tab, navigate to **SIP > SIP Server Tables**.

1. Click the **Create** ( ) icon.
2. In the **Description** field, enter a descriptive name for the SIP Server Table.
3. From the **Type** drop-down box, select **SIP Server.**
4. Click **OK**.



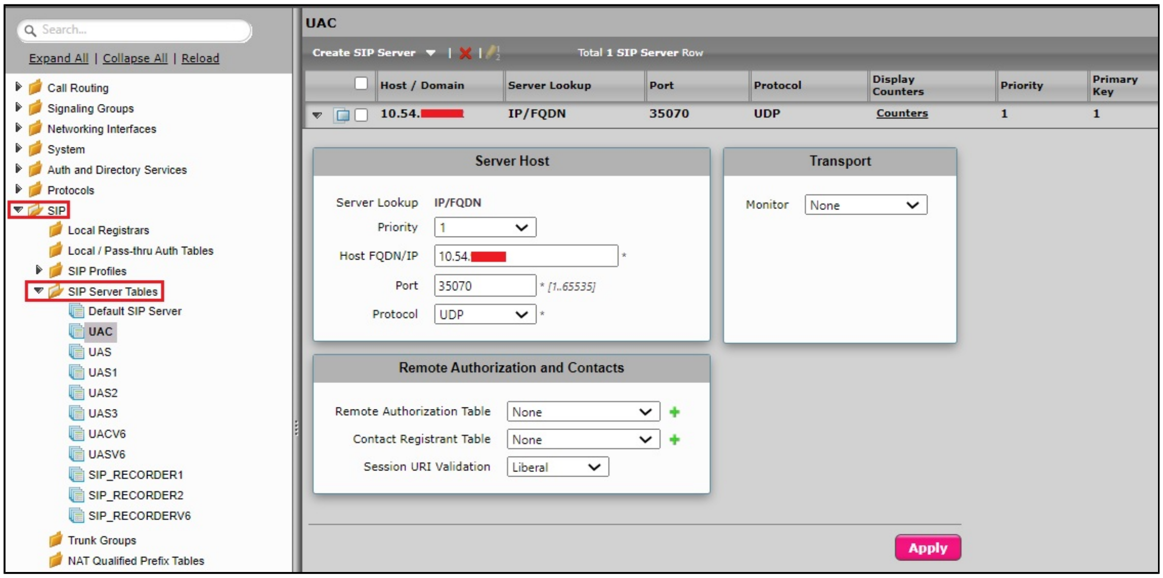
SIP Server Table Entry

From the **Settings** tab, navigate to **SIP > SIP Server Tables**.

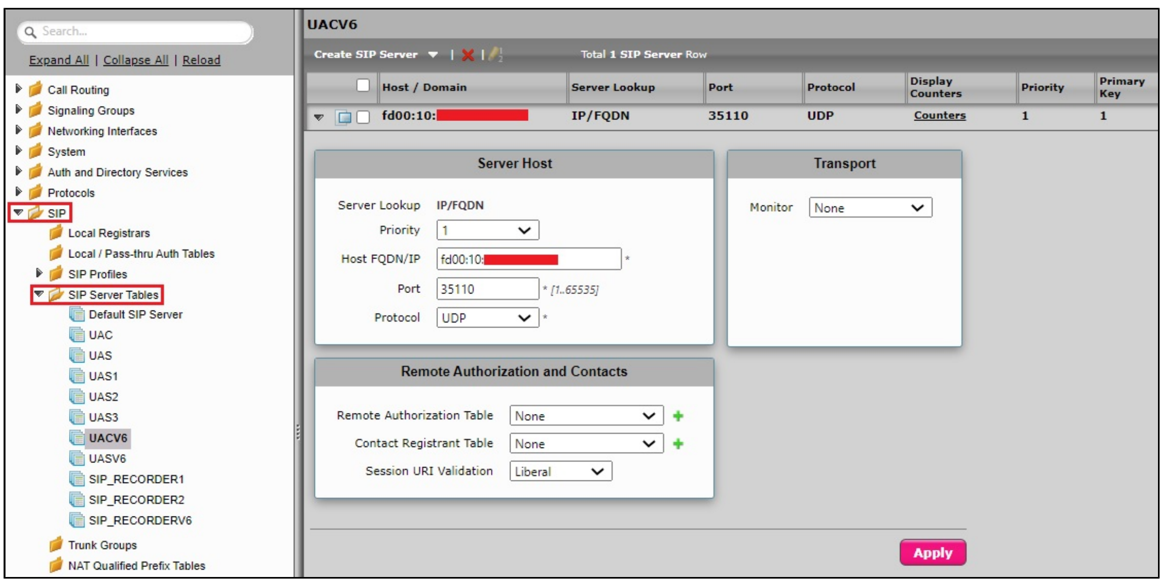
1. Click on the desired SIP Server Table.

2. From the **Create SIP Server** drop-down list, select **IP/FQDN**.

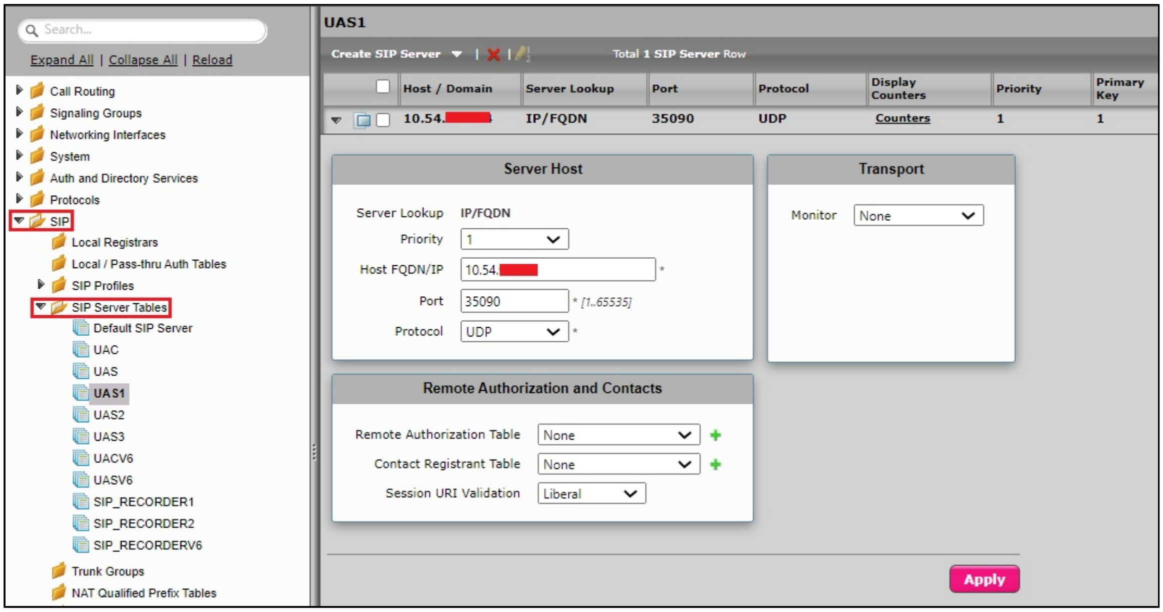
UAC - IPv4



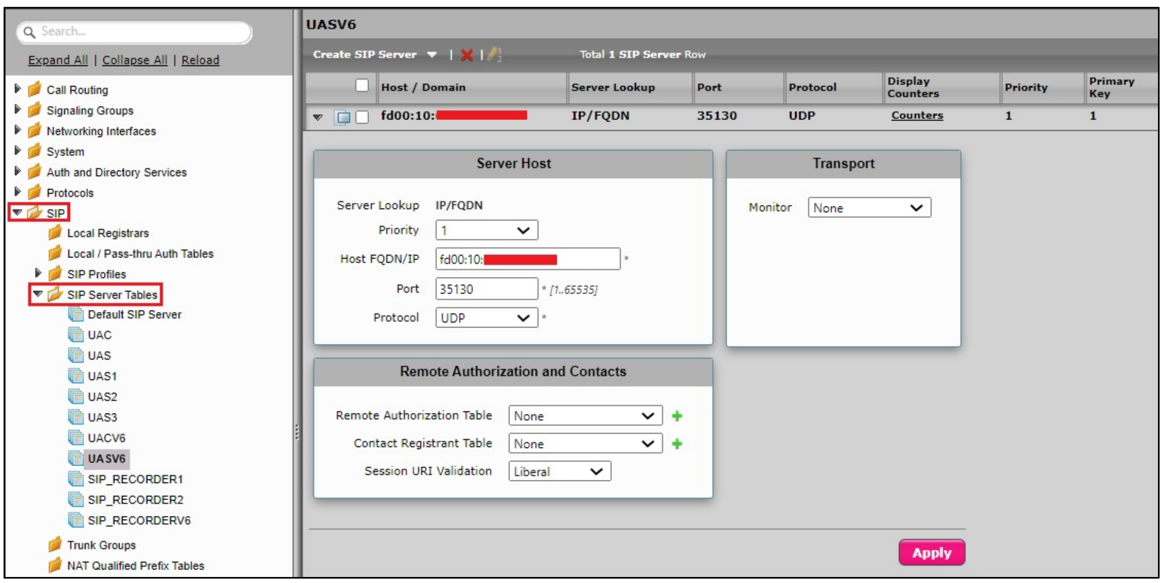
UAC - IPv6



UAS - IPv4



UAS - IPv6



> **Note**
> The number of Sip Server Table Entries depends on the requirements.

SIPREC configuration on Ribbon SBC SWe Lite

SIP Server Table for SIPREC

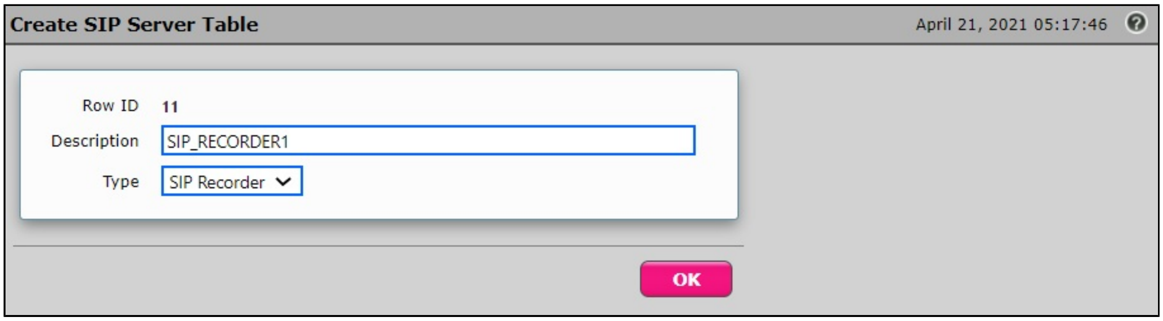
SIP Recorder

A SIP Recorder Table contains information about the Network interface through which the SRC initiates recording requests toward the SRS. To support the SIPREC, the SBC Edge acts as a Session Recording Client (SRC), initiating a Recording Session (RS) toward a Session Recording Server (SRS). The SBC Edge initiates a recording session for all the Communication Sessions (CS). The CS output is based on the SBC Edge's Web UI configuration for enabling recording. The SIP Server (SIP Recorder) supports either an FQDN or IP Address (V4 or V6). Each SIPREC Server entry enables configuring multiple servers. When the standby SRS is configured, the SBC Edge sends the recording first to the active SRS. If the request fails (due to server reachability fault), the SBC SWe Lite sends the recording session to the standby SRS.

From the **Settings** tab, navigate to **SIP > SIP Server Tables**.

1. Click the **Create** (+) icon.

2. In the **Description** field, enter a descriptive name for the SIP Server Table.
3. From the **Type** drop-down box, select **SIP Recorder.**
4. Click **OK**.

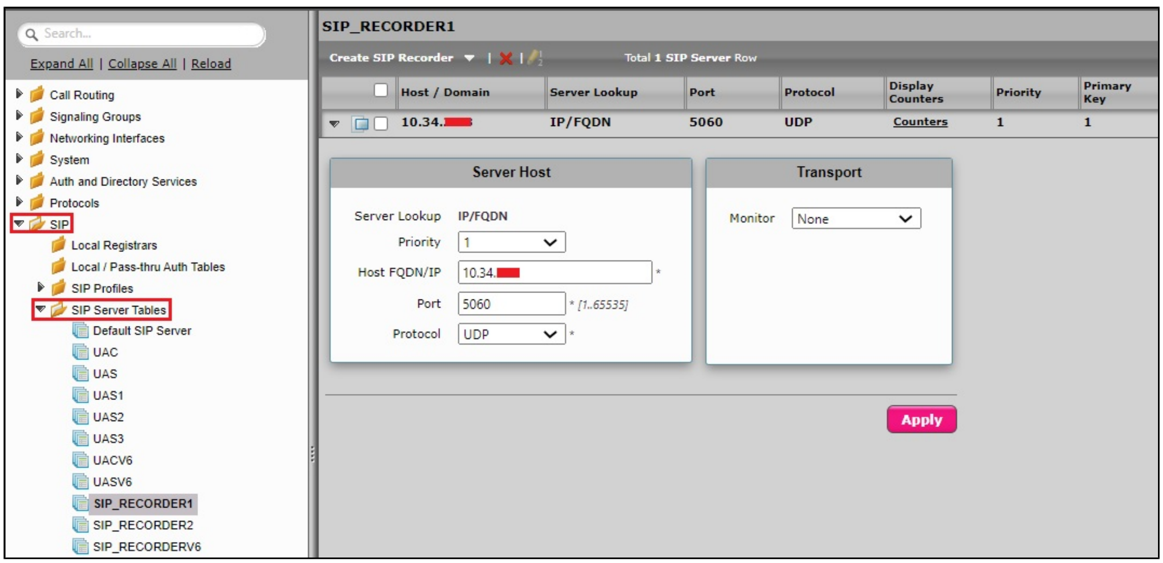


SIP Server Table entry for SIPREC

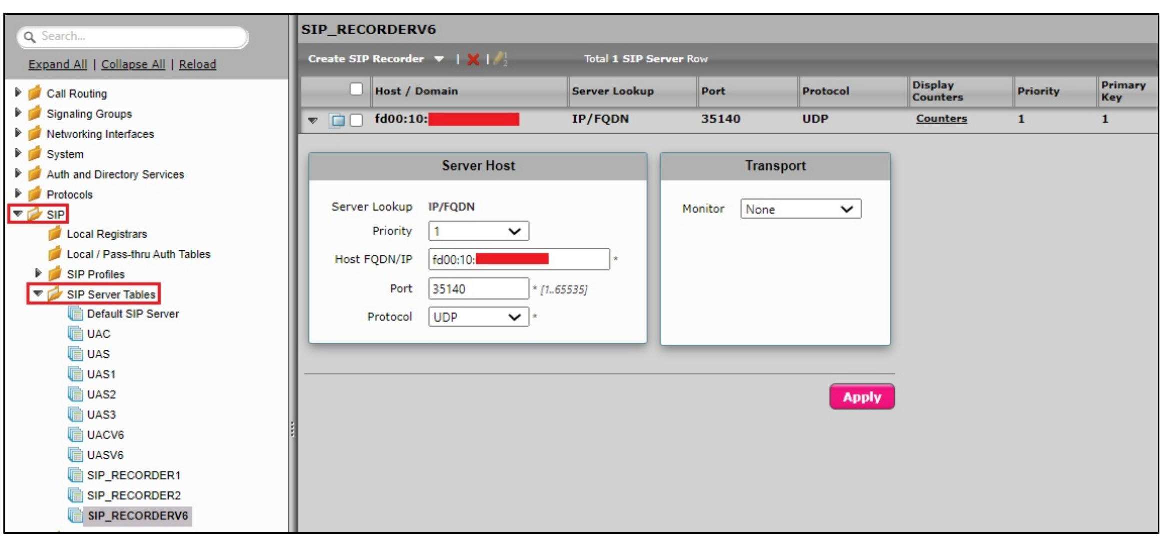
From the **Settings** tab, navigate to **SIP > SIP Server Tables**

1. Click on the desired SIP Server Table.
2. From the **Create SIP Server** drop-down list, select **IP/FQDN**.

SIPREC - IPv4



SIPREC - IPv6

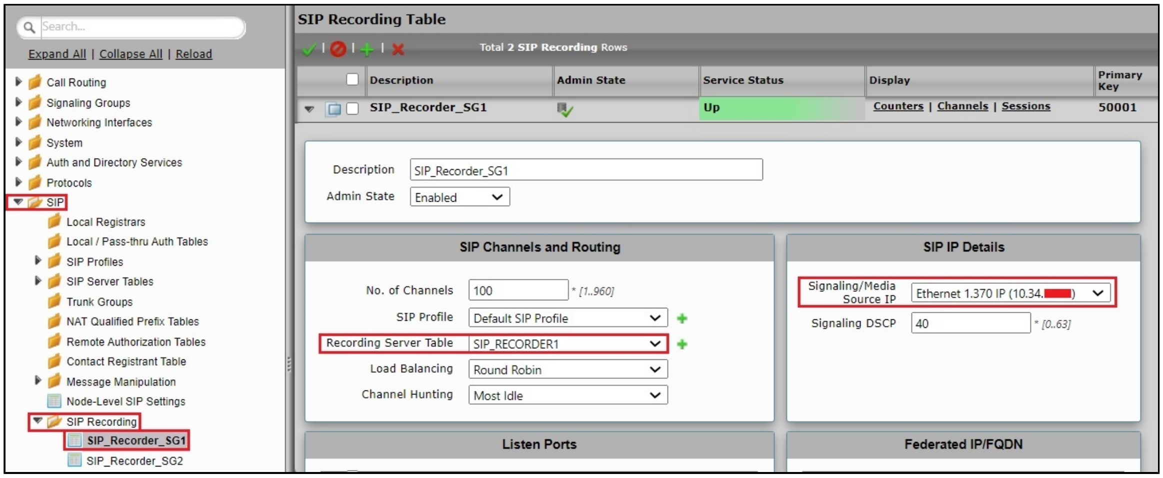


SIP Recording Table entry

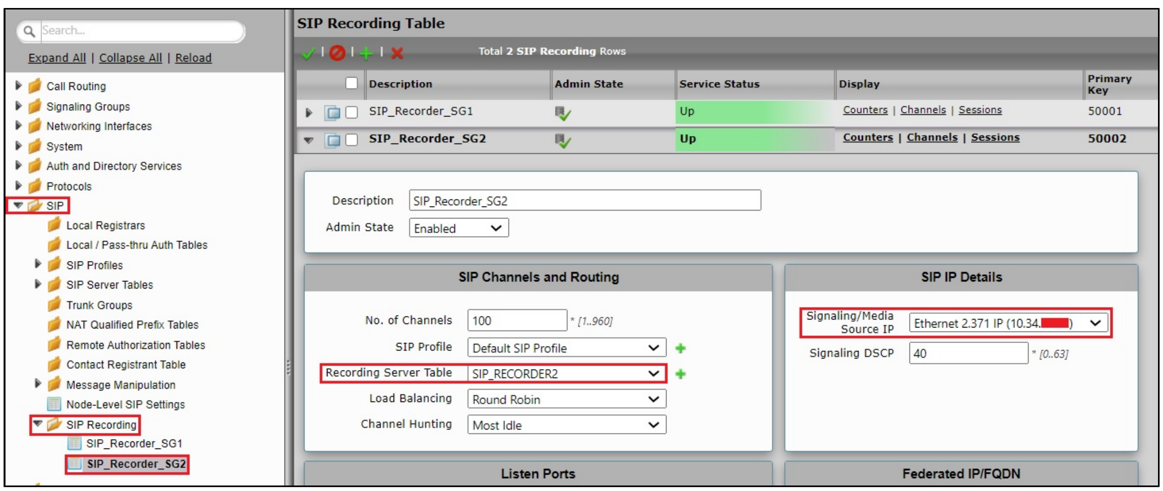
A SIP Recorder Table contains information about how a Signaling Group starts a SIP Recording (SIPREC) session. Through the configuration options, you select the Recording Server (SIP Server), SIP channels, routing, and media, which directs the SBC to communicate with the Session Recording Server (SRS).

From the **Settings** tab, navigate to **SIP > SIP Recording**.

SIP Recording Table 1



SIP Recording Table 2



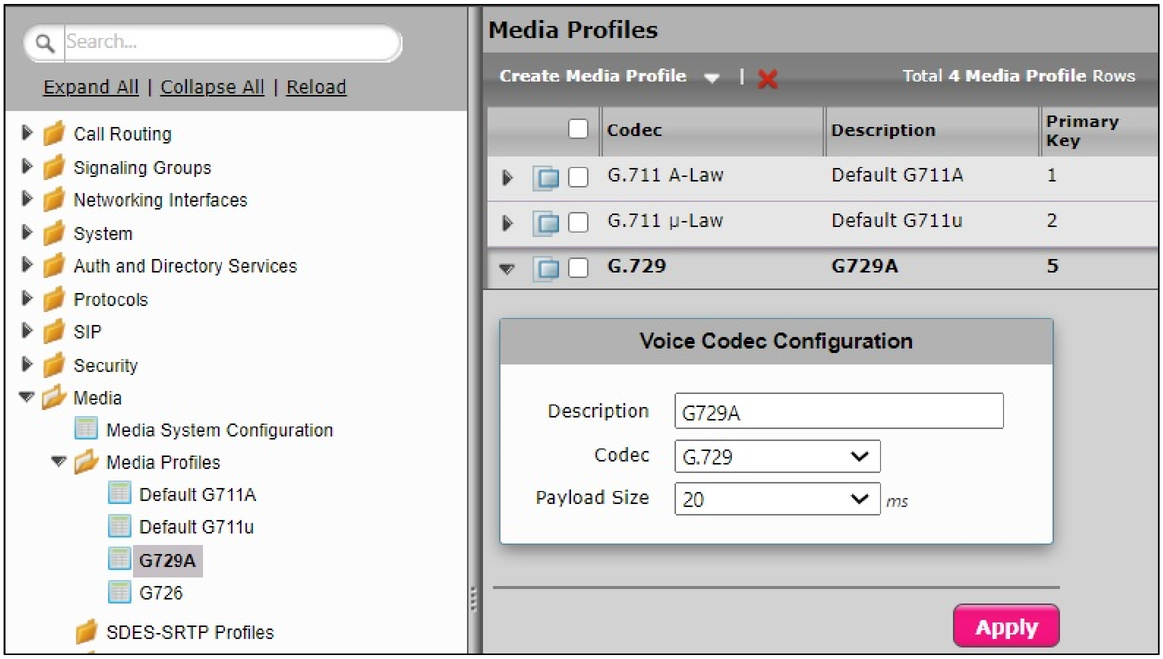
> **Tip**
> For details on the SIP Recording (SIPREC) feature, refer to Working with SIP Recording - SIPREC.

Configure Media Profiles

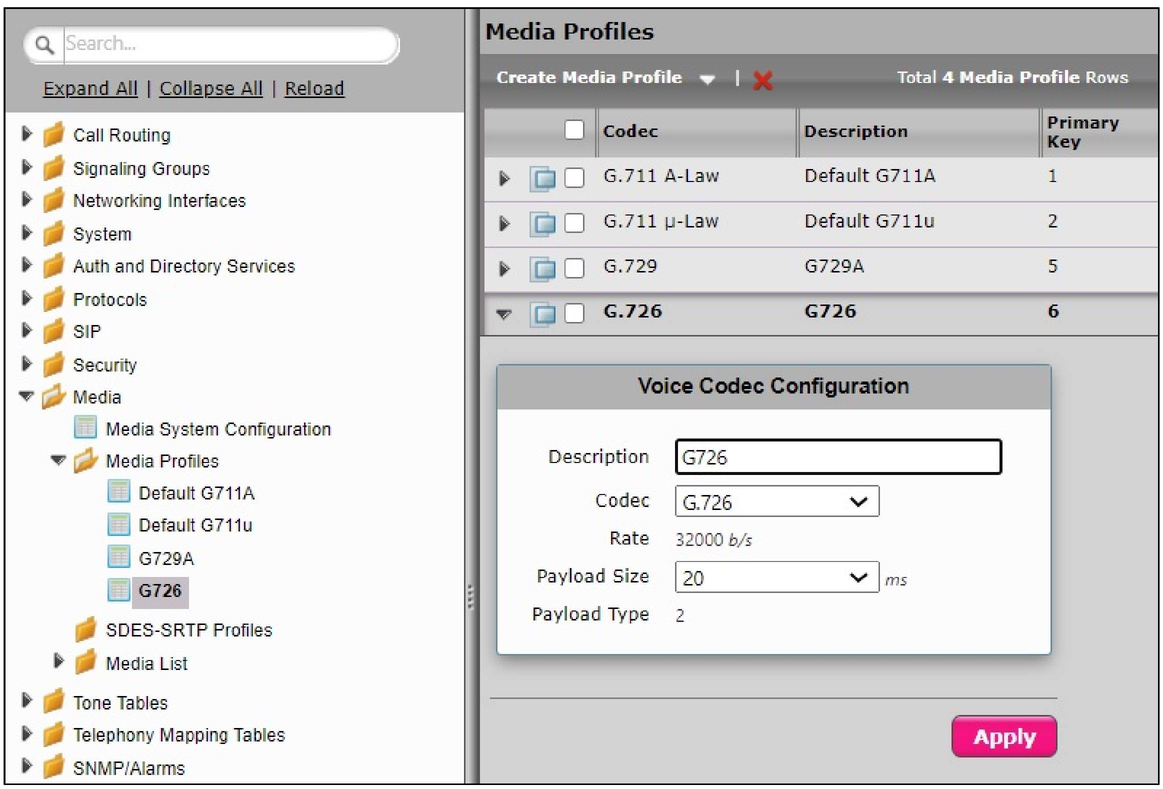
From the **Settings** tab, navigate to **Media > Media Profiles**.

1. From the **Create Media Profile** drop-down box at the top of the **Media Profiles** page, select **Voice Codec Profile.**
2. From the **Codec** drop-down box, select a codec.

Codec - G.729



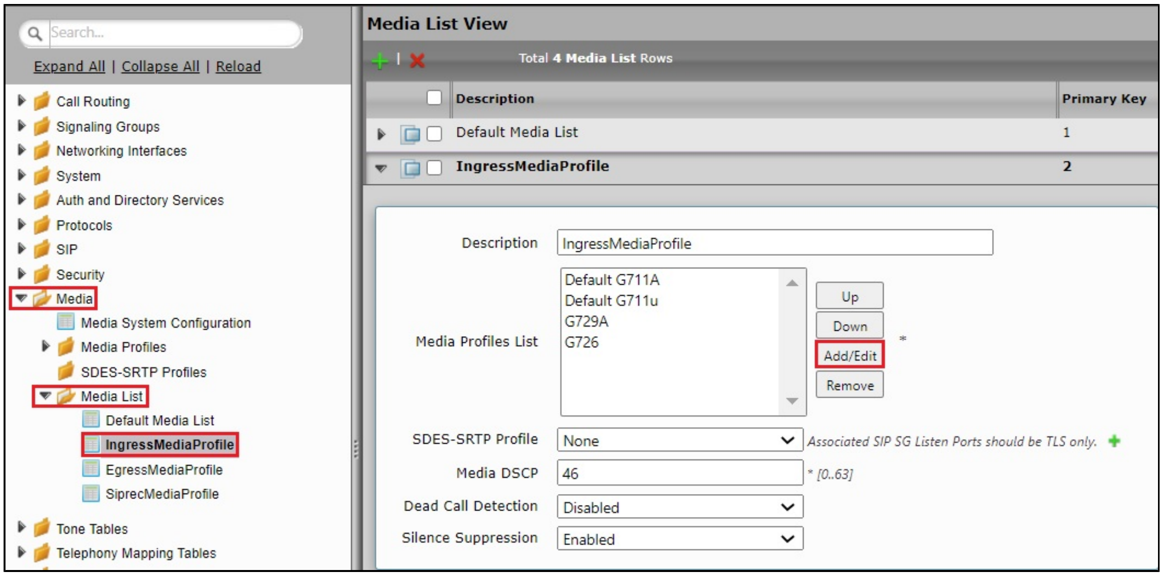
Codec - G.726

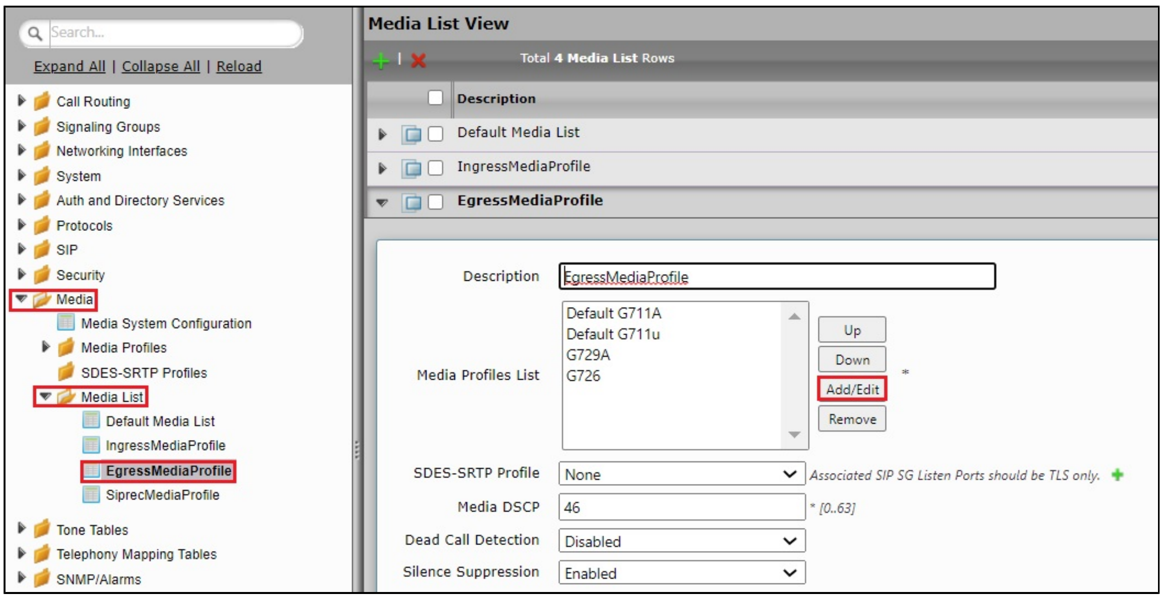


Attach Media Profiles to Media lists

From the **Settings** tab, navigate to **Media > Media Lists**.

- Click the Create Media List (+) icon at the top of the Media List View page.
- Provide the desired description.
- Click **Add/Edit** and select the **Media Profiles List**.
- Click **OK**.





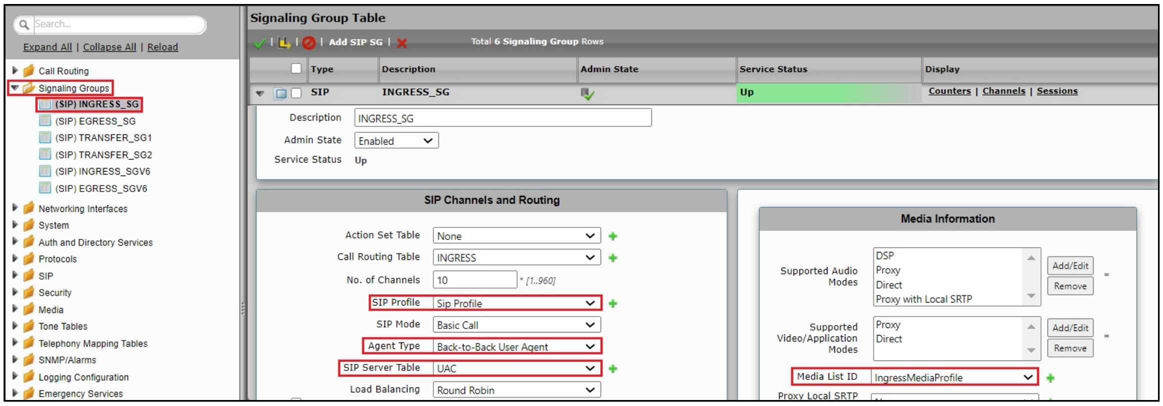
Configure Signaling Groups

Signaling groups allow grouping telephony channels for routing and shared configuration. They are used for routing calls and selecting Call Routes.

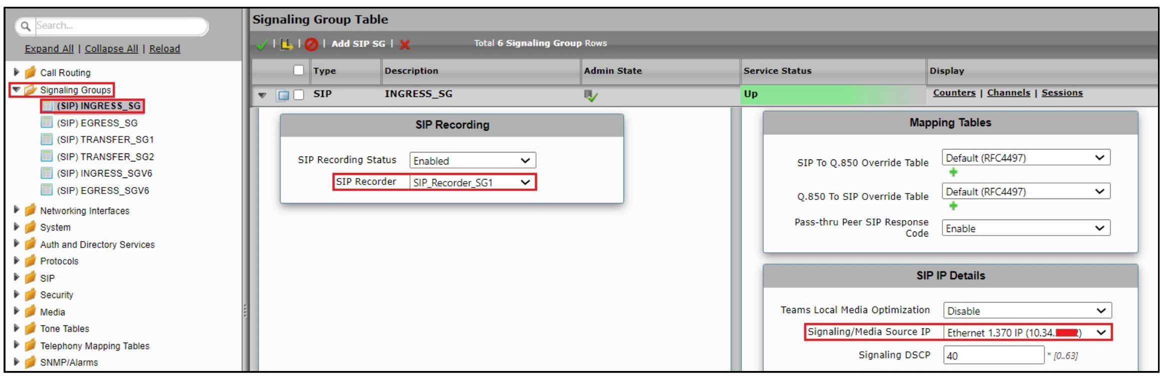
From the **Settings** tab, navigate to **Signaling Groups (Add SIP SG)**.

INGRESS_SG

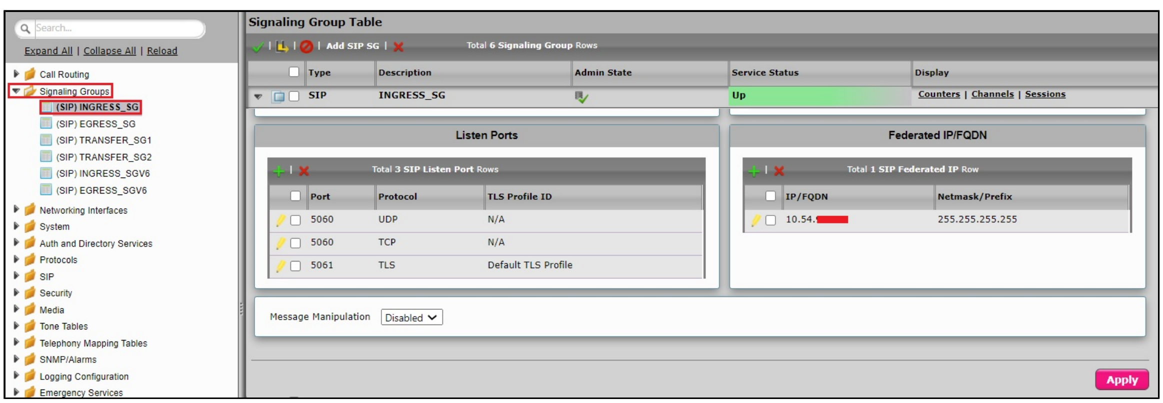
- Attach the Sip Profile you created earlier.
  - Specifies the SIP Profile for this Signaling Group.
- Select the Agent Type as Back-to-Back User Agent.
  - The SBC maintains the state and participates in all SIP signaling between both endpoints.
- Attach the SIP Server Table "UAC".
  - Specifies the SIP Server Table for this Signaling Group.
- Select the appropriate Media List.
  - Specifies the Media List this Signaling Group uses.



- Enable SIP Recording and attach the Recording Server Table created for SIP recording.
  - When the SIPREC is enabled for the specific Signaling Group, this field allows you to select an entry from a SIP Recording Table, using the drop-down list. This list is populated from the entries configured in the SIP Recording table. For details, refer to Creating and Modifying Entries in the SIP Recorder Table.
- Select Ethernet 1(IPv4) as the **Signaling/Media Source IP**
  - Specifies the Logical IP address for receiving SIP messages. Use this address as the source IP for all SIP messages, leaving the SBC SWe Lite or SBC 1000/2000 through this Signaling Group.

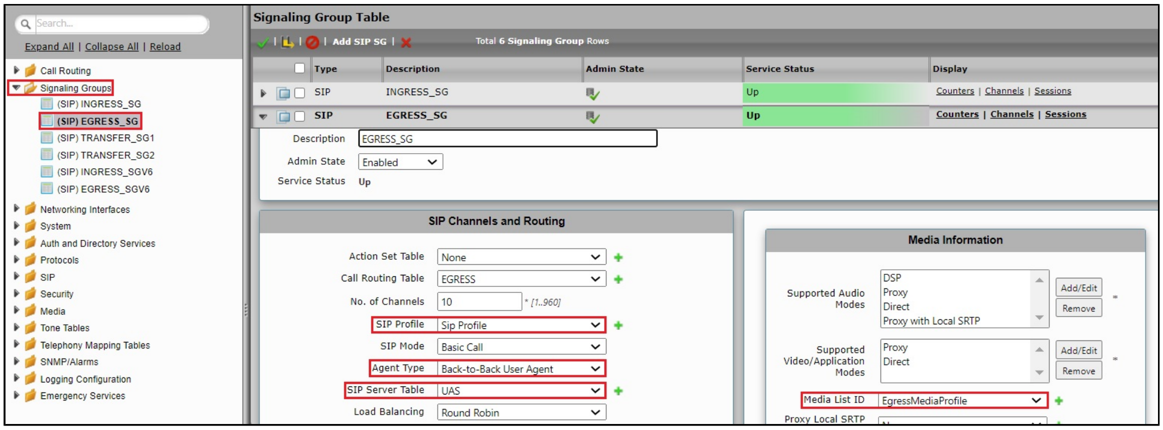


- Configure the UAC IP Address in the Federated IP/FQDN field.
  - The Federated IP/FQDN feature acts as an access control, defining from which server a SIP Signaling Group will accept messages.

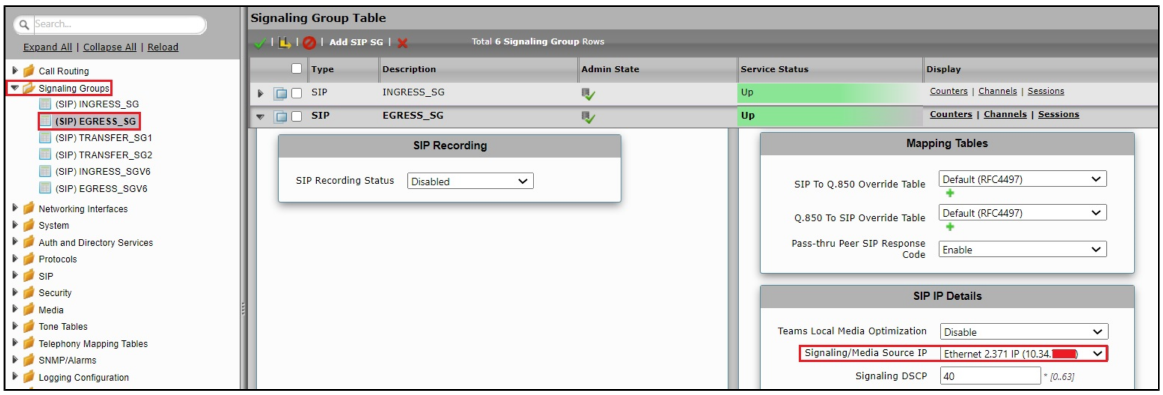


EGRESS_SG

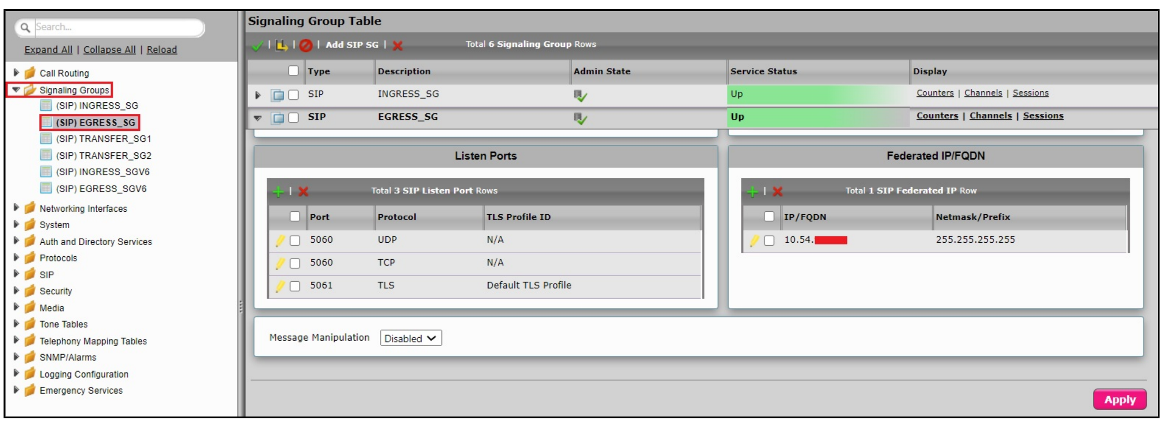
- Attach the Sip Profile you created earlier.
- Select the Agent Type as Back-to-Back User Agent.
- Attach the SIP Server Table "UAS".
- Select the appropriate Media List.



- Select Ethernet 2 (IPv4) as the **Signaling/Media Source IP**.

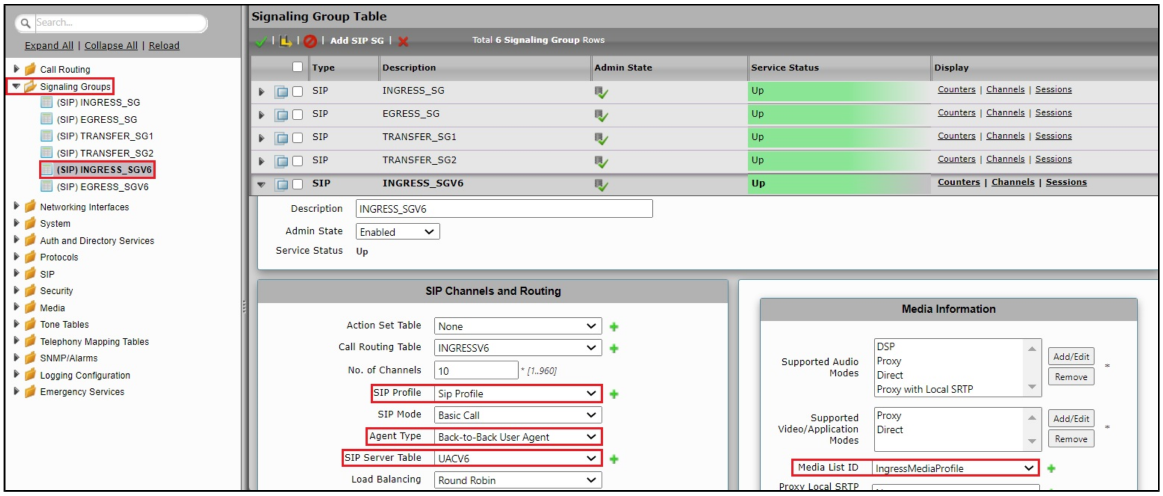


- Configure the UAS IP Address in the Federated IP/FQDN field.

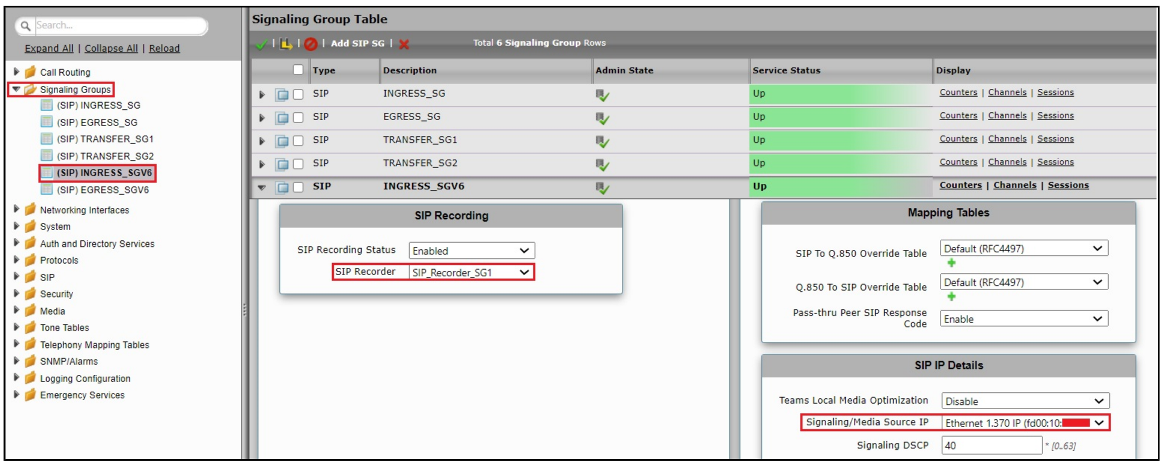


INGRESS_SGV6

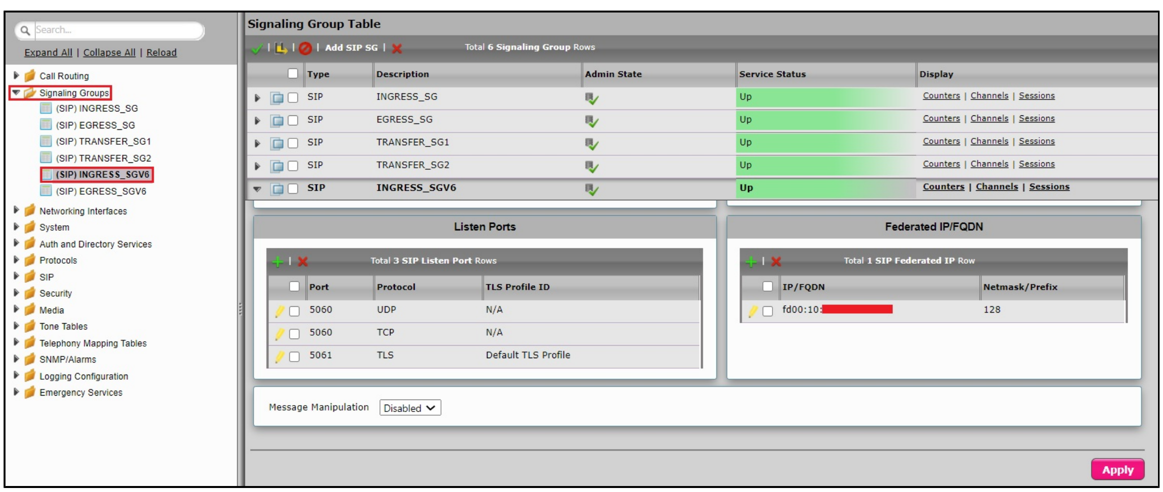
- Attach the Sip Profile you created earlier.
- Select the Agent Type as Back-to-Back User Agent.
- Attach the SIP Server Table "UACV6".
- Select the appropriate Media List.



- Enable SIP Recording and attach the Recording Server Table created for the SIP recording.
- Select Ethernet 1(IPv6) as the **Signaling/Media Source IP**.

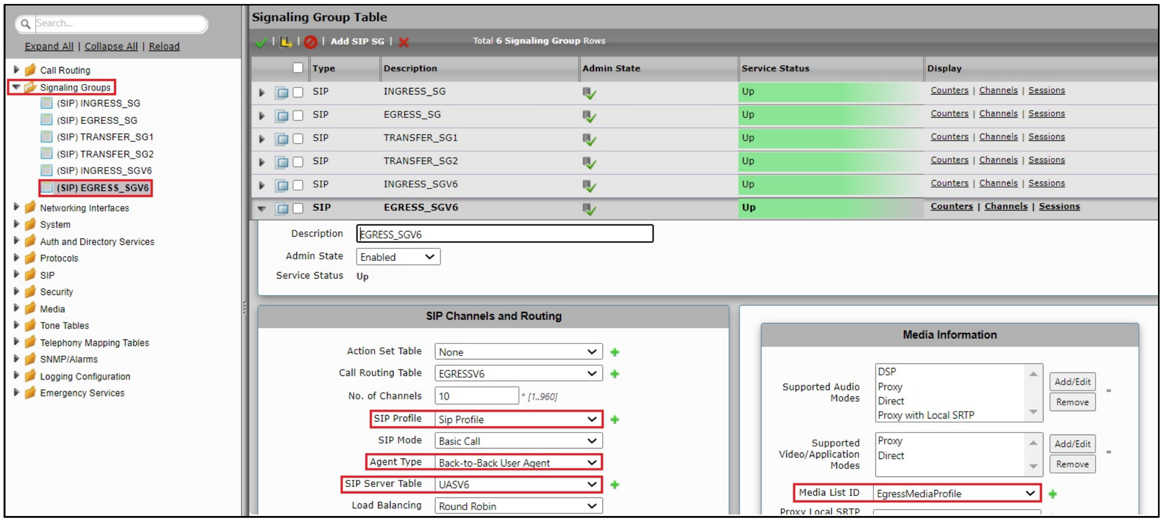


- Configure the UACV6 IP Address in the Federated IP/FQDN field.

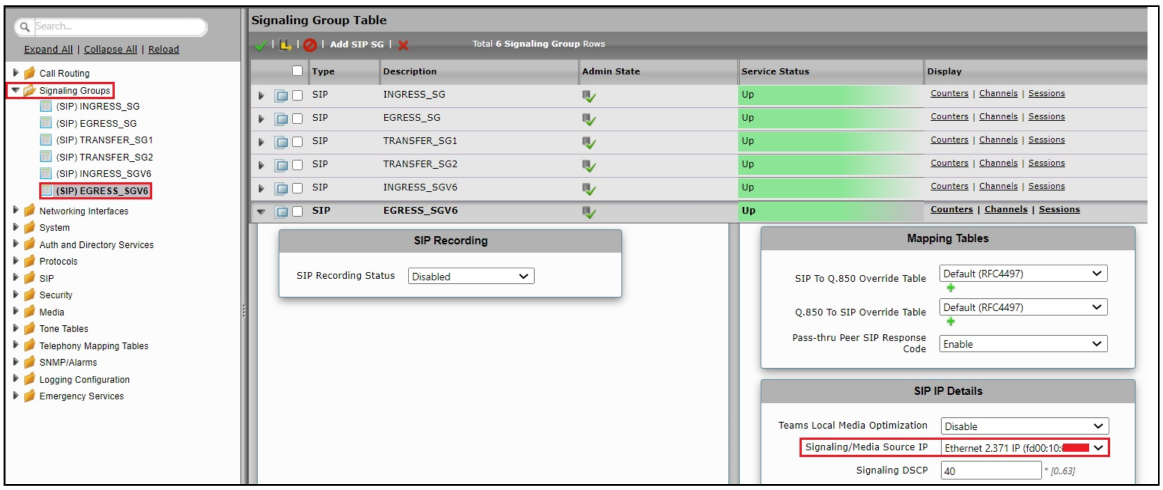


EGRESS_SGV6

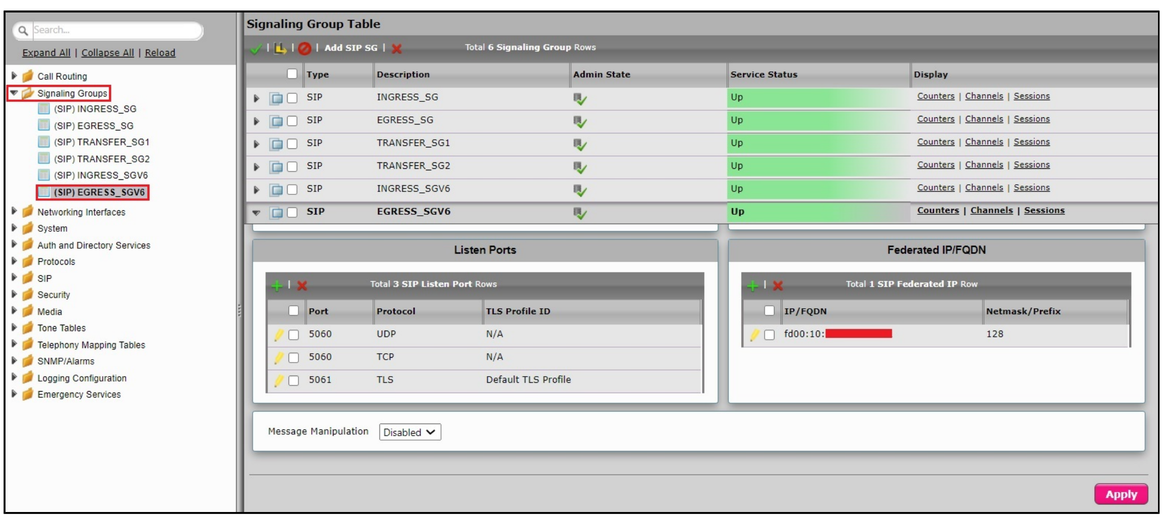
- Attach the Sip Profile you created earlier.
- Select the Agent Type as Back-to-Back User Agent.
- Attach the SIP Server Table "UASV6".
- Select the appropriate Media List.



- Select Ethernet 2 (IPv6) as the **Signaling/Media Source IP**.



- Configure the UASV6 IP Address in the Federated IP/FQDN field.



Configure Transformation Tables

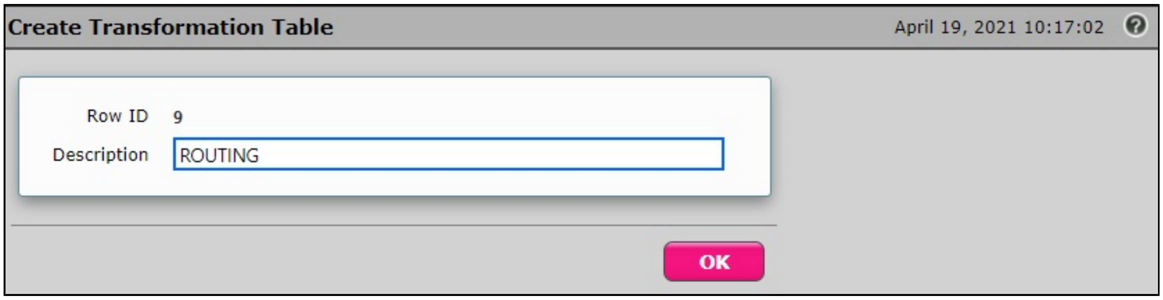
Transformation Tables facilitate the conversion of names, numbers, and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number or a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table and is available for user selection. Transformation tables are also configurable as a reusable pool that Action Sets can reference.

To Create a Transformation Table

Each Transformation Table contains a list of entries for creating routing rules. Create each rule in the available order until you reach the end of the table, or when a mandatory entry fails to execute.

From the **Settings** tab, navigate to **Call Routing > Transformation**.

1. Click the **Create** ( ) icon.
2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.



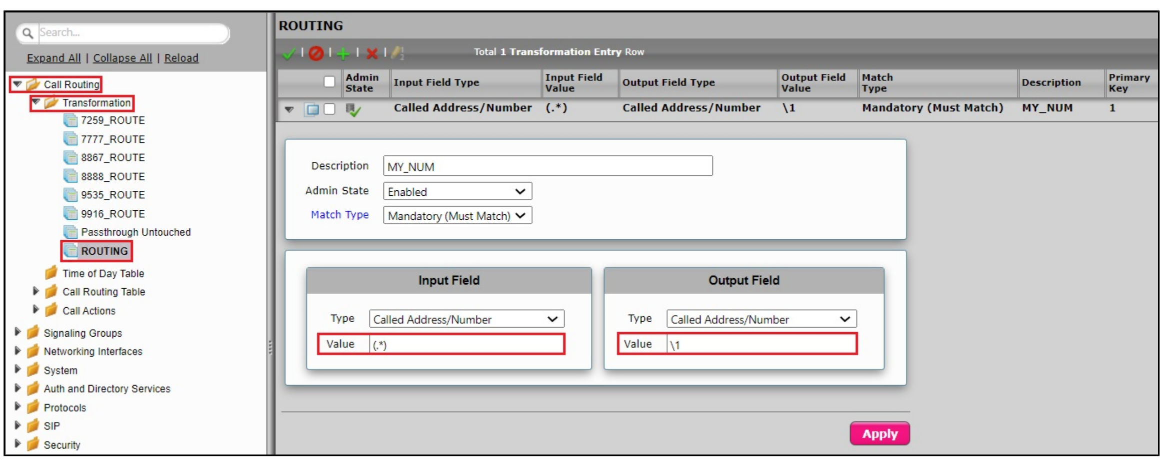
Creating an Entry in a Message Transformation Table

1. Click the **Create( )** icon next to the table you created in the previous step.
2. Set the following fields:

   Admin State:
   Enabled - The default state is Enabled.

   Match Type:
   Optional: Optional entries must match at least one of the Input Field types.
   When a call arrives at a Transformation Table, the incoming message contains several Informational Elements (IEs). These IEs include important call information, such as Called Address/Number, Called Extension, Calling Name, Redirecting Number, and others.
   Each IE is processed row-by-row in the Transformation Table.

   Value (Input/Output):
   Specifies the value to match against the selected type. Depending upon the type selected, values are free-form or selected from a menu.
3. Click Apply.



Note
For details on Transformation Table Entry configuration, refer to Creating and Modifying Entries to Transformation Tables. For call digit matching and manipulation through the use of regular expressions, refer to Creating Call Routing Logic with Regular Expressions.

Configure Call Routing Tables

Call Routing tables allow you to configure flexible routes for transferring calls between Signaling Groups and translating the calls.

From the **Settings** tab, navigate to **Call Routing** > **Call Routing Table**.

Modifying an Entry in a Call Routing Table

1. Click the **expand** ( ) icon next to the entry you wish to modify.
2. Edit the entry properties as required.

Creating an Entry in a Call Routing Table

Call Routing Tables are one of the central connection points of the system, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists, and the three types of Signaling Groups (ISDN, SIP, and CAS).

In the SBC Edge, call routing occurs between **Signaling Groups**.

To route any call to or from a call system connected to the SBC, you must first configure a Signaling Group to represent that device or system. The following list illustrates the hierarchical relationships of the various Telephony routing components of an SBC call system:

- Signaling Group describes the source call and points to a routing definition known as a Call Route Table.
- Call Route Table contains one or more Call Route Entries.
- Call Route Entries points to the destination Signaling Group(s).

Each call routing entry describes how to route the call and also points to a Transformation Table, which defines the conversion of names, numbers, and other fields when routing a call.

To create an entry:

1. Click the **Create Routing Entry** ( ) icon.
2. Set the following fields:

   Admin State:

   Enabled - Enables the call route entry for routing the call, displaying it in the configuration header as .

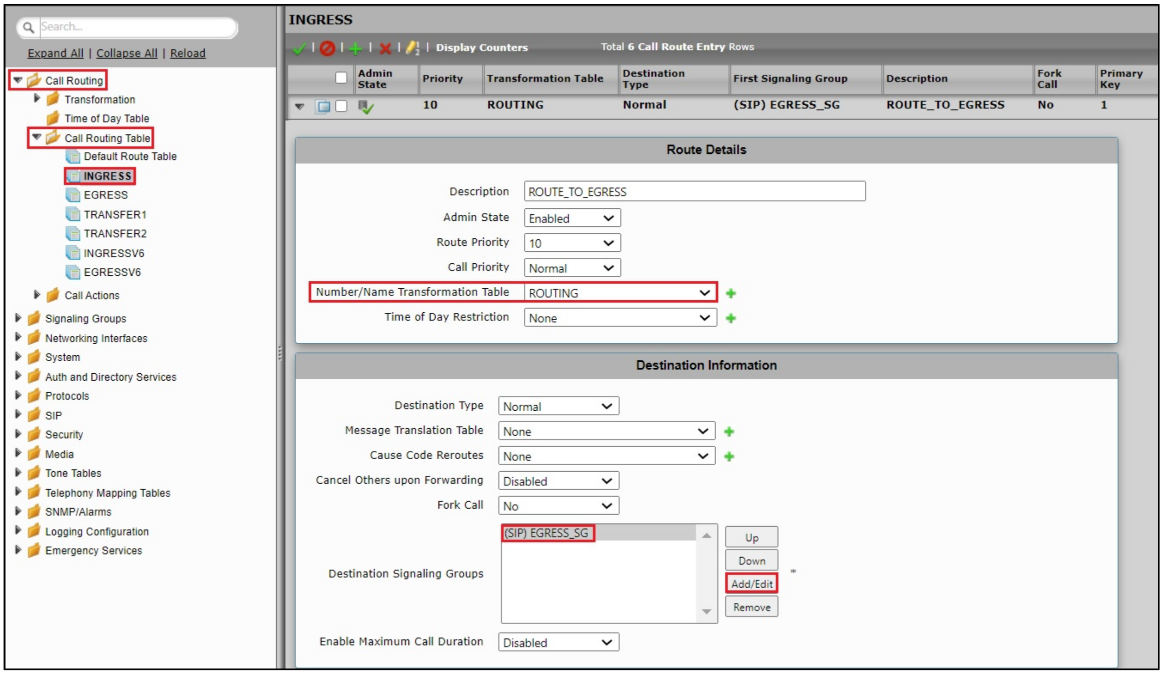
   Route Priority:
   Shows the priority of the route from 1 (highest) to 10 (lowest). Regardless of the order of the routes in the table, higher priority routes are matched first, before matching the lower priority routes.

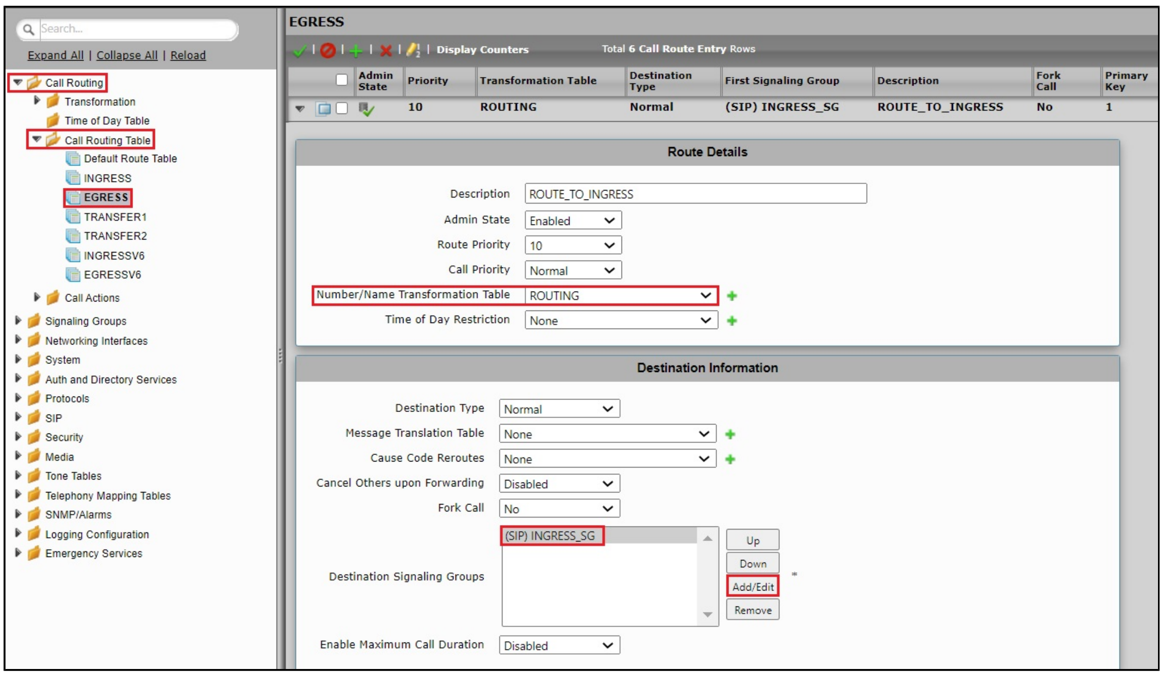
   Number/Name Transformation Table:
   Specifies the Transformation Table for this routing entry. The drop-down list is populated from the entries in the Transformation Table.

   Destination Signaling Groups:
   Specifies the Signaling Groups used as the destination of calls. The first operational Signaling Group from the list is chosen to place the call. Click the Add/Edit button to select the destination signaling group.

   Audio Stream Mode:
   DSP (default entry): The SBC uses DSP resources for media handling (transcoding); however, it does not support the capabilities and features between endpoints if they are not supported within the SBC (codec/capability mismatch). When you configure DSPs, the Signaling Groups support the DSP in a specific order.

   Media Transcoding:
   Enabled: Enable Transcoding on SIP-to-SIP calls.
3. Click **Apply**.





SBC SWe Lite Configuration with TLS

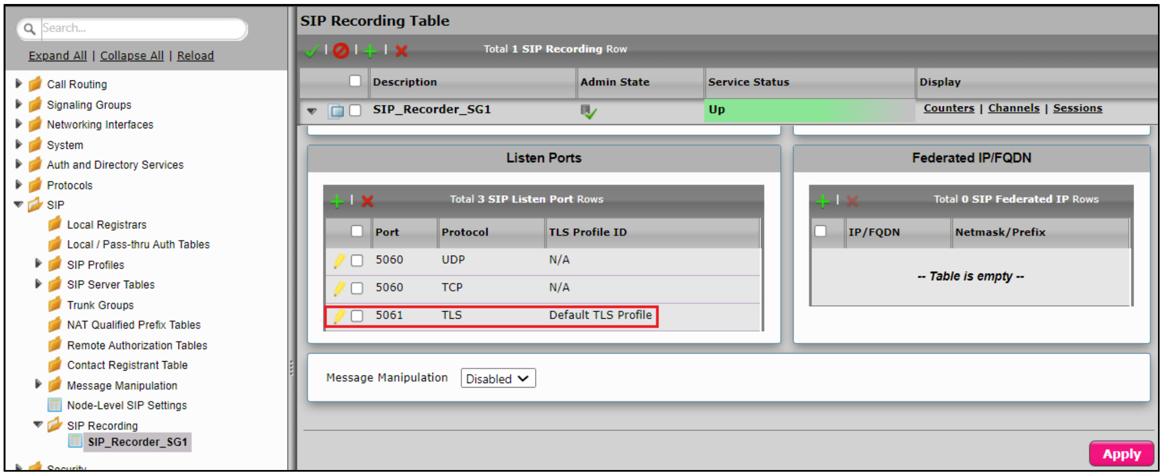
This section describes the steps to configure the SBC SWe Lite with TLS for the SIPREC.

Modify SIP Recording Table entry

A SIP Recorder Table contains information that a Signaling Group uses to start a SIP Recording (SIPREC) session. Use the configuration options to select the Recording Server (SIP Server), SIP channels, routing, and media, which direct the SBC to communicate with the Session Recording Server (SRS).

From the **Settings** tab, navigate to **SIP > SIP Recording**.

- Configure the TLS Listen Port and attach the TLS Profile.

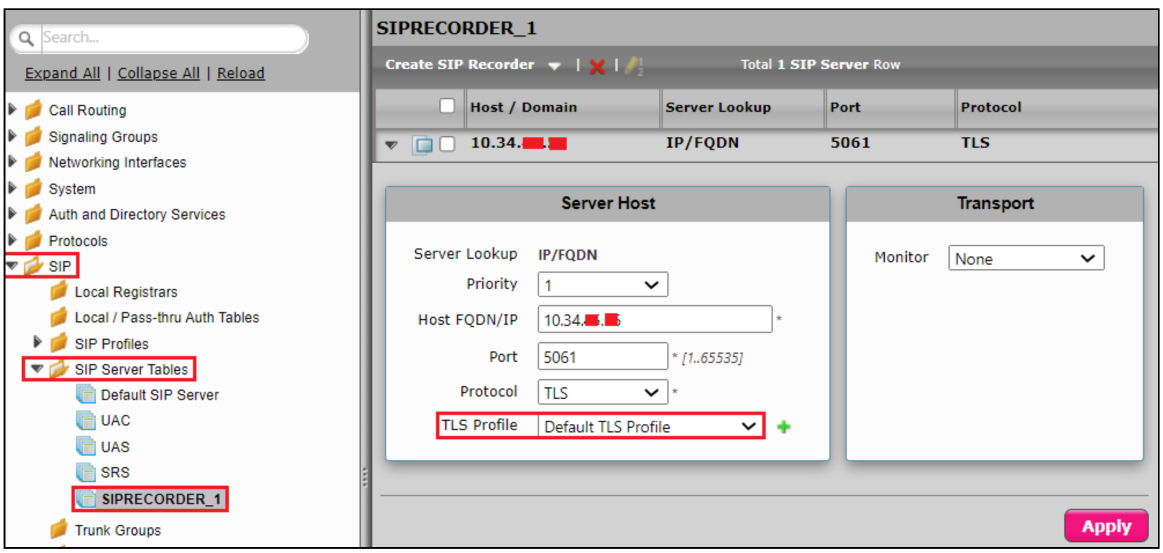


Update SIP Server Table

SIP Server Tables contain information about the SIP devices connected to the SBC Edge. The entries in the tables provide information about the IP Addresses, ports, and protocols used for communicating with each server. The table entries also contain links to counters that are useful for troubleshooting.

From the **Settings** tab, navigate to **SIP > SIP Server Tables > SIPRECORDER_1.** Click the expand ( ) icon next to the entry.

1. Select the TLS protocol with Port Number 5061.
2. Attach the TLS Profile.



NICE Engage Configuration

Make sure you meet the following configuration requirements:

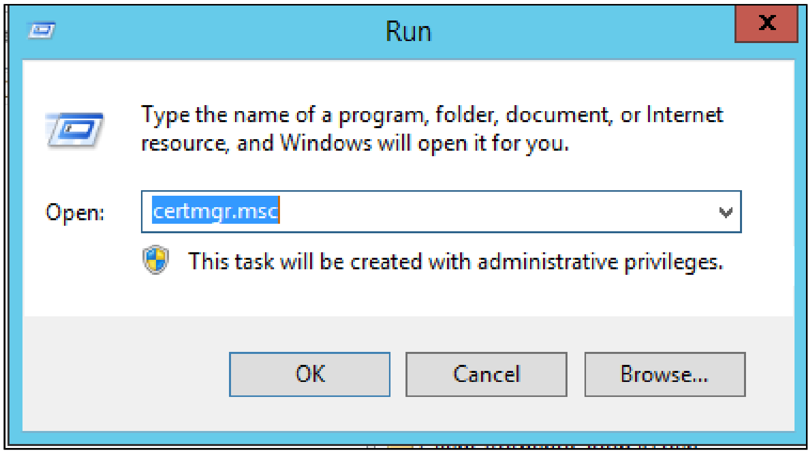
- Ensure that the Nice Integration Dispatch service is running on the NICE server.
- Note that the SBC SWe Lite specific configurations are not required on the NICE server since it accepts SIP traffic from all the IP Addresses.
- Import the SBC Primary Certificate to the Application Server of the NICE Engage Platform (Version: 6.15).

> **Info**
> Make sure that the NICE Engage Platform is running on 6.15 or later versions for TLS support.

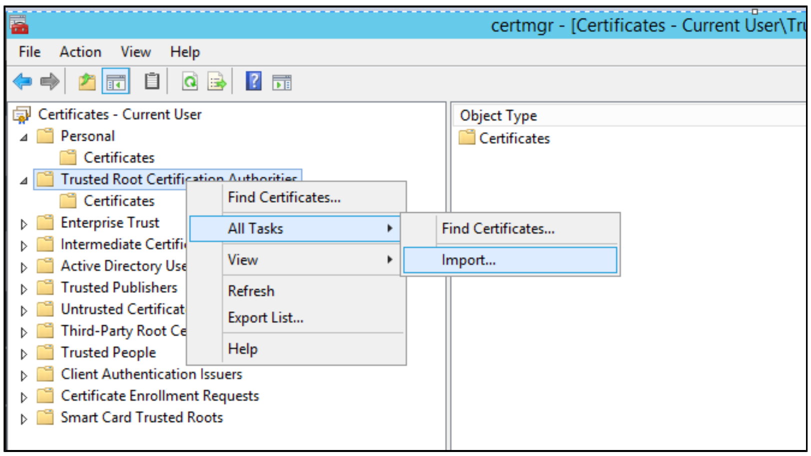
Trusted Certificate installation on the Application server

You must export and copy the certificate installed on each server in .cer format to all the other servers. For example, if you exported the certificate from the appserver, then be sure to copy it to AIR1/AIR2 and Interact servers.

1. Copy AIR1, AIR2, Interaction Server, and SWe Lite root certificates to the Application Server.
2. Open the Run command box in Windows, type **certmgr.msc**, and press **OK**.



3. From the certmgr window, navigate to **Trusted Root Certification Authorities > Certificates**. Right-click and select **All Tasks > Import**.

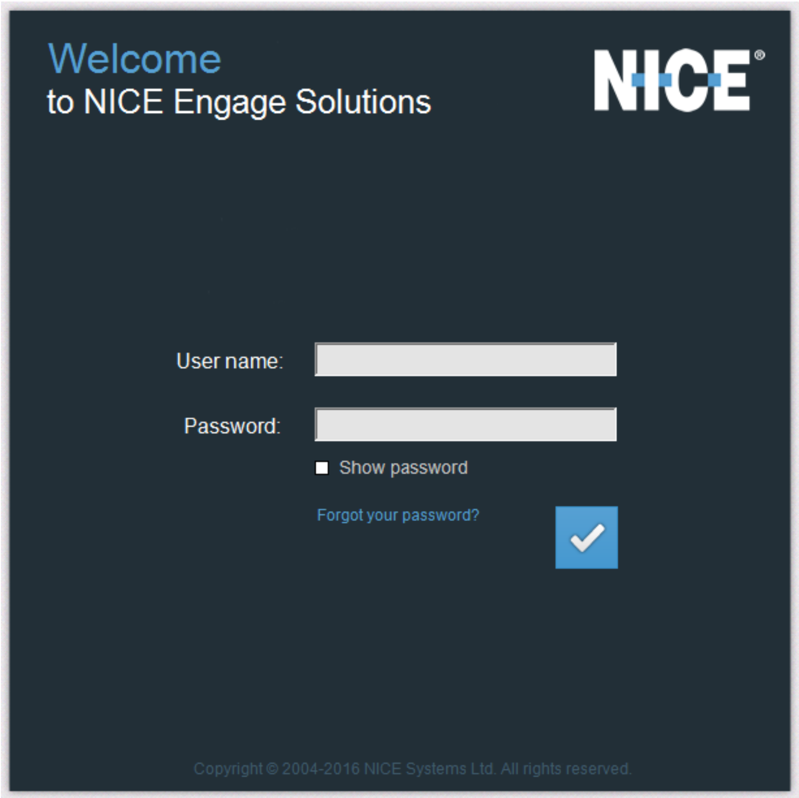


4. In the Import Certificate window, select the .cer certificate that you copied in step1 and import it to T**rusted Root Certification Authorities > Certificates**. Click **Finish**.
5. Repeat step 4 for other .cer certificates that you copied earlier.
6. Repeat the above steps to import each certificate for other servers.

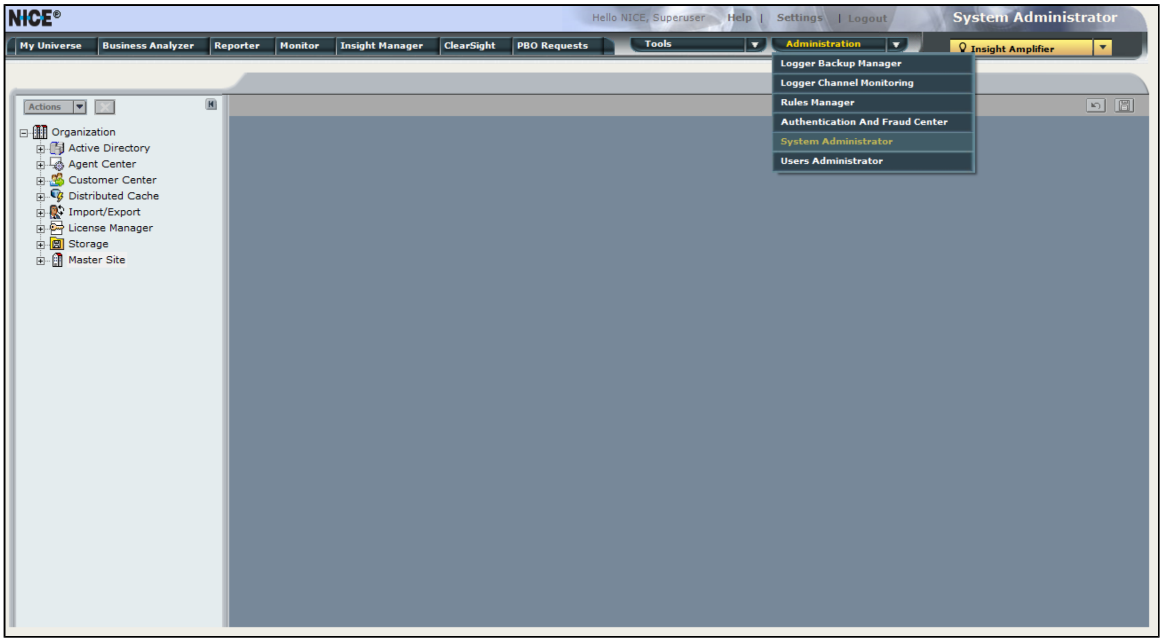
TLS Configuration on NICE Desktop Application

1. Open the NICE Desktop Application in a web browser of the Application Server.

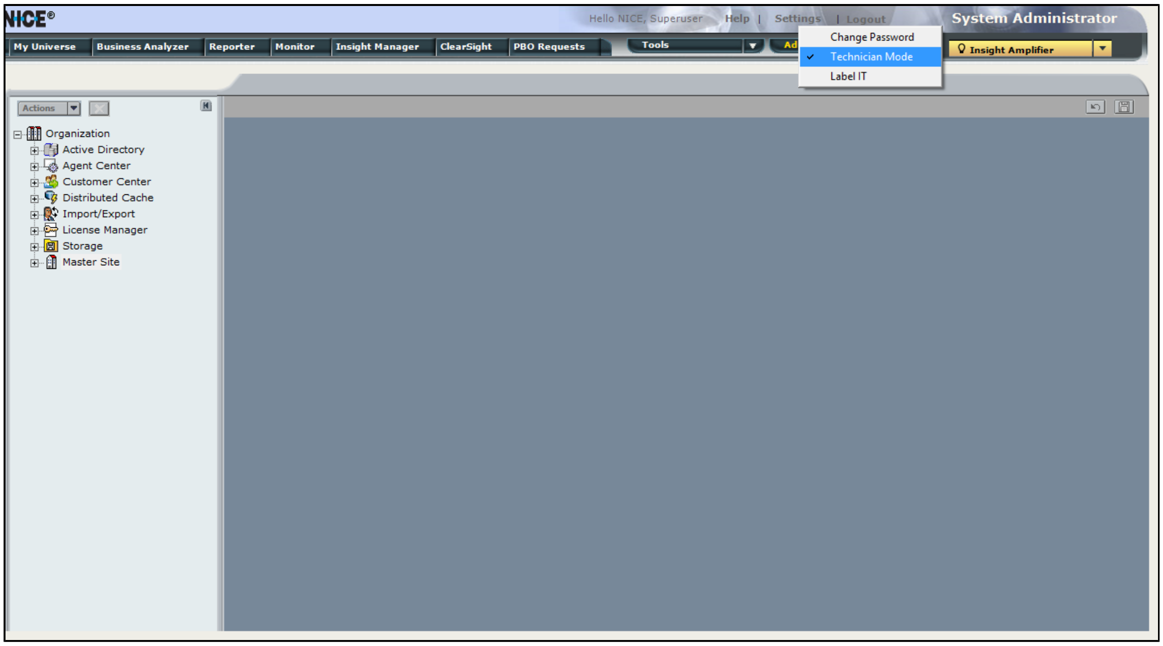
2. Provide a valid User Name and Password and log in to the Application.



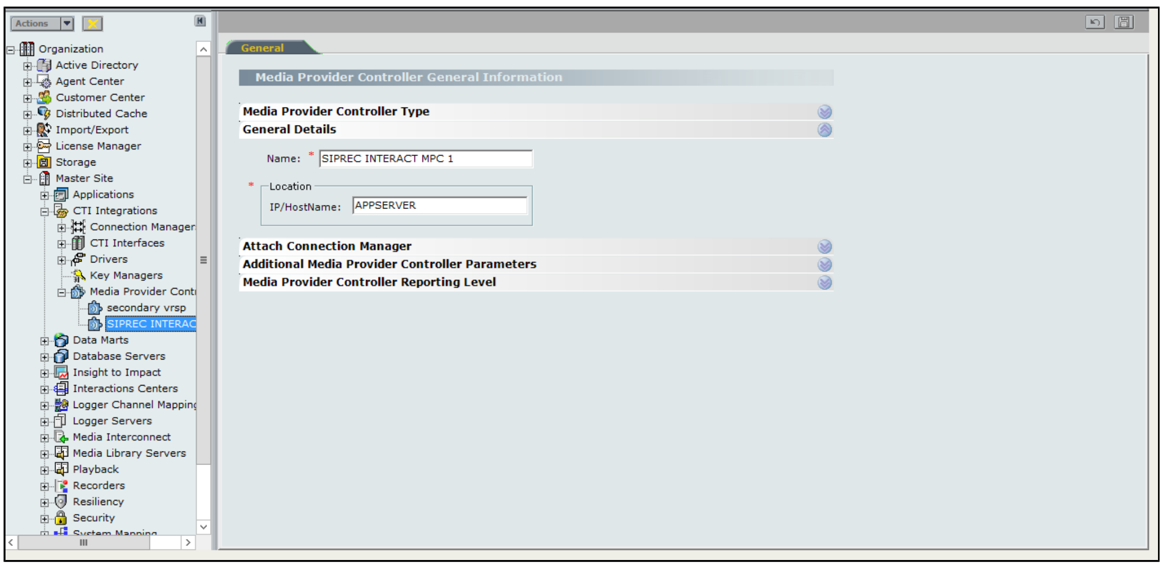
3. Navigate to **Administration > System Administrator**.



4. Navigate to **Settings** and select **Technician Mode**.

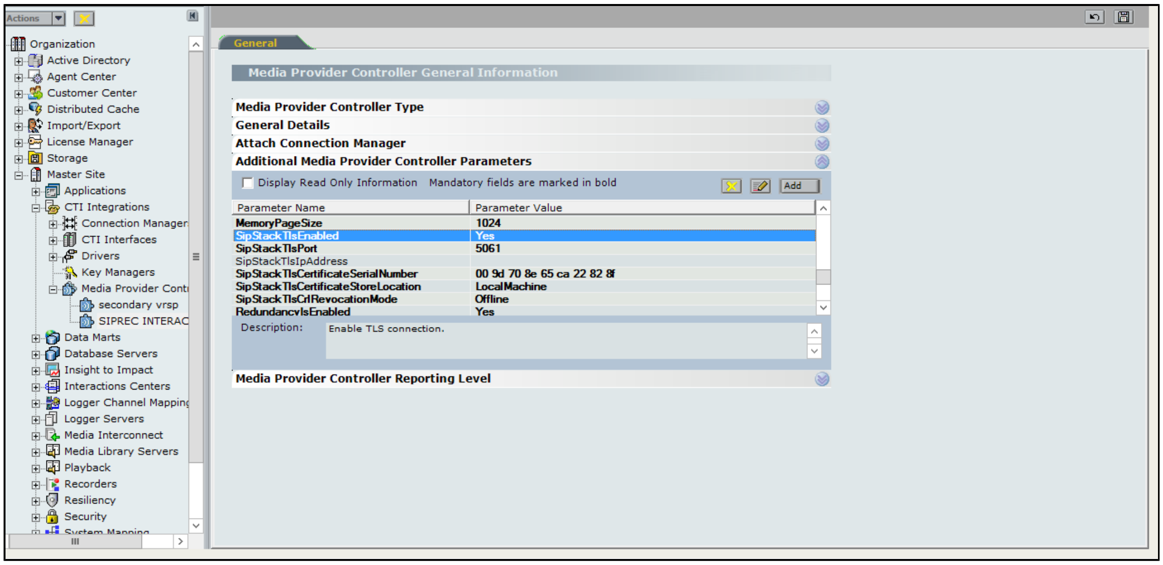


5. From the left Navigation Pane, go to **Master Site > CTI Integrations > Media Provider Controllers > Select VRSP server**.

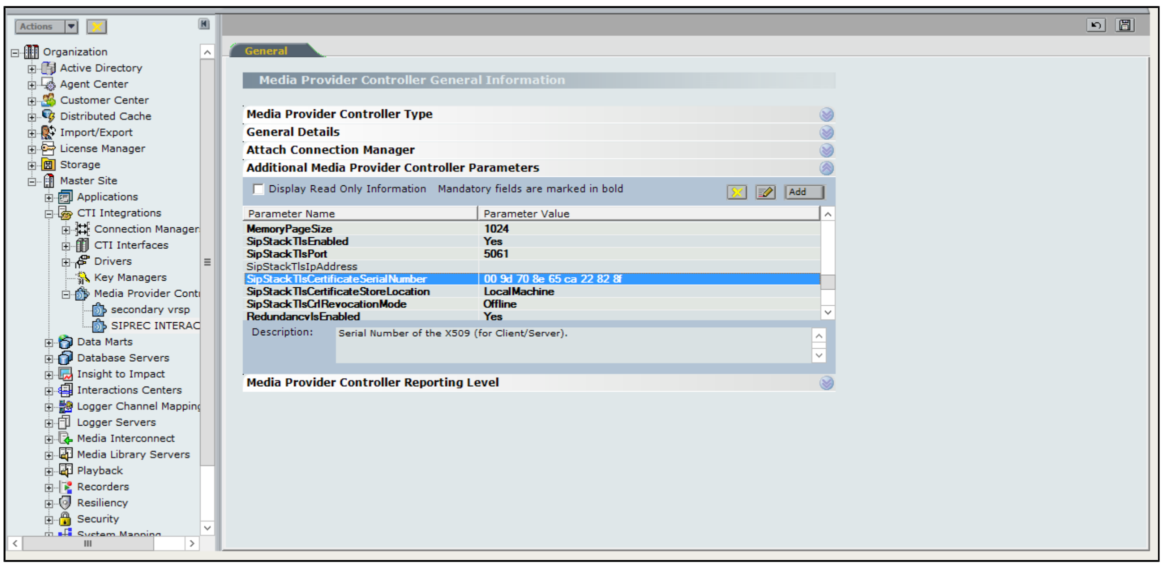


6. Expand the additional **Media Provider Controller** parameters.

7. Set the value of the **Sip Stack Tls Enabled** parameter to **Yes**.

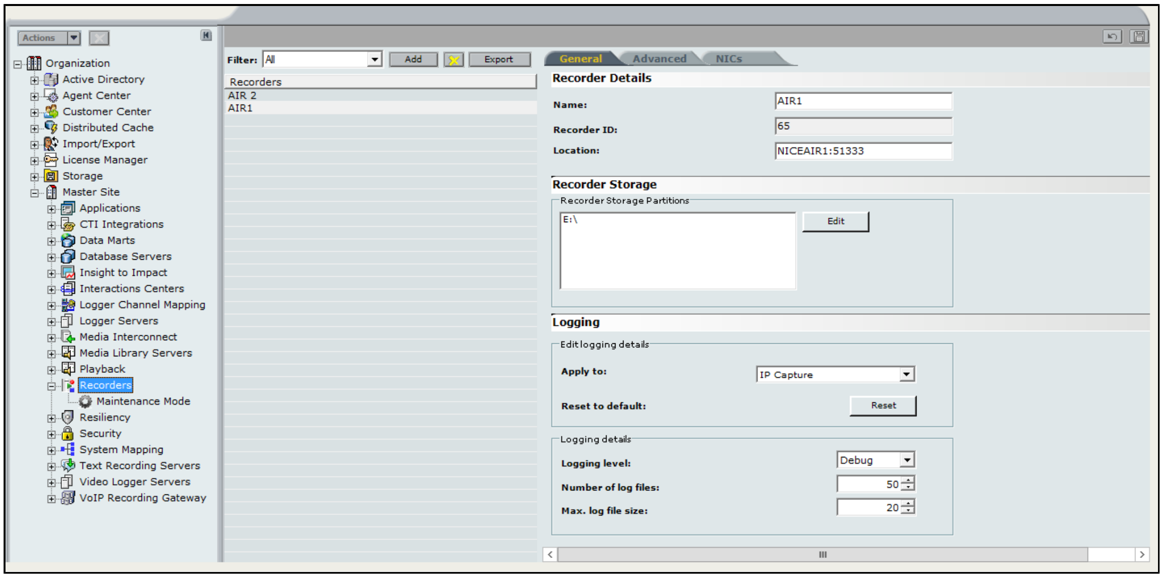


8. Select **Sip Stack TlsCertificateSerialNumber** and then enter the serial number of the APPSERVER certificate. Refer to How to get certificate serial number to obtain the certificate serial number.



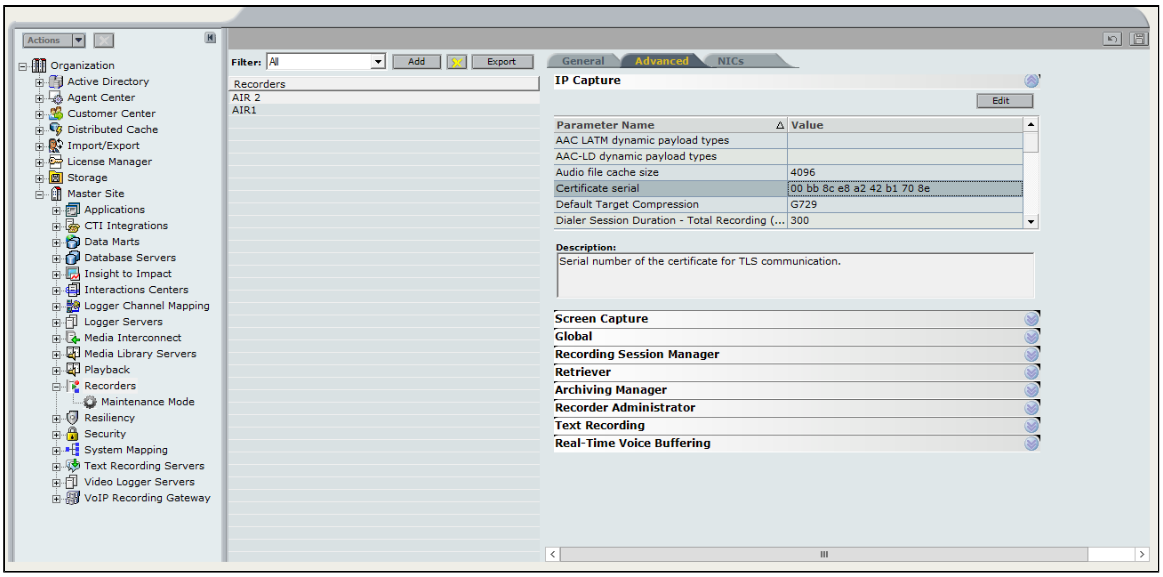
9. Click the **Save** icon displayed on the right-hand corner of the Application.

10. Navigate to **Master Site > CTI Integrations > Recorders** and select **AIR1**.

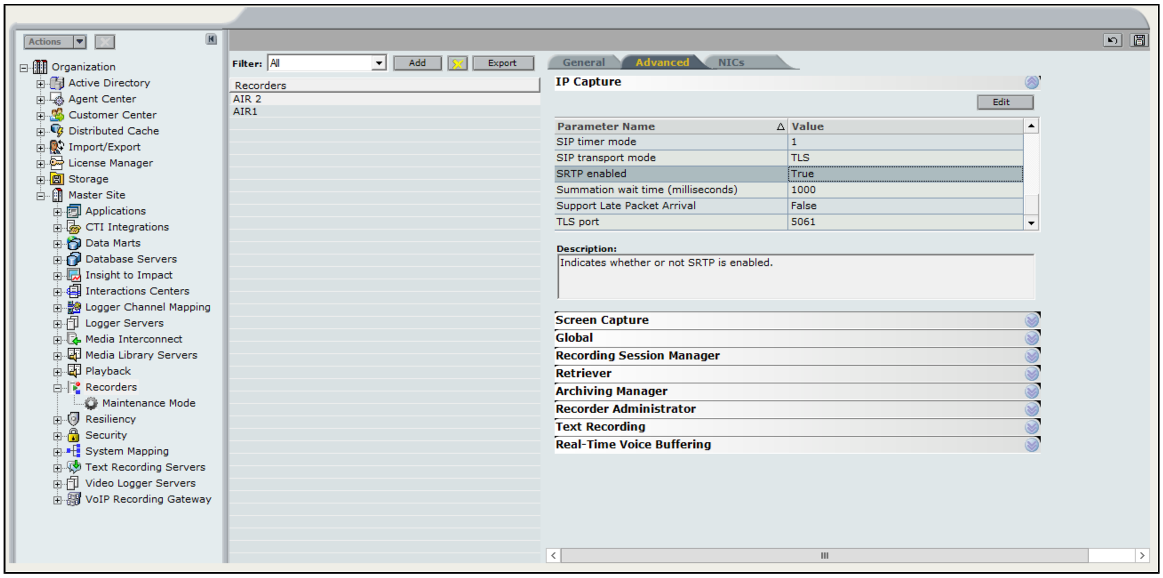


11. After selecting **AIR1**, click on the **Advanced** tab and expand **IP Capture**.

12. Select the **Certificate Serial** parameter, enter the serial number of the AIR1 certificate, and save your changes.



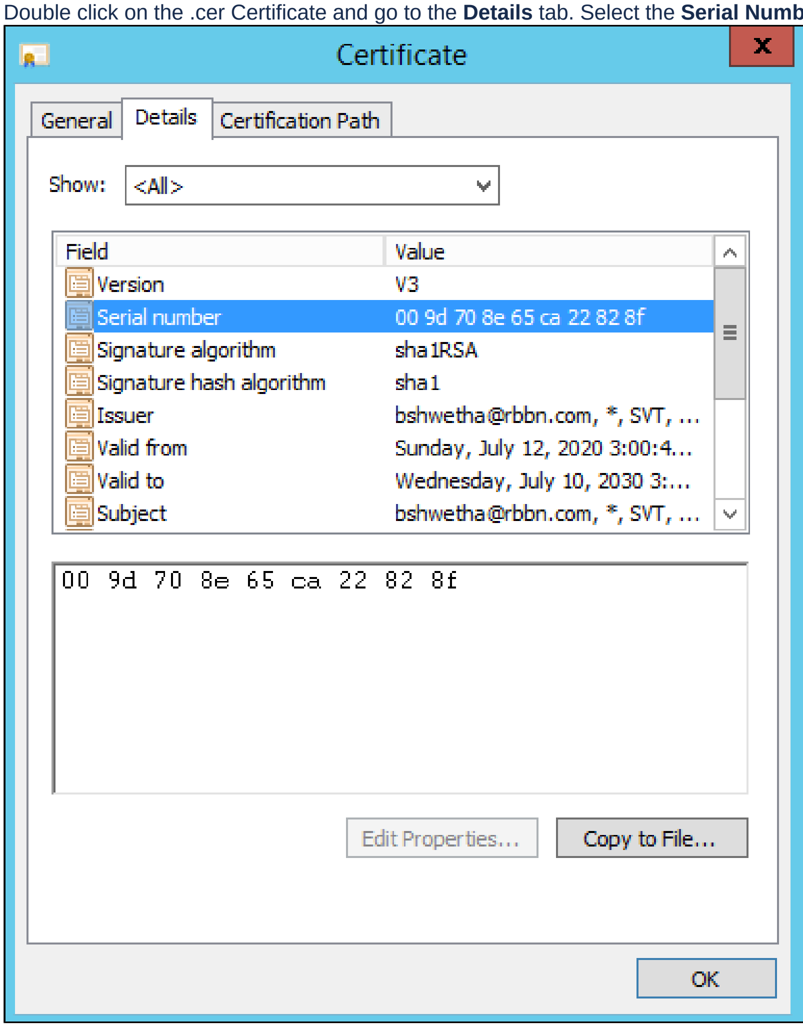
13. Select the **SIP transport mode** parameter and update it to the TLS.



14. Repeat the procedure from step10 to step13 for AIR2 using the certificate serial number of the AIR2 certificate.
15. Click **Save** displayed on the right-hand corner of the Application.
16. In the CTI Integrations branch, click **Apply**.
17. Restart the following services on the Application server and AIR servers:
    - NICE Dispatch Service
    - NICE Recorder Administrator
    - Media Provider Controller manager
    - NICE IP capture

How to get the Certificate Serial number

Double click on the .cer Certificate and go to the **Details** tab. Select the **Serial Number** field and copy the serial number of the certificate.



Supplementary Services and Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

Table 3 : Feature Coverage

Sr. No	Supplementary Services/Features	Coverage
1	SIPREC License Test	✔
2	Call Setup and Termination	✔
3	IP-Interworking	✔
4	Direct Media	✔
5	Call Transfer (Blind/Unattended)	✔
6	Call Transfer (Attended)	✔
7	Multiple Call Transfer - Blind	✔
8	Multiple Call Transfer - Attended	✘
9	Call with Audio and Video	✘
10	DTMF - Inband and RFC2833	✔

11	Round Robin Option for SRS recorder	✔
12	Channel Hunting	✔
13	Metadata Validation	✔
14	Transcode Calls	✔
15	4xx/5xx Response Handling	✔
16	Call Hold and Resume	✔
17	Call Forward - Unconditional, Busy, and No Answer	✔
18	SIP Keepalive	✔
19	MESSAGE/INFO/REFER/SUBSCRIBE/NOTIFY Handling	✔
20	Long Duration Calls	✔
21	Upgrade and Downgrade Test	✔
22	FAX	✔
23	Basic Calls - Skype Clients	✔
24	Transfer Calls (Blind and Attended) - Skype Clients	✔
25	Conference Calls - Skype Clients	✔
26	Call Park and Retrieve	✔
27	Basic Calls - Teams Clients	✔
28	Call Hold and Resume - Teams Clients	✔
29	Call Transfer before and after connect - Teams Clients	✔
30	Call Queue	✔
31	Music On Hold	✔
32	Call Conference	✔
33	Voice Mail	✔
34	Simultaneous Ringing	✔
35	E911 Calls	✔
36	Group Call Pickup	✔
37	SRTP on Recording Session	✘

Legend

Supported	✔
Not Supported	✘

Caveats

Note the following limitations about this Interop:

- SBC SWe Lite does not honor Request/Response from the SIPREC with a=inactive/sendonly/sendrecv
- SBC SWe Lite does not send encrypted media to the SIPREC.
- SBC SWe Lite supports recording of incoming calls only.

Support

For any support related queries about this guide, please contact your local Ribbon representative or the following numbers and website:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: https://ribboncommunications.com/about-us

References

For detailed information about Ribbon products and solutions, visit:
https://ribboncommunications.com/products

For detailed information about the NICE Engage platform, visit:
https://www.nice.com/

Conclusion

This Interoperability Guide describes how to successfully configure the NICE interop for Ribbon SBC SWe Lite and NICE Engage platform SIPREC server.

The guide provides information about all tested features and capabilities. It records all limitations, notes, and observations to provide you with an accurate understanding of what this guide covers and what it does not.

Configuration guidance in this document enables you to replicate the same base setup; however, you may require additional configuration changes to suit the exact deployment environment.