Ribbon SBC SWe Lite R9.0 Interop with MIDA Recorder : Interoperability Guide

Table of Contents

Interoperable Vendors

Copyright

Document Overview

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

> ⚠ From Release 11.0.0 onwards, Ribbon "**SBC SWe Lite**" is rebranded as "**SBC SWe Edge**".

About Ribbon SBC SWe Lite

The Ribbon Session Border Controller Software Edition Lite (SBC SWe Lite) provides best-in-class communications security. Microservices designed to optimize resource allocation, dynamic scaling, and 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 MIDA Recorder platform

Mida Recorder is a Multimedia Recording System for professional and telephony networks that supports all relevant communication technologies in a single future-proof platform. The Mida Recorder records all your voice and video communications, regardless of the sub-systems where they’re coming from, implementing a real Unified Recording System (URS).

About SIP Recording

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

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

SIP Recording on the SBC SWe Lite supports the following:

- Stores call information for quality analysis.
- Records call and media sessions on a third-party recording server.
- Checks the call detail records and determines if a call is recording or not.
- Provides call detail records for recorded calls.

Scope

This document provides configuration best practices for deploying Ribbon's SBC SWe Lite for MIDA Recorder 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

This guide does not provide detailed configurations that meet 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. For more information, see Working with Licenses.
  - This interop also requires the acquisition of SIPREC license.
- MIDA Recorder Platform
  - MIDA server running on 3.1.x version.
  - Licenses for recording application and expected traffic.

Product and Device Details

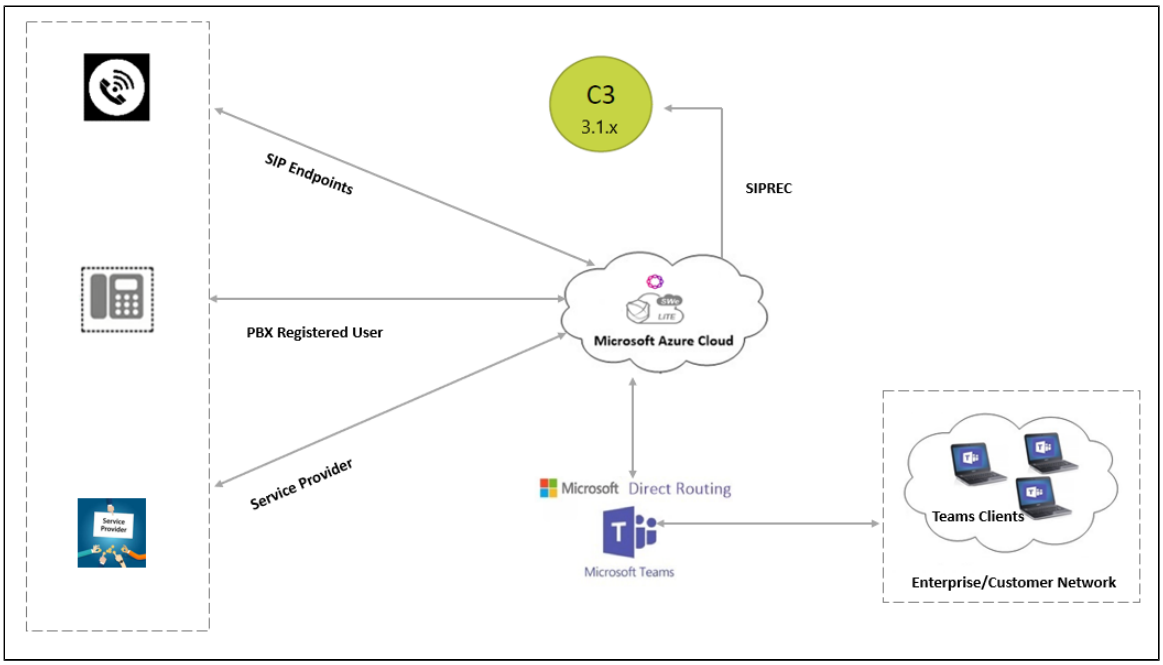
The configuration uses the following equipment and software:

Table 1: Requirements

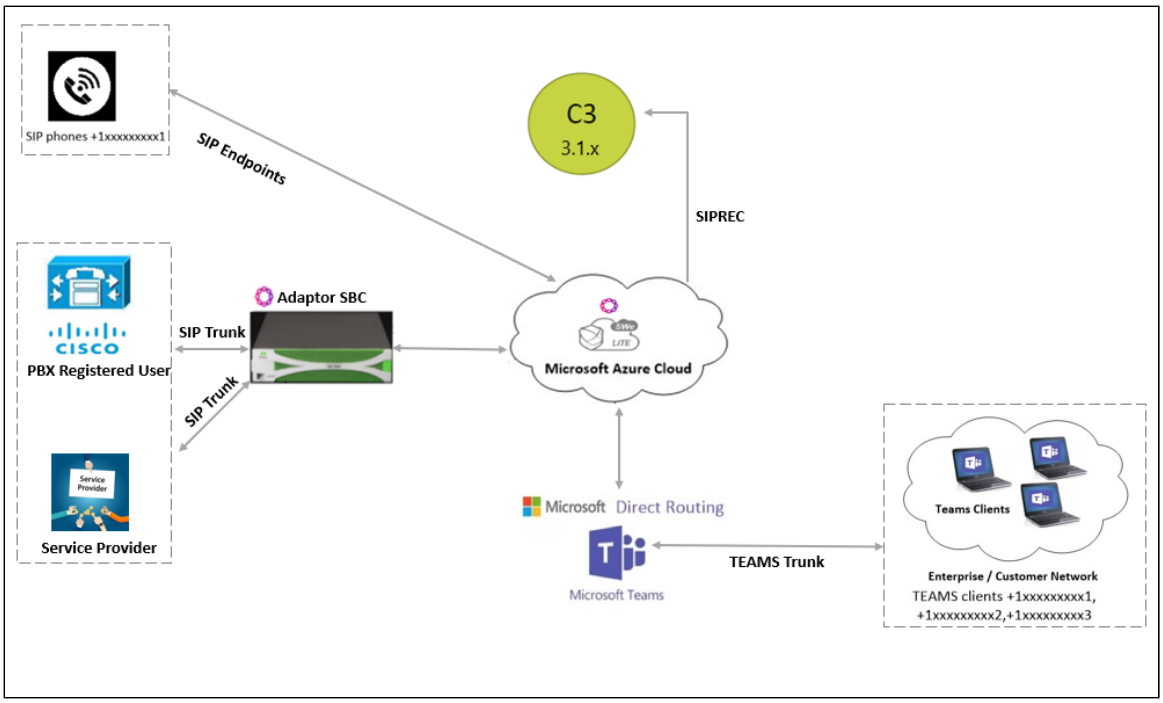
Product	Equipment/ Devices	Software/ Firmware Version
Ribbon Communications	Ribbon SBC SWe Lite	9.0.7
Third-party Equipment	MIDA Recorder	3.1.2
Third Party Phones	Kapanga Softphone	1.00
	Phonerlite	2.93
Administration and Debugging Tools	Wireshark	3.2.7
	LX Tool	2.1.0.6

Network Topology

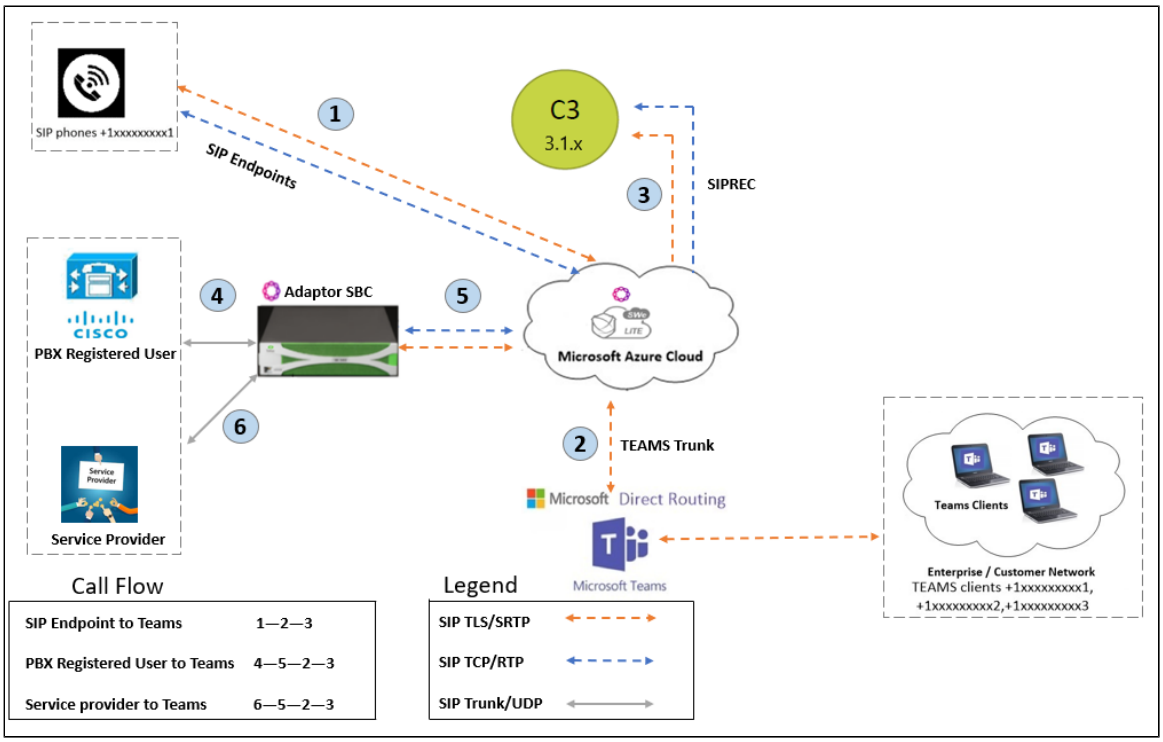
Deployment Topology



IOT Lab Topology

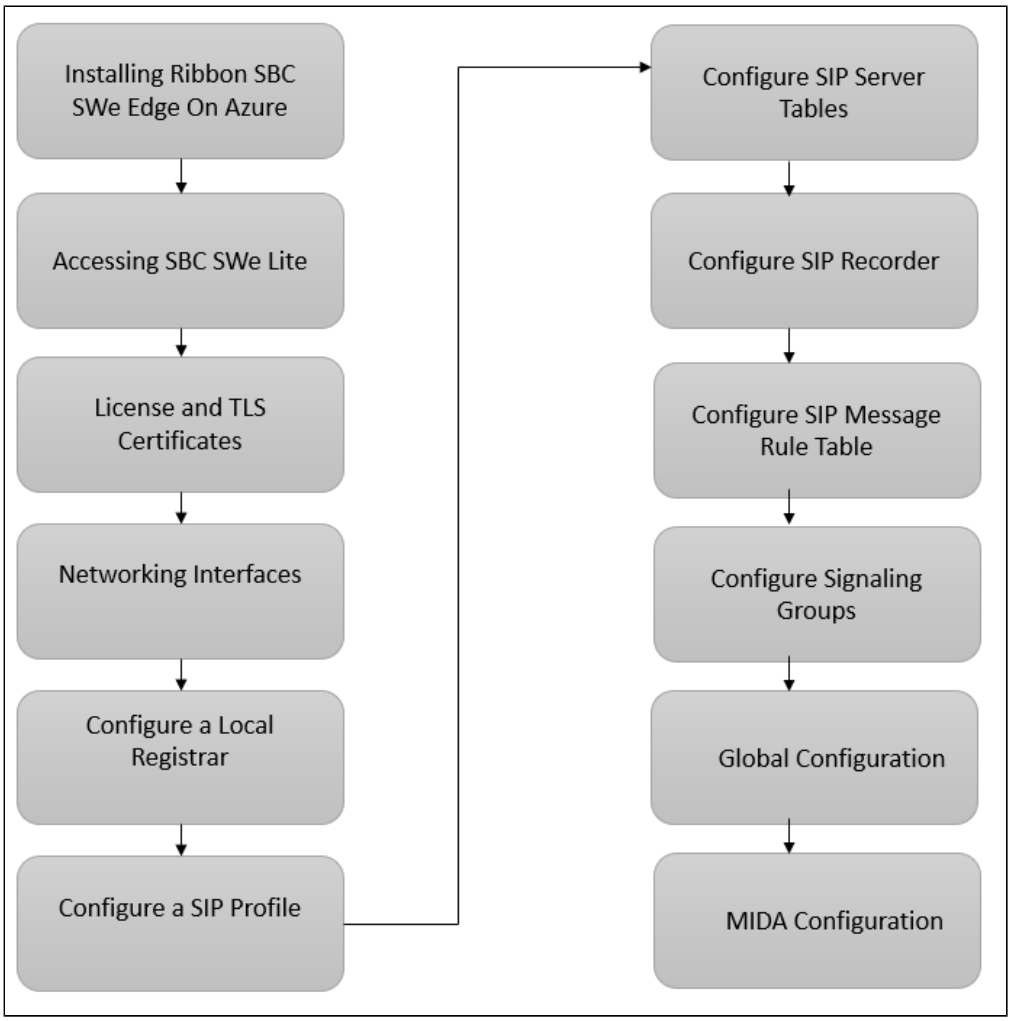


Signaling and Media Flow



Document Workflow

To successfully configure the MIDA Recorder, use the following workflow. Ribbon recommends that you complete the procedures in each section in the following sequence.



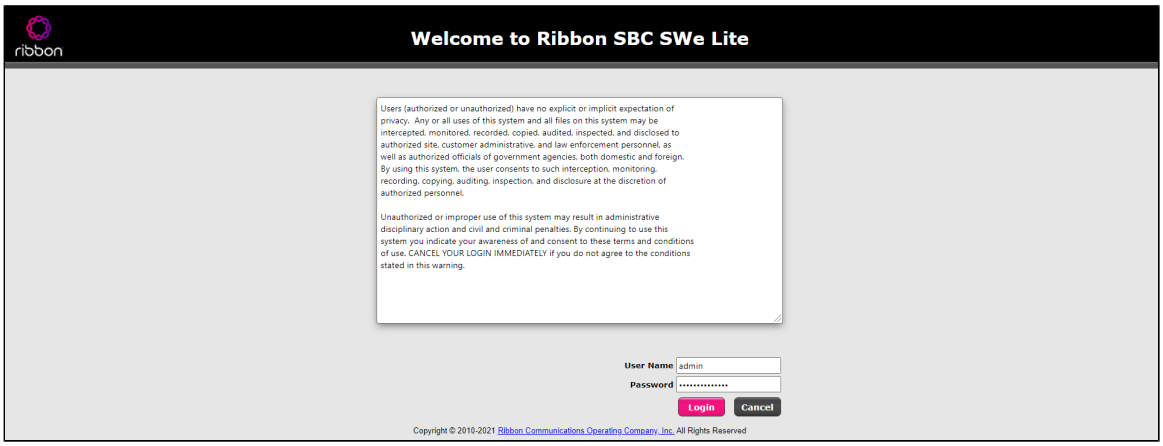
Ribbon SBC SWe Edge Configuration

Installing Ribbon SBC SWe Edge On Azure

The SBC SWe Edge is available for deployment in Azure. It is created as a virtual machine (VM) hosted in Azure. To deploy an SBC SWe Edge instance, refer to Deploying an SBC SWe Edge from the Azure Marketplace.

Accessing SBC SWe Lite

1. Open any browser and enter the SBC SWe Lite IP address.
2. Click **Enter** and log in with a valid User ID and Password.

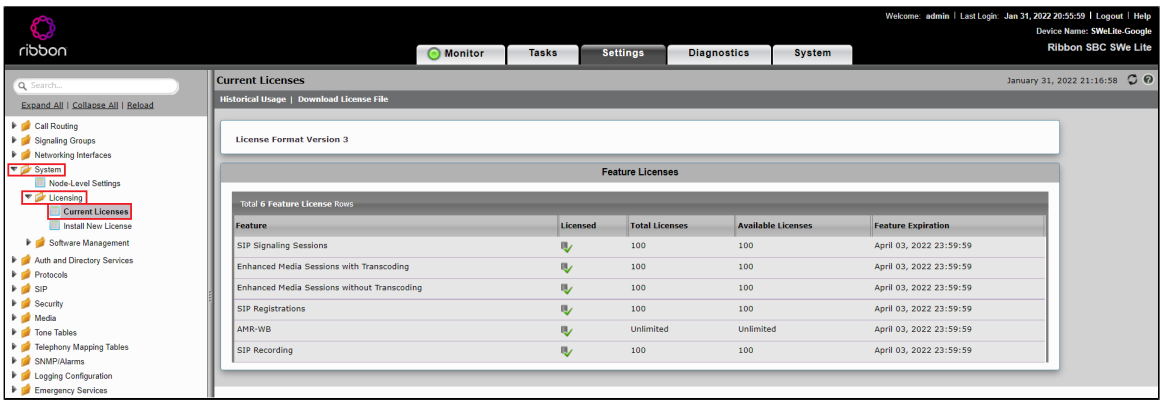


License and TLS Certificates

View License

This section describes how to view the status of each license along with a copy of the license keys installed on your SBC. The **Feature Licenses** pan el enables you to verify whether a feature is licensed, along with the number of remaining licenses available for a specific feature at run-time.

From the **Settings** tab, navigate to **System > Licensing > Current Licenses**.

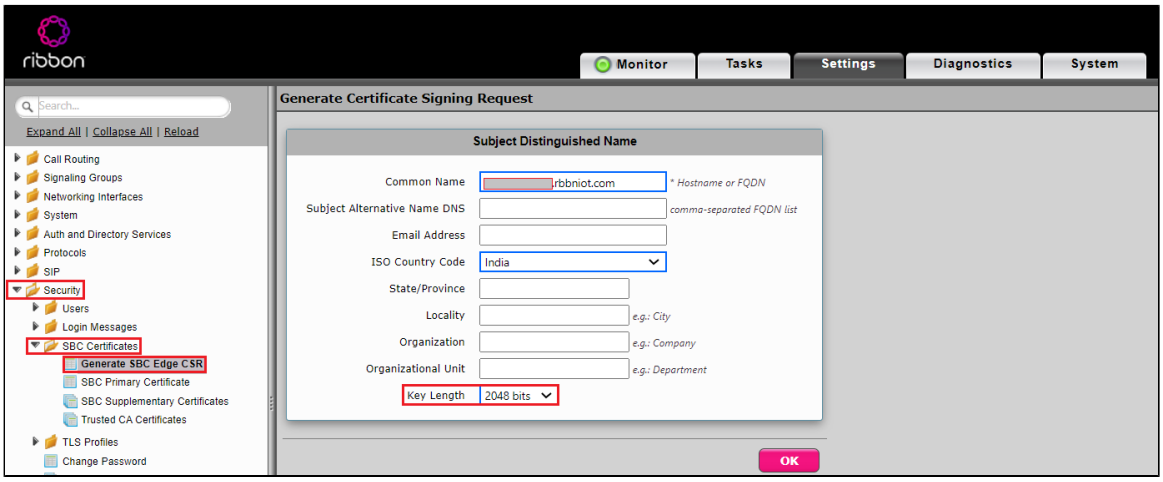


For more details on Licenses, refer to Working with Licenses.

SBC Certificate

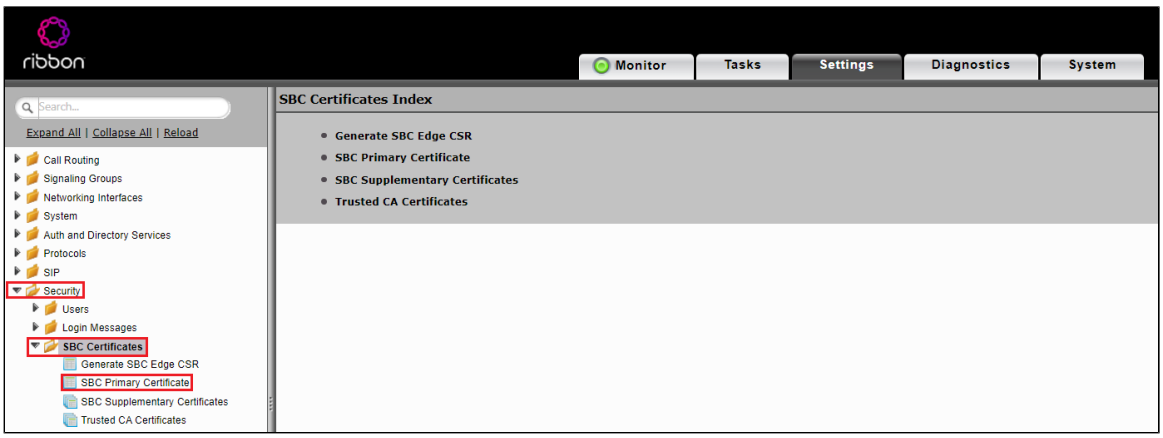
1. From the **Settings** tab, navigate to **Security > SBC Certificates > Generate SBC Edge Certificates.**

2. Provide the **Common Name** of the SBC that includes Host and Domain.
3. Set Key Length to 2048 bits.
4. Provide the location information.
5. Click OK. The CSR generates and displays in the result text box.



Provide the CSR to the Certificate Authority (CA) . CA generally provides the following certificates:

- SBC Certificate
- CA's Root Certificate
- Intermediate Certificate



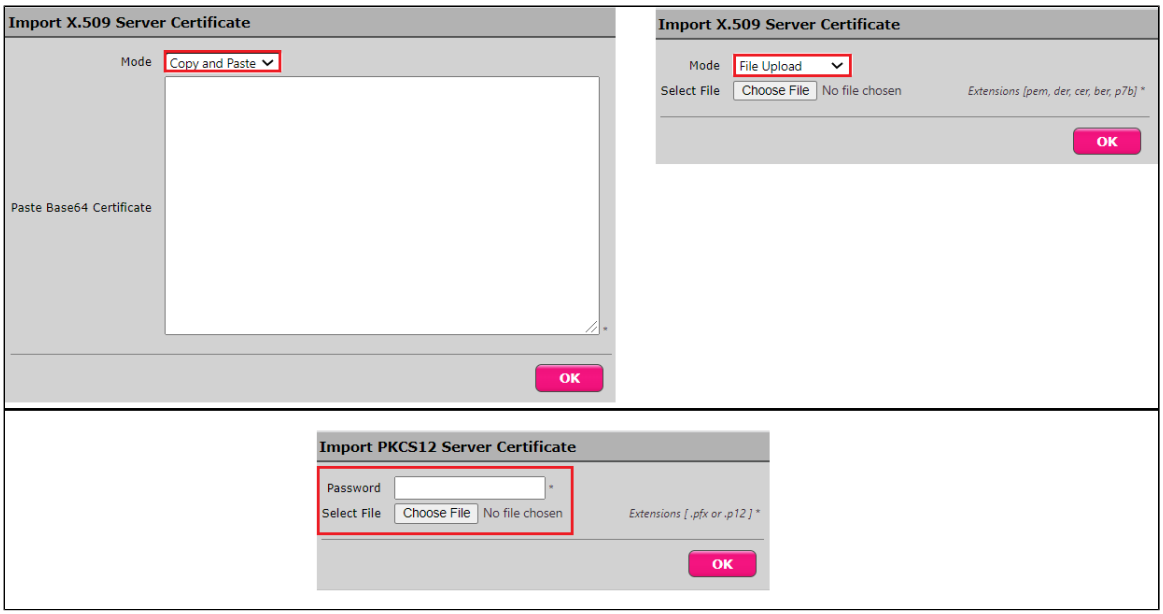
You can import the SBC Primary Certificate in the following ways.

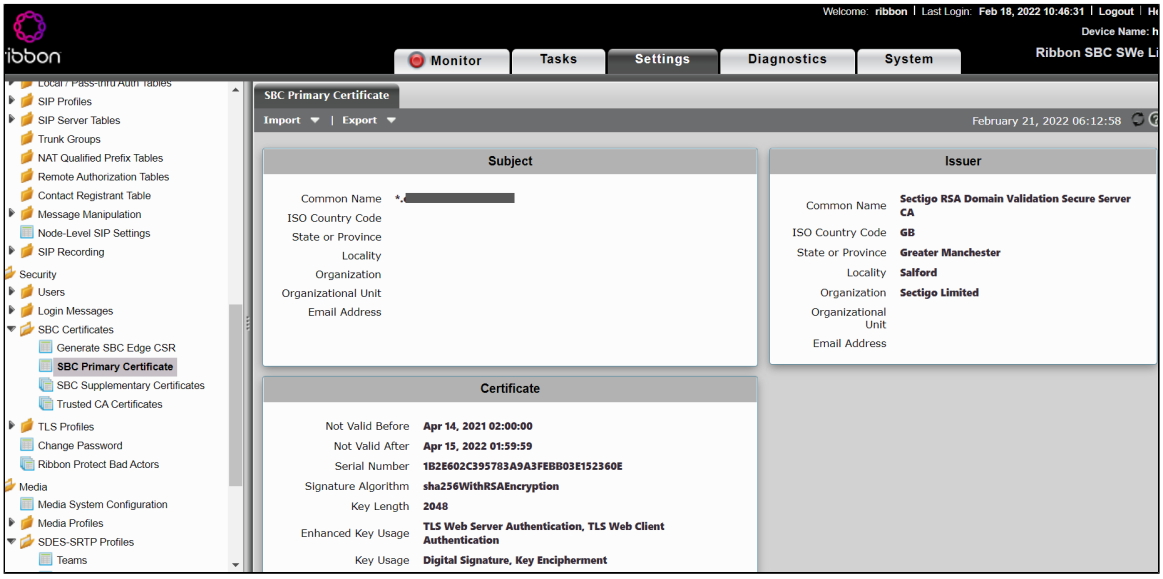
To import an X.509 signed certificate:

1. Select **X.509 Signed Certificate** from the Import menu at the top of the page.
2. Choose the import mode (**Copy and Paste** or **File Upload**) from the Mode pull-down menu.
3. If you choose **File Upload**, use the Browse button to find the file, and click **OK**.
4. If you choose **Copy and Paste**,
    a. Open the file in a text editor and paste the contents into the Paste Base64 Certificate text field.
    b. Click **OK**.

To import a PKCS12 Certificate and Key:

1. Select **PKCS12 Certificate** and **Key** from the Import menu at the top of the page.
2. Enter the password to export the certificate in the **Password** field.
3. Find the PKCS certificate and key file and click **OK**.





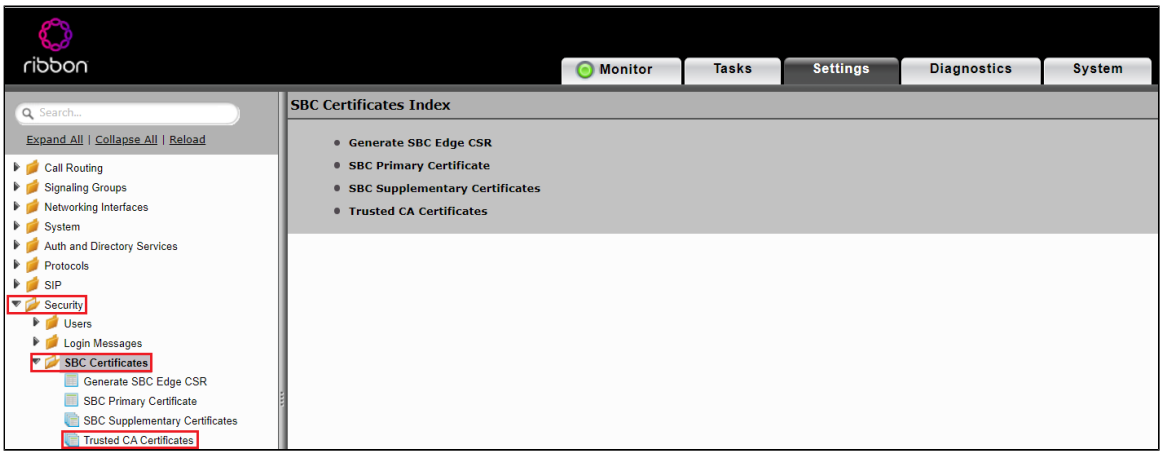
Trusted CA Certificates

A Trusted CA Certificate is issued by a Trusted Certificate Authority. Trusted CA Certificates are imported to the SBC SWe Edge to establish their authenticity on the network.

1. For TLS to work, a **Trusted CA (Certificate Authority)** is required. For this interop, GoDaddy is used as **Trusted CA**.
2. Add an entry in the Public DNS to resolve Ribbon SBC SWe Edge FQDN to **Public IP Address**.
3. Ensure that you have the following certificates as part of the **root certificate trust**.

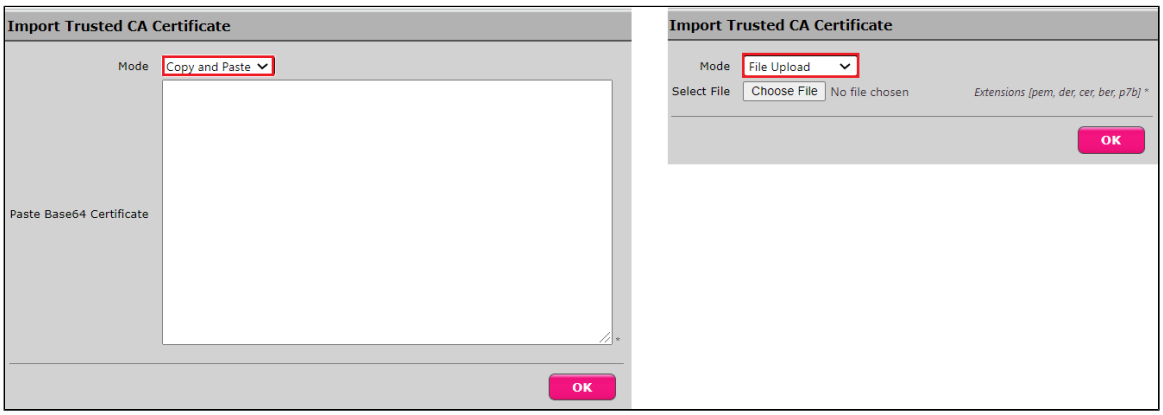
- GTS Root R1
- GlobalSign R2 (if required)

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**, select the **File** button to find the file.
4. Click **OK**.



When the **Verify Status** field in the Certificate panel indicates **Expired** or **Expiring Soon**, replace the Trusted CA Certificate. You must delete the old certificate to successfully import a new certificate.

Most Certificate Vendors sign the SBC Edge certificate with an intermediate certificate authority. There is at least one, but there could be several intermediate CAs in the certificate chain. When importing the Trusted Root CA Certificates, import the root CA certificate and all Intermediate CA certificates. Failure to import all certificates in the chain causes the import of the SBC Edge certificate to fail. Please refer to Unable To Get Local Issuer Certificate for more information.

Networking Interfaces

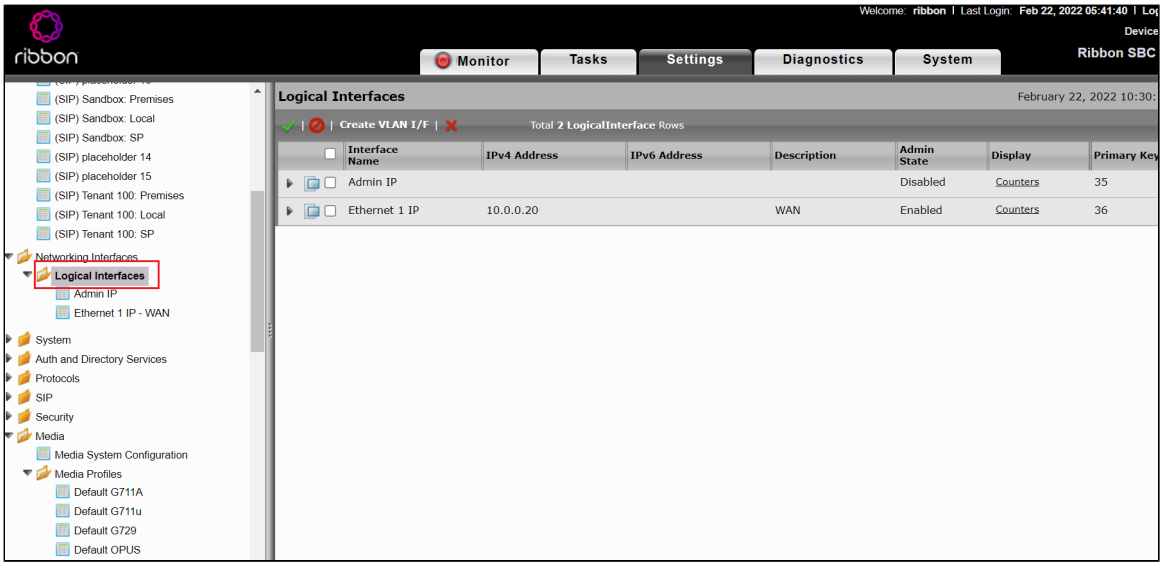
The SBC SWe Lite supports five system-created logical interfaces known as Administrative IP and Ethernet 1 IP. In addition to the system-created logical interfaces, the Ribbon SBC SWe Lite also supports user-created VLAN logical sub-interfaces.

Access the Administrative IP and Ethernet 1 IP from the **Settings** tab, and then navigate to **Networking Interfaces > Logical Interfaces.**

Ribbon recommends that you use two interfaces with two different VLANs instead of configuring a single interface.

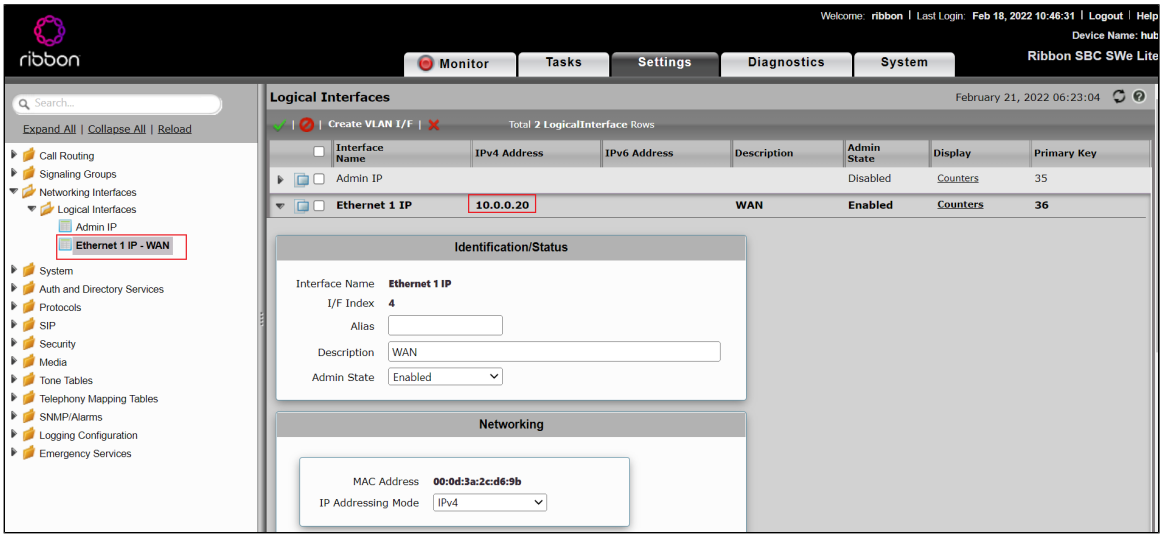
Administrative IP

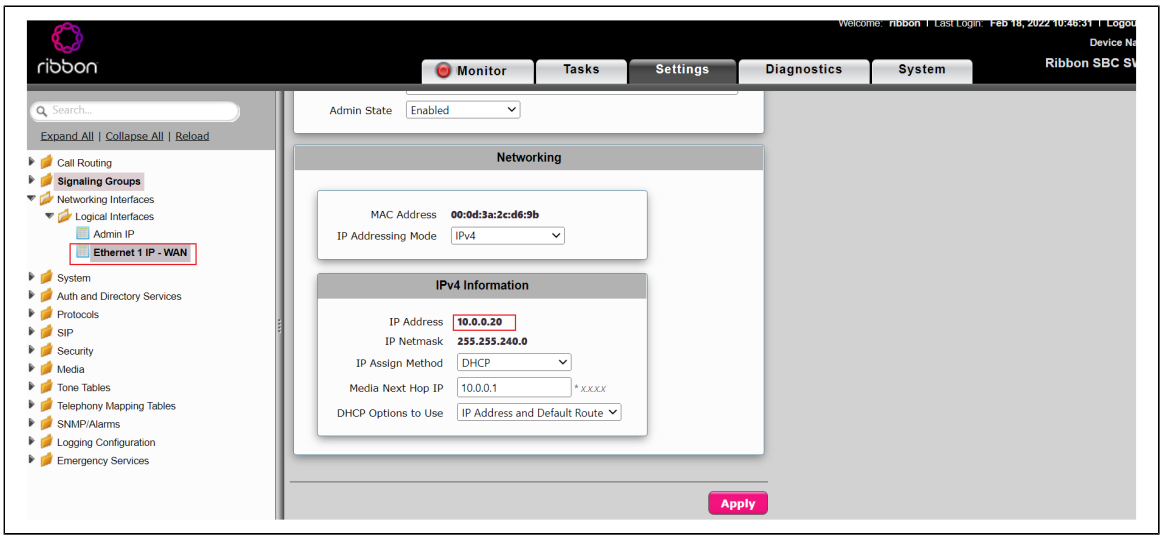
The SBC SWe Lite system supports a logical interface called the Administrative IP (Admin IP), which is also known as the Management IP. A Static IP or DHCP is used to run the Initial Setup of the SBC SWe Lite system.



Ethernet 1 IP

Ethernet 1 IP is assigned an IP address for transporting all the VoIP media packets (for example, RTP and SRTP) and all protocol packets (for example, SIP, RTCP, and TLS). The DNS servers of the customer's network must map to the SBC SWe Lite system hostname to this IP address. In the default software, **Ethernet 1 IP** is enabled, and an IPv4 address is acquired through a connected DHCP server. This IP address is used for performing the Initial Setup on the SBC SWe Lite.





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 that you can only access through one point or one interface, that is, single path access or a default route.

Derive the **Private IP address** and **Gateway** for each interface on AWS.

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'.

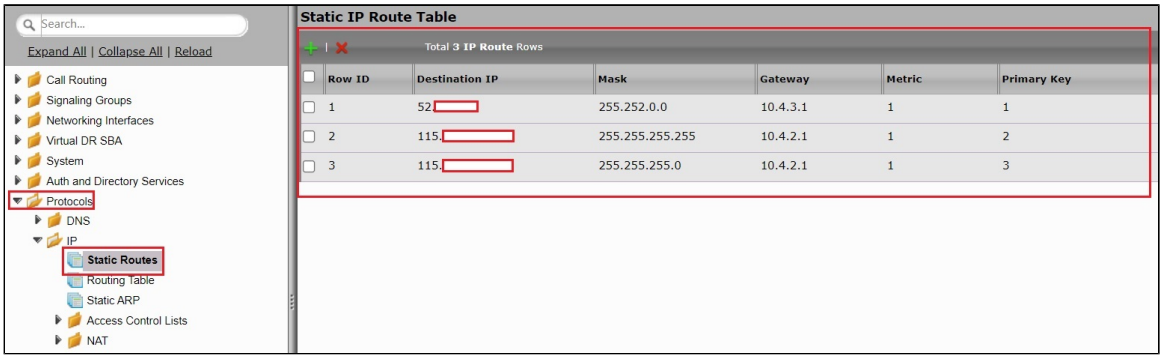
Gateway

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

Metric

Specifies the cost of this route and therefore indirectly specifies 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 to dynamic routes.

From the **Settings** tab, navigate to **Protocols > IP > Static Routes** to configure static routes. Click the + icon to add the entries.



Configure a Local Registrar

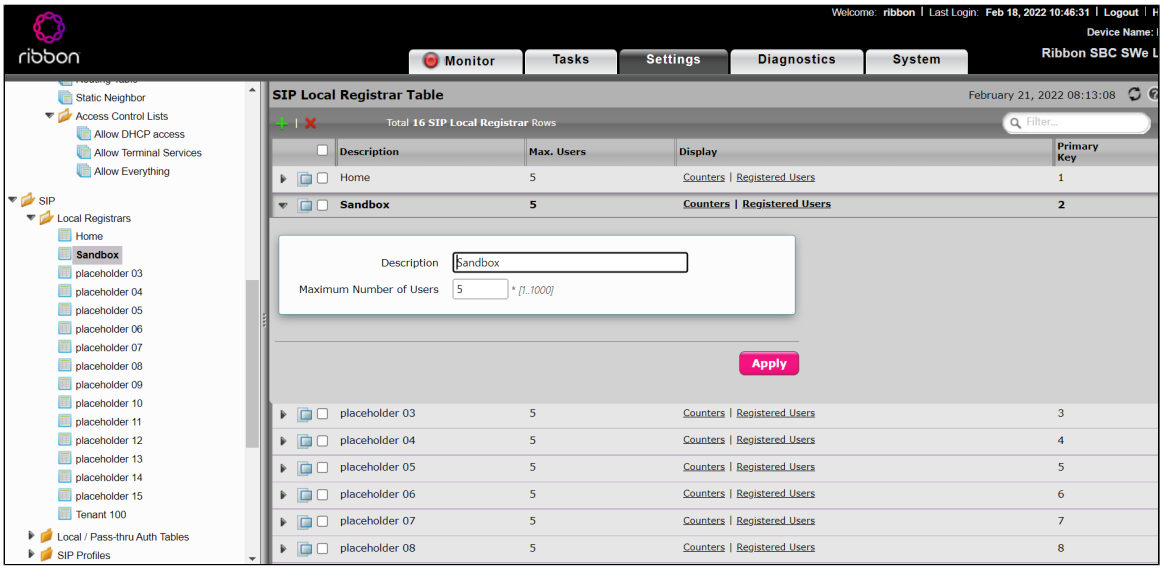
SIP Registration allows users to upload their current locations for use by proxy servers. Registration creates bindings in a location service for a particular domain that associates an address-of-record URI with one or more contact addresses.

Registration entails sending a **REGISTER** request to a special type of User-Agent Server (UAS) known as a registrar. A registrar acts as the front-end to the location service for a domain, reading and writing mappings based on the contents of REGISTER requests.

The Broadsoft AS handles the registration for its users with **authentication**.

> Registration on SBC Edge with the **reg-key** parameter will provide support in the upcoming release.

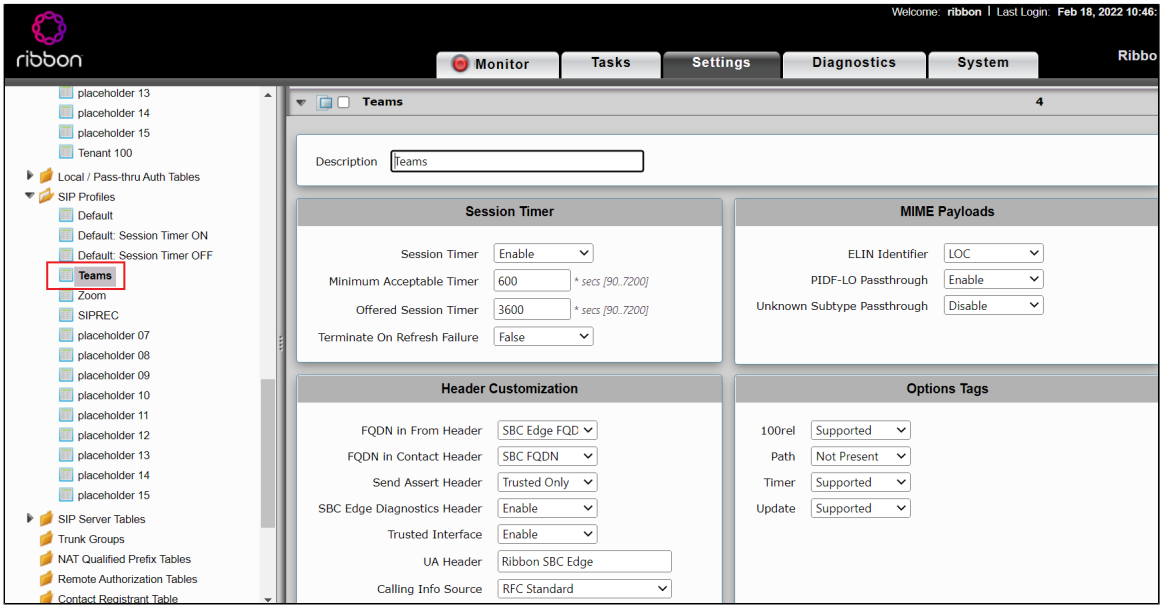
To configure a local registrar, navigate to **SIP > Local Registrars**.

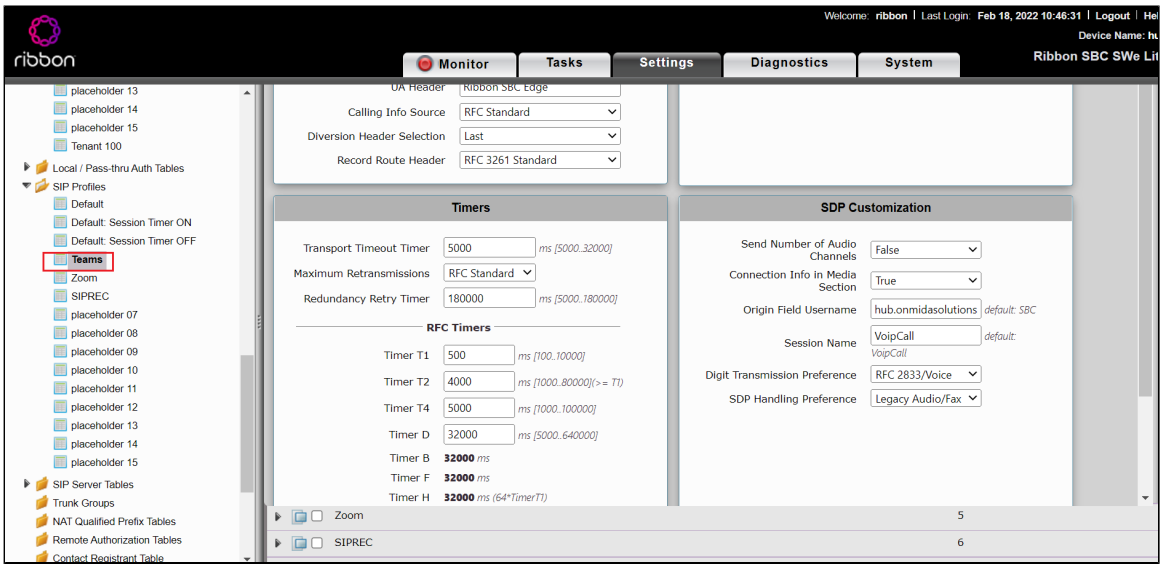


Configure a SIP Profile

SIP Profiles control the 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.

To configure a profile, navigate to **SIP > SIP Profiles**.





Configure SIP Server Tables

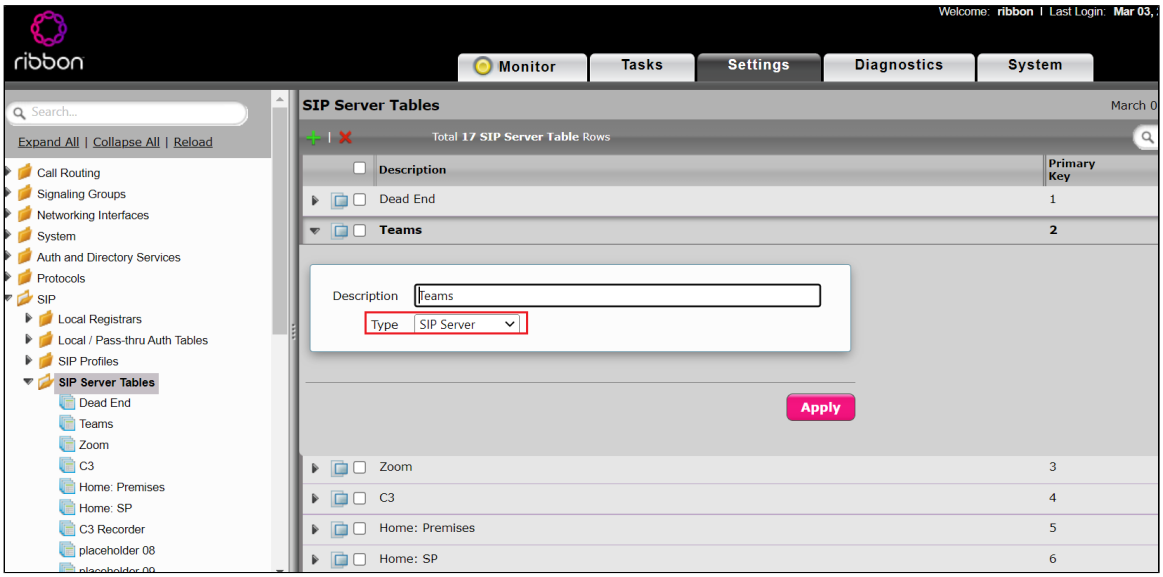
SIP Server Tables contain information about the SIP devices connected to the SBC Edge. The tables provide information about the IP addresses, ports, and protocols used to communicate with each server.

Use the following SIP devices:

- **Teams**: Provides information about the Teams endpoint.
- **C3**: Provides information about the C3 Recorder.
- **Service provider**: Provides information about Service Provider endpoints.
- **Premises**: Provides information about Premises endpoints.

To configure the tables,

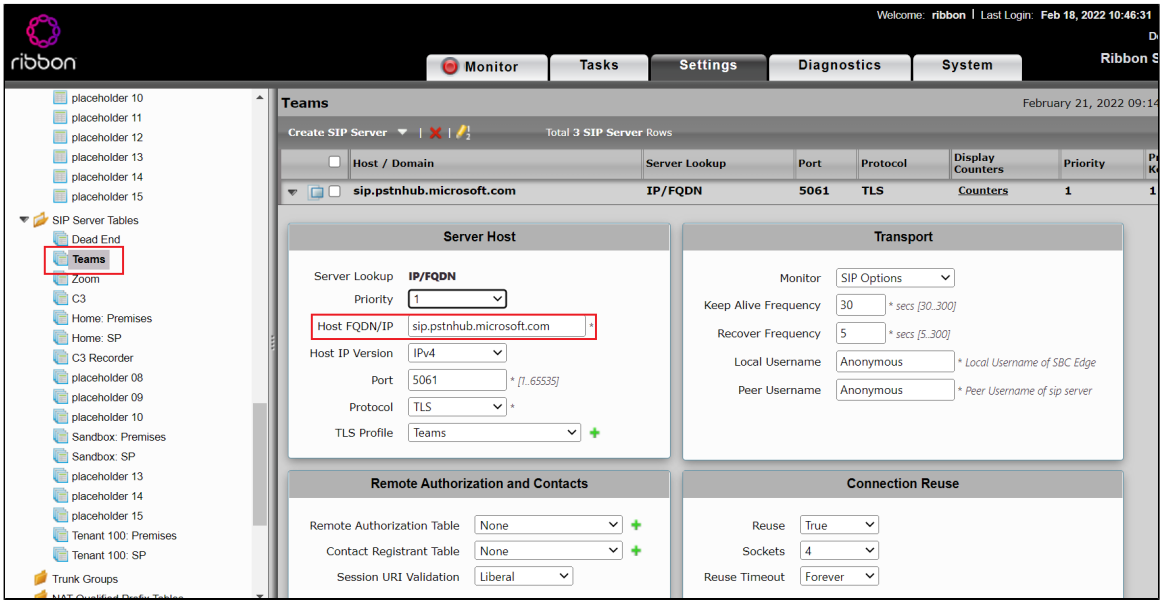
1. Navigate to **SIP > SIP Server Tables**.
2. Provide a name for the SIP Server.
3. From the Type drop-down list, choose **SIP Server.**
4. Click OK.



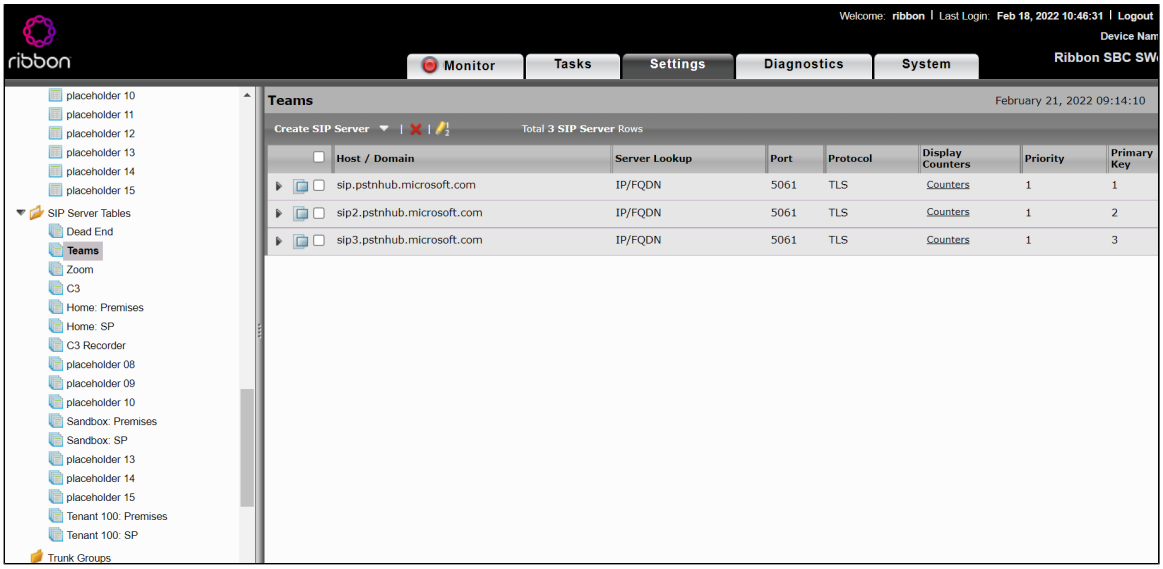
SIP Server Table Entry for Teams

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

3. Enable **OPTION** pings by selecting SIP Options from the Monitor field.
4. Click OK.

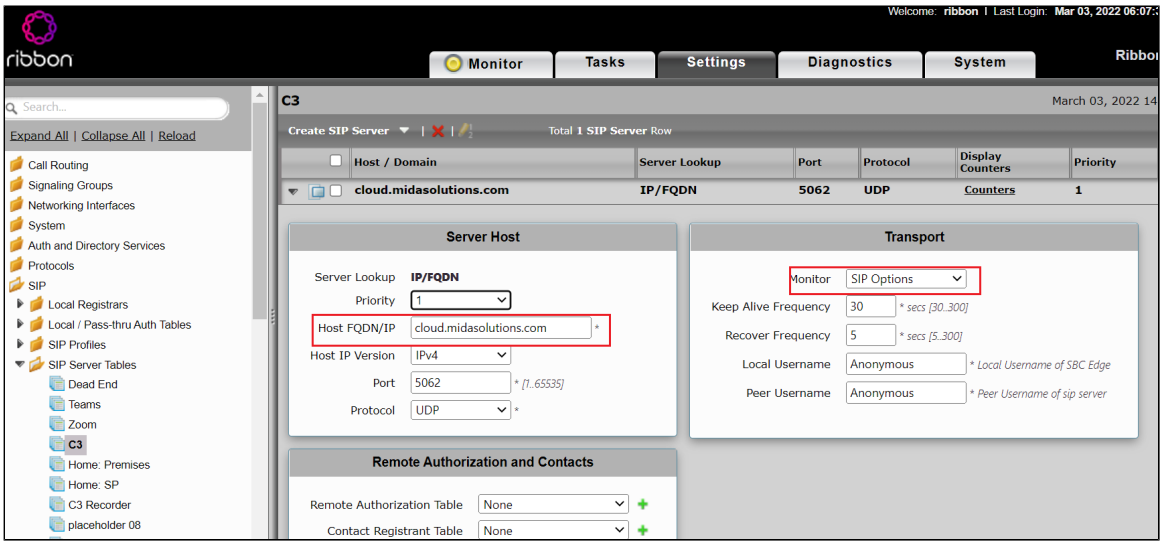


Note
Repeat the same steps for different HOST FQDN.



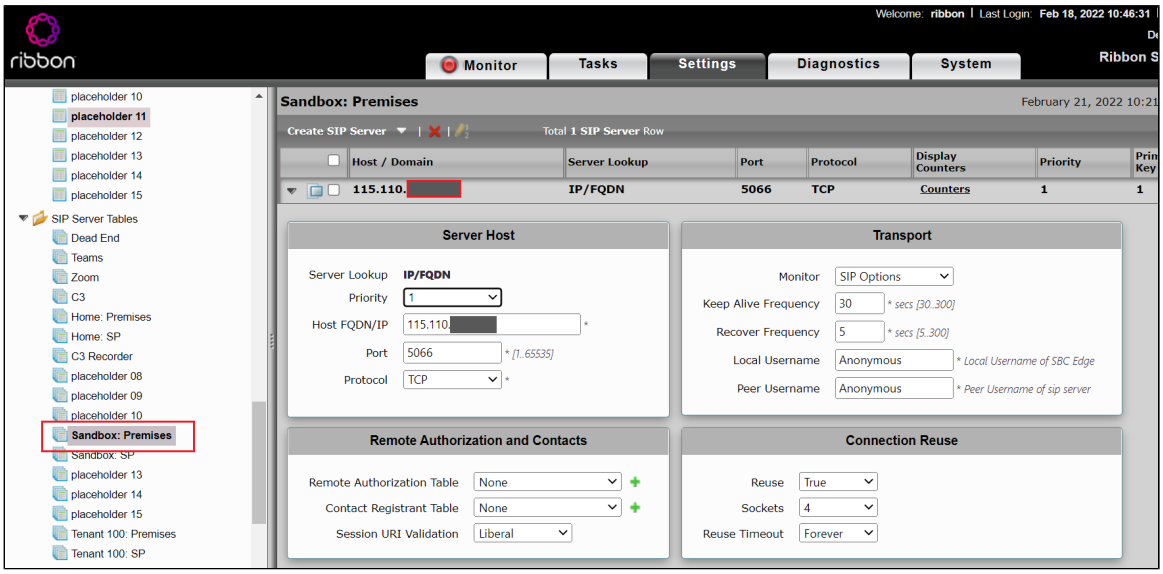
SIP Server Table Entry for C3 Recorder

1. Click on the SIP Server Table that you just created.
2. From the Create SIP Server drop-down list, select **IP/FQDN.**
3. Enable **OPTION** pings by selecting SIP Options from the Monitor field.
4. Click OK.



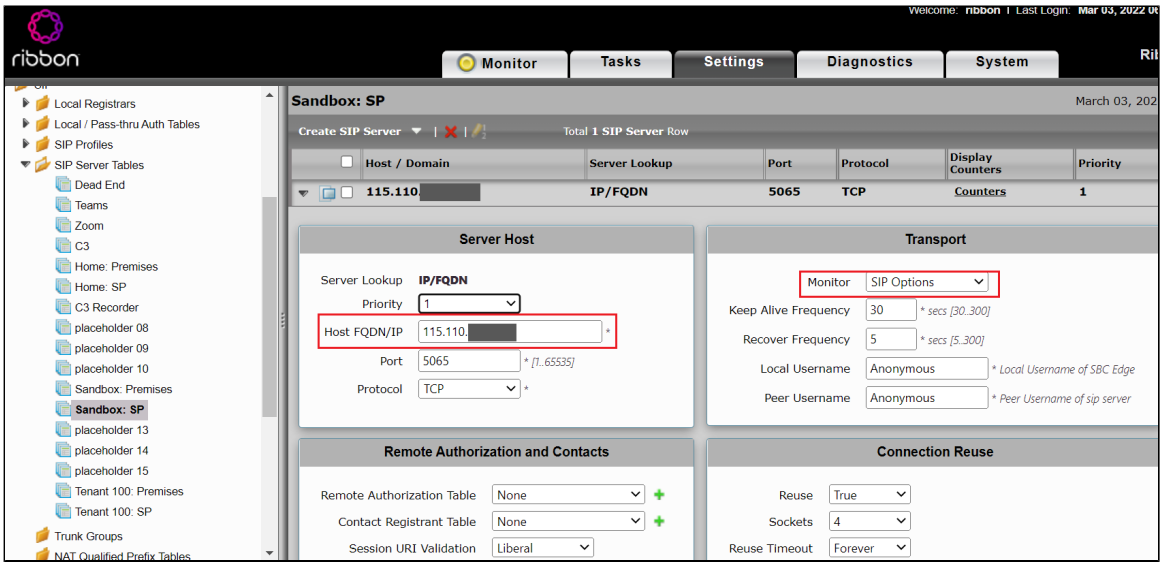
SIP Server Table Entry for Premises

1. Click on the SIP Server Table that you just created.
2. From the Create SIP Server drop-down list, select **IP/FQDN.**
3. Enable **OPTION** pings by selecting SIP Options from the Monitor field.
4. Click OK.



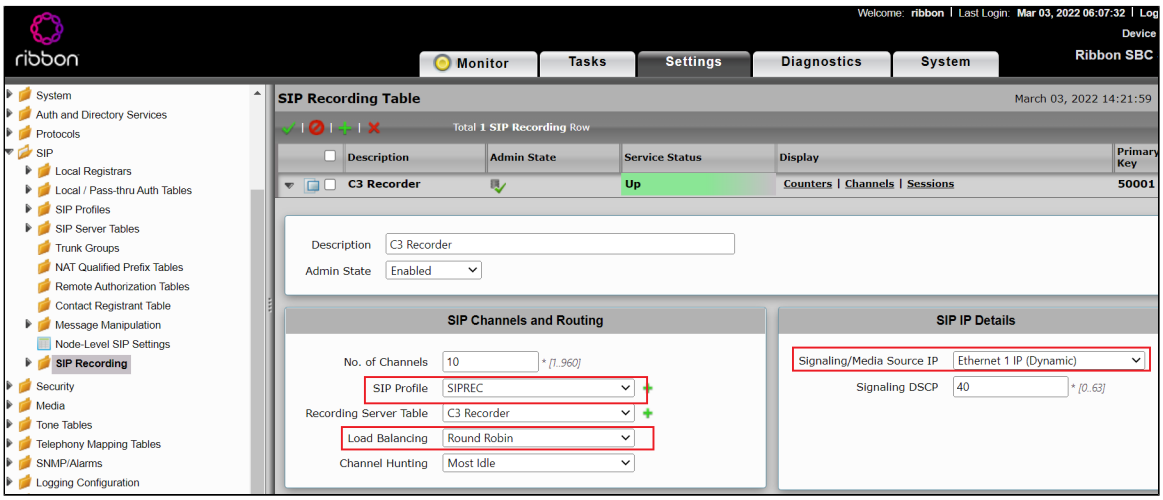
SIP Server Table Entry for Service Provider

1. Click on the SIP Server Table that you just created.
2. From the Create SIP Server drop-down list, select **IP/FQDN.**
3. Enable **OPTION** pings by selecting SIP Options from the Monitor field.
4. Click OK.

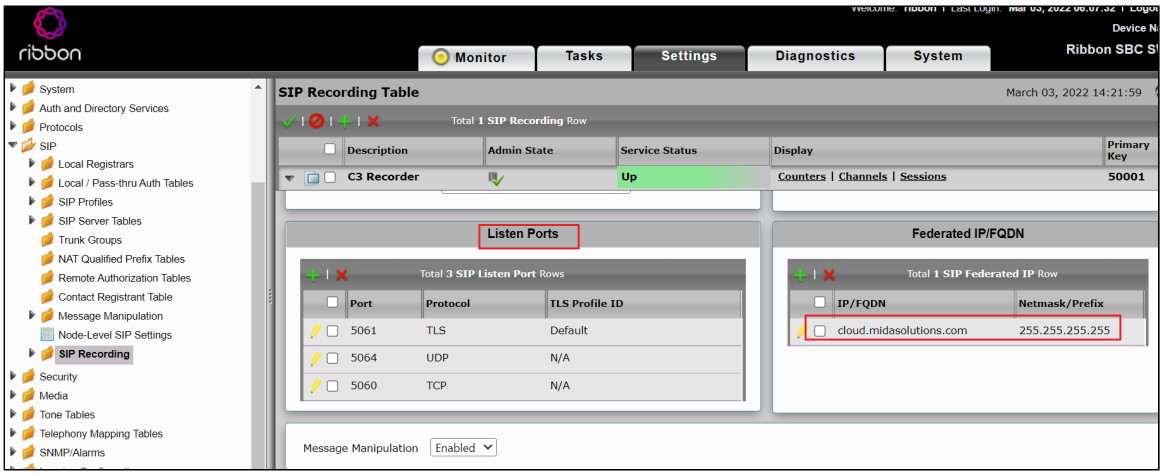


Configure SIP Recorder

1. Navigate to **SIP > SIP Recording.**
2. Provide a name for the Recorder Server.
3. From the Type drop-down list, choose **SIP Profile.**
4. From Load Balancing drop-down list, choose **Round Robin.**



1. Provide Listening ports for TLS/UDP/TCP.
2. Provide Federated IP.
3. Click OK.



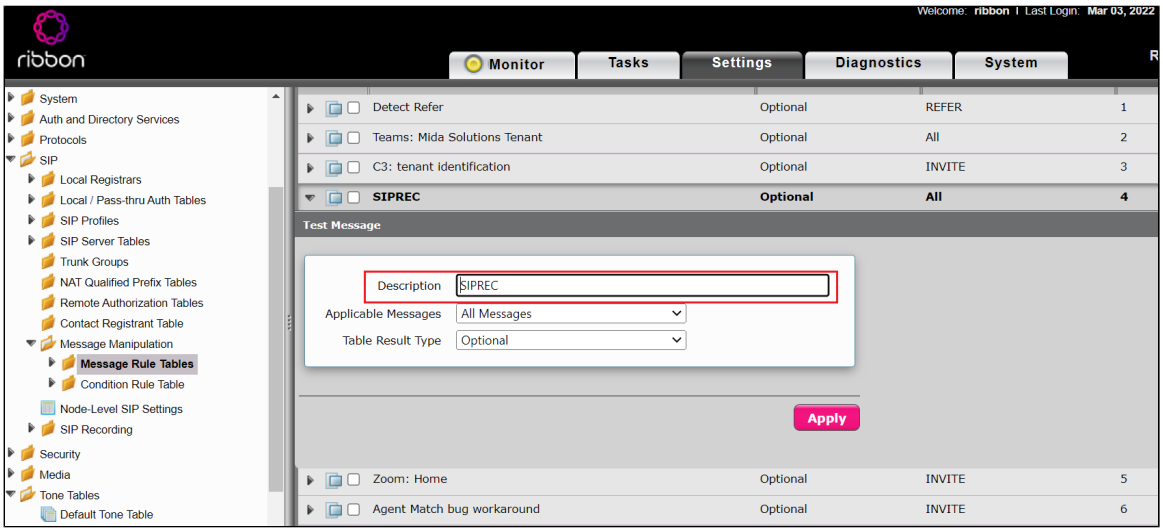
Configure SIP Message Rule Table

The SBC Edge allows a maximum of 100 SIP Message Rule Tables and a maximum of 32 SIP Message rules per table. The maximum of 32 SIP Message rules per table includes all SIP rule types: Header, Request, Status, and Raw.

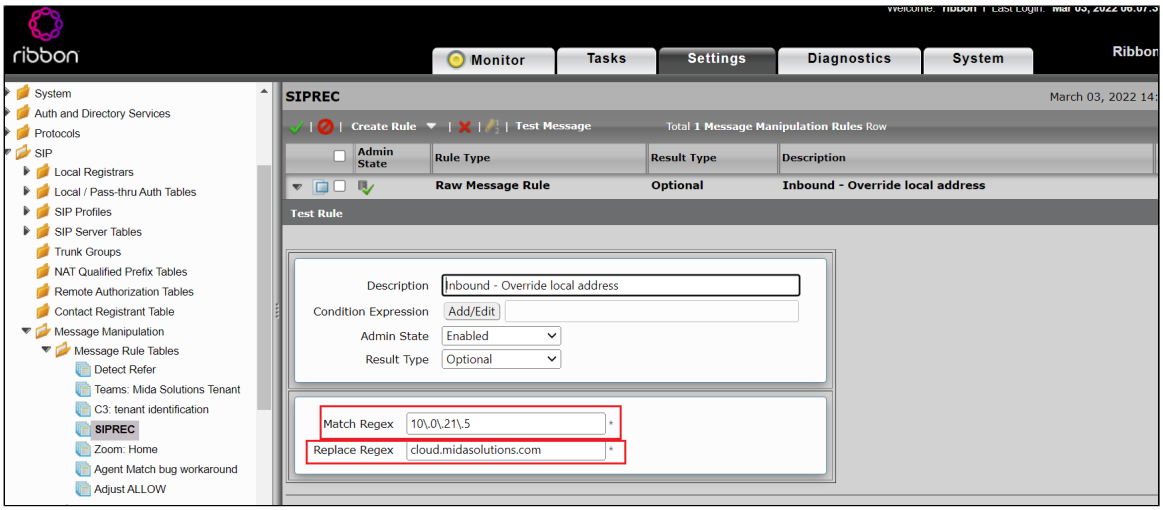
To configure the table, navigate to **SIP > Message Manipulation > Message Rule Tables**.

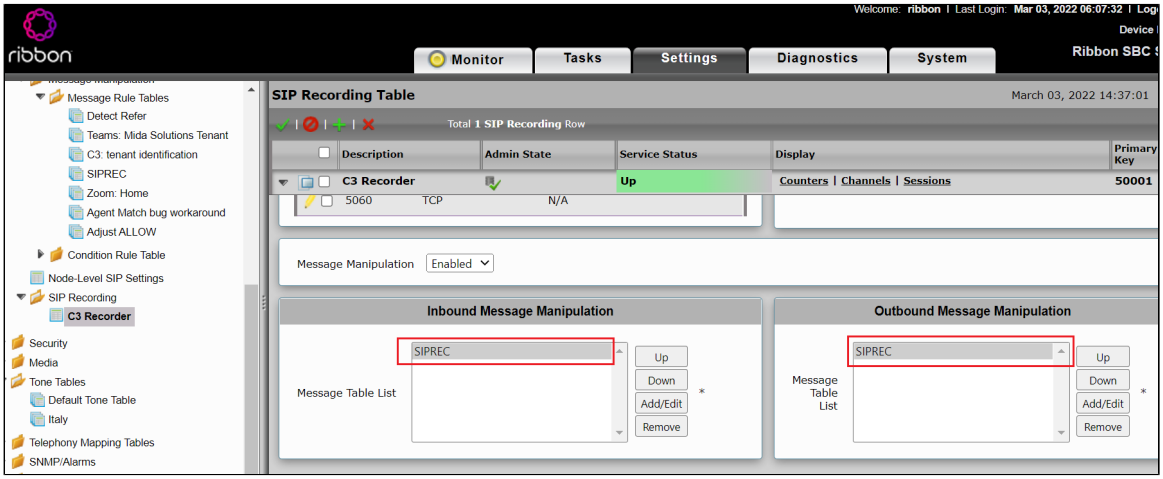
SIPREC is used to convert an IP address to FQDN for the C3 Recorder.

1. Enter **SIPREC** in the Description field.
2. From the drop-down list, select the values for the **Applicable Messages** and **Table Result Type** fields.



1. Expand the Message Rule table, select SIPREC, and select the values for **Match Regex** and **Replace Regex** from the drop-down list.
2. Attach the message rule to the **SIP Recorder.**

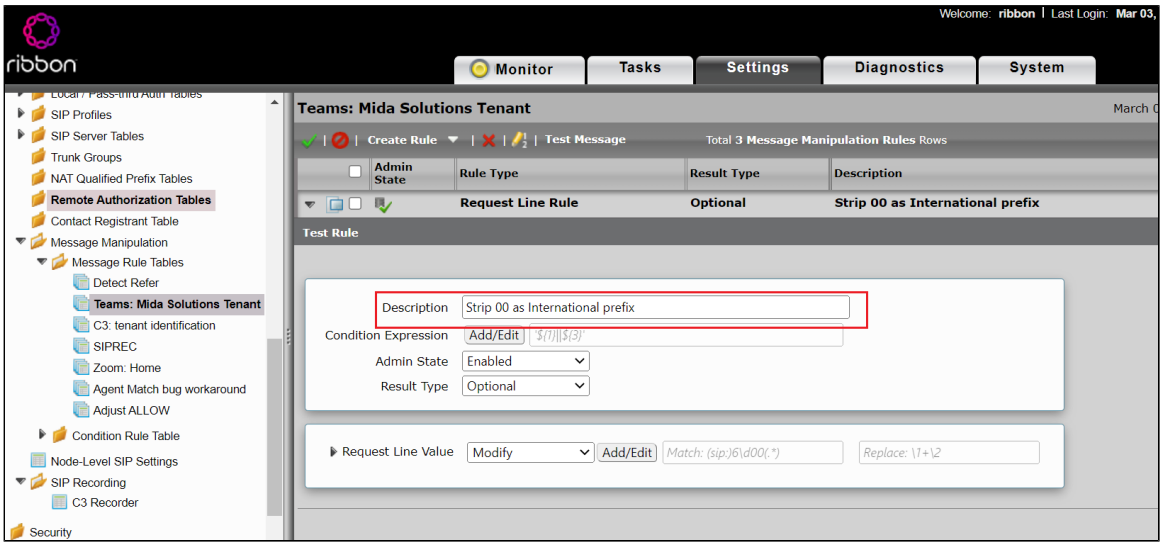




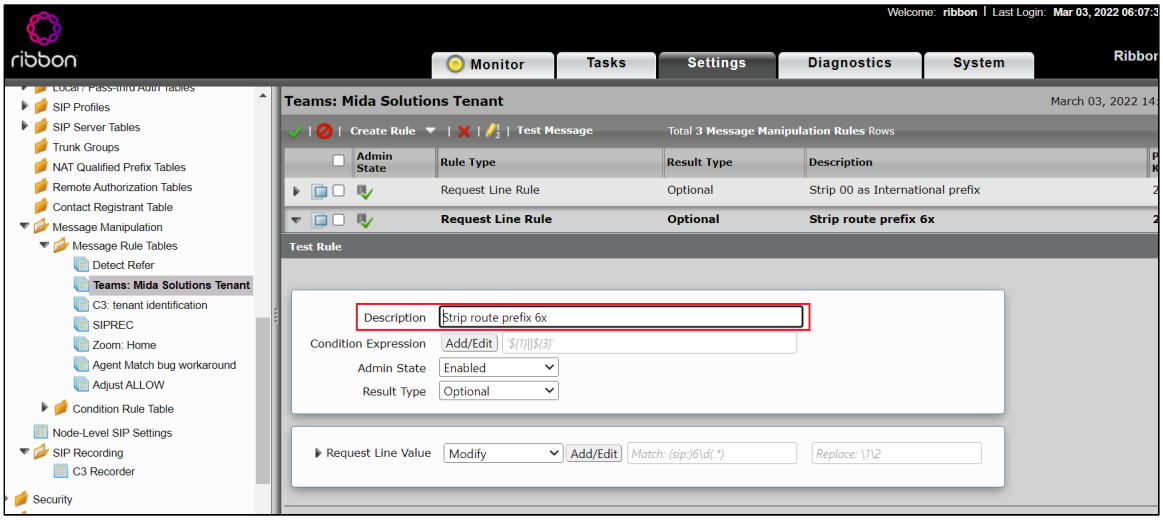
Teams MIDA Solutions Tenant

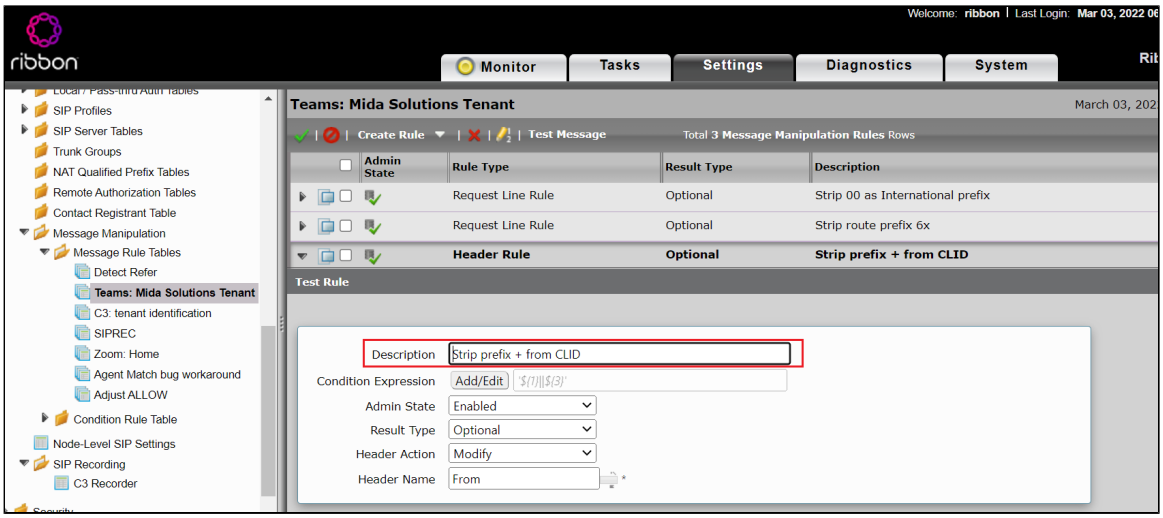
To configure this rule,

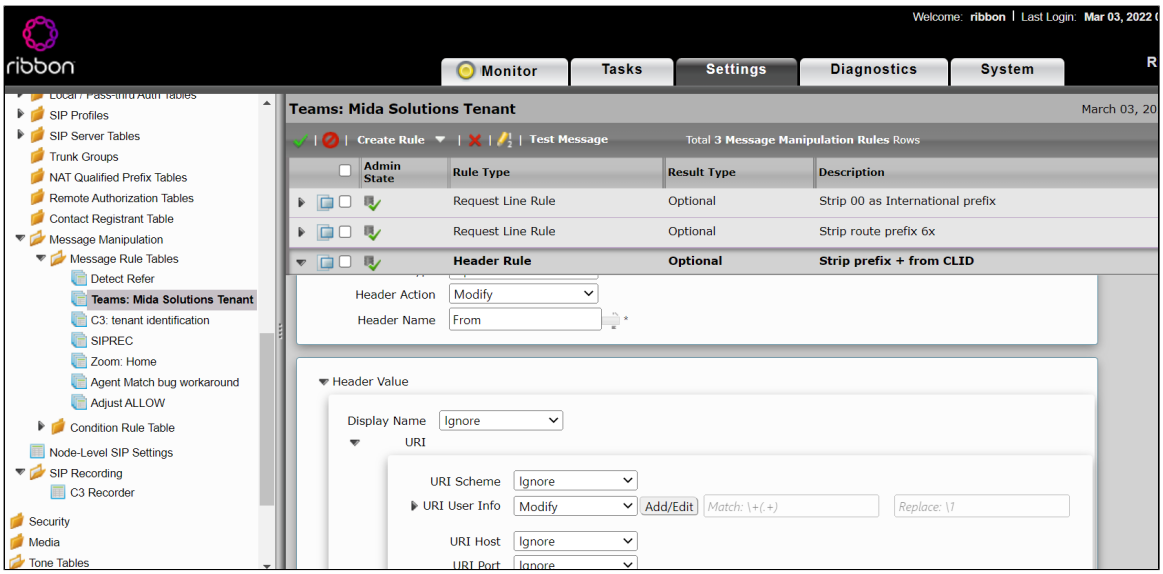
1. Navigate to **SIP > Message Manipulation > Message Rule Tables**.
2. Add **Strip 00 as International prefix** in the **Description** field.



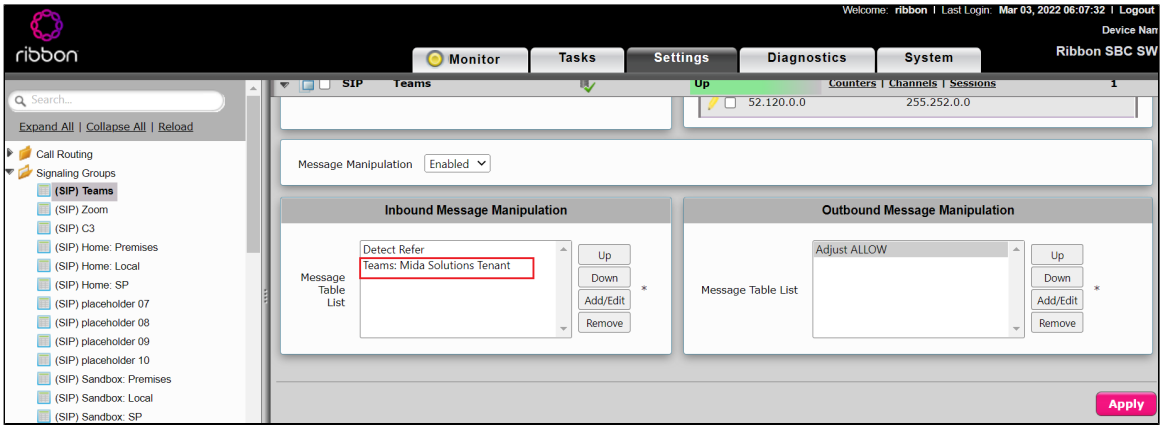
1. Strip route prefix **6x.**
2. Strip **prefix + from Call ID.**







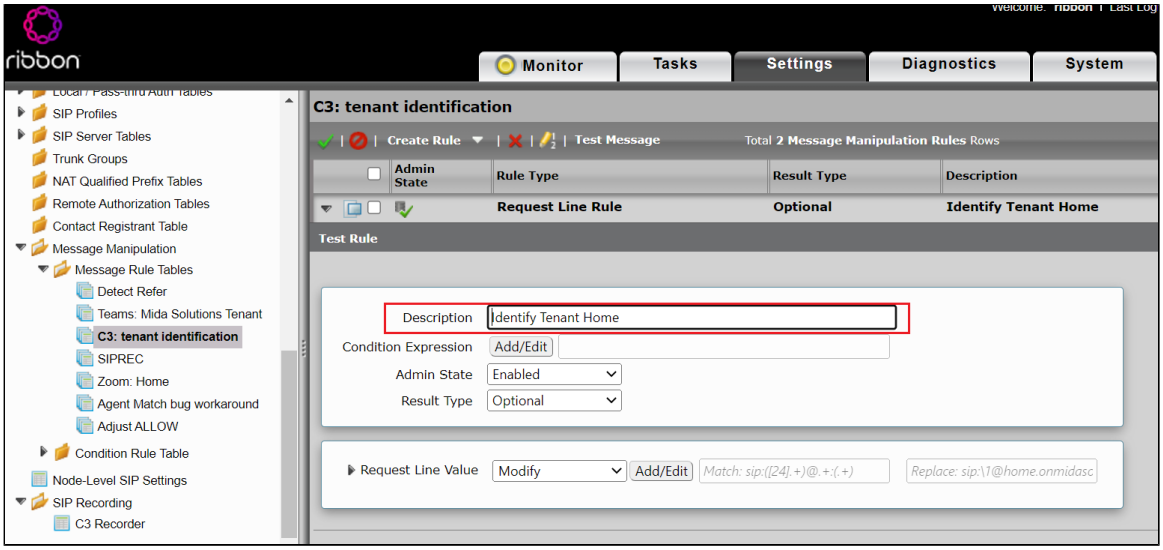
1. Attach created message rule to the **Teams Signaling group.**

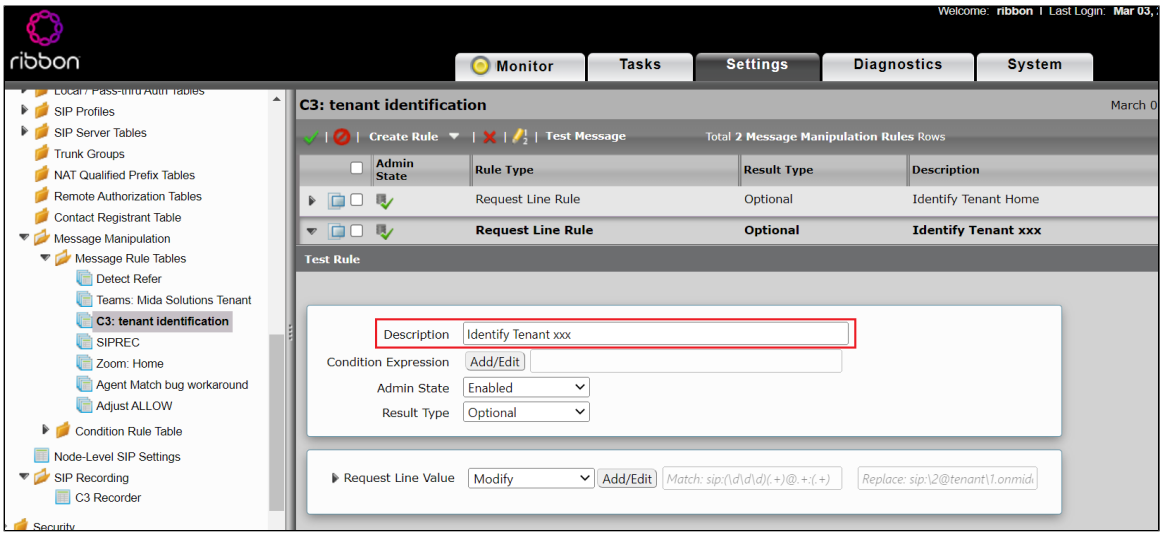


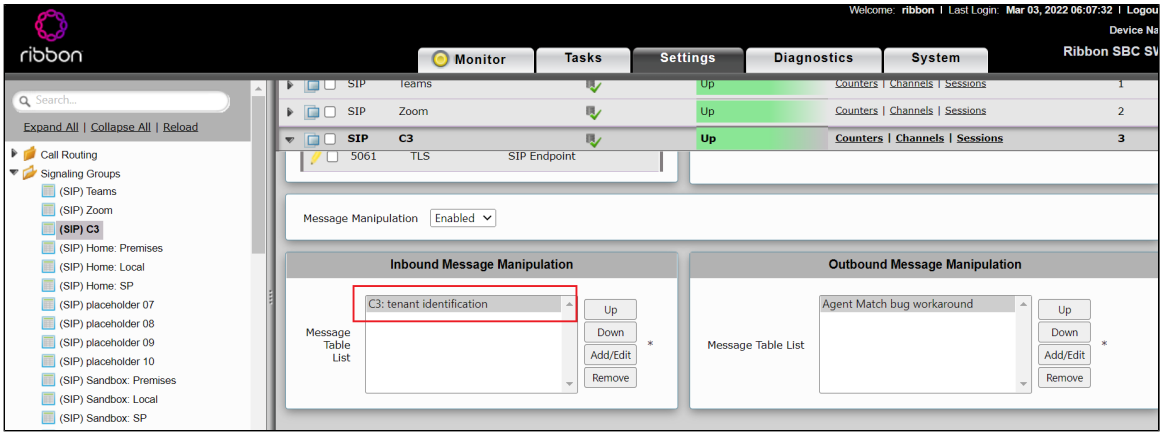
C3: tenant identification

To configure this rule,

1. Navigate to **SIP > Message Manipulation > Message Rule Tables.**
2. Tenant Home.
3. Identify Tenant xxx.
4. Attach created message rule to the **C3 Recorder.**



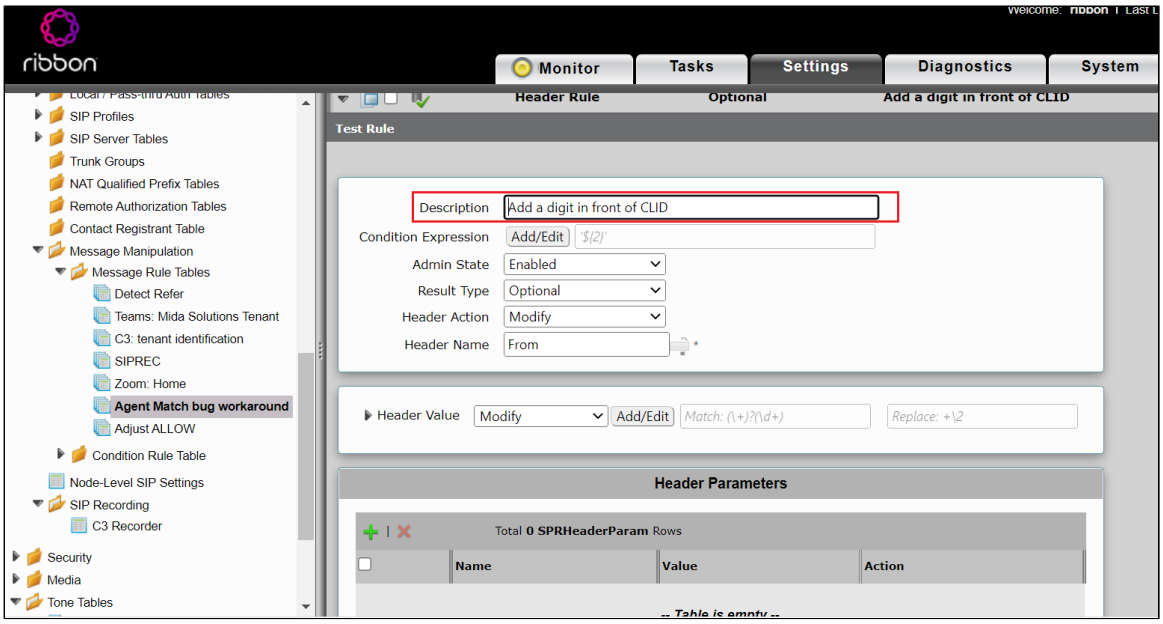


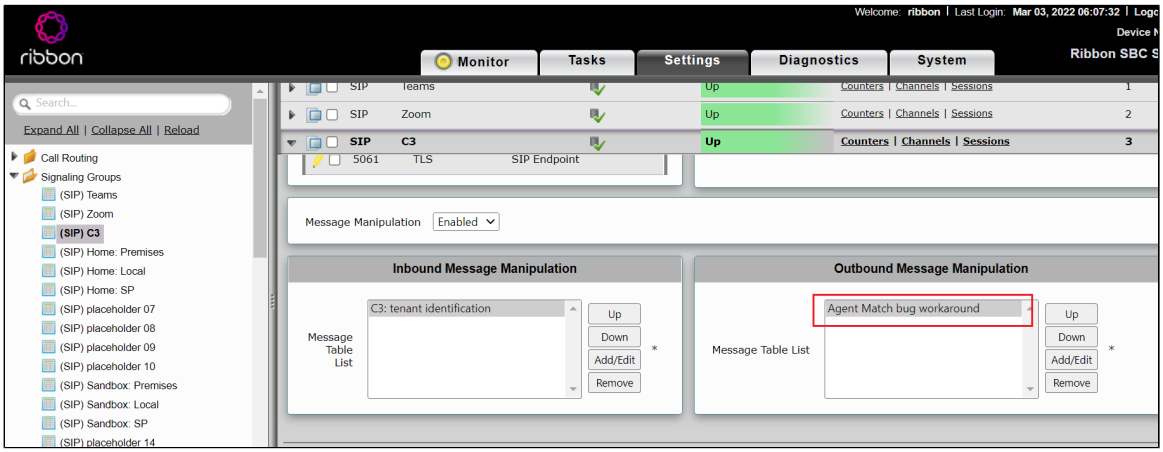


Agent Match bug workaround

To configure this rule,

1. Navigate to **SIP > Message Manipulation > Message Rule Tables.**
2. Add a digit in front of CLID.
3. Attach created message rule to the **C3 Recorder.**

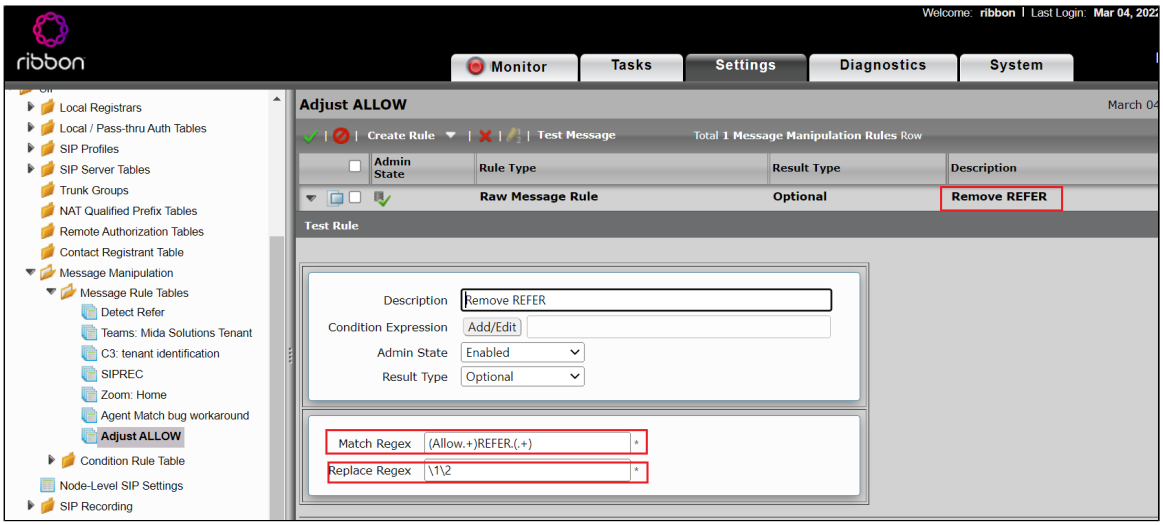


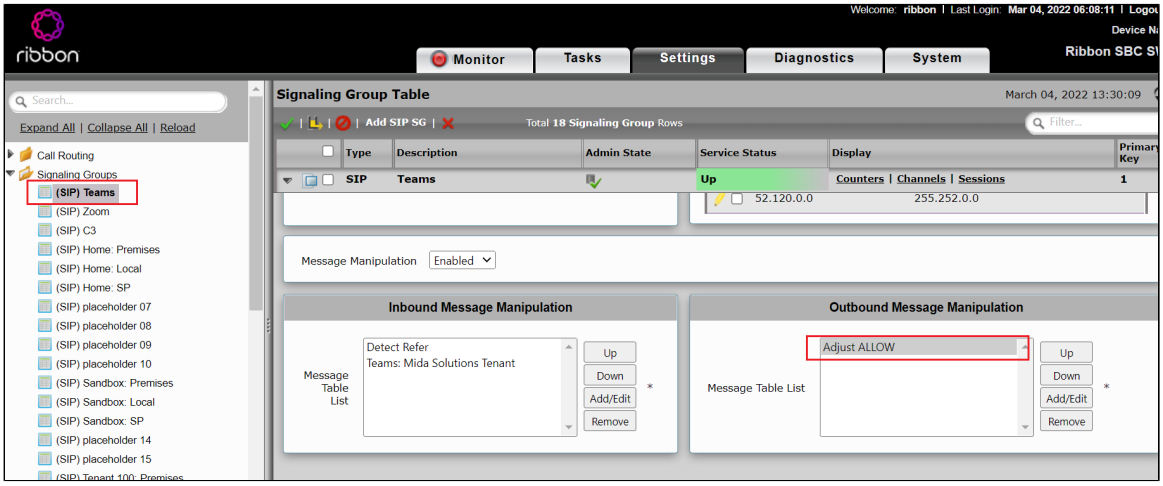


Adjust ALLOW

This rule is used to disable REFER in outbound message manipulation.

1. Navigate to **SIP > Message Manipulation > Message Rule Tables**. Note that the SWeLite does not receive any REFER message for proces sing.
2. Attach created message rule to the Teams Signaling Group.





Configure Signaling Groups

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

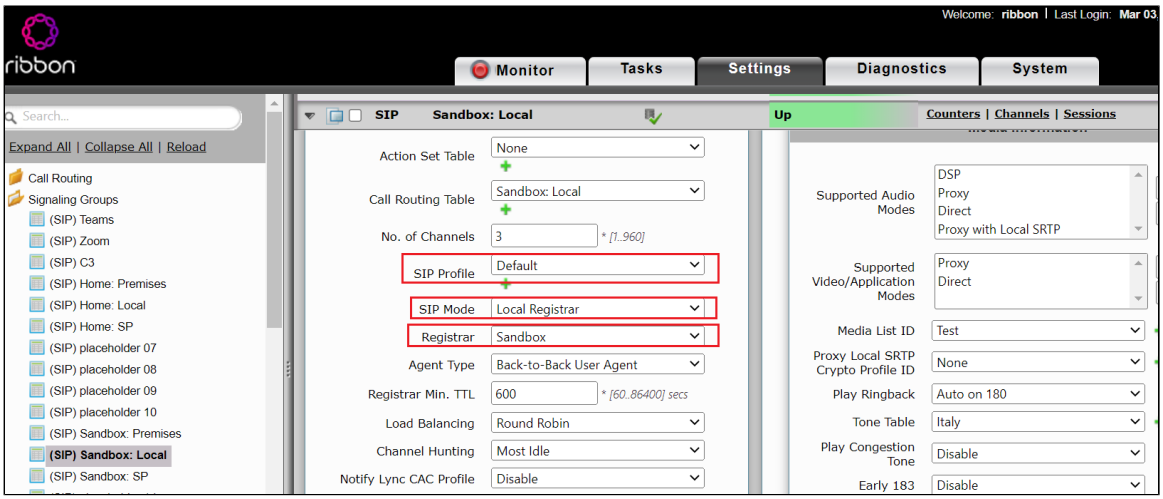
Signaling Groups include

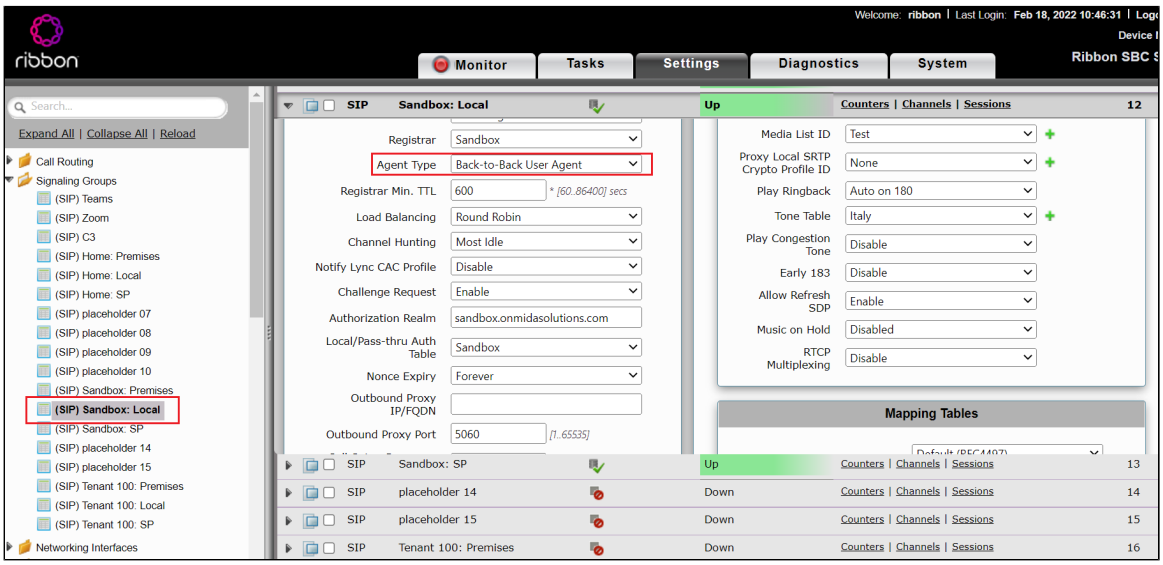
- Sandbox_Local_SG
- Sandbox_Teams_SG
- Sandbox_ServiceProvider_SG
- Sandbox_Premises_SG
- C3_SG

Use the following procedures to configure Signaling Groups.

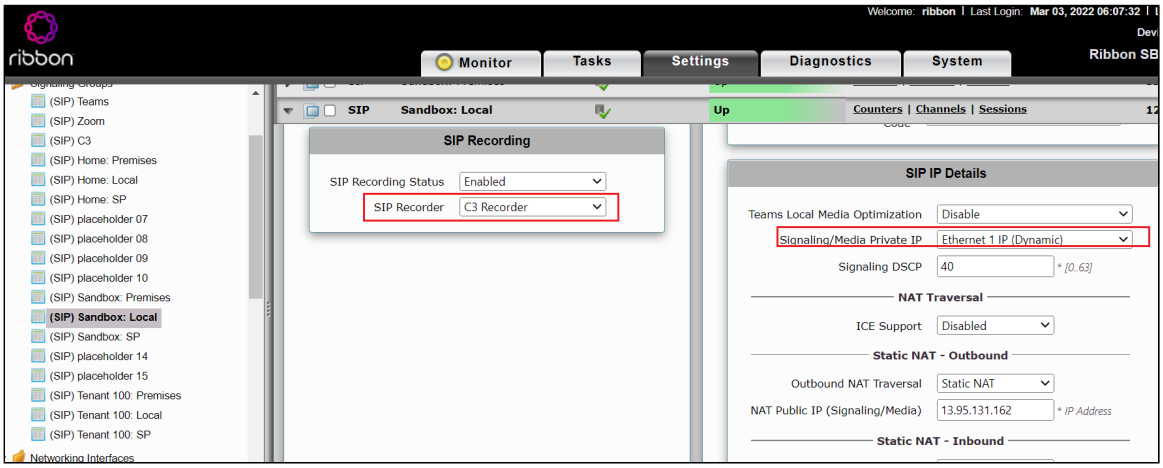
Sandbox_Local_SG

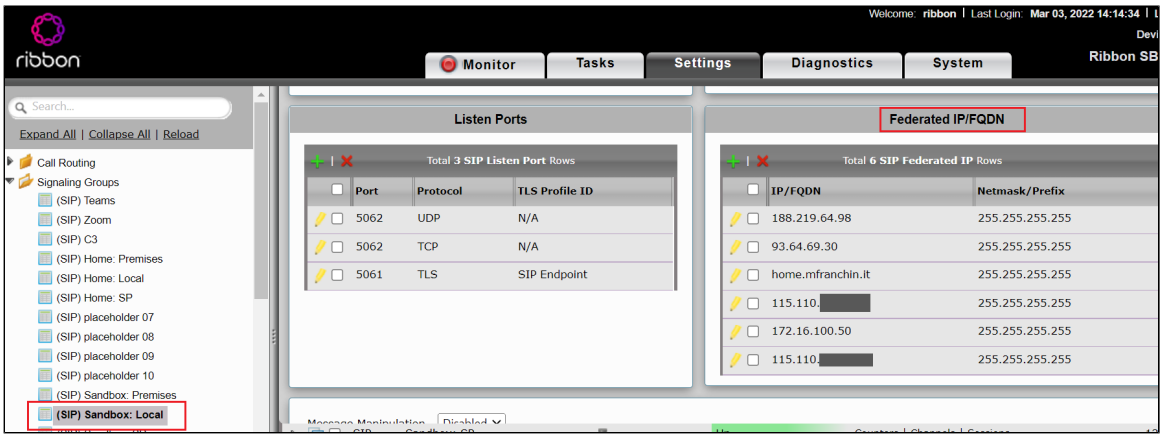
1. Navigate to **Signaling Groups**.
2. Click **Add SIP SG.**
3. In **SIP Profile**, choose the "Sip Profile" created in step 5.
4. In **SIP Mode**, select **Local Registrar** and attach the SIP Local Registrar created in step 4.
5. In Agent Type, select **Back-to-back user agent.**





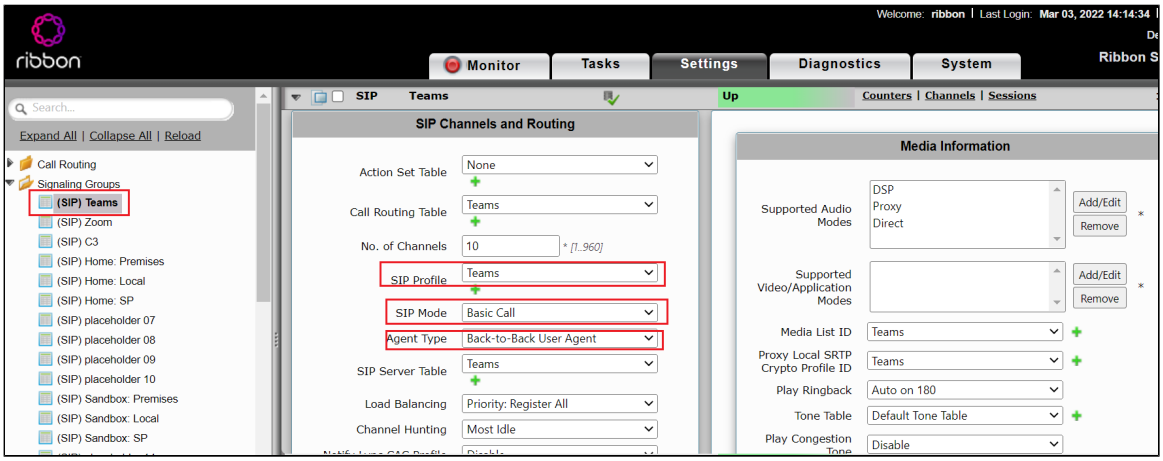
1. Enable SIP recording, and attach the Recording Server Table created for the SIP recording.
2. Select Ethernet 1 as the **Signaling/Media Source IP.**
3. Configure the IP addresses as the Federated IPs for the **Sandbox_LOCAL_SG**

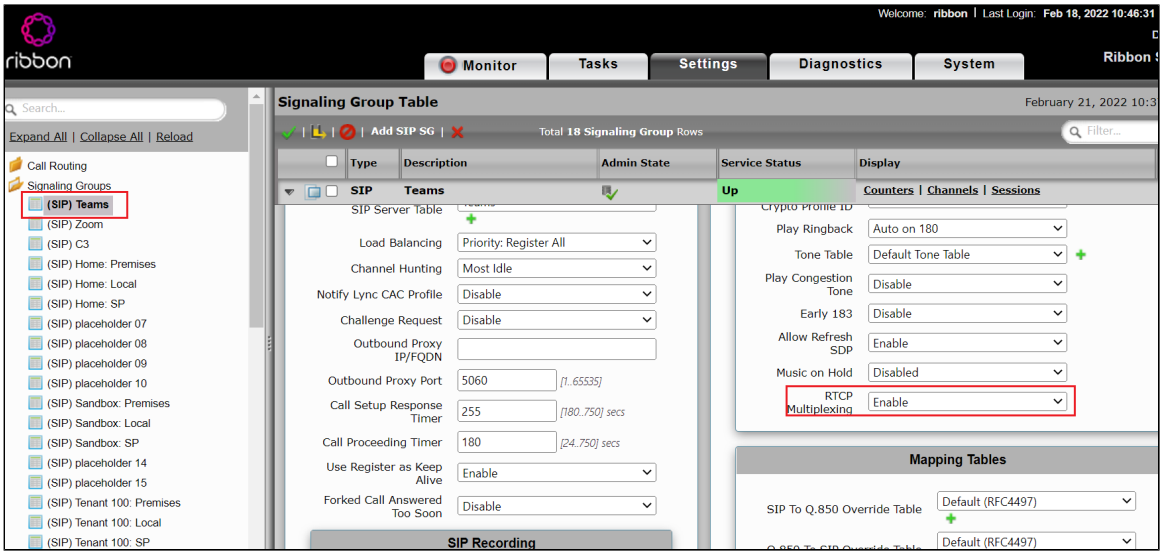


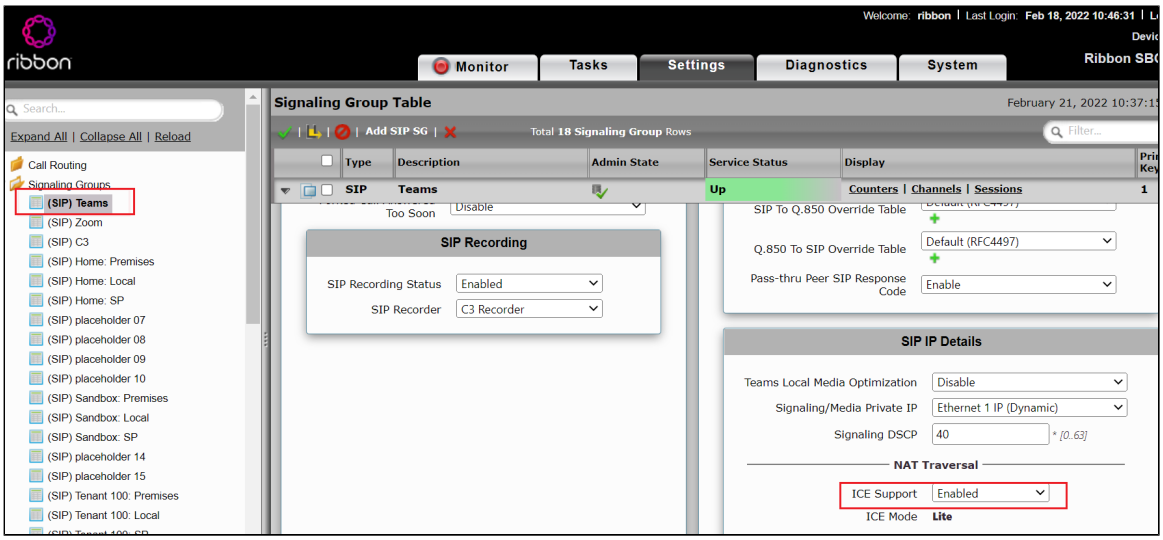


Sandbox_Teams_SG

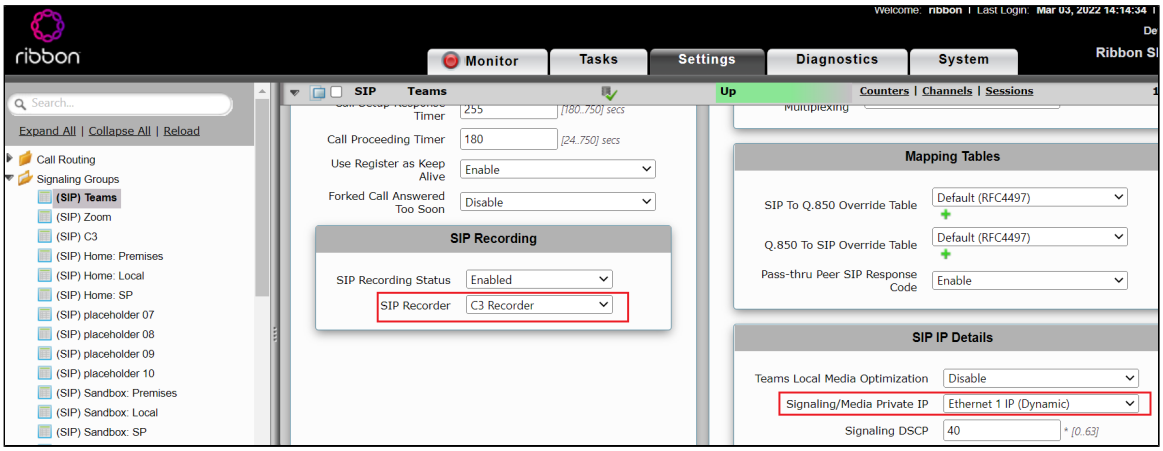
1. In **SIP Profile**, choose the "Sip Profile" created in step 5.
2. In Agent Type, select **Back-to-back user agent.**
3. In **SIP Mode**, select Basic Call.
4. Enable **RTCP multiplexing** and **Icelite**

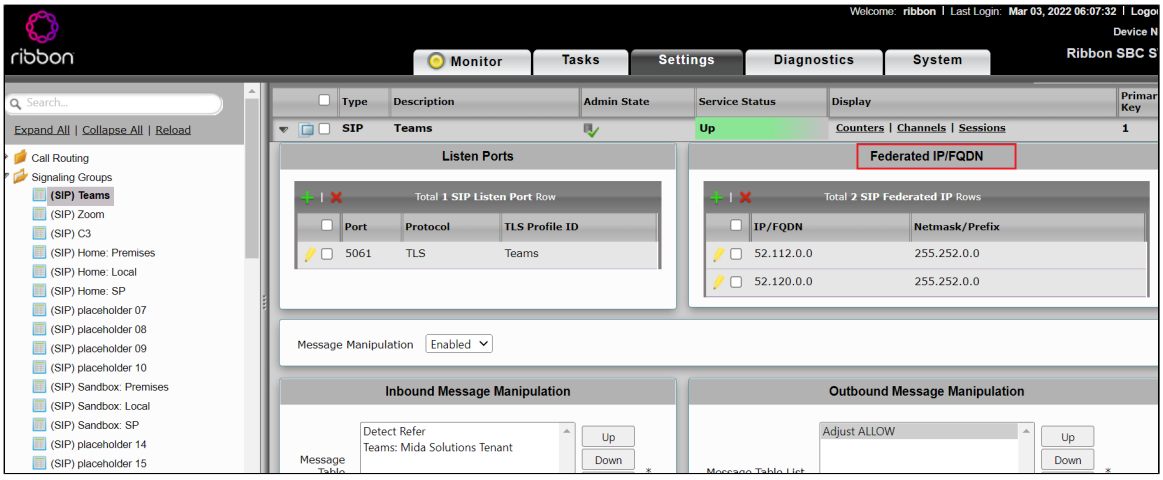






1. Enable SIP recording and attach the Recording Server Table created for the SIP recording.
2. Select Ethernet 1 as the **Signaling/Media Source IP.**
3. Configure the IP addresses as the Federated IPs for the **Teams_SG**

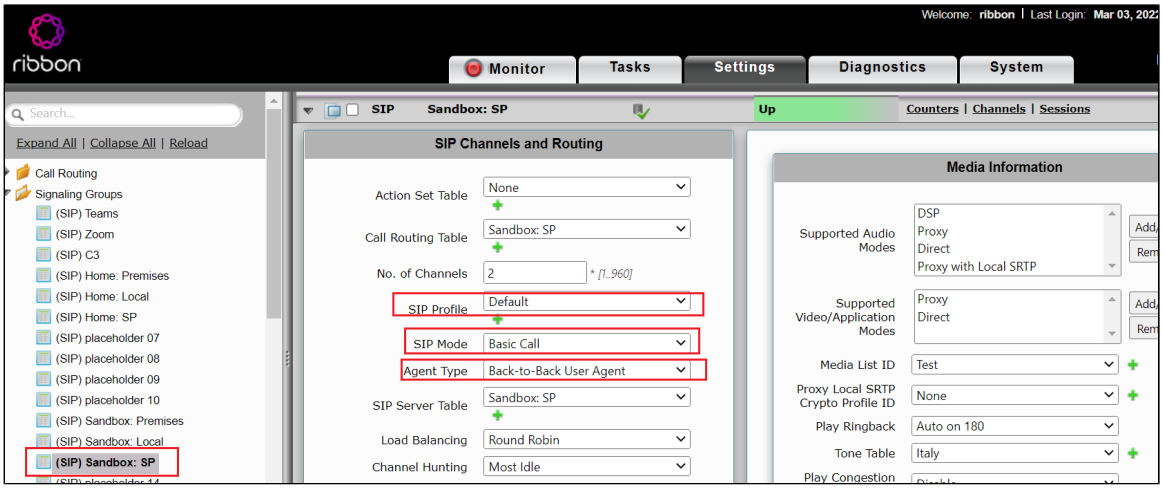


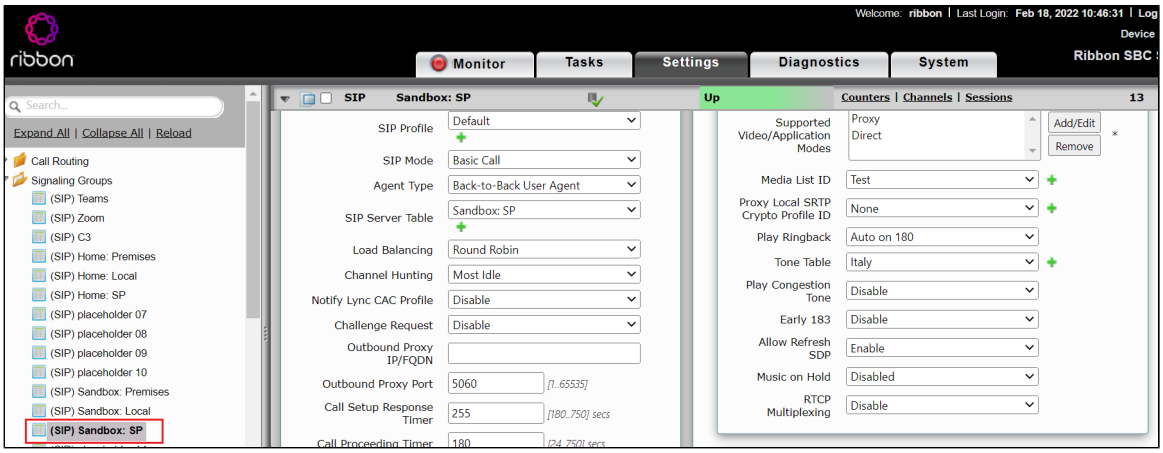


Sandbox_ServiceProvider_SG

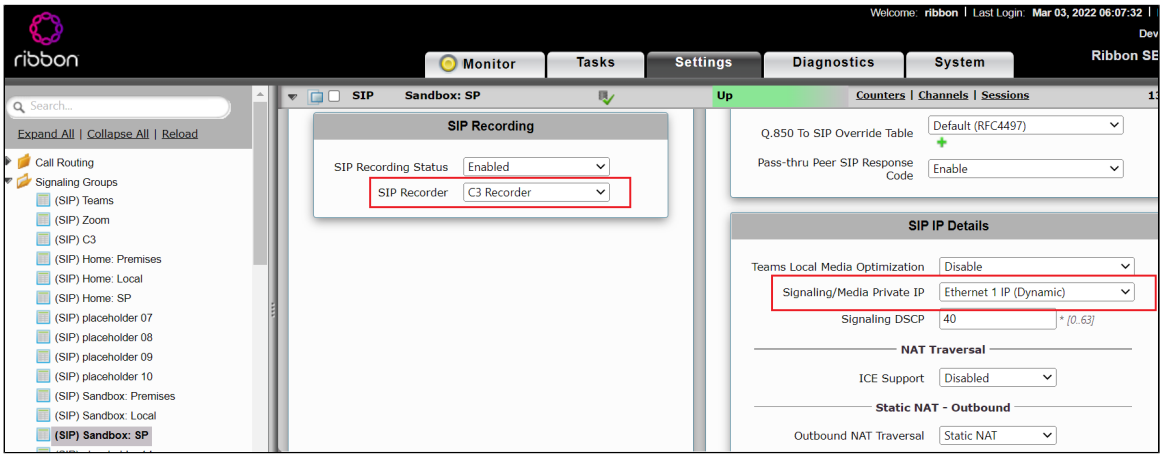
1. In **SIP Profile**, choose the "Sip Profile" created in step 5.
2. In Agent Type, select **Back-to-back user agent.**

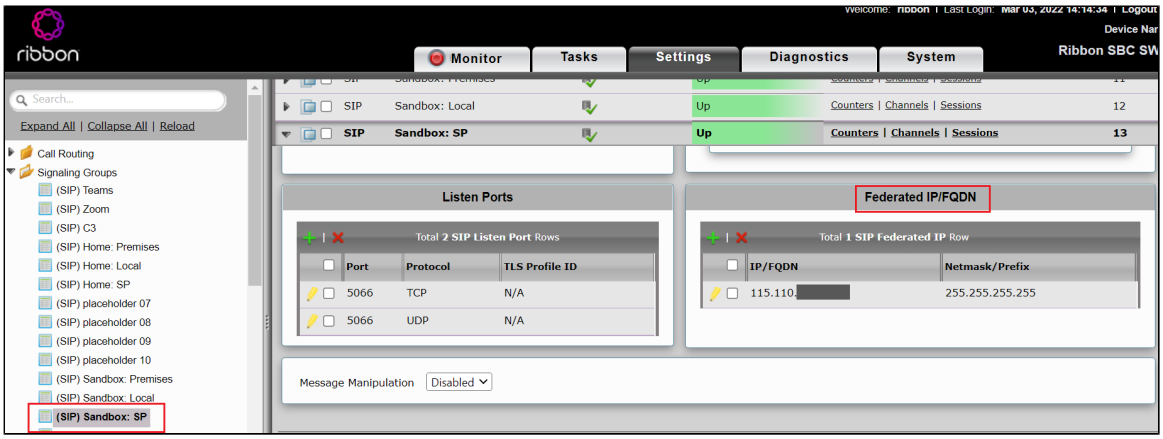
3. In **SIP Mode**, select Basic Call.





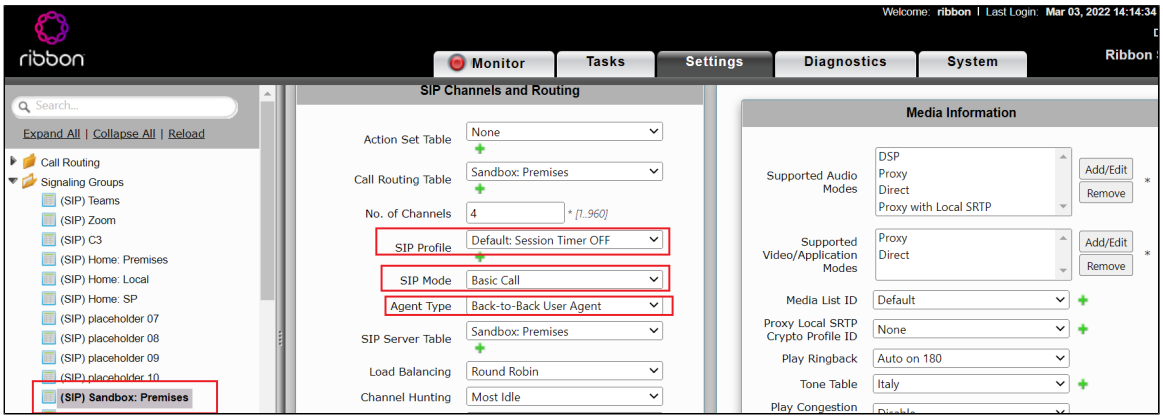
1. Enable SIP recording and attach the Recording Server Table created for the SIP recording.
2. Select Ethernet 1 as the **Signaling/Media Source IP.**
3. Configure the IP addresses as the Federated IPs for the **ServiceProvider_SG.**

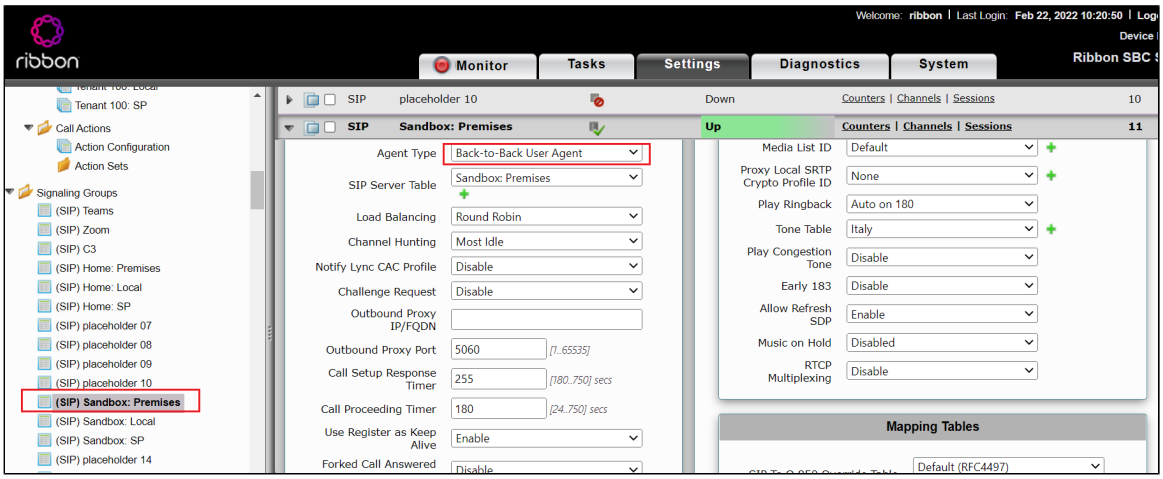




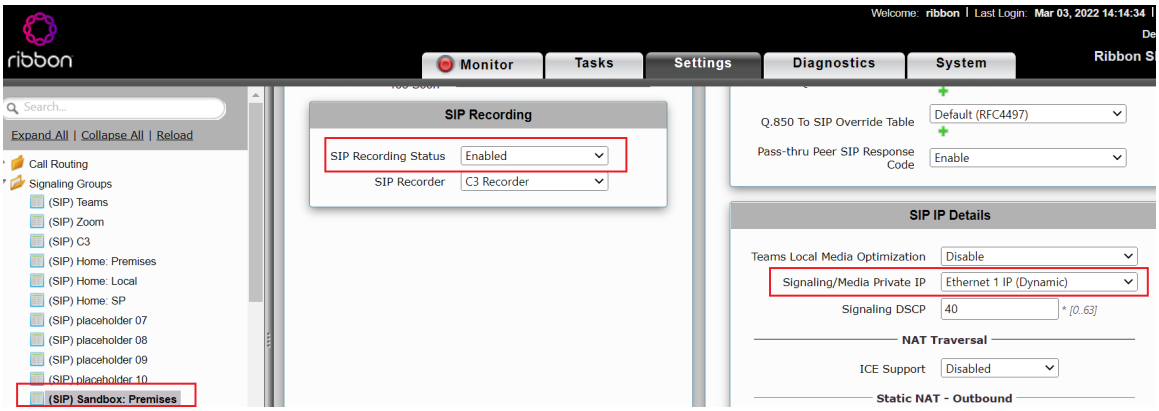
Sandbox_Premises_SG

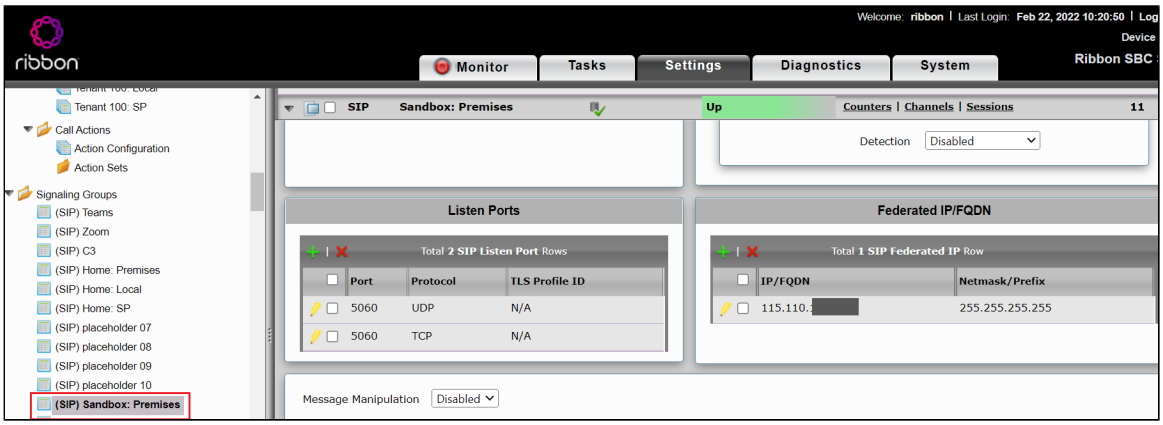
1. In **SIP Profile**, choose the "Sip Profile" created in step 5.
2. In Agent Type, select **Back-to-back user agent.**
3. In **SIP Mode**, select Basic Call.





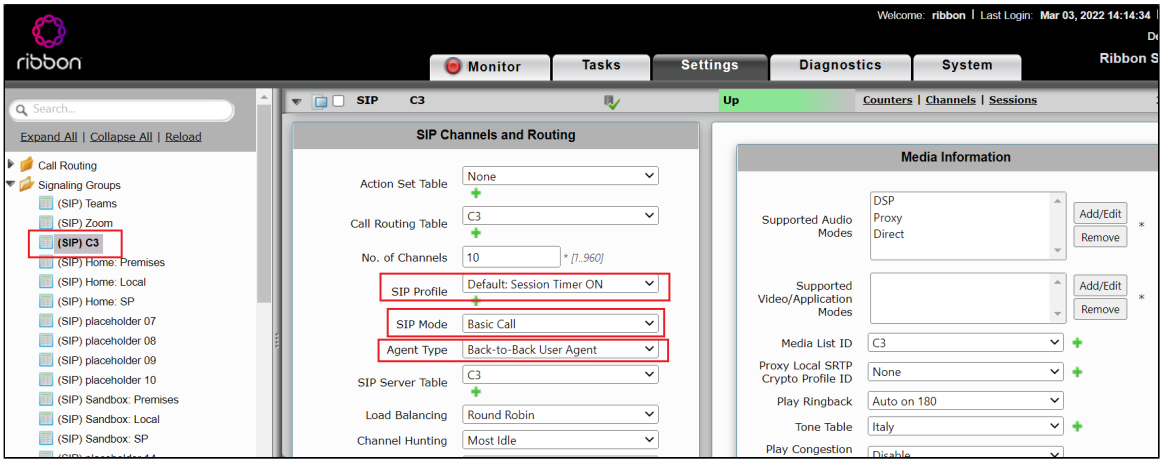
1. Enable SIP recording and attach the Recording Server Table created for SIP recording.
2. Select Ethernet 1 as the **Signaling/Media Source IP.**
3. Configure IP addresses as the Federated IPs for the **Premises_SG**

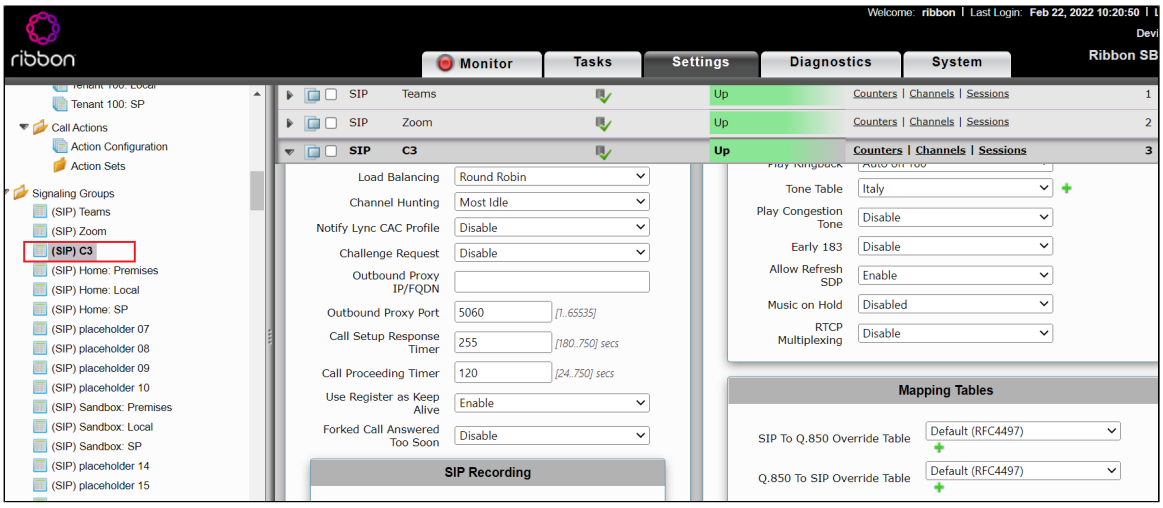




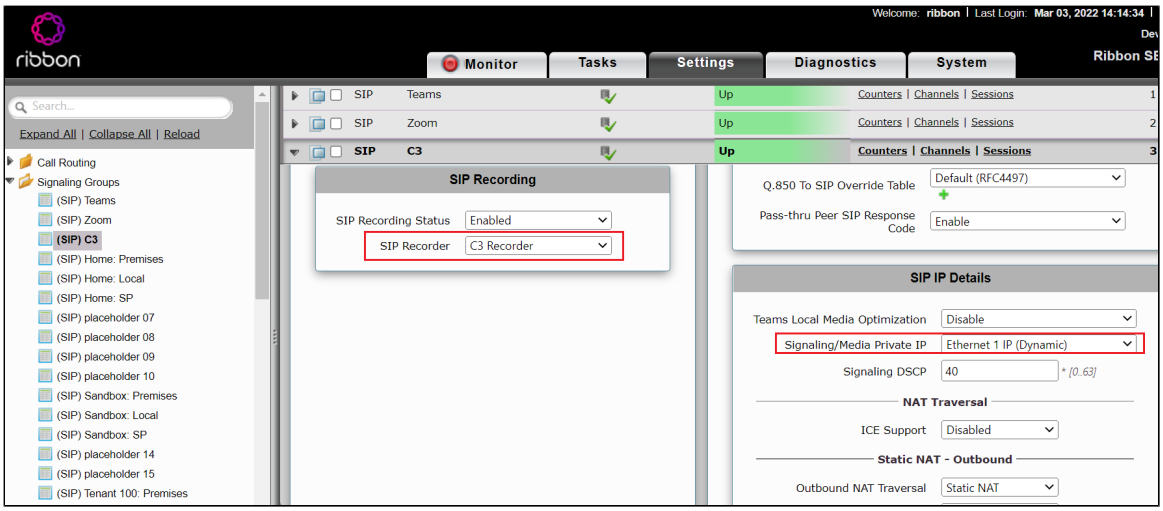
C3_SG (Recorder SG)

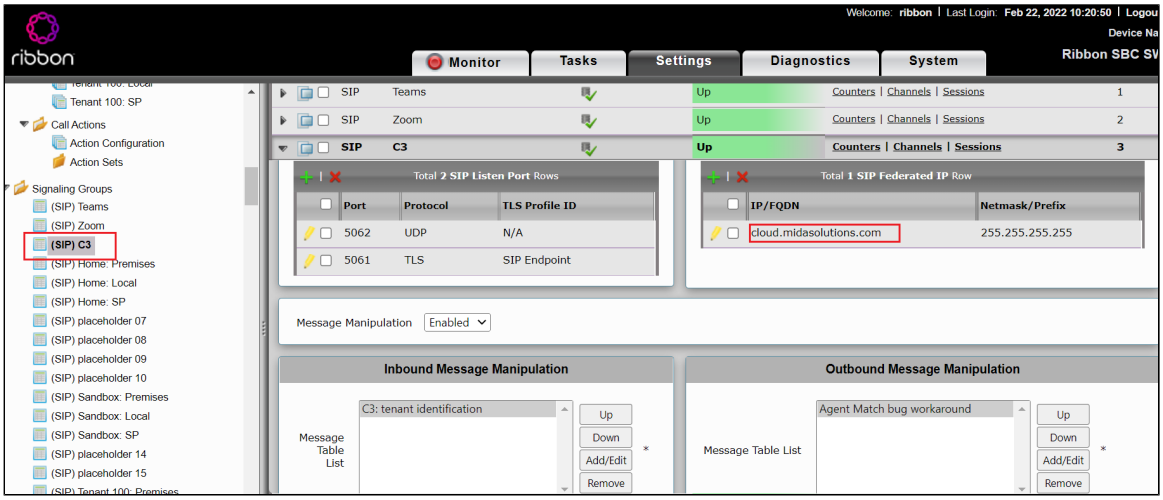
1. In **SIP Profile**, choose the "Sip Profile" created in step 5.
2. In Agent Type, select **Back-to-back user agent.**
3. In **SIP Mode**, select Basic Call.





1. Enable SIP recording and attach the Recording Server Table created for SIP recording.
2. Select Ethernet 1 as the **Signaling/Media Source IP**.
3. Configure the Recorder IP addresses or fqdn as the Federated IPs for the **C3_SG.**

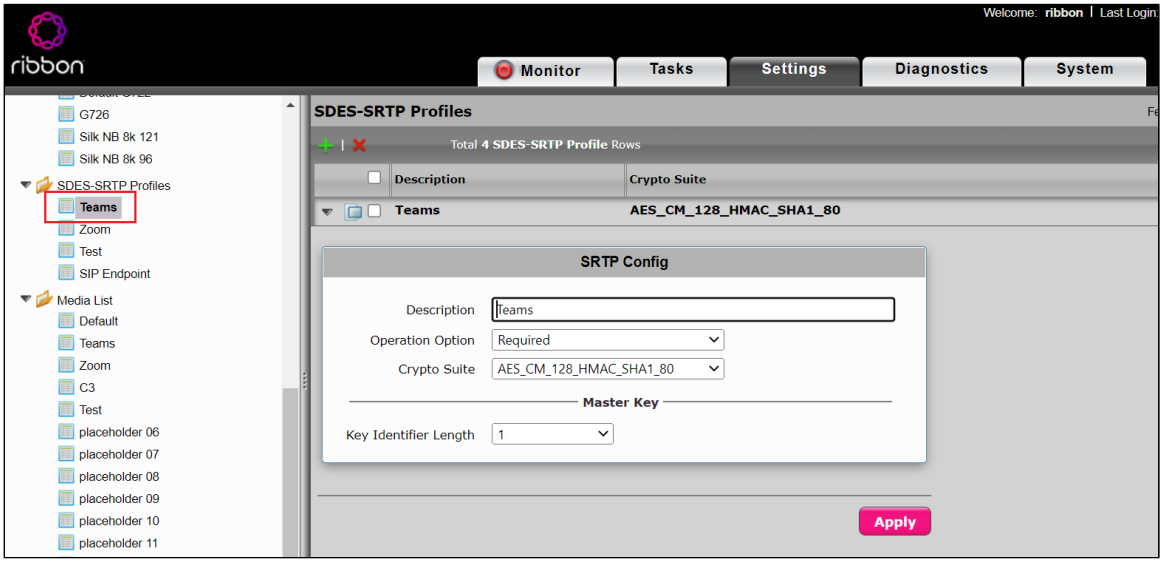




SRTP Profile for Teams

SDES-SRTP Profiles define a cryptographic context that is used in SRTP negotiation. SDES-SRTP Profiles required for enabling encryption and SRTP are applied to Media Lists. SDES-SRTP Profiles was previously named Media Crypto Profiles.

From the **Settings** tab, navigate to **Media > SDES-SRTP Profiles.** Click the + icon to create a new SRTP profile.



Perform the following steps to complete the configuration:

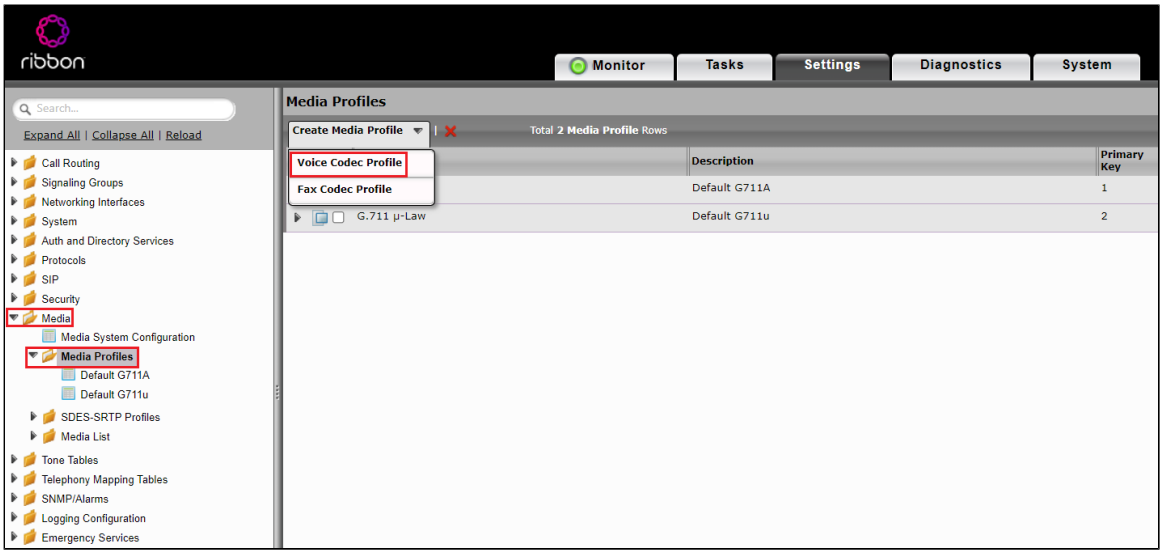
1. Provide the desired description for the profile.
2. Set Operation Option as "**Required**". This setting permits call connections only if you can use encryption for the call. If the peer device does not support **SRTP** (Secure Real Time Protocol) for voice encryption over the IP network, the call setup will fail.
3. Attach the Crypto suite "**AES_CM_128_HMAC_SHAI_80**" - A crypto suite algorithm that uses the 128 bit AES-CM encryption key and a 80 bit HMAC_SHA1 message authentication tag length.
4. Key Identifier Length set to "0" - Set this value to **1** to enable the MKI in SDP.
5. Click **OK.**

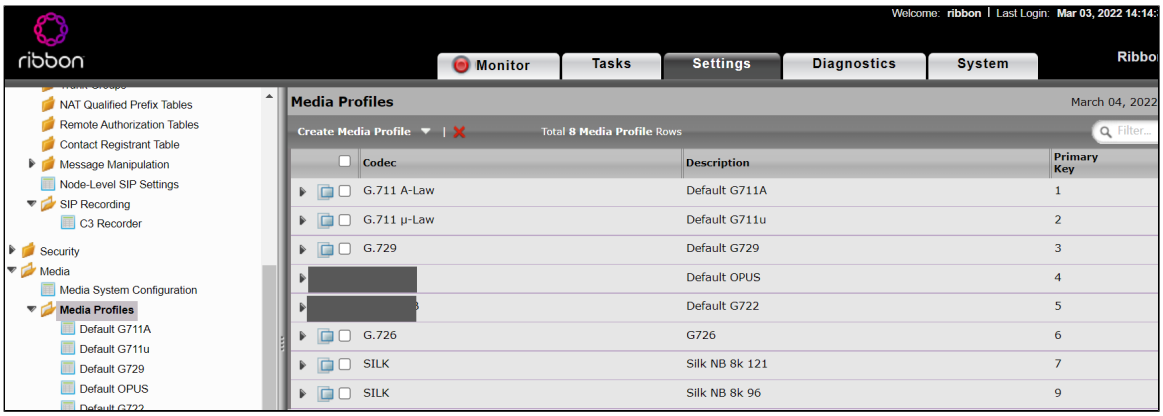
Global Configuration

Media Profiles

Media Profiles allow you to specify the individual voice and fax compression codecs and their associated settings, for inclusion in a Media List. Different codecs provide varying levels of compression, allowing one to reduce bandwidth requirements at the expense of voice quality.

From the **Settings** tab, navigate to **Media > Media Profiles.** From the **Create Media Profile** drop-down list, select **Voice Codec Profile**



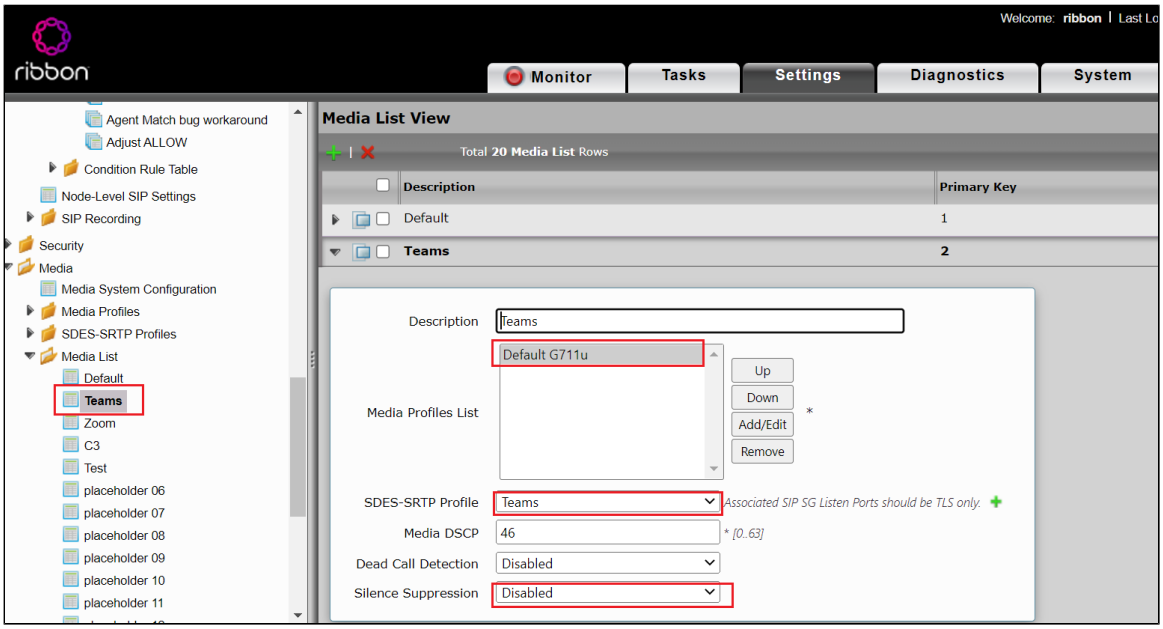


Ensure not to configure OPUS and G722 . For more information, see Caveat.

Media List

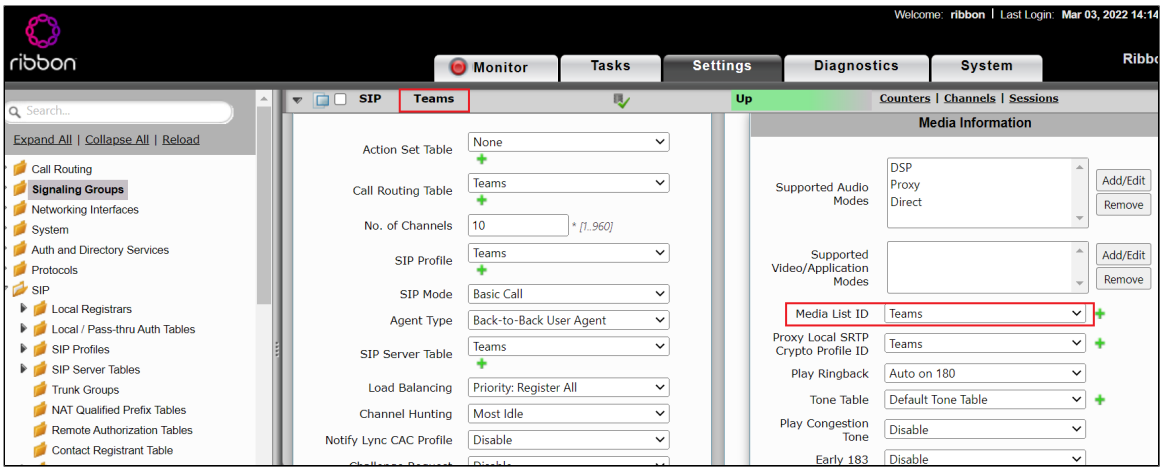
To create a Media List for Teams endpoint,

1. Attach SRTP profile created in earlier step
2. Disable **Silence Suppression** flag.
3. Configure only one supported codec for Teams leg to avoid in-dialog codec change.



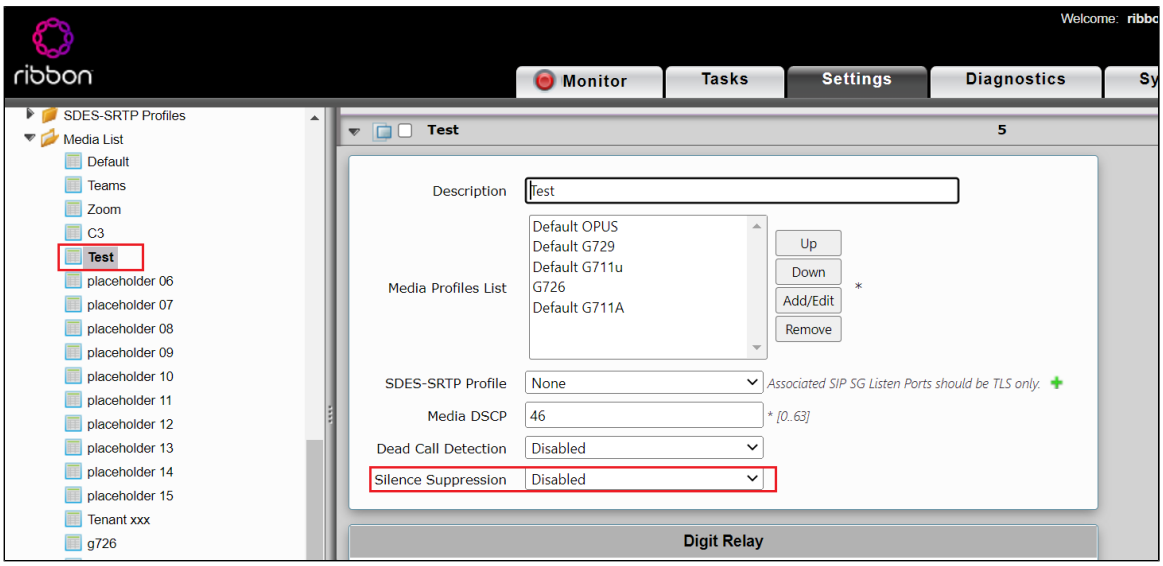
Silence Suppression flag is disabled since the MIDA Recorder does not support CN payload.

- Attach created Media List to Teams Signaling SG

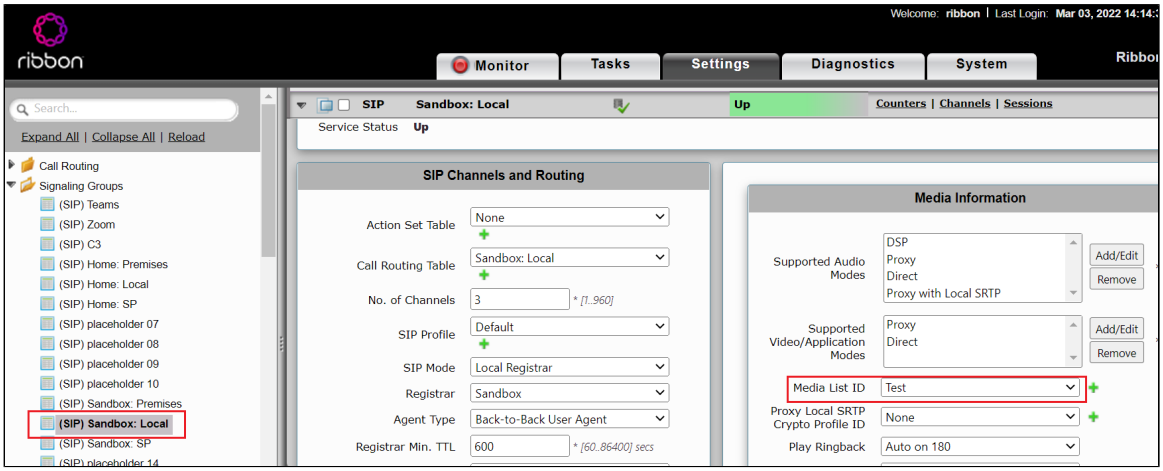


To create Media List for other endpoints,

- Disable **Silence Suppression** flag.



- Attach created Media List to other Signaling SG

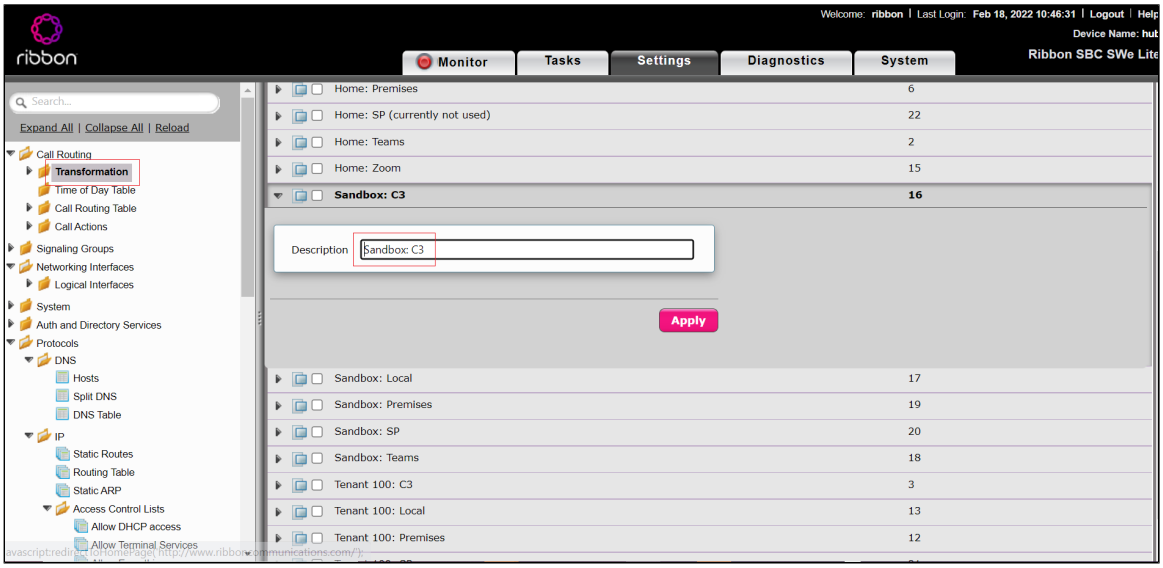


Transformation Table

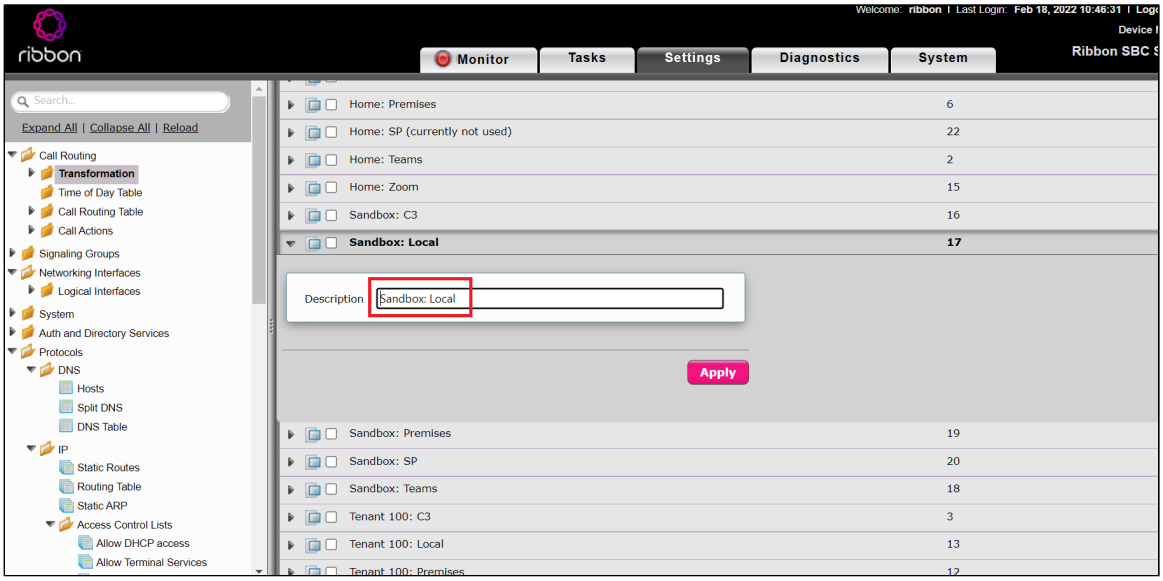
Transformation Tables facilitate the conversion of names, numbers, and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number, or a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table. In addition, Transformation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

From the Settings tab, navigate to **Call Routing > Transformation**. Click the + icon to create a Transformation Table.

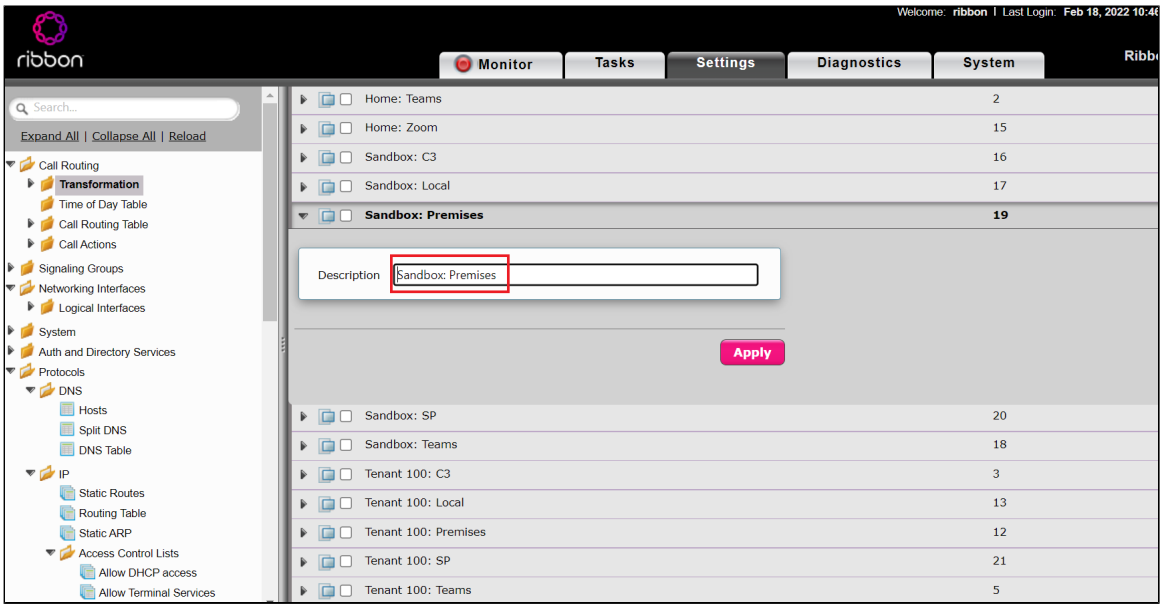
1. Provide a name for the Transformation Table in the **Description field**.
2. Provide name of **C3 recorder.**
3. Click **OK.**



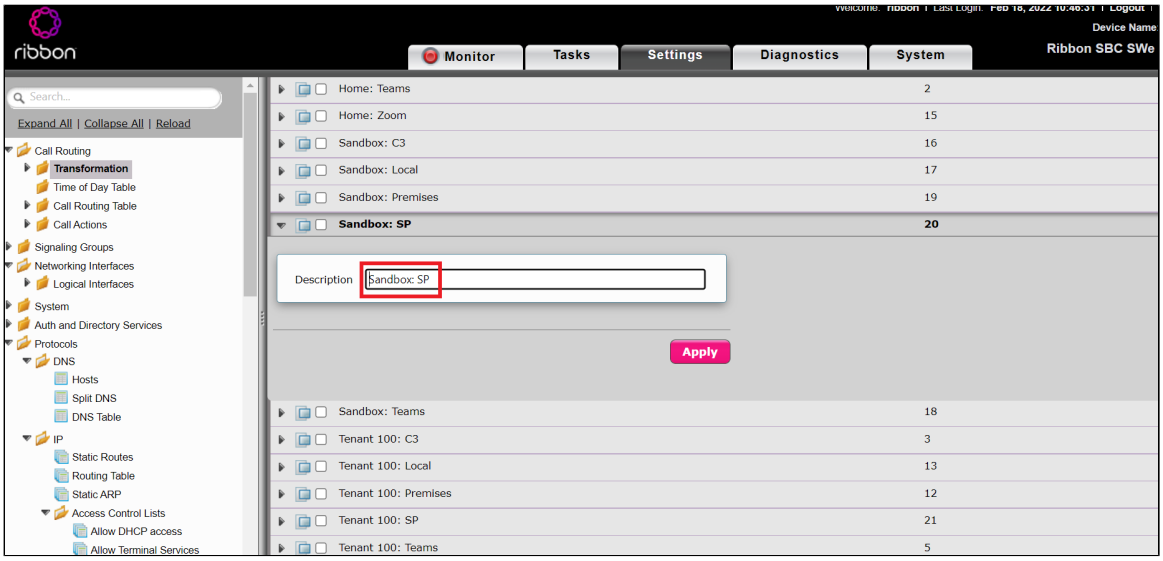
1. Provide a name for the Transformation Table in the **Description field.**
2. Provide name of **Sandbox:Local.**
3. Click **OK**.



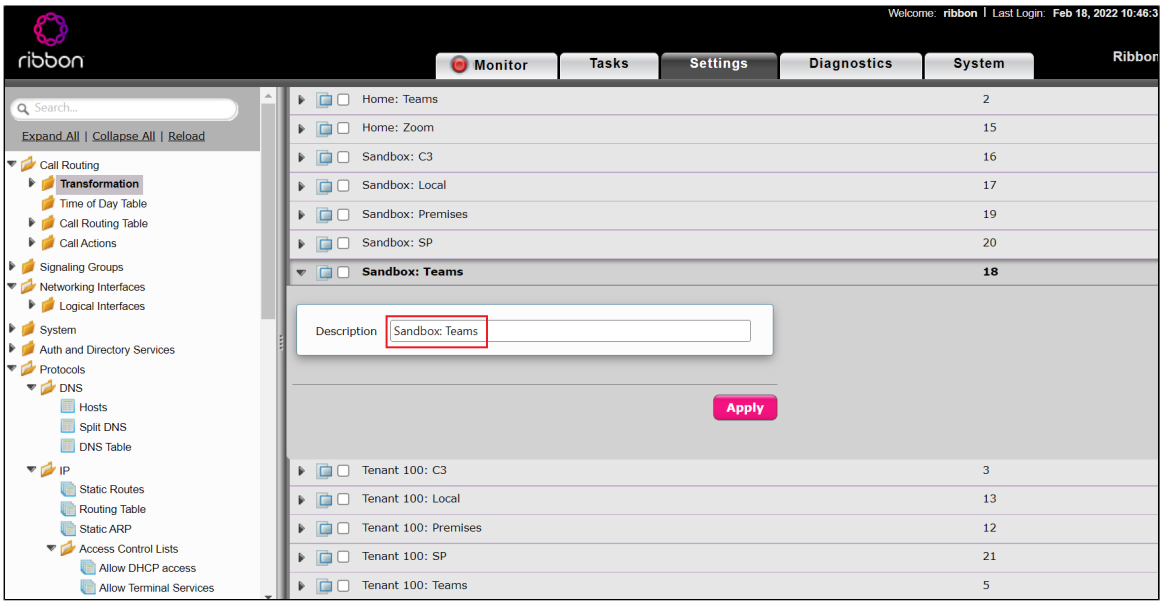
1. Provide a name for the Transformation Table in the **Description field.**
2. Provide name of **Premises**.
3. Click OK.



1. Provide a name for the Transformation Table in the **Description field.**
2. Provide name of **Service Provider.**
3. Click **OK**.



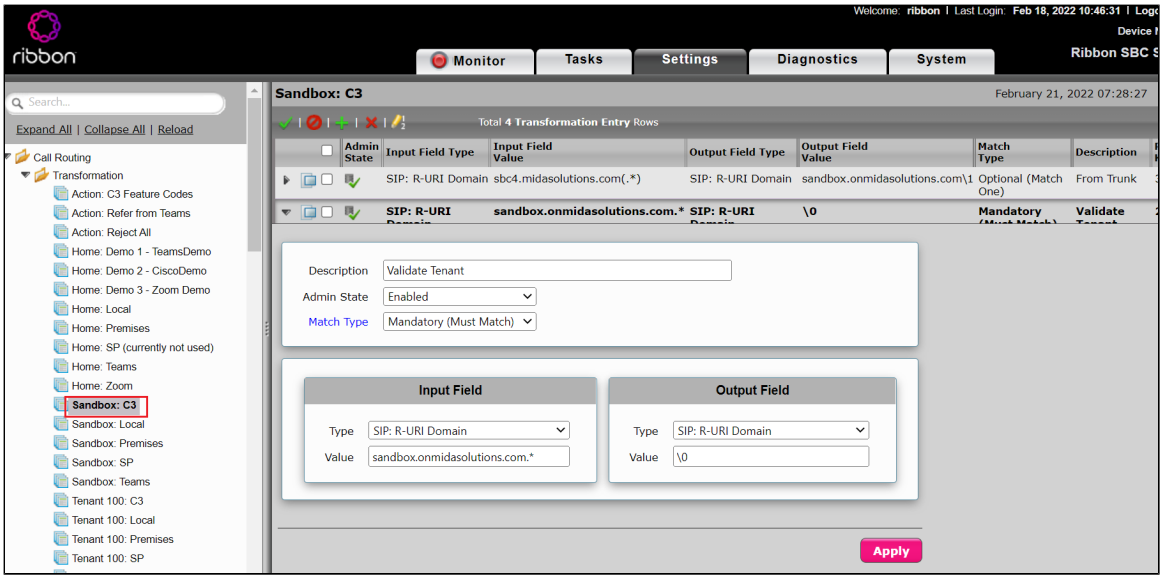
1. Provide a name for the Transformation Table in the **Description field.**
2. Provide name for **Teams.**
3. Click **OK.**

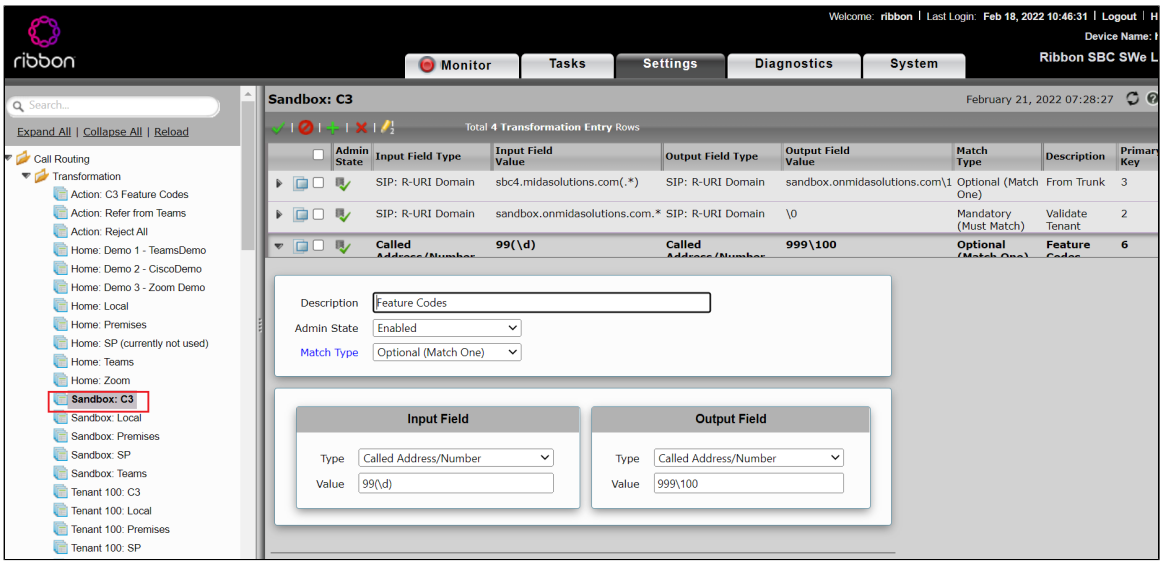


Transformation Table Entry

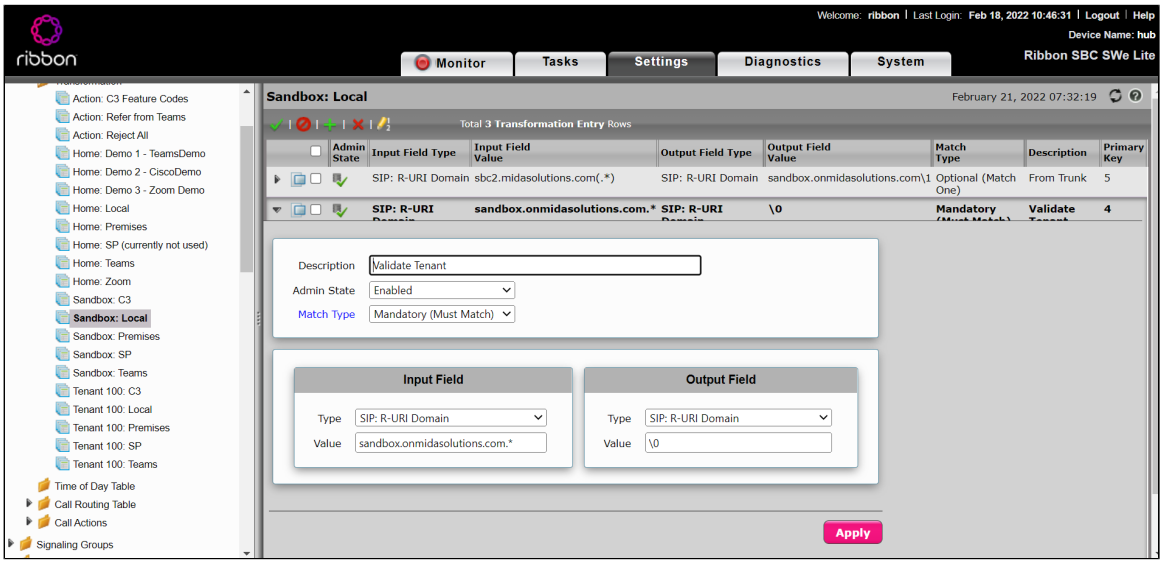
1. Click on the **Transformation Table** created in the previous step.
2. Click the + icon to create an entry
3. Provide the values in the **Input** and **Output** fields.
4. Click OK.

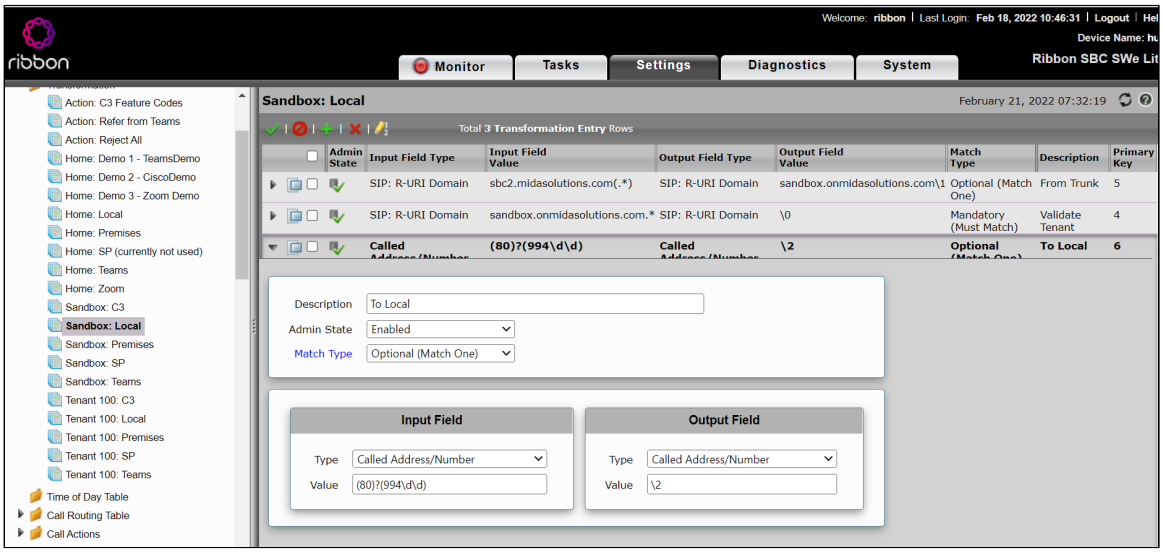
Transformation Entry for C3 Recorder



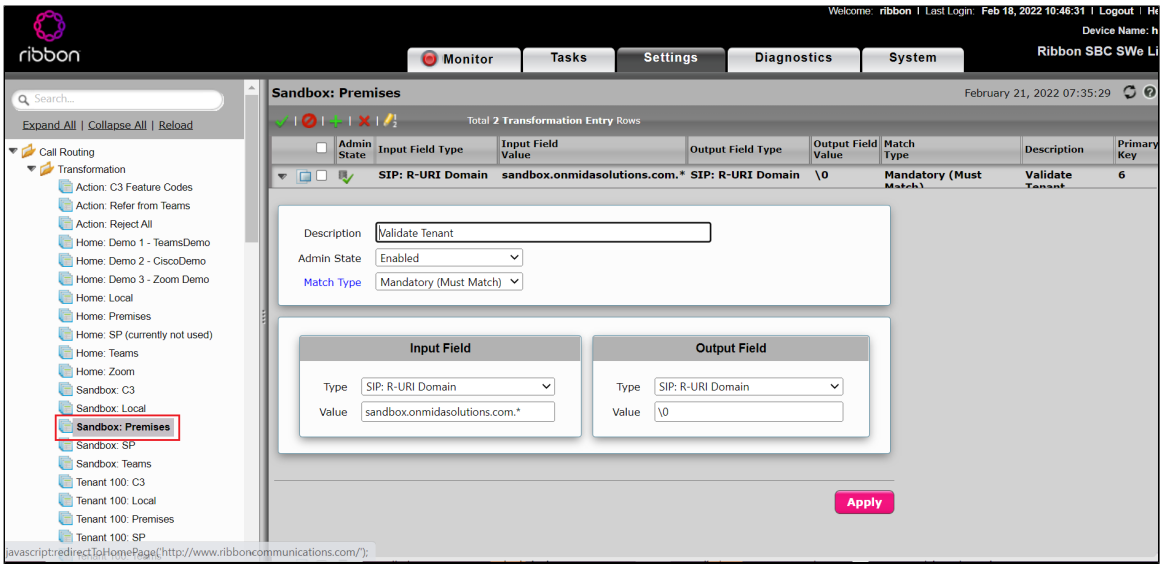


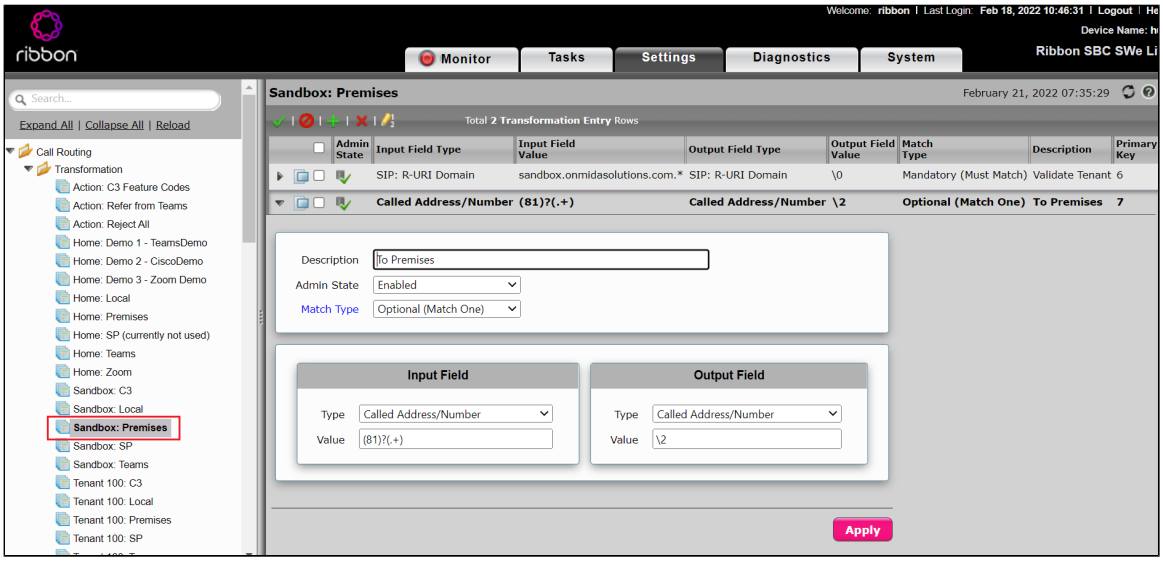
Transformation Entry for Sandbox:Local



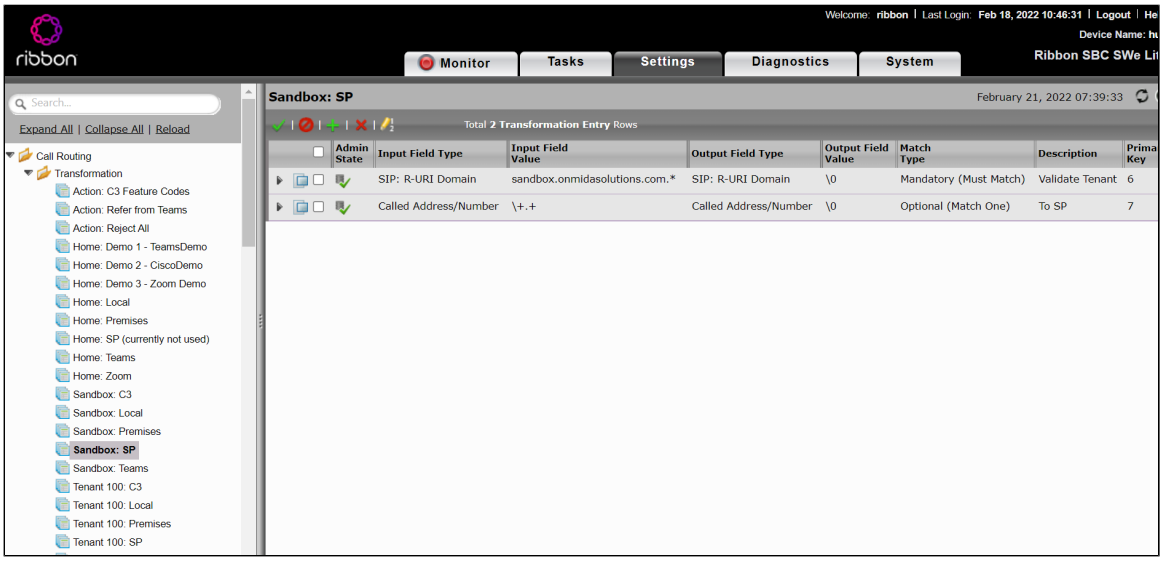


Transformation Entry for Sandbox:Premises

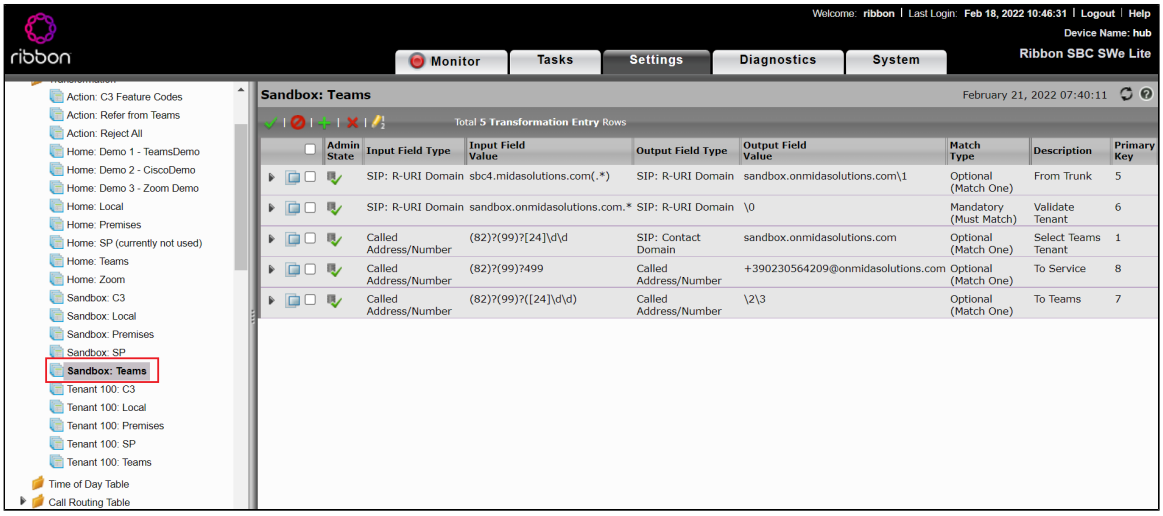




Transformation Entry for Service Provider



Transformation Entry for Teams endpoint

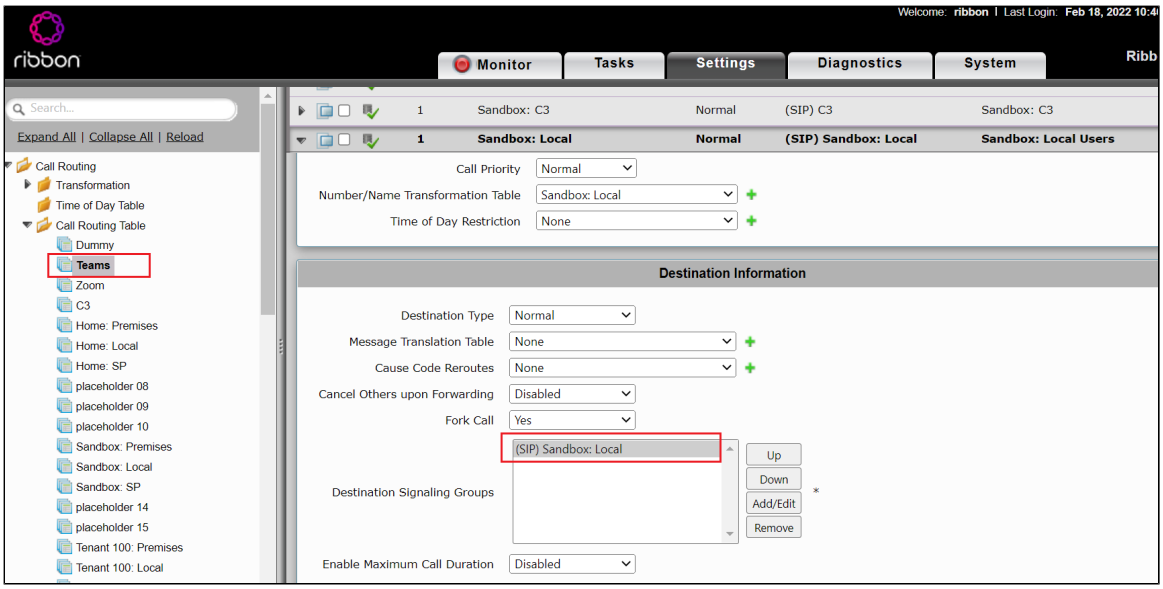


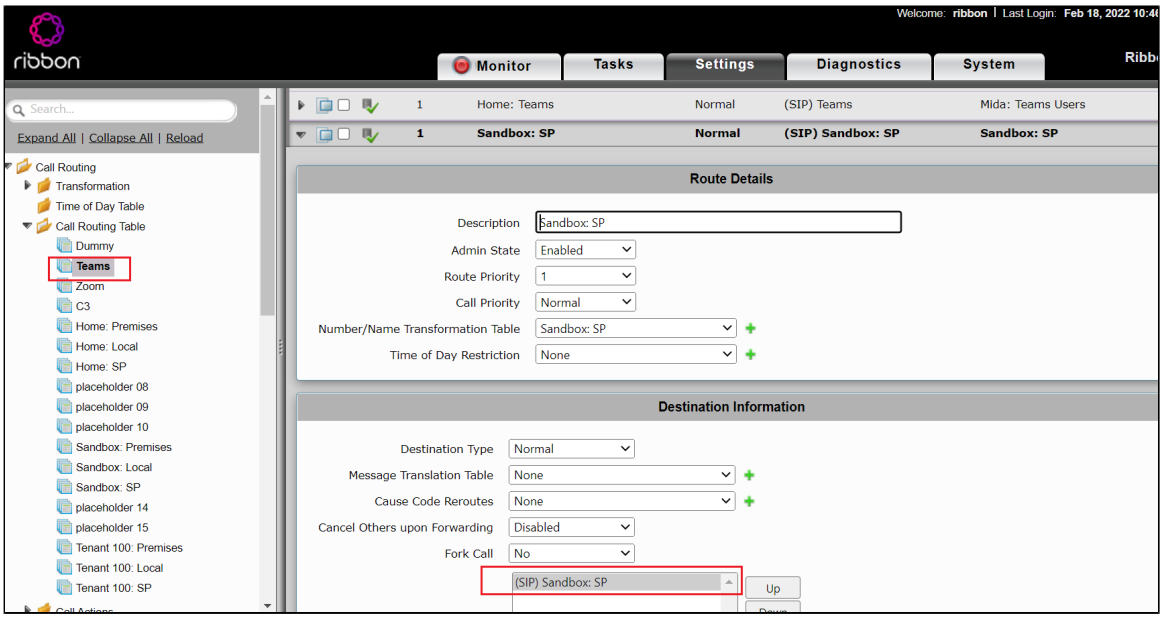
Configure Call Routing Tables

Call Routing allows calls to be carried between signaling groups, thus allowing calls to be carried between ports, and between protocols (like ISDN to SIP). Routes are defined by Call Routing Tables, which allow for flexible configuration of which calls are carried, and how they are translated.

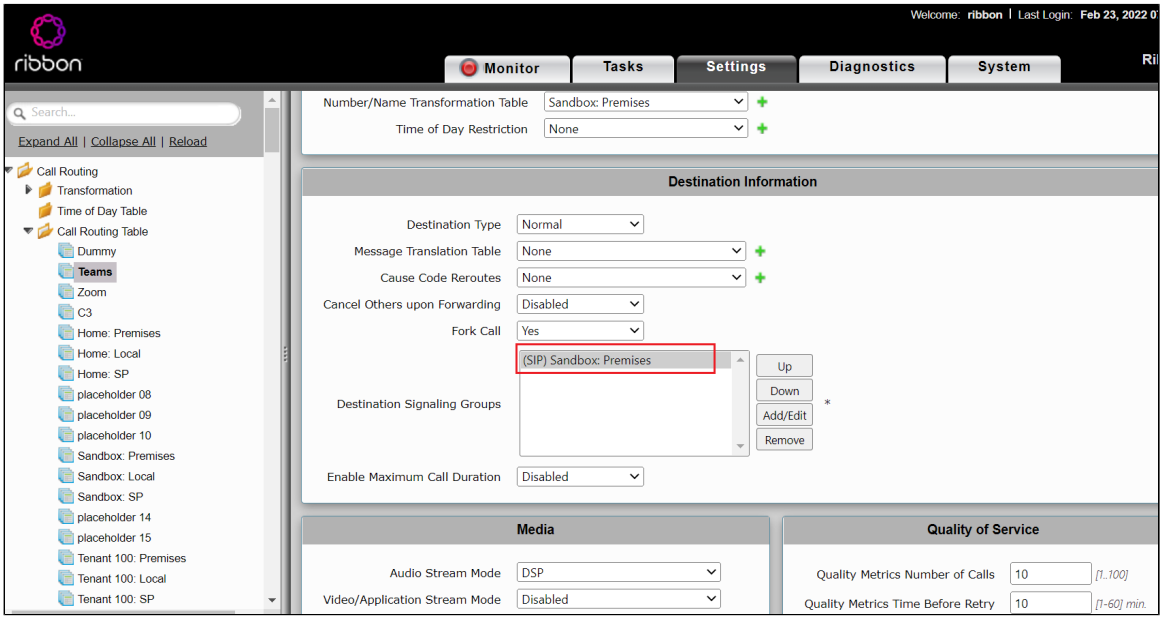
TEAMS

1. Navigate to **Call Routing > Call Routing Table**.
2. Attach the Transformation Table entry created in the previous step.
3. Select the **Destination Signaling Group** as LOCAL_SG.

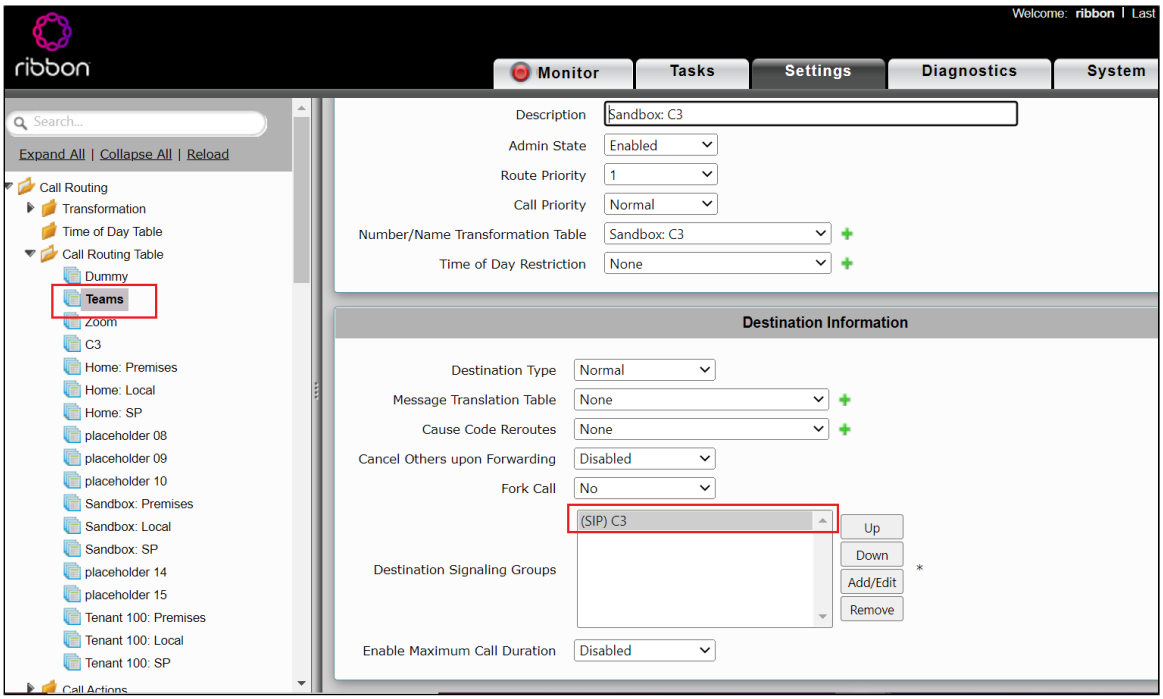




1. Select the **Destination Signaling Group** as Sandbox_Premises_SG

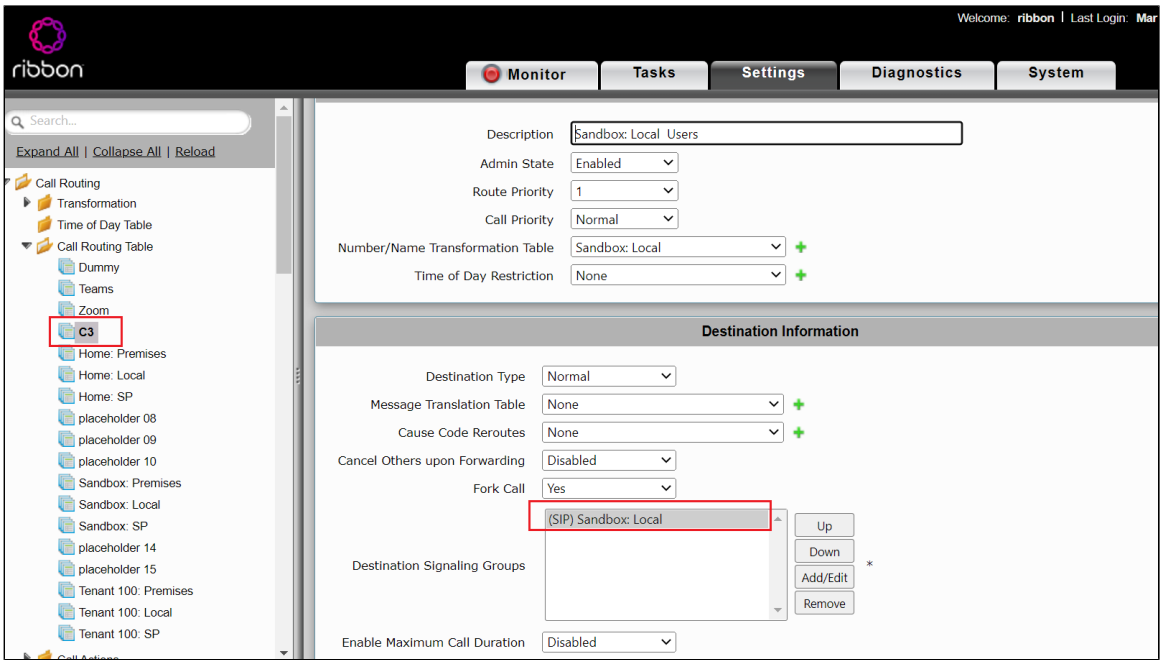


1. Select the **Destination Signaling Group** as Sandbox_C3_SG

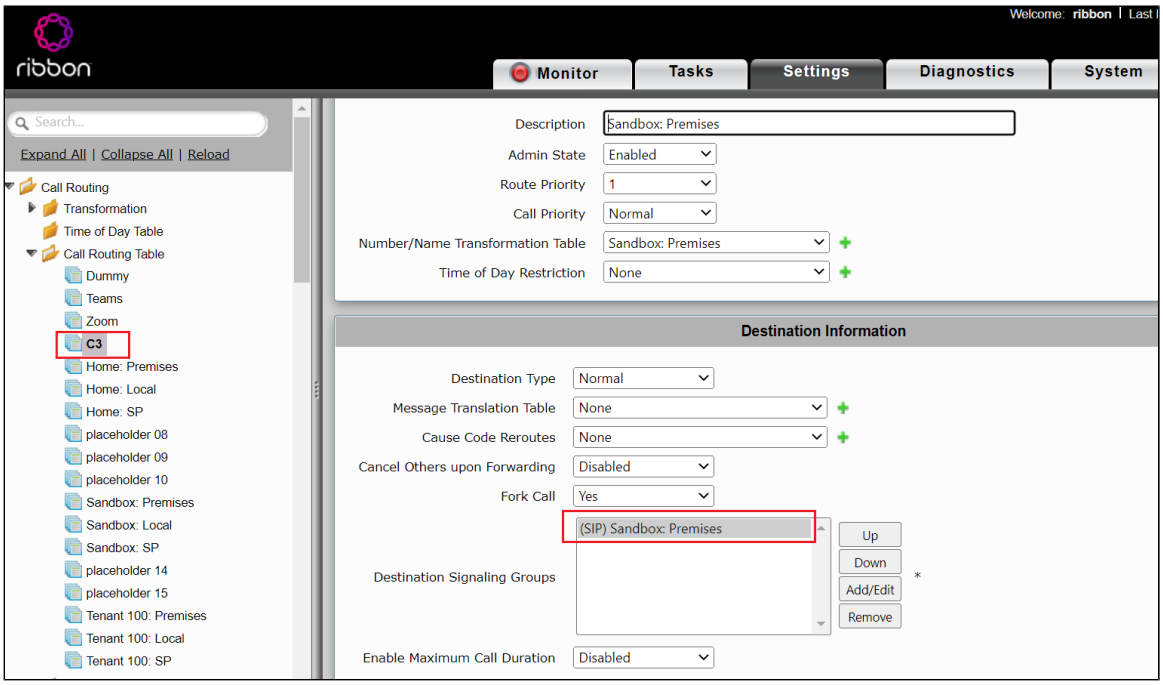


C3

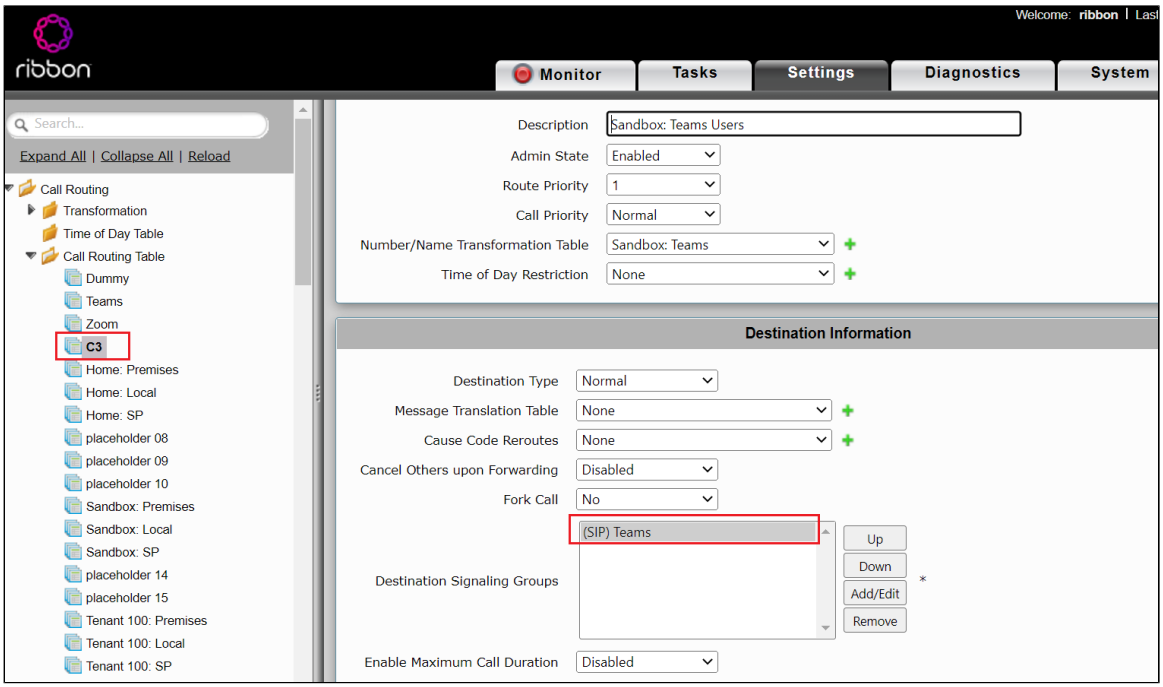
1. Navigate to **Call Routing > Call Routing Table**.
2. Attach the Transformation Table entry created in the previous step.
3. Select the **Destination Signaling Group** as LOCAL_SG.



1. Select the **Destination Signaling Group** as Premises_SG.

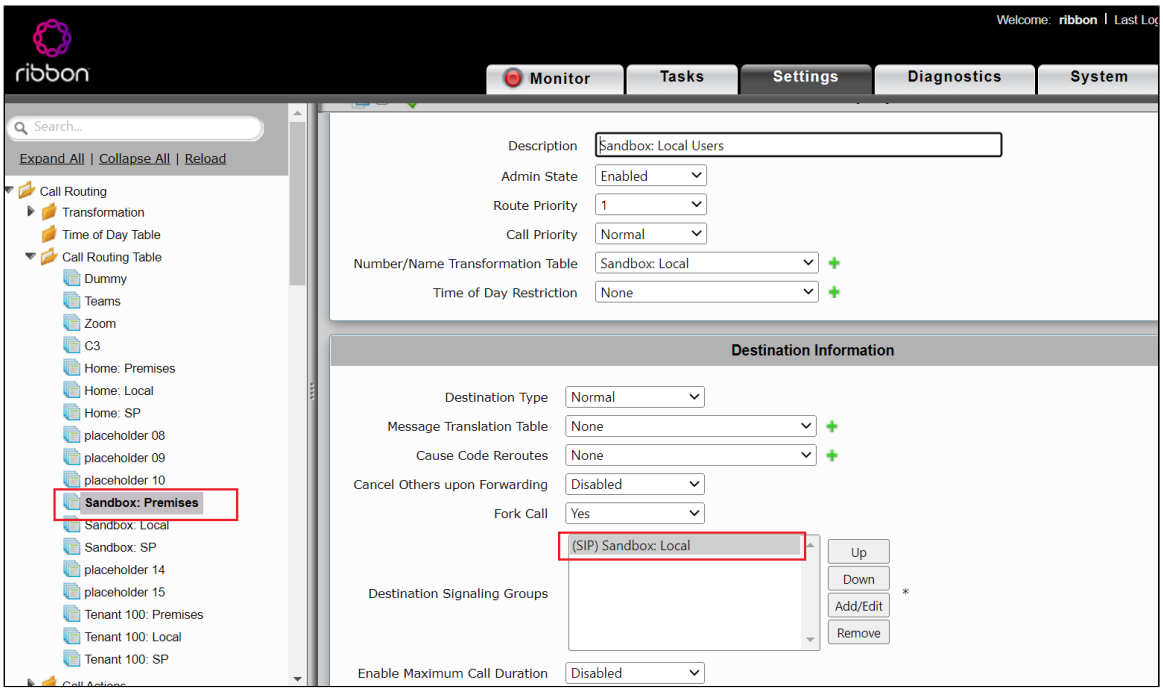


1. Select the **Destination Signaling Group** as Teams_SG.

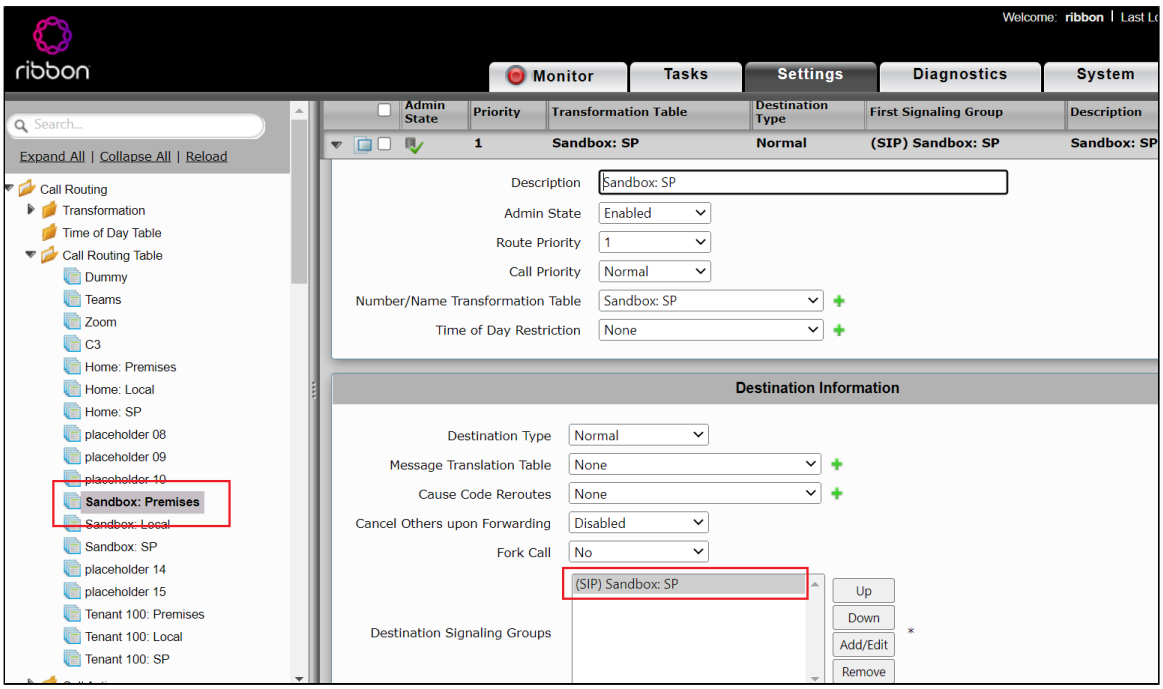


Sandbox_Premises

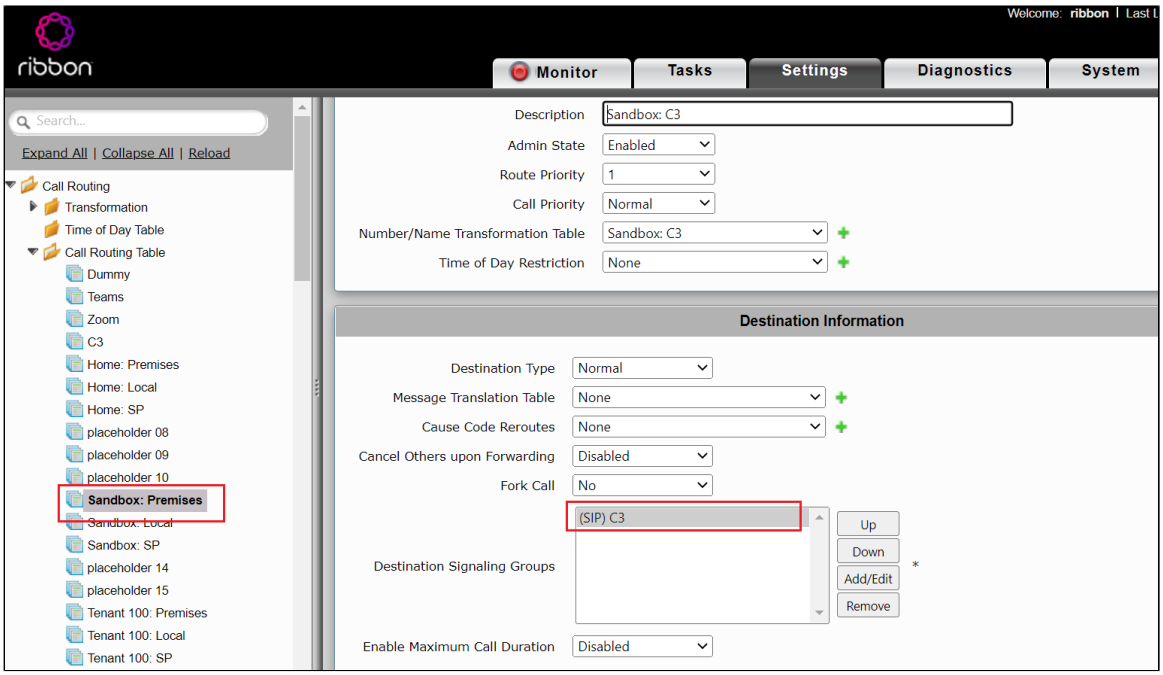
1. Navigate to **Call Routing > Call Routing Table**.
2. Attach the Transformation Table entry created in the previous step.
3. Select the **Destination Signaling Group** as LOCAL_SG.



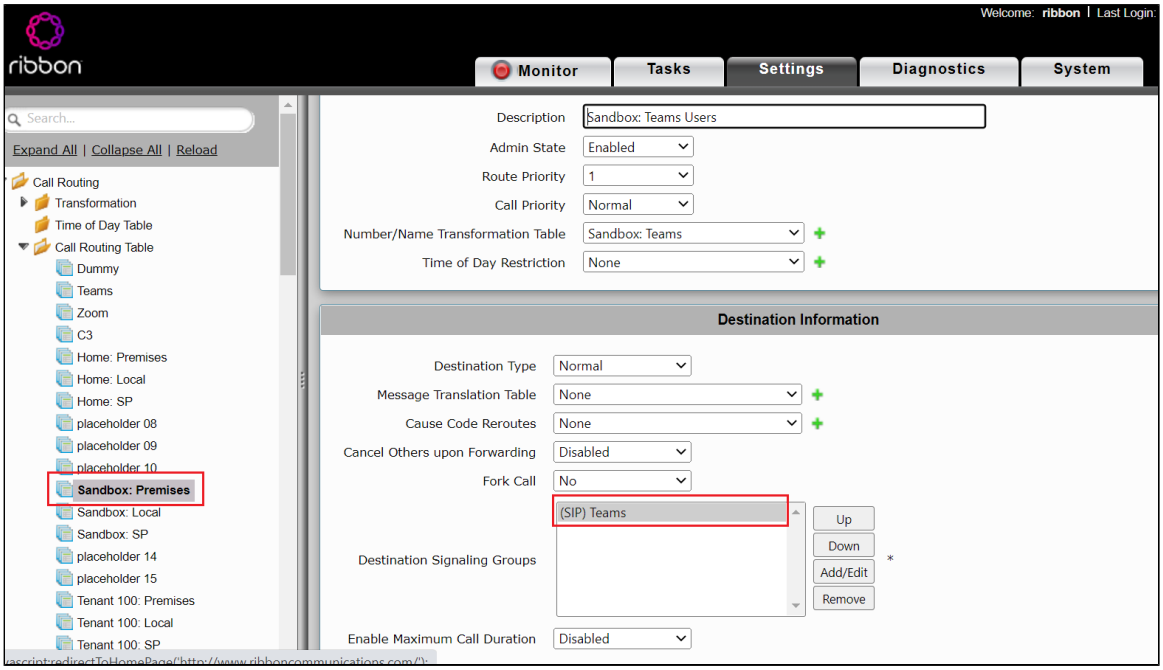
1. Select the **Destination Signaling Group** as Service_Provider_SG.



1. Select the **Destination Signaling Group** as C3_SG.

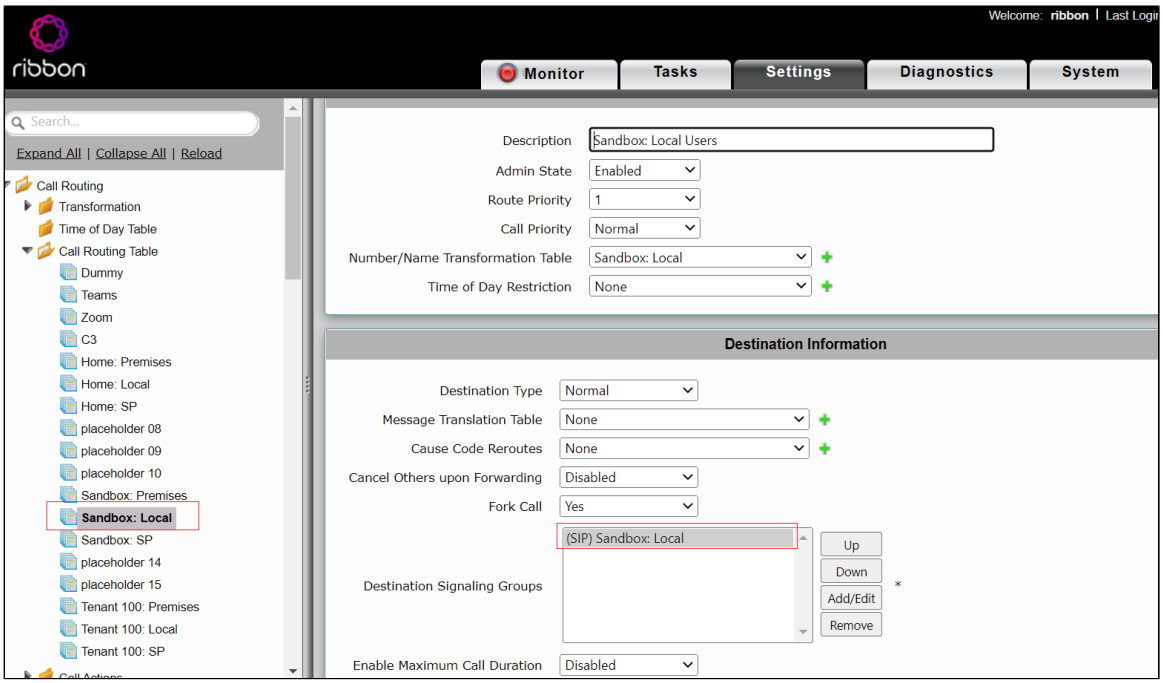


1. Select the **Destination Signaling Group** as Sandbox_Teams_SG.

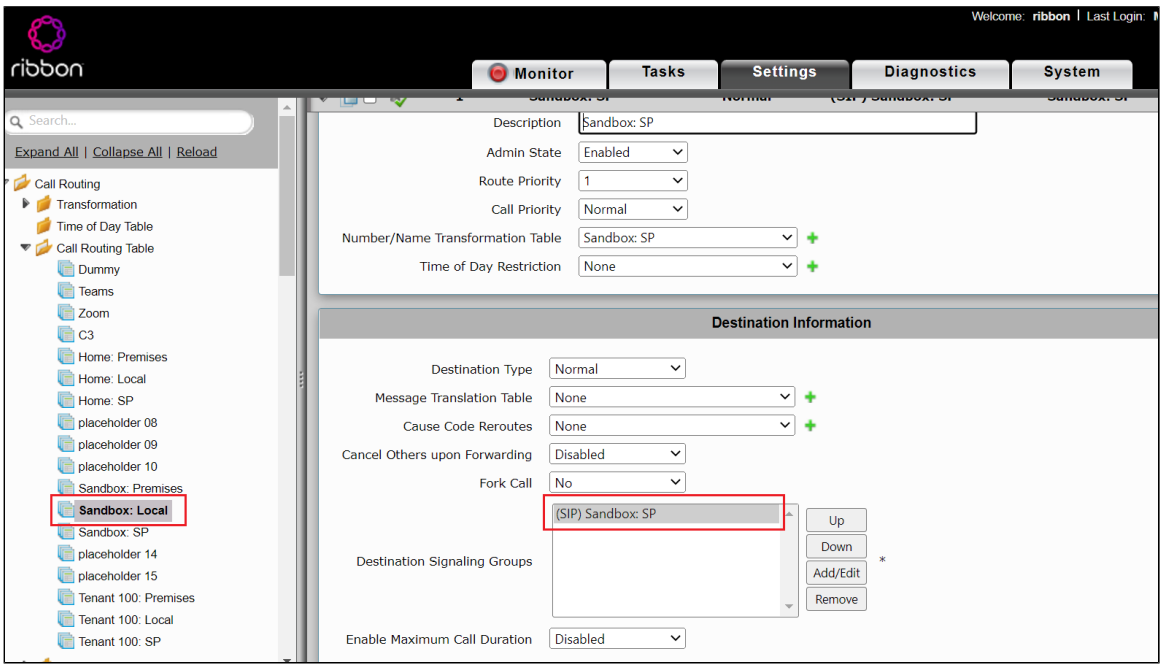


Sandbox_Local

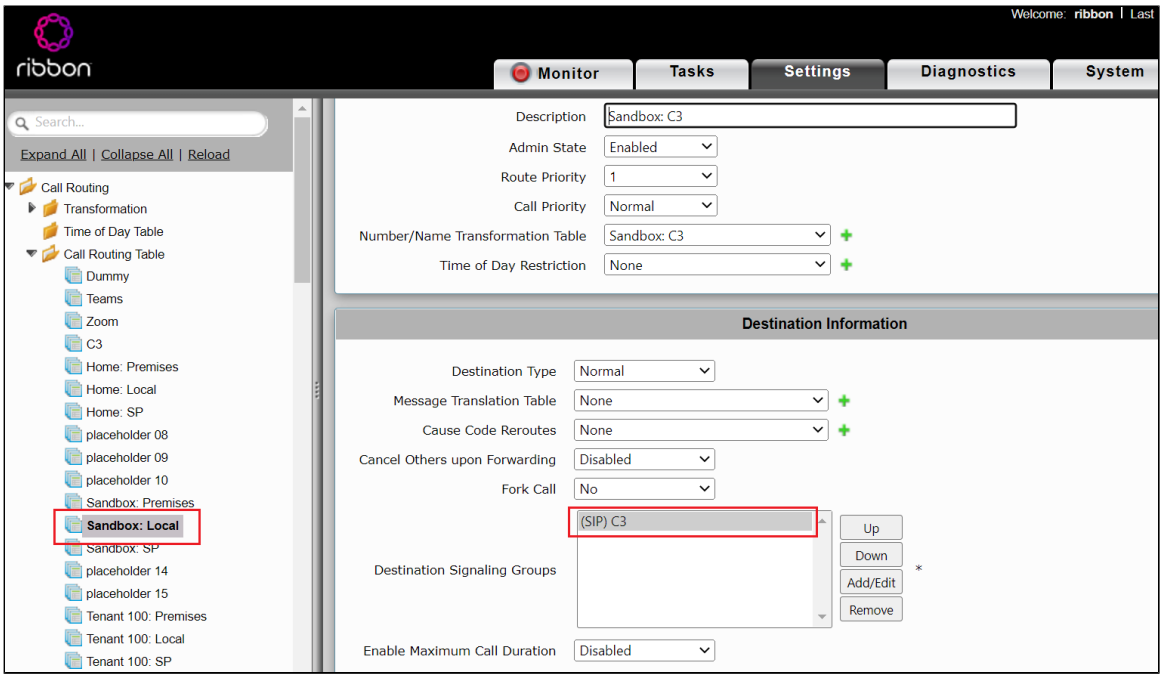
1. Navigate to **Call Routing > Call Routing Table**
2. Attach the Transformation Table entry created in the previous step.
3. Select the **Destination Signaling Group** as LOCAL_SG.



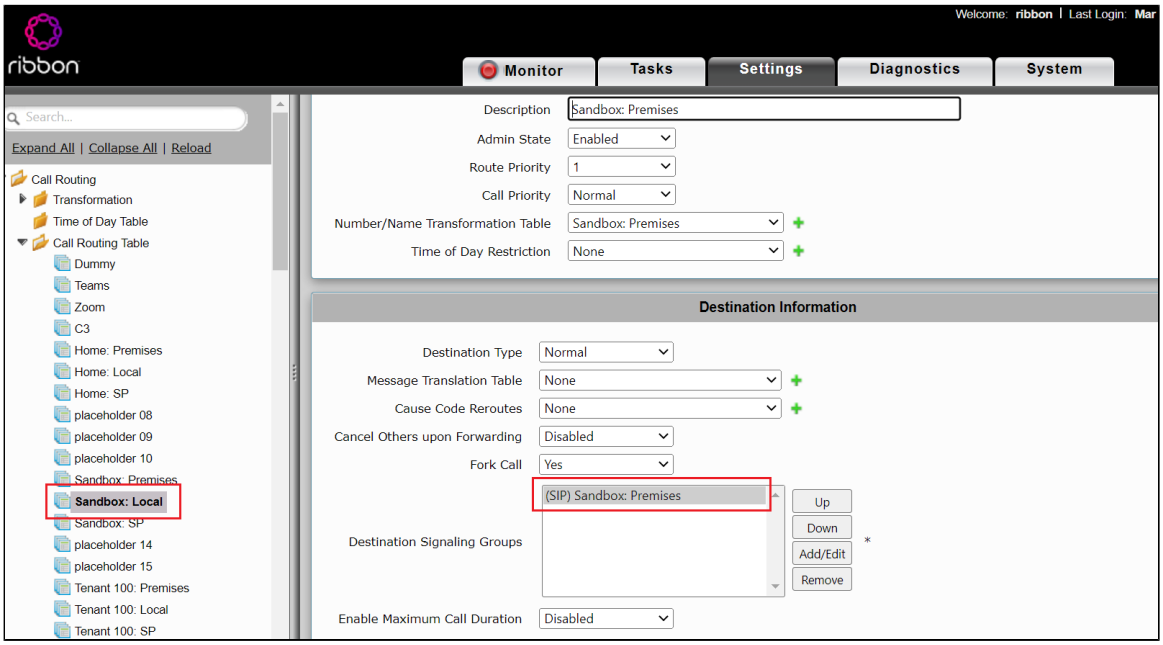
1. Select the **Destination Signaling Group** as Service_Provider_SG.



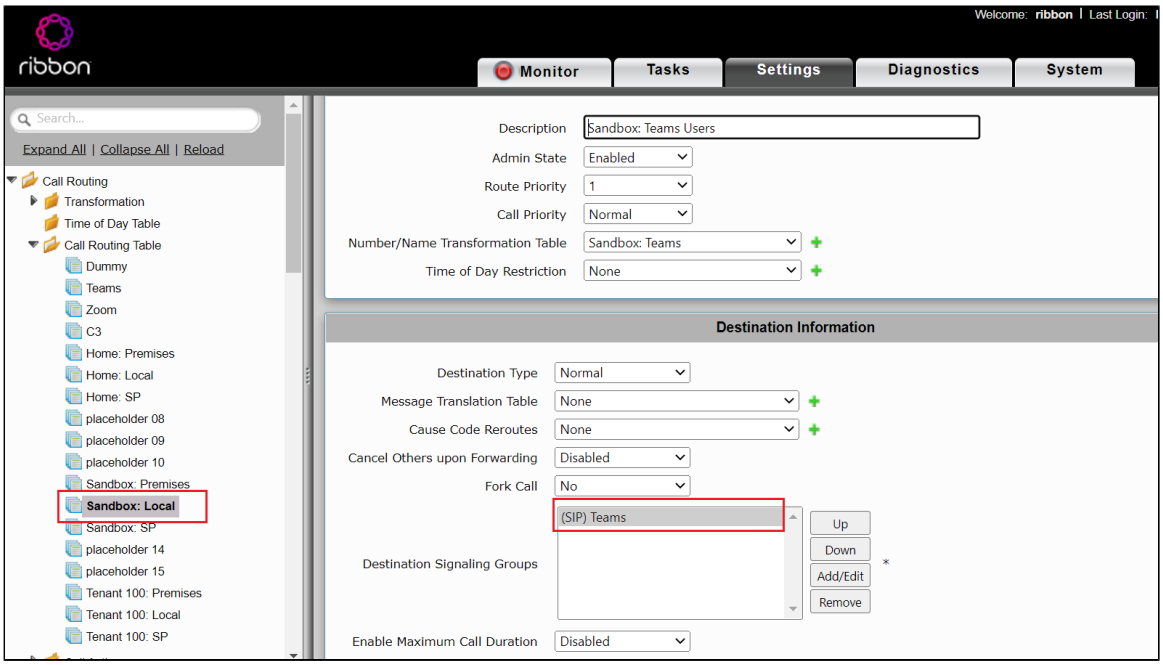
1. Select the **Destination Signaling Group** as C3_SG.



1. Select the **Destination Signaling Group** as Sandox_Premises_SG.

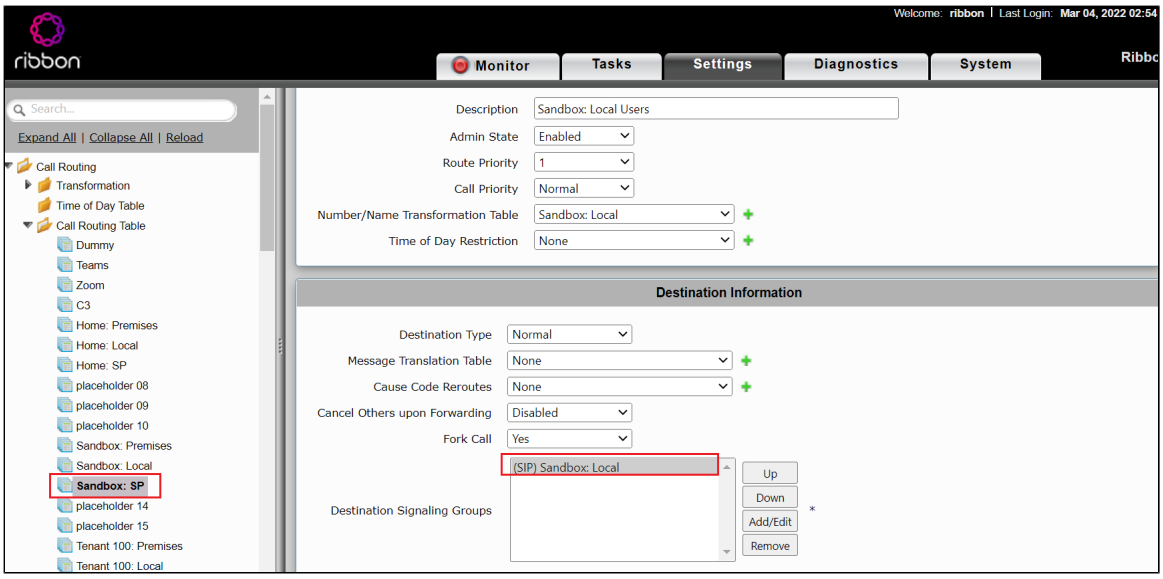


1. Select the **Destination Signaling Group** as Teams_SG.

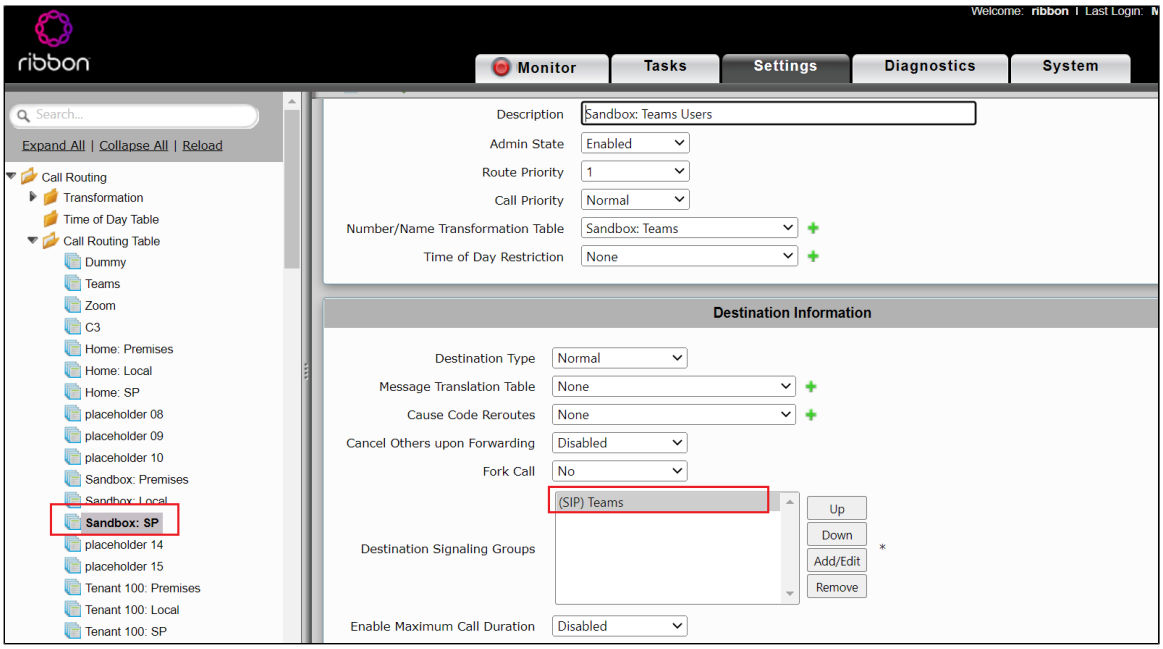


Sandbox_ServiceProvider

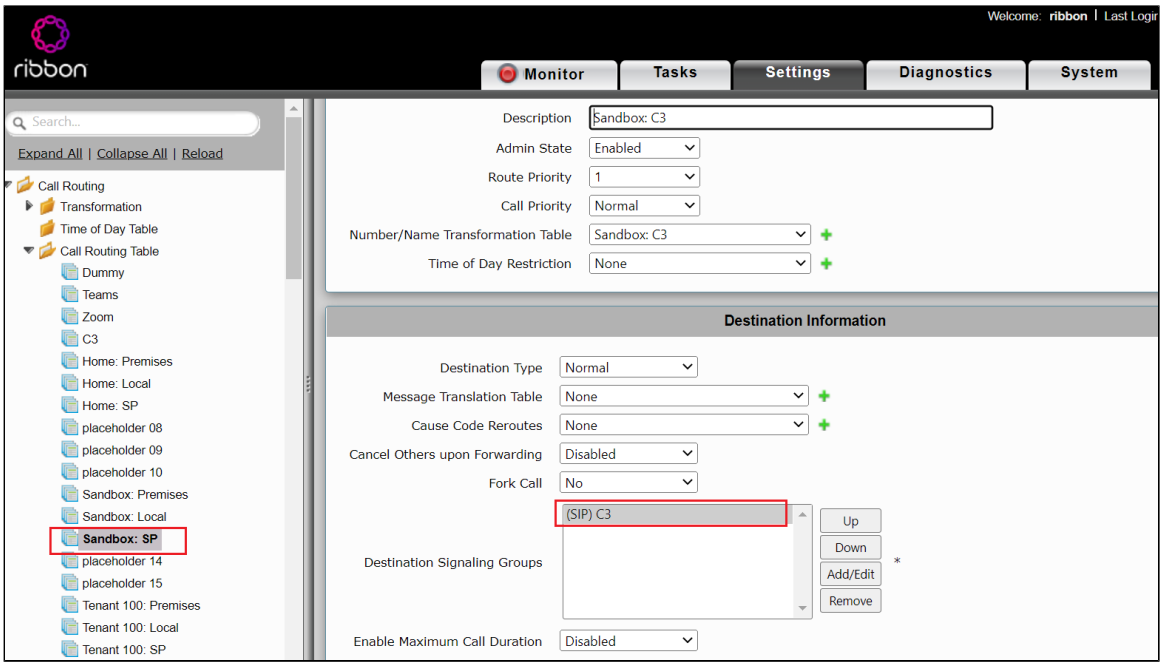
1. Navigate to **Call Routing > Call Routing Table**
2. Attach the Transformation Table entry created in the previous step.
3. Select the **Destination Signaling Group** as LOCAL_SG.



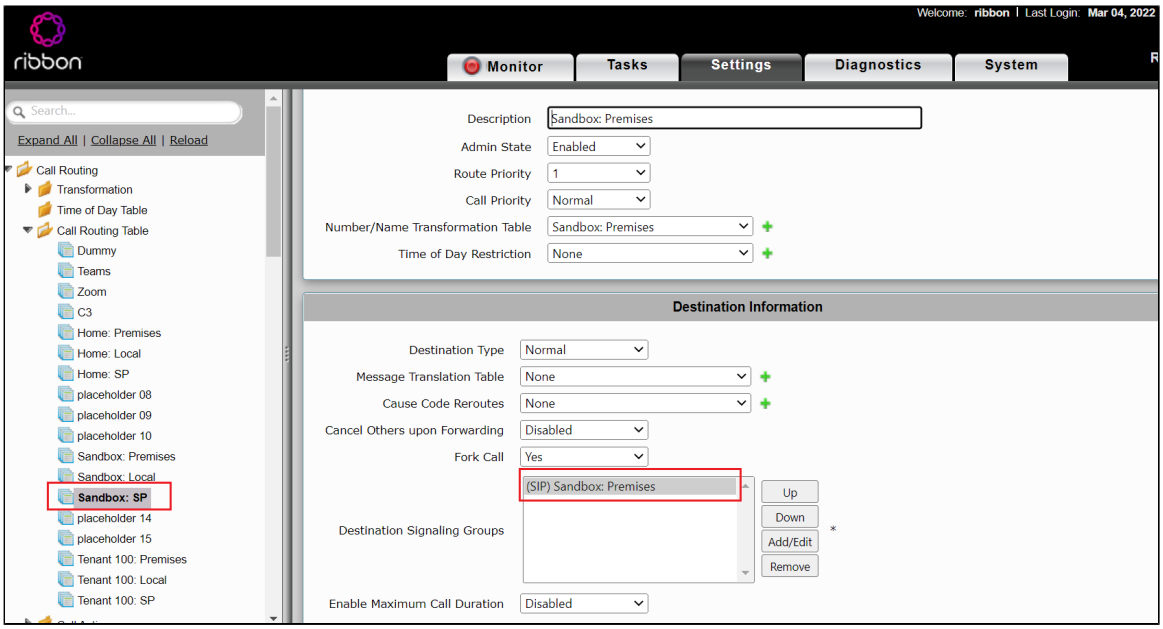
1. Select the **Destination Signaling Group** as Teams_SG.



1. Select the **Destination Signaling Group** as C3_SG.



1. Select the **Destination Signaling Group** as Premises_SG.



MIDA Configuration

To configure the MIDA Recorder, visit https://www.midasolutions.com/

Supplementary Services and Features Coverage

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

Sr. No.	Supplementary Services/ Features	Coverage
1	Call Setup and Termination over TLS/TCP	✓
2	Call Transfer (Blind/Unattended)	✓
3	Call Transfer (Consultative/Attended)	✓
4	Call hold and Resume (with MOH V1 enabled)	✓
5	Long Duration	✓
6	DTMF handling-OutofBand	✓
7	Direct Media	✓
8	DTMF - Inband and RFC2833	✓
9	Round Robin Option for SRS recorder	✓
10	4xx/5xx Response Handling	✓
11	Call Forward - No Answer	✓
12	Call Park and Retrieve	✓
13	Simultaneous Ringing	✓
14	SRTP on Recording Session	✗

15	Session Refresh	✓
16	Transcoded calls	✓
17	Call Mute (Comfort Noise)	✗

Legend

Supported	✓
Not Supported	✗

Caveats

The following items should be noted in relation to this Interop. These are either limitations or test observations pertaining to this Interoperability.

- SBC SWe Lite does not send encrypted media to the SIPREC as it is currently not supported.
  - Fix for this issue would be a part of upcoming releases.
- SWe Lite does not send Re-INVITE for Recording Server when codec renegotiation occurs between two endpoints via UPDATE.
  - Fix for this issue would be a part of upcoming releases.
- Coredump occurs on SWe Lite when OPUS codec is negotiated between two endpoints.
  - Issue is fixed in Release 9.0.9.
- Long duration calls fail as SWe Lite doesn't send session refresh INVITE with SAVP and crypto towards Teams endpoint.
  - Issue is fixed in Release 9.0.8.
- There is no audio observed when G722 codec is negotiated between two endpoints.
  - Issue is fixed in Release 9.0.8.
- CN (Comfort Noise) parameter is not honored by MIDA Recorder.

Support

For any support related queries about this guide, please contact your local Ribbon representative or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: https://ribboncommunications.com/services/ribbon-support-portal

References

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

For detailed information about MIDA products and solutions, please visit:
https://www.midasolutions.com/

Conclusion

This Interoperability Guide describes how to configure Ribbon SBC SWe Lite with the MIDA Recorder.

All features and capabilities tested are detailed within this document - any limitations, notes or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there may be additional configuration changes required to suit the exact deployment environment.