Ribbon SBC Edge SWe Lite R9.0 on AWS Interop with Cisco UCM and Microsoft Teams Direct Routing for Twilio Elastic SIP Trunking

Interoperability Guide

Table of Contents

Interoperable Vendors

amazon web services CISCO Microsoft Teams twilio

Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document provides the configuration details for Ribbon's SBC SWe Lite interworking with Twilio Elastic SIP Trunk, Microsoft Teams Direct Routing and Cisco Unified Communication Manager.

About Ribbon SBC SWe Lite

The Ribbon Session Border Controller Software Edition Lite (SBC SWe Lite) provides best-in class communications security. The SBC SWe Lite dramatically simplifies the deployment of robust communications security services for SIP Trunking, Direct Routing, and Cloud UC services. SBC SWe Lite operates natively in the Azure and AWS Cloud as well as on virtual machine platforms including Microsoft Hyper-V, VMware and Linux KVM.

About Twilio Elastic SIP Trunking

Twilio has developed an advanced SIP trunking service that addresses the key challenges that are holding back enterprises from realizing their communications transformation goals. Twilio Elastic SIP Trunking delivers global PSTN connectivity that enables enterprises to increase business agility, reduce costs and deliver uniform global reach.

About Microsoft Teams Direct Routing

Microsoft Phone System Direct Routing allows connection of a supported customer-provided Session Border Controller (SBC) to a Microsoft Phone System. Direct Routing enables using virtually any PSTN trunk with Microsoft Phone System and configuring interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

About Cisco Unified Communication Manager

Cisco Unified Communication Manager is a core call-control application of Cisco UCM. It provides enterprise-class call control, session management, voice, video, messaging, mobility and conferencing services in a way that is efficient, highly secure, scalable and reliable.

Scope

This document provides configuration best practices for deploying Ribbon's SBC SWe Lite with Cisco Unified Communication Manager (CUCM) and Microsoft Teams for Twilio Elastic SIP Trunking 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 which best meets their requirements.

Non-Goals

It is not the goal of this guide to provide detailed configurations that will 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 with the purpose of configuring 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 any required troubleshooting.

Prerequisites

The following aspects are required before proceeding with the interop:

- Amazon Web Services (AWS) subscription
- Ribbon SBC SWe Lite on AWS
- SBC SWe Lite License
    - This interop requires the acquisition and application of cloud SIP sessions, as documented at Cloud-Based SBC SWe Lite Deployment Licenses

- Public IP Addresses
- Twilio Elastic SIP Trunk
  - Contact Twilio for Domain, IP and Port information
  - For more details, visit https://www.twilio.com/docs/sip-trunking or see the " Twilio Elastic SIP Trunk Configuration" section of this document
- TLS Certificates for SBC SWe Lite
  - Please refer to Working with Certificates

Product and Device Details

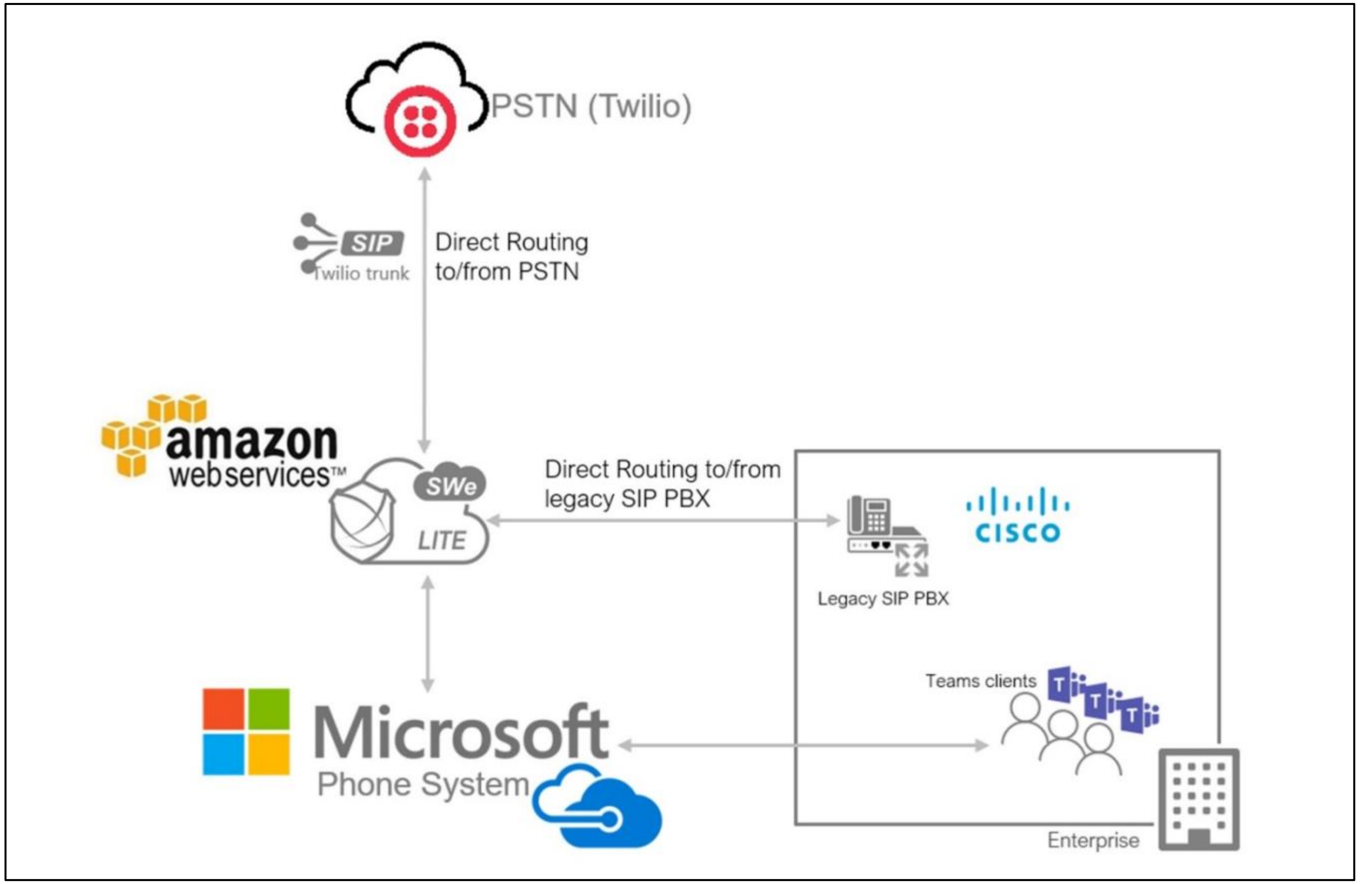
The configuration uses the following equipment and software:

Table 1: Requirements

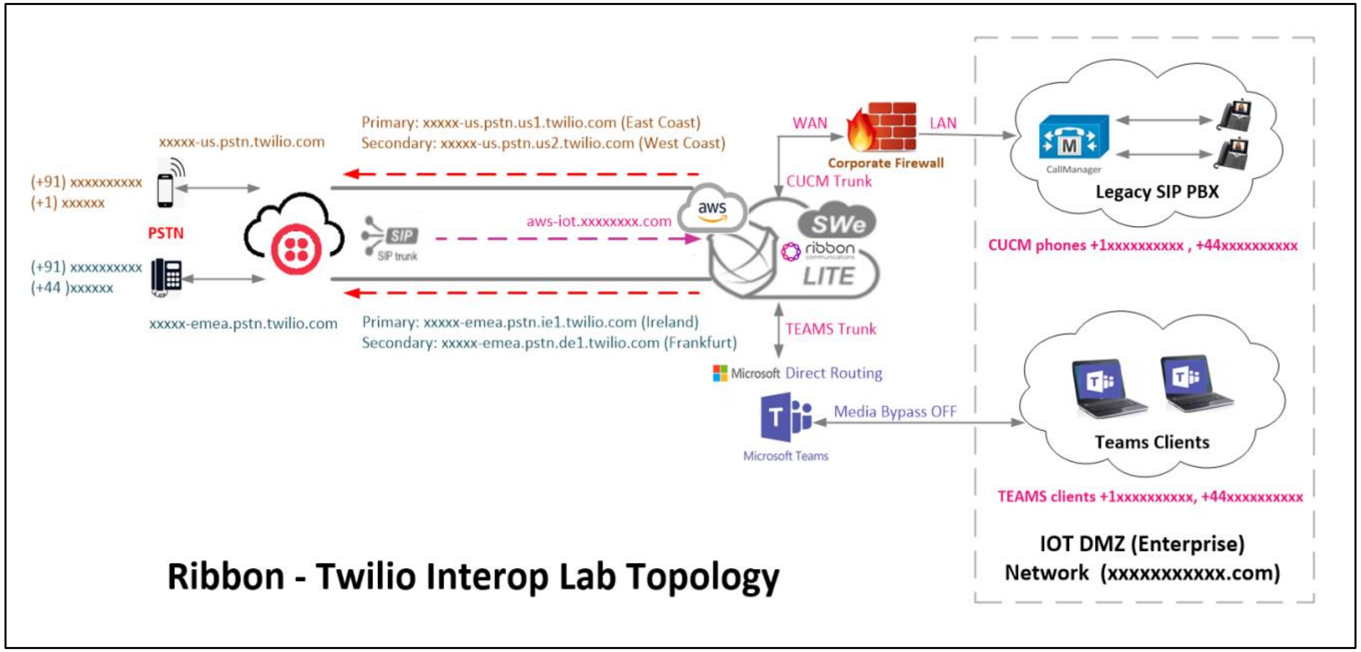
Product	**Equipment**	**Software Version**
Ribbon Networks	Ribbon SBC Swe Lite	9.0.1
Third-party Equipment	Cisco Unified Communication Manager	12.5.1.11900-146
Microsoft Corporation	Microsoft Teams Client	1.3.00.30866
Twilio	Elastic SIP Trunking service	NA
Administration and Debugging Tools	Wireshark LX Tool	3.2.7 2.1.0.6

Network Topology and E2E Flow Diagrams

SBC SWe Lite - Twilio Deployment Topology



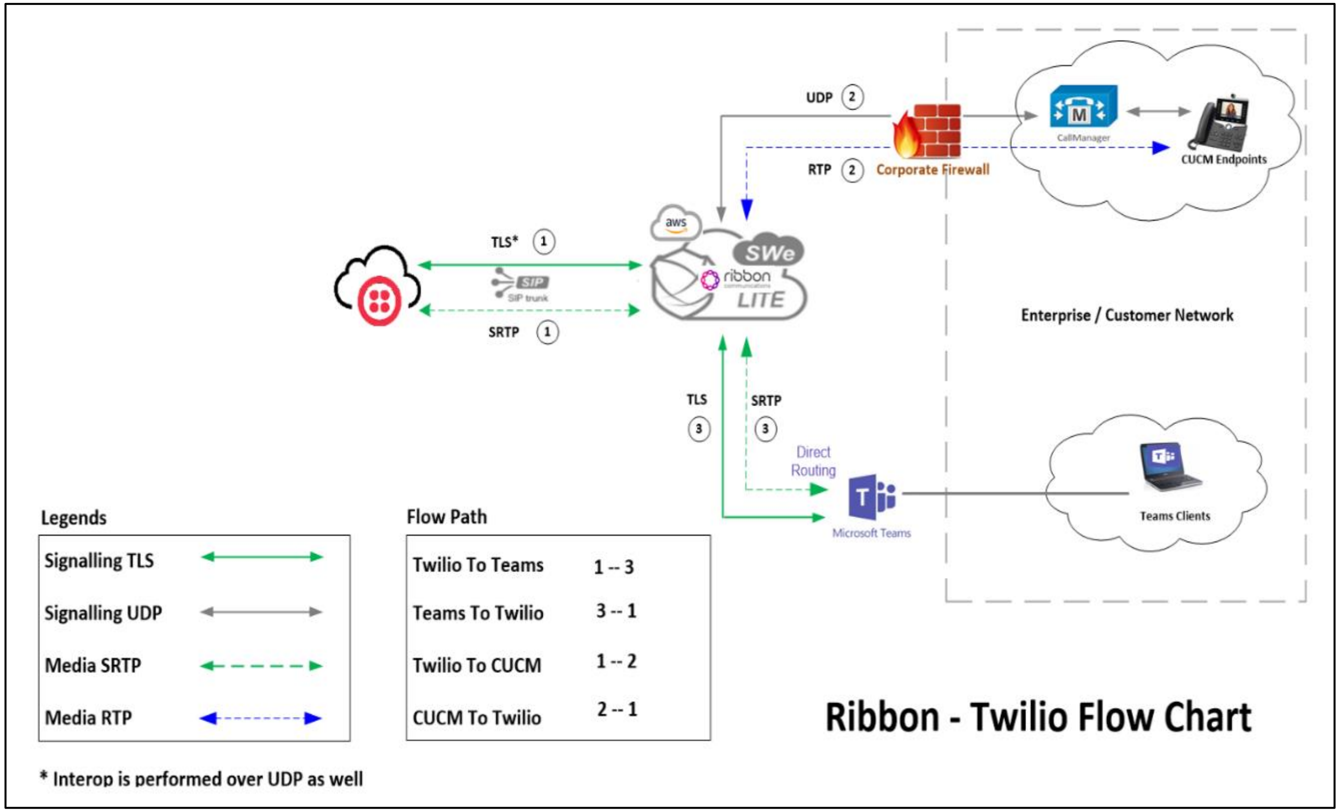
SBC SWe Lite - Twilio Lab Topology


xxxxx-us.pstn.twilio.com
Primary: xxxxx-us.pstn.us1.twilio.com (East Coast)
Secondary: xxxxx-us.pstn.us2.twilio.com (West Coast)
(+91) xxxxxxxxxx
(+1) xxxxxx
PSTN
(+91) xxxxxxxxxx
(+44)xxxxxx
SIP
SIP trunk
aws-iot.xxxxxxxx.com
aws
xxxxx-emea.pstn.twilio.com
Primary: xxxxx-emea.pstn.ie1.twilio.com (Ireland)
Secondary: xxxxx-emea.pstn.de1.twilio.com (Frankfurt)
WAN
LAN
Corporate Firewall
CUCM Trunk
SWe
ribbon communications
LITE
TEAMS Trunk
Microsoft Direct Routing
Media Bypass OFF
Microsoft Teams
CallManager
Legacy SIP PBX
CUCM phones +1xxxxxxxxxx , +44xxxxxxxxxx
Teams Clients
TEAMS clients +1xxxxxxxxxx, +44xxxxxxxxxx
IOT DMZ (Enterprise)
Network (xxxxxxxxxxx.com)
Ribbon - Twilio Interop Lab Topology

Note

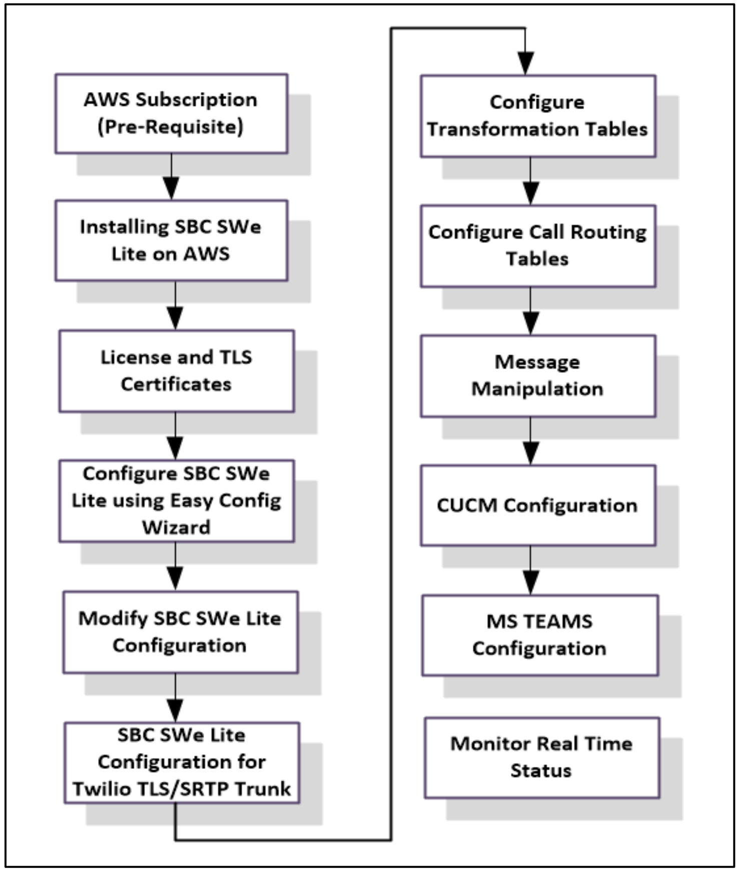
Two Trunks (US and EMEA) were included for testing purpose. Customers can configure the Trunks as per their requirement.

Signaling and Media Flow



Document Workflow

The sections in this document follow the sequence below. The reader is advised to complete each section for the successful configuration.


AWS Subscription (Pre-Requisite)
Installing SBC SWe Lite on AWS
License and TLS Certificates
Configure SBC SWe Lite using Easy Config Wizard
Modify SBC SWe Lite Configuration
SBC SWe Lite Configuration for Twilio TLS/SRTP Trunk
Configure Transformation Tables
Configure Call Routing Tables
Message Manipulation
CUCM Configuration
MS TEAMS Configuration
Monitor Real Time Status

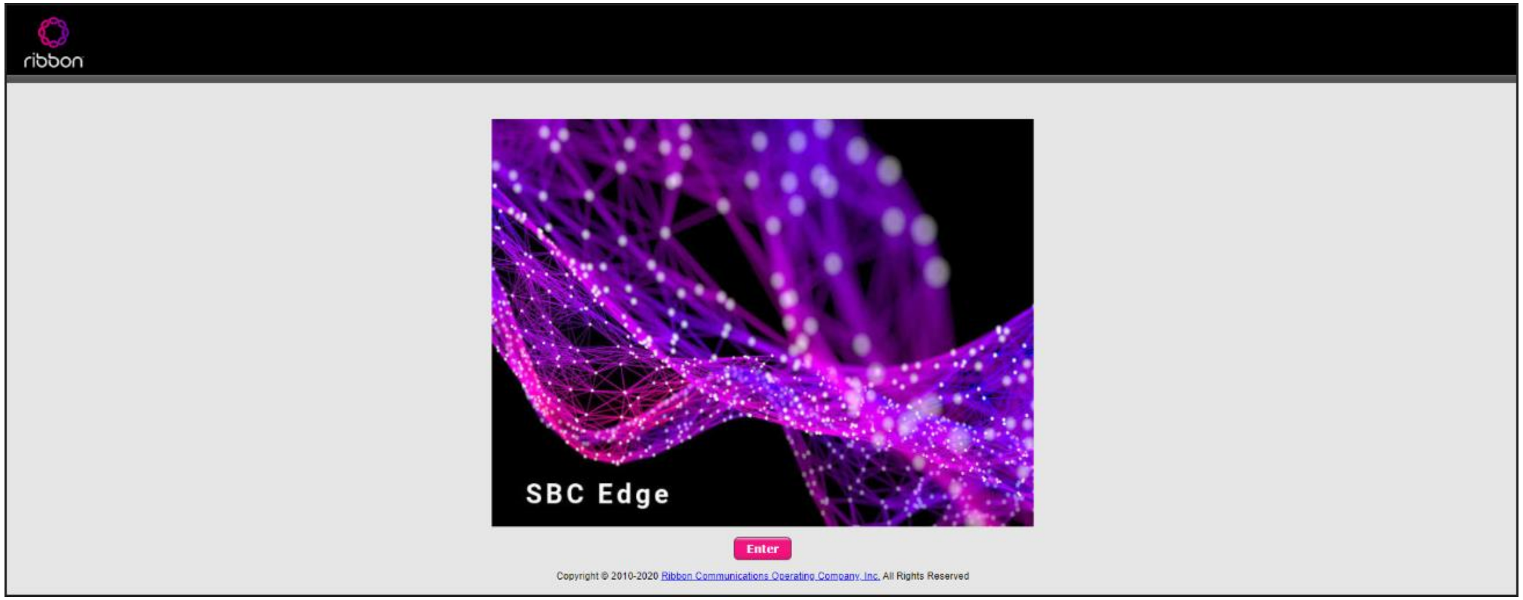
Installing SBC SWe Lite on AWS

The SBC SWe Lite is available for deployment in AWS. It is created as a virtual machine (VM) hosted in AWS. To deploy an SBC SWe Lite instance, refer to Deploying an SBC SWe Lite via Amazon Web Services-AWS. Once SWe Lite instance is successfully created on AWS, kindly retrieve the allocated NAT Public IPs, Ethernet IPs & Management IPs. Also ensure Twilio IP addresses are whitelisted on AWS access list. For more details, kindly find the link given in the references section.

SBC SWe Lite Configuration

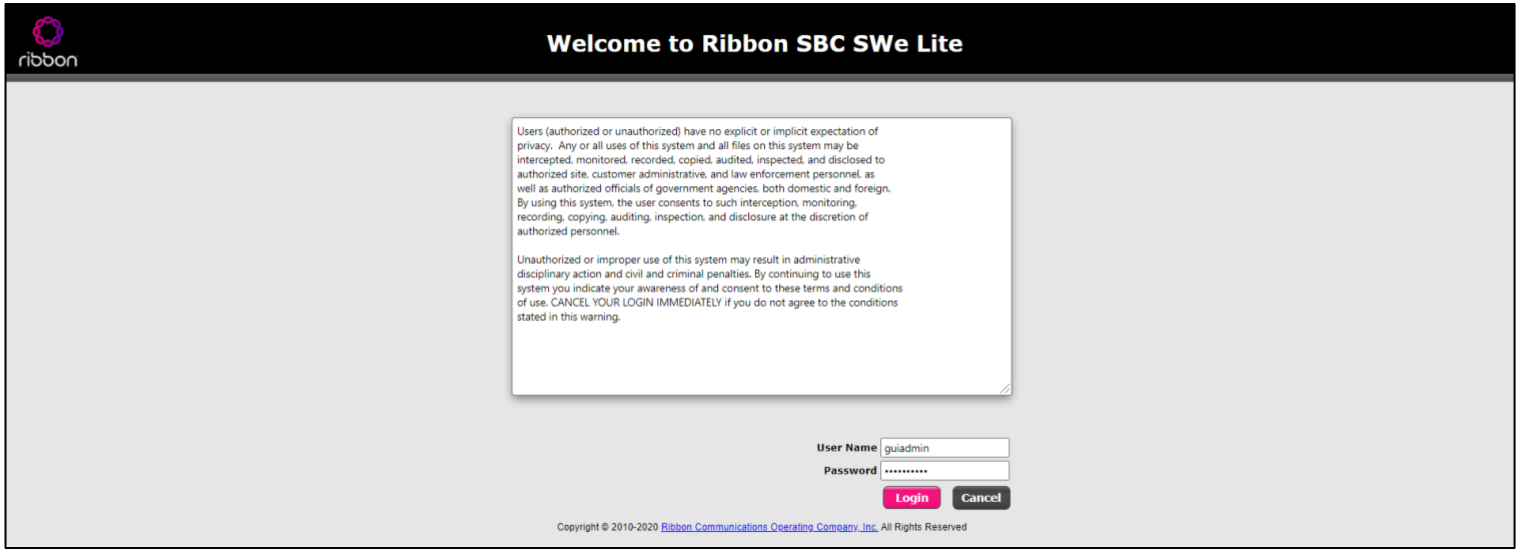
Accessing SBC SWe Lite

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



Copyright © 2010-2020 Ribbon Communications Operating Company, Inc. All Rights Reserved

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



Welcome to Ribbon SBC SWe Lite

Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, customer administrative, and law enforcement personnel, as well as authorized officials of government agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. CANCEL YOUR LOGIN IMMEDIATELY if you do not agree to the conditions stated in this warning.

User Name: guiadmin

Password: ••••••••••

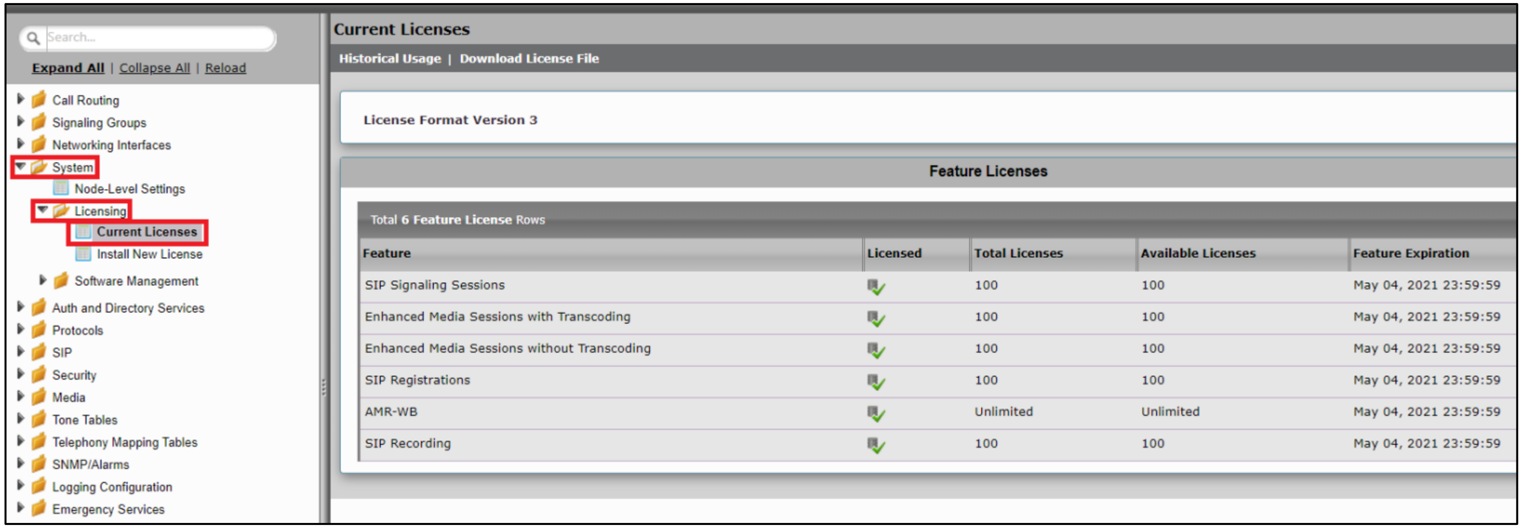
Copyright © 2010-2020 Ribbon Communications Operating Company, Inc. All Rights Reserved

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 panel enables you to verify whether a feature is licensed, along with the number of remaining licenses available for a given feature at run-time.

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



Current Licenses

License Format Version 3

Feature Licenses

Total 6 Feature License Rows

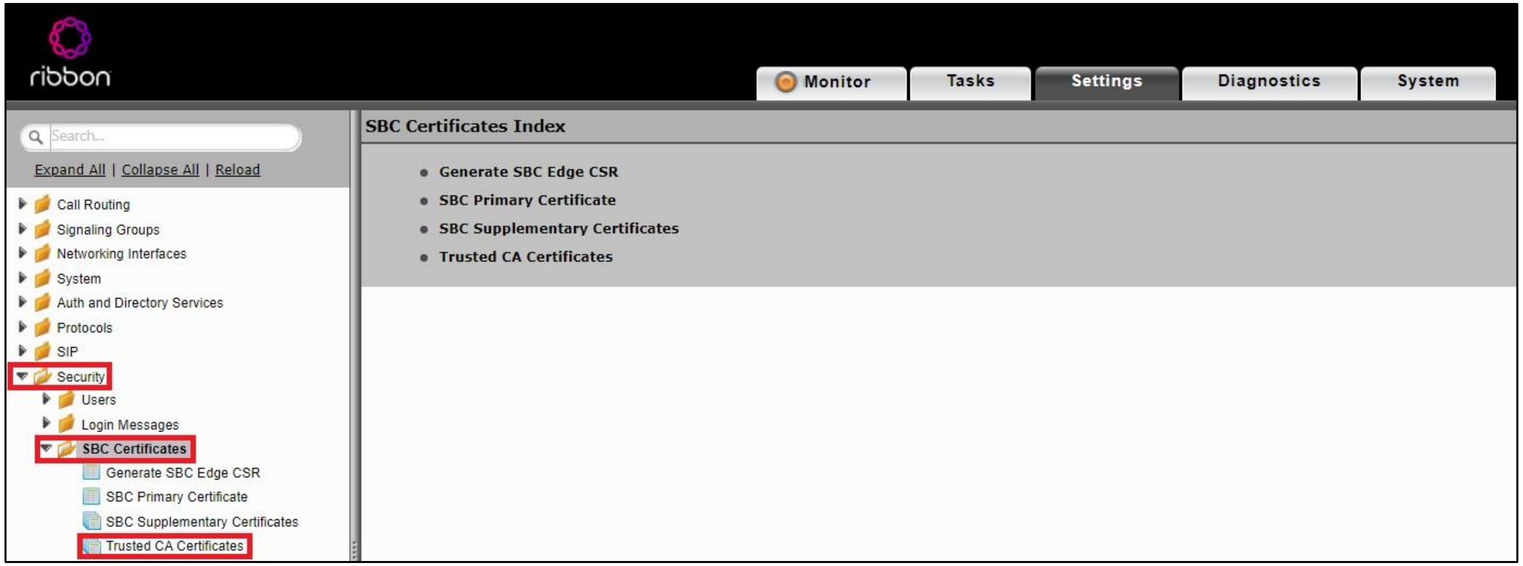
Feature	Licensed	Total Licenses	Available Licenses	Feature Expiration
SIP Signaling Sessions	✓	100	100	May 04, 2021 23:59:59
Enhanced Media Sessions with Transcoding	✓	100	100	May 04, 2021 23:59:59
Enhanced Media Sessions without Transcoding	✓	100	100	May 04, 2021 23:59:59
SIP Registrations	✓	100	100	May 04, 2021 23:59:59
AMR-WB	✓	Unlimited	Unlimited	May 04, 2021 23:59:59
SIP Recording	✓	100	100	May 04, 2021 23:59:59

For more details on Licenses, refer to Cloud-Based SBC SWe Lite Deployment Licenses.

Import Trusted Root CA Certificates

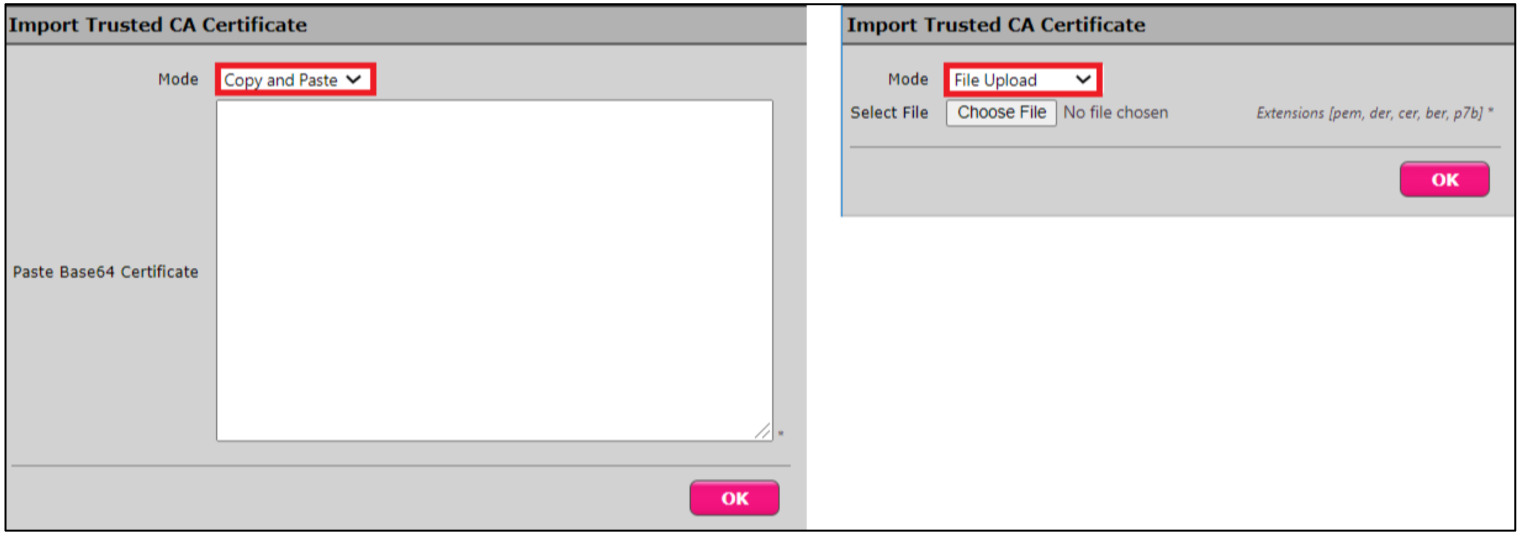
A Trusted CA Certificate is a certificate issued by a trusted certificate authority. Trusted CA Certificates are imported to the SBC SWe Lite to establish its authenticity on the network.

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



This section describes the process of importing Trusted Root CA Certificates, using either the File Upload or Copy and Paste methods.

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.



Import Trusted CA Certificate

Mode: Copy and Paste

Paste Base64 Certificate

Import Trusted CA Certificate

Mode: File Upload

Select File: Choose File No file chosen

Extensions [pem, der, cer, ber, p7b] *

Follow the above steps to import the Service Provider's (Twilio) Root and Intermediate certificates of their Public CA.

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

Note

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 before importing a new certificate successfully.

Warning

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.

View Networking Interfaces

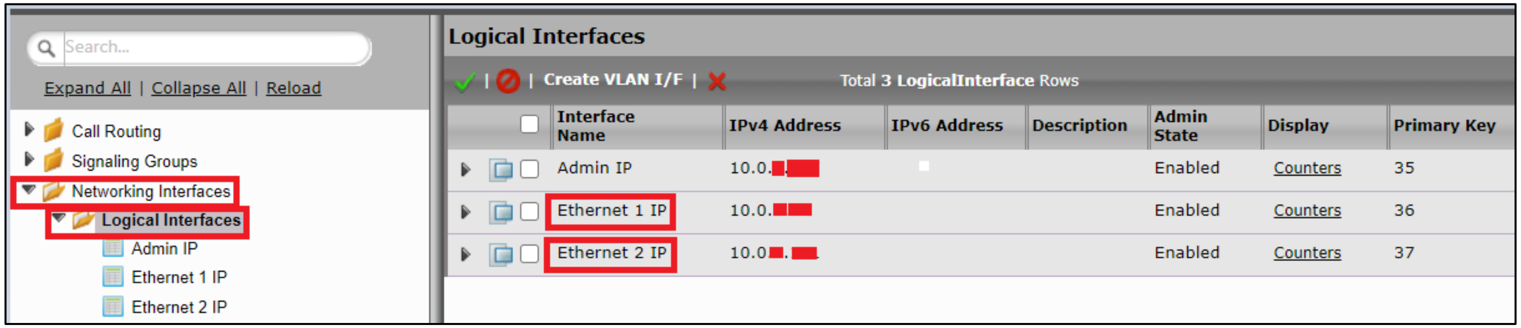
The SBC SWe Lite supports five system created logical interfaces (known as Administrative IP, Ethernet 1 IP, Ethernet 2 IP, Ethernet 3 IP, and Ethernet 4 IP). In addition to the system created logical interfaces, the Ribbon SBC SWe supports user-created VLAN logical sub-interfaces.

Administrative IP, Ethernet 1 IP and Ethernet 2 IP are used for this interop.

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

Administrative IP

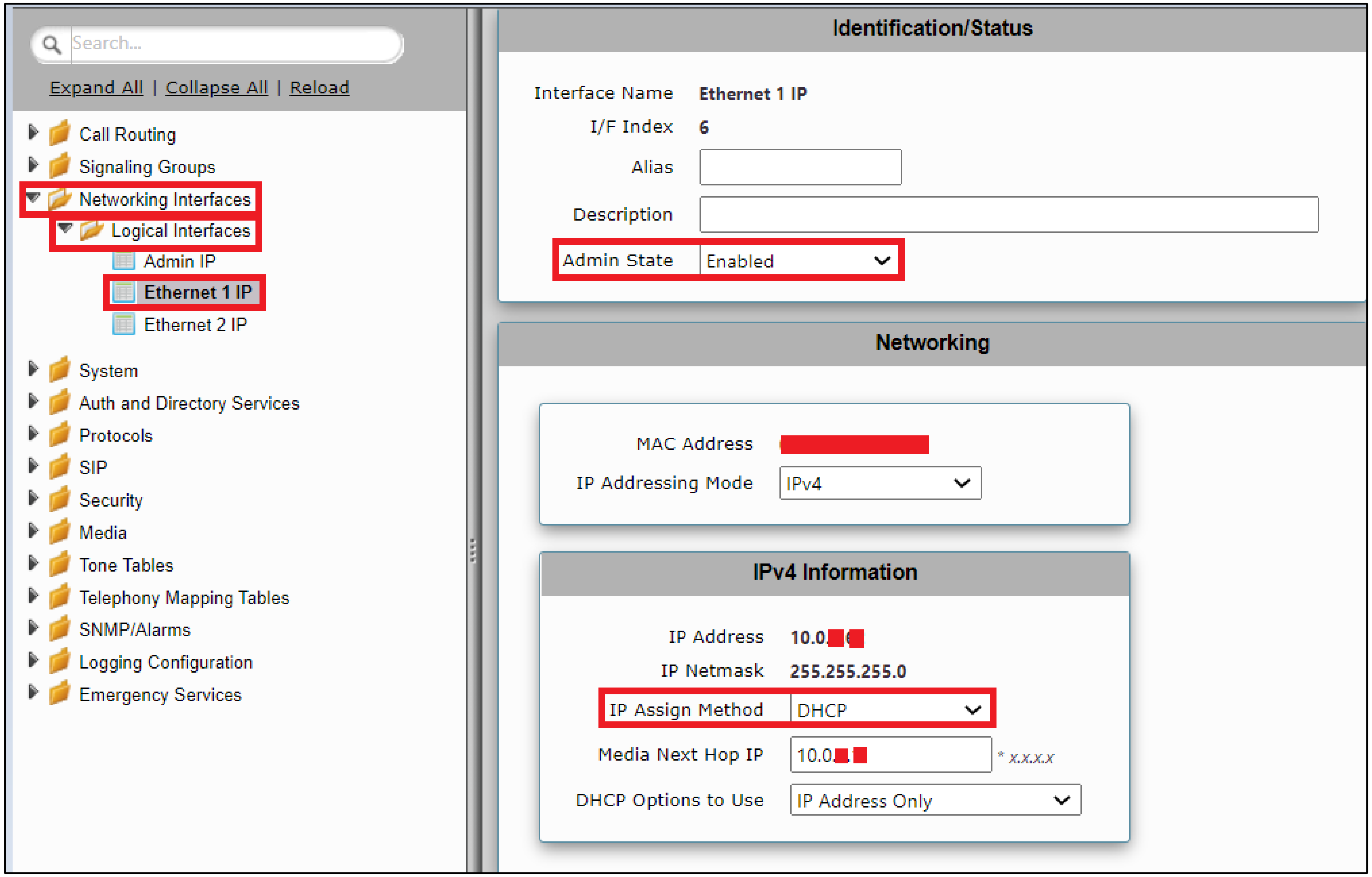
The SBC SWe Lite system supports a logical interface called the Admin IP (Administrative IP, also known as the Management IP). A Static IP or DHCP is used for running Initial Setup of the SBC SWe Lite system.



	Interface Name	IPv4 Address	IPv6 Address	Description	Admin State	Display	Primary Key
□	Admin IP	10.0.[redacted]			Enabled	Counters	35
□	Ethernet 1 IP	10.0.[redacted]			Enabled	Counters	36
□	Ethernet 2 IP	10.0[redacted].[redacted]			Enabled	Counters	37

Ethernet 1 IP

Ethernet 1 IP is assigned an IP address used for transporting all the VOIP media packets (for example, RTP, SRTP) and all protocol packets (for example, SIP, RTCP, TLS). DNS servers of the customer's network should map 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 via a connected DHCP server. This IP address is used for performing Initial Setup on the SBC SWe Lite.



Identification/Status

Interface Name	Ethernet 1 IP
I/F Index	6
Alias	
Description	
Admin State	Enabled

Networking

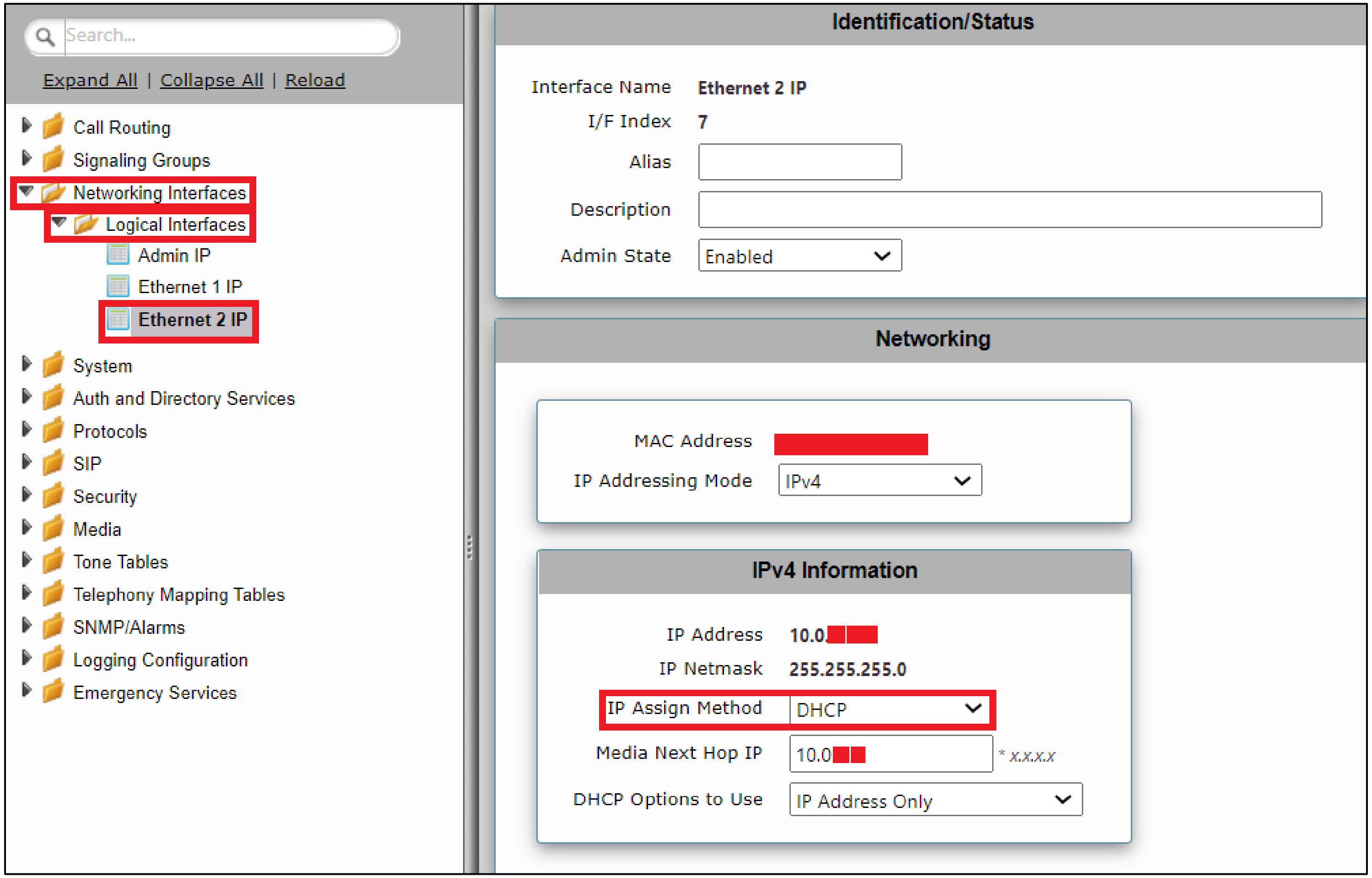
MAC Address	[redacted]
IP Addressing Mode	IPv4

IPv4 Information

IP Address	10.0.[redacted]
IP Netmask	255.255.255.0
IP Assign Method	DHCP
Media Next Hop IP	10.0.[redacted] * x.x.x.x
DHCP Options to Use	IP Address Only

Ethernet 2 IP

After initial configuration, you may configure this logical interface using the Settings or Tasks tabs in the WebUI, or you can use the IP address configured during Initial Setup.



Identification/Status

Interface Name: Ethernet 2 IP
I/F Index: 7
Alias:
Description:
Admin State: Enabled

Networking

MAC Address: [redacted]
IP Addressing Mode: IPv4

IPv4 Information

IP Address: 10.0[redacted]
IP Netmask: 255.255.255.0
IP Assign Method: DHCP
Media Next Hop IP: 10.0[redacted] * x.x.x.x
DHCP Options to Use: IP Address Only

Configure Static Routes

Static routes are used to create communication to 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 (single path access or default route).

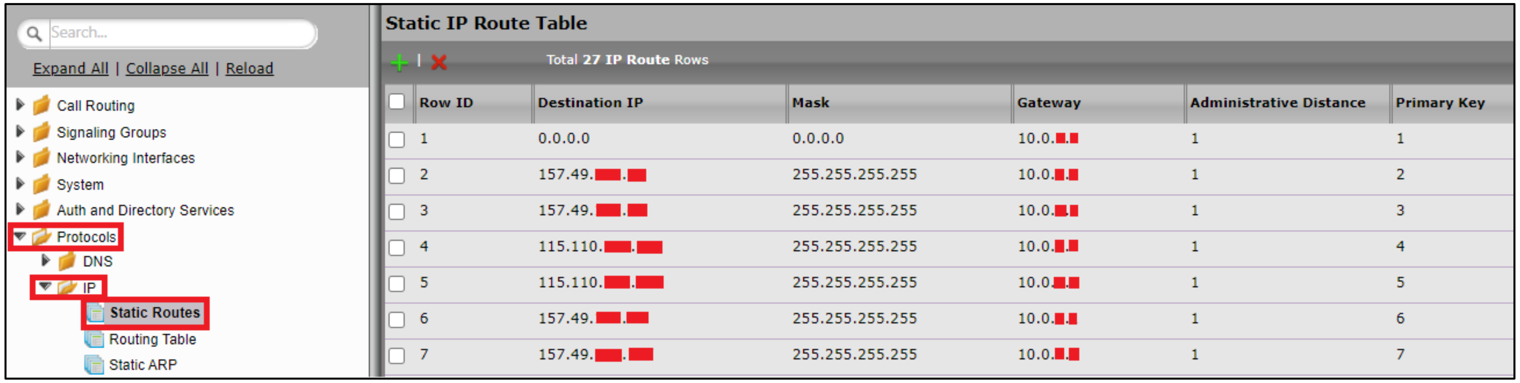
Derive the Private IP address and Gateway for each interface on AWS.

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.



Static IP Route Table

Total 27 IP Route Rows

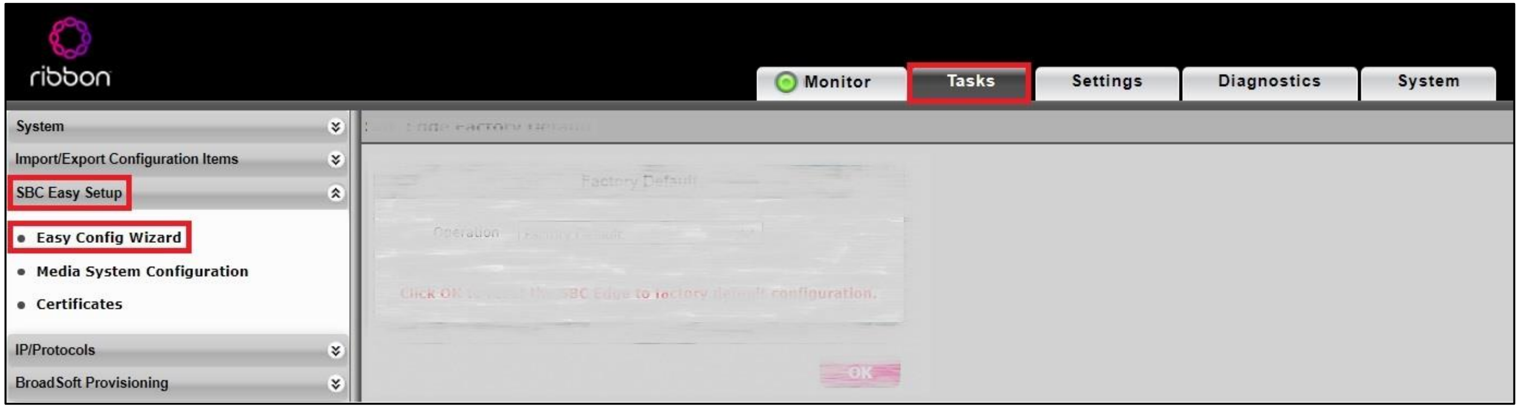
□	Row ID	Destination IP	Mask	Gateway	Administrative Distance	Primary Key
□	1	0.0.0.0	0.0.0.0	10.0.[redacted]	1	1
□	2	157.49.[redacted]	255.255.255.255	10.0.[redacted]	1	2
□	3	157.49.[redacted]	255.255.255.255	10.0.[redacted]	1	3
□	4	115.110.[redacted]	255.255.255.255	10.0.[redacted]	1	4
□	5	115.110.[redacted]	255.255.255.255	10.0.[redacted]	1	5
□	6	157.49.[redacted]	255.255.255.255	10.0.[redacted]	1	6
□	7	157.49.[redacted]	255.255.255.255	10.0.[redacted]	1	7

Easy Config Wizard

Access the Easy Configuration Wizard

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, navigate to **SBC Easy Setup > Easy Config Wizard.** The Easy Configuration screen opens.

The SBC Edge WebUI provides a built-in Easy Configuration wizard that lets you quickly and easily deploy the SBC for operation with provider endpoints (SIP trunk, ISDN PSTN trunk, or IP PBX trunk) and user endpoints (Microsoft Teams, Microsoft On Premises - Skype for Business/Lync, IP Phones, or ISDN PBX or IP PBX).



Navigating the Wizard

As the wizard runs, it directs you through three configuration steps:

Step 1: Set the following parameters to describe the topology for the telephony service provider and user ends of the scenario.

- **Application**: Click the drop-down arrow, then select the Service Provider and user endpoint types that the SBC is to connect to.
- **Scenario Description**: Type up to 32 characters to describe the connectivity scenario.
- **Telephone Country**: Click the drop-down arrow, then select the country in which the telephone services operate.
- **Emergency Services**: Choose **ELIN Identifier**, **E911/E112**, or **None** as the emergency services type.
- **SIP Sessions**: Type a number from 1-1200 to indicate the SIP sessions to allocate for the scenario.

Step 2: Configure the items required for the endpoints selected, fields display based on the endpoint selection in Step 1.

Step 3: The Easy Config validates the final parameters and displays a read-only summary of the configuration that the wizard will apply when you click **Finish** at Step 3. Before you click **Finish**, you can return to previous steps to make adjustments to the data summarized.

The wizard displays the following buttons for navigation:

- **Previous**: Moves back to the previous step.
- **Next**: Advances to the next step when the current step is validated and complete.
- **Finish**: Submits the data to the SBC.
- **Cancel**: Cancels the Easy Configuration data entered and redirects to the main WebUI.

Configure SBC SWe Lite using Easy Config Wizard

During this interop:

- Multi-legged approach was used to configure Twilio US SIP Trunk and Microsoft Teams (Application: SIP Trunk ↔ Microsoft Teams)
- Single-legged approach was used to configure Twilio EMEA SIP Trunk (Application: SIP Trunk)
- Single-legged approach was used to configure CUCM (Application: IP PBX)

Tip

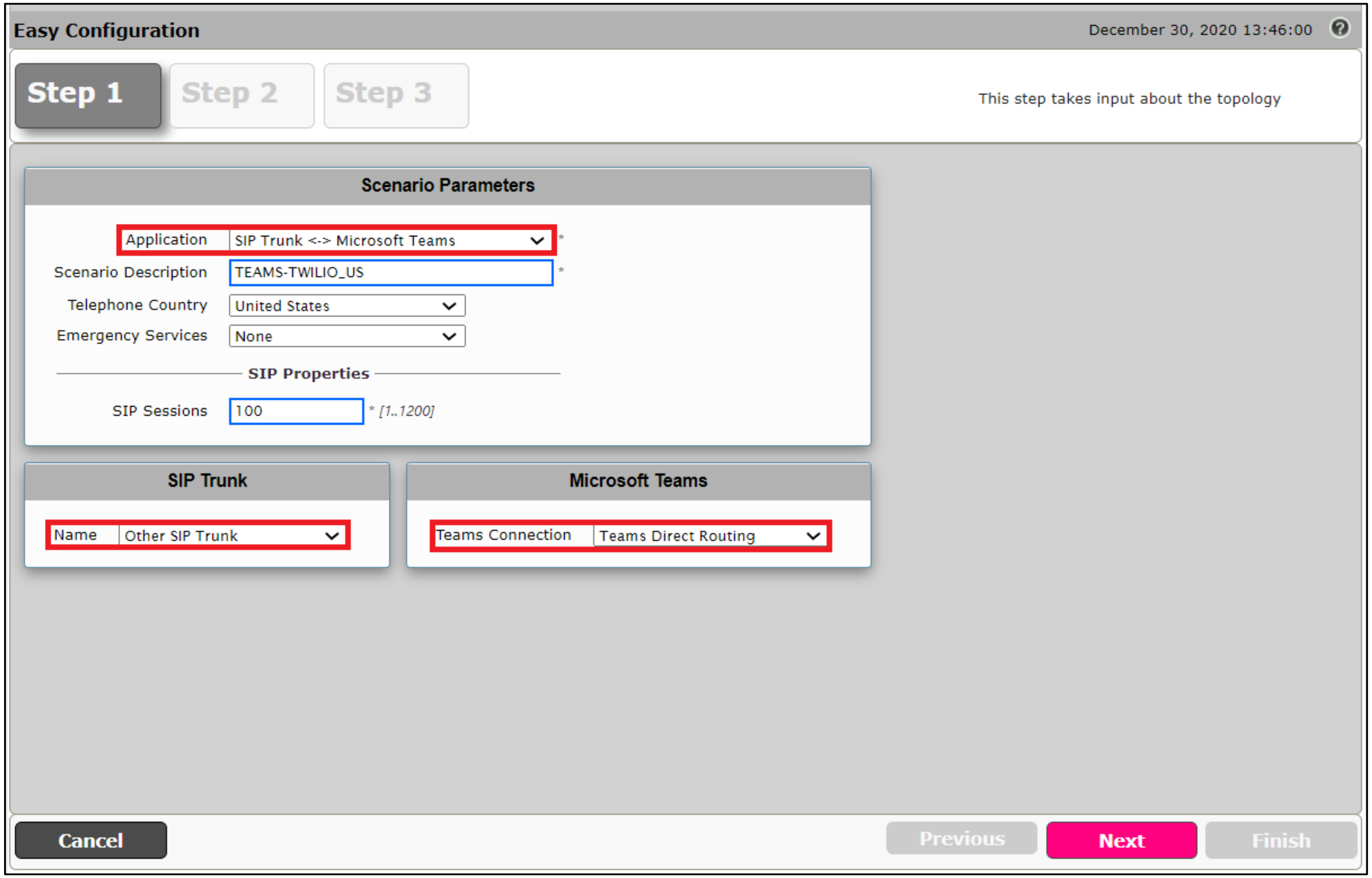
Customers can also choose any standard approach to configure SBC SWe Lite using Easy Config Wizard. The following are a few possible ways:

- Use the Multi-legged approach to configure Twilio EMEA SIP Trunk and Microsoft Teams (Application: SIP Trunk ↔ Microsoft Teams)
    - Then, use the Single-legged approach to configure Twilio US SIP Trunk (Application: SIP Trunk) and CUCM (Application: IP PBX)
- Use the Multi-legged approach to configure Twilio US SIP Trunk and CUCM (Application: SIP Trunk ↔ IP PBX)
    - Then, use the Single-legged approach to configure Twilio EMEA SIP Trunk (Application: SIP Trunk) and MS Teams (Application: Microsoft Teams)
- Use the Multi-legged approach to configure Twilio EMEA SIP Trunk and CUCM (Application: SIP Trunk ↔ IP PBX)
    - Then, use the Single-legged approach to configure Twilio US SIP Trunk (Application: SIP Trunk) and MS Teams (Application: Microsoft Teams)

Configure SBC SWe Lite for Twilio US Trunk and for Microsoft Teams

Step 1: Configure US Trunk for Twilio along with Microsoft Teams using Multi-legged approach by following the steps below:

1. Choose **SIP Trunk ↔ Microsoft Teams** from the Application dropdown.
2. Provide the Description.
3. Select **United States** in the **Telephone Country** field.
4. Type a number from 1-1200 against **SIP Sessions** field.
5. Select SIP Trunk Name as Other SIP Trunk for Twilio (US Trunk) and Microsoft Teams Connection as Teams Direct Routing.
6. Click **Next**.



Easy Configuration

December 30, 2020 13:46:00

This step takes input about the topology

Scenario Parameters

Application: SIP Trunk <-> Microsoft Teams *

Scenario Description: TEAMS-TWILIO_US *

Telephone Country: United States

Emergency Services: None

SIP Properties

SIP Sessions: 100 * [1..1200]

SIP Trunk

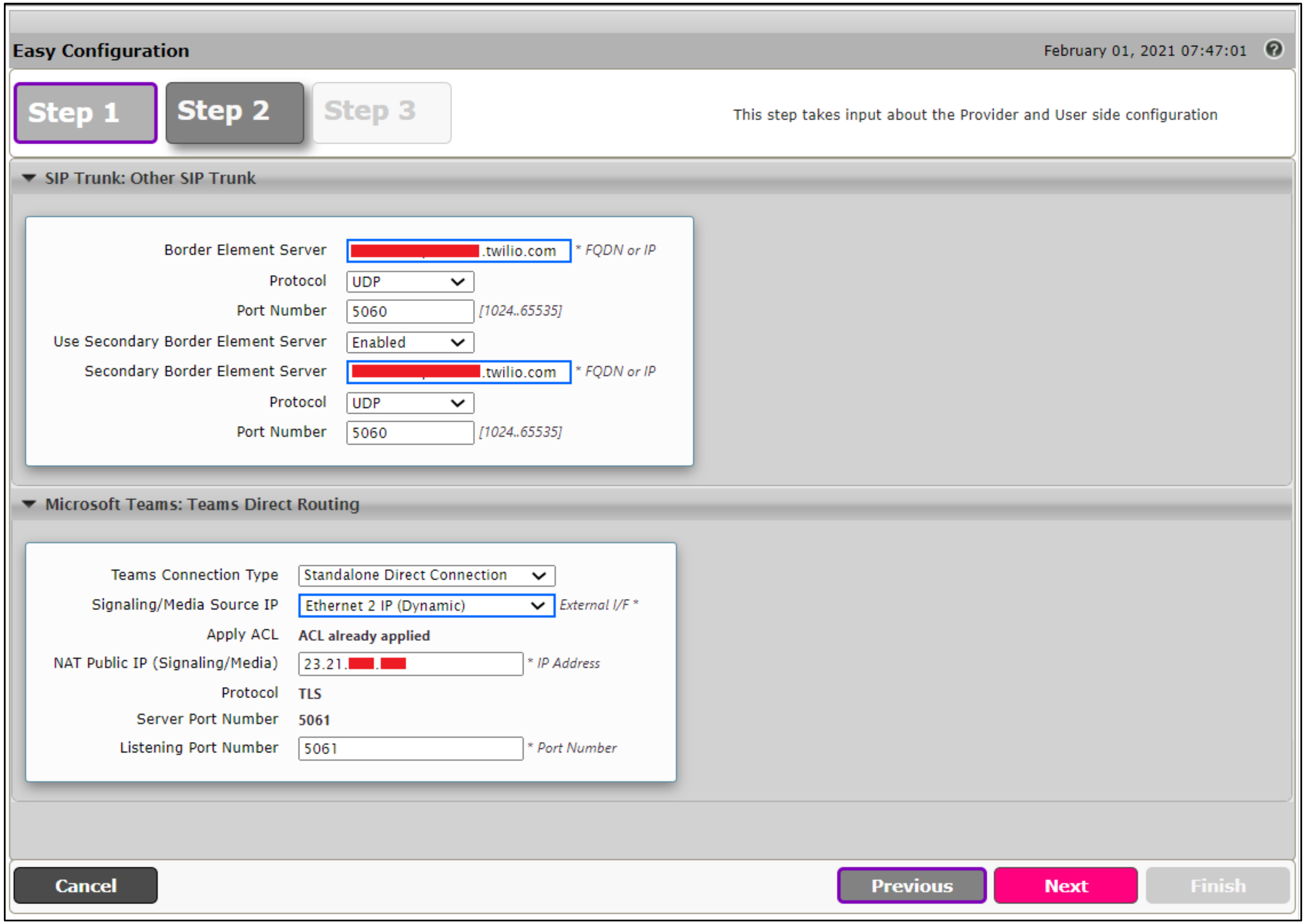
Name: Other SIP Trunk

Microsoft Teams

Teams Connection: Teams Direct Routing

Step 2: After selecting the scenario in Step 1, the following template displays. Complete this step by performing the below actions:

1. Provide the FQDNs for Primary and Secondary Border Element servers. The traffic is sent to these FQDNs from SBC SWe Lite.
2. Use UDP with port number 5060 for Twilio SIP trunk configuration.
3. For MS Teams configuration, select the **External interface** (in this case Ethernet 2). After selecting Signaling/Media source IP, an IP address appears in the NAT public IP field. Check if the IP is correct and proceed by clicking **Next**.



This step takes input about the Provider and User side configuration

SIP Trunk: Other SIP Trunk

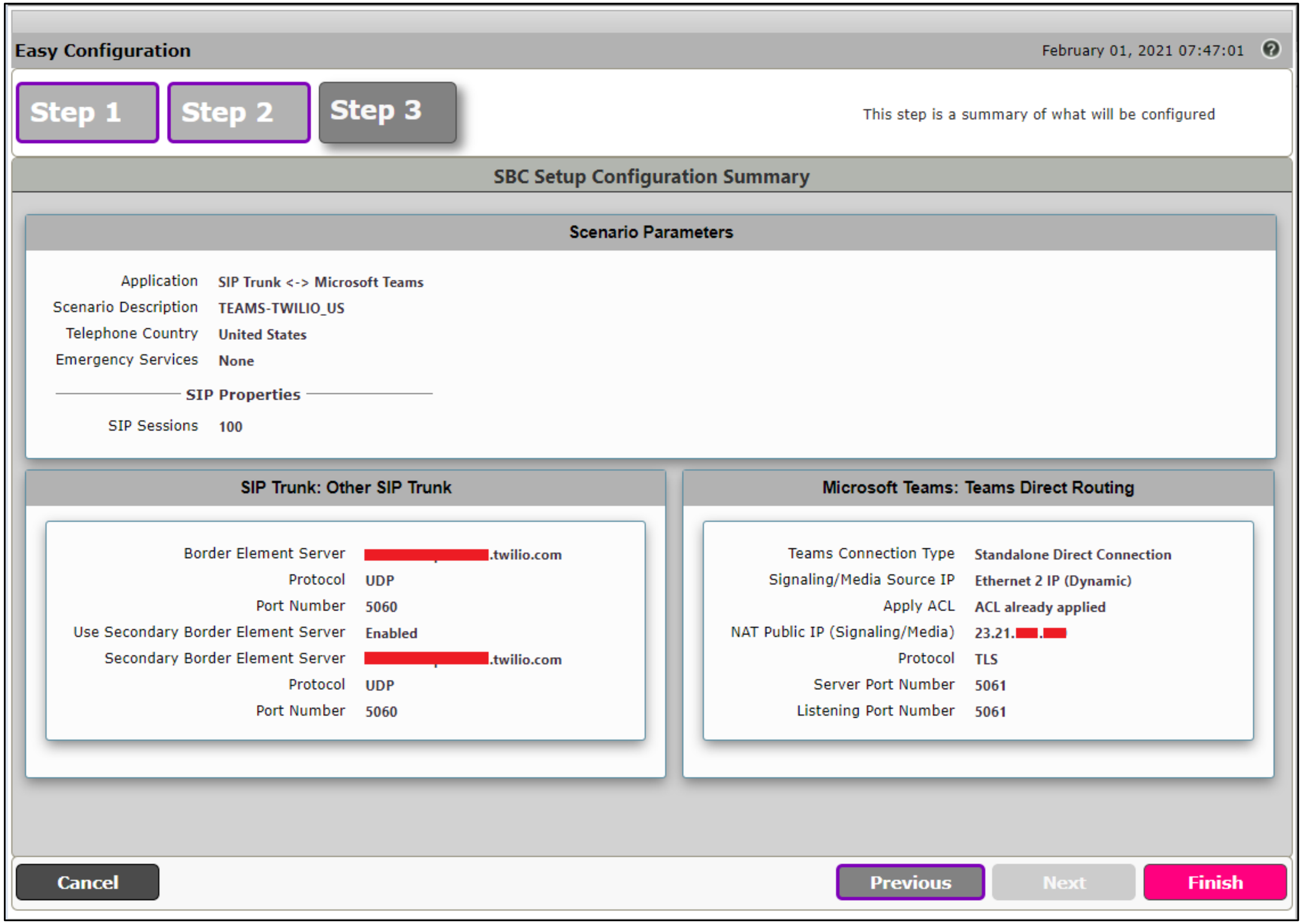
Border Element Server	[redacted].twilio.com	* FQDN or IP
Protocol	UDP	
Port Number	5060	[1024..65535]
Use Secondary Border Element Server	Enabled	
Secondary Border Element Server	[redacted].twilio.com	* FQDN or IP
Protocol	UDP	
Port Number	5060	[1024..65535]

Microsoft Teams: Teams Direct Routing

Teams Connection Type	Standalone Direct Connection	
Signaling/Media Source IP	Ethernet 2 IP (Dynamic)	External I/F *
Apply ACL	ACL already applied	
NAT Public IP (Signaling/Media)	23.21.[redacted].[redacted]	* IP Address
Protocol	TLS	
Server Port Number	5061	
Listening Port Number	5061	* Port Number

Step 3: This step displays a read-only summary of the configuration.

1. Check if the information entered in the previous steps is correct. If the entered information is wrong, return to the previous step by clicking **Previous** and modify the required field.
2. Click **Finish** to complete the configuration.



Easy Configuration

February 01, 2021 07:47:01

This step is a summary of what will be configured

SBC Setup Configuration Summary

Scenario Parameters

Application	SIP Trunk <-> Microsoft Teams
Scenario Description	TEAMS-TWILIO_US
Telephone Country	United States
Emergency Services	None

SIP Properties

SIP Sessions	100

SIP Trunk: Other SIP Trunk

Border Element Server	[redacted].twilio.com
Protocol	UDP
Port Number	5060
Use Secondary Border Element Server	Enabled
Secondary Border Element Server	[redacted].twilio.com
Protocol	UDP
Port Number	5060

Microsoft Teams: Teams Direct Routing

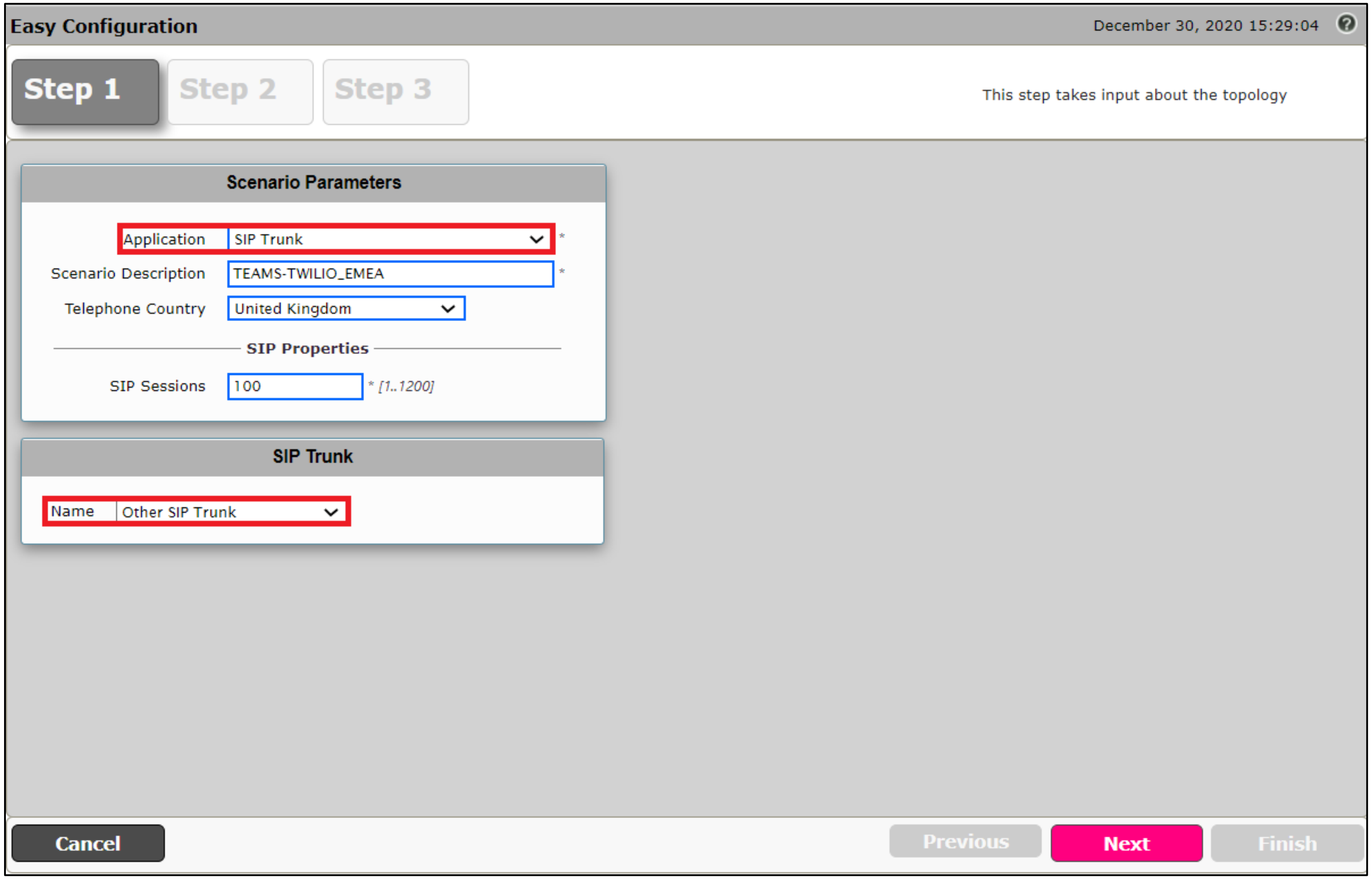
Teams Connection Type	Standalone Direct Connection
Signaling/Media Source IP	Ethernet 2 IP (Dynamic)
Apply ACL	ACL already applied
NAT Public IP (Signaling/Media)	23.21.[redacted].[redacted]
Protocol	TLS
Server Port Number	5061
Listening Port Number	5061

- A pop up window appears once all the 3 steps are completed. Click **OK** to continue.
- Wait for the configuration to complete and click **OK** on the next window. This will complete the configuration of Twilio US Trunk and Microsoft Teams.

Configure SBC SWe Lite for Twilio EMEA Trunk

Step 1: Use Single-legged approach for Twilio EMEA Trunk configuration.

1. Select **SIP Trunk** from the Application dropdown.
2. Provide the Scenario Description.
3. Select United Kingdom in the **Telephone Country** field.
4. Type a number from 1-1200 against **SIP Sessions** field.
5. Select Other SIP Trunk for Twilio (EMEA Trunk) as **SIP Trunk Name**.
6. Click **Next**.



This step takes input about the topology

Scenario Parameters

Application: SIP Trunk *

Scenario Description: TEAMS-TWILIO_EMEA *

Telephone Country: United Kingdom

SIP Properties

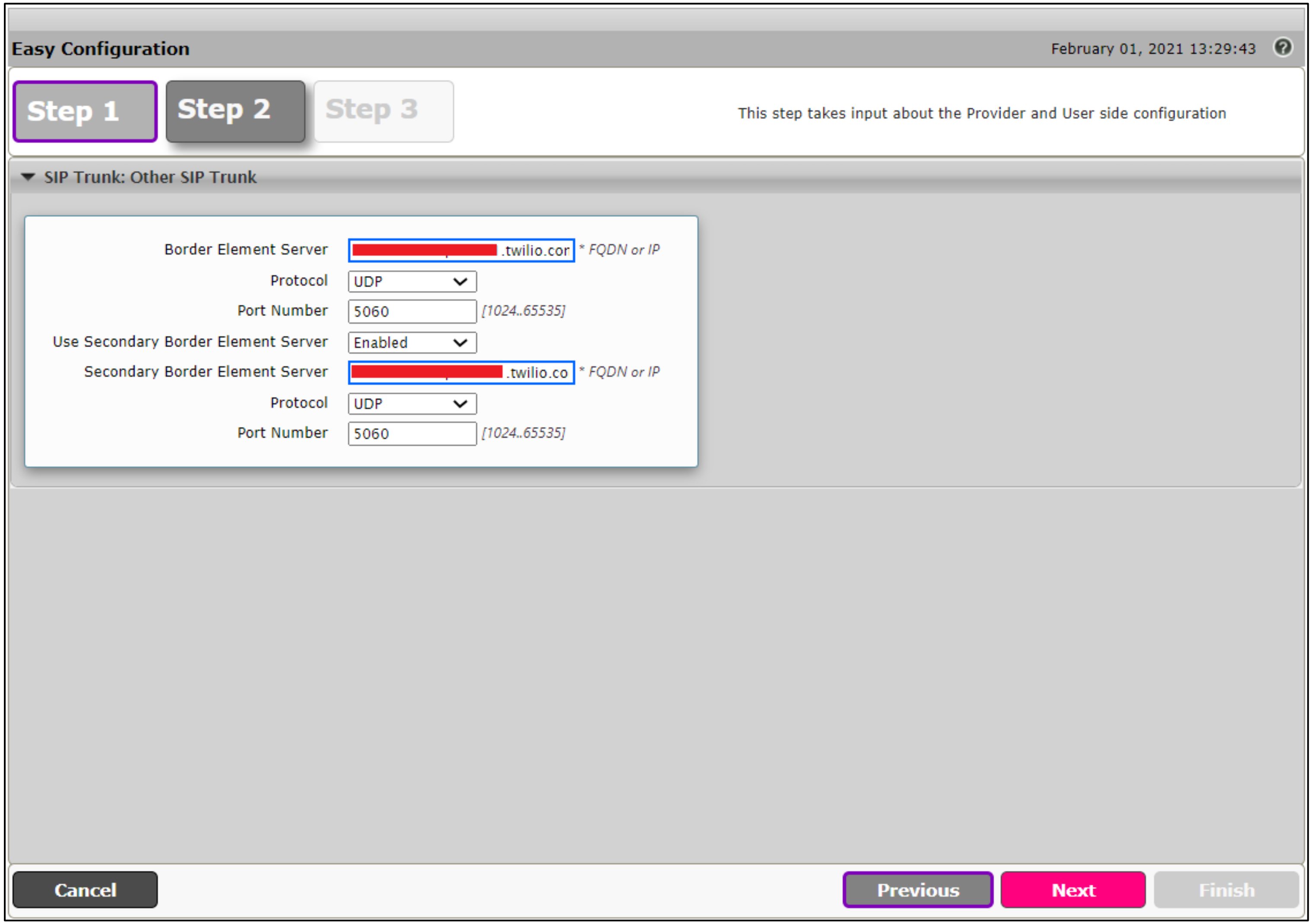
SIP Sessions: 100 * [1..1200]

SIP Trunk

Name: Other SIP Trunk

Step 2: Complete the step by performing the below actions:

4. Set the FQDNs for Primary and Secondary Border Element Servers (Refer to the **Twilio Create a new Trunk → Termination** section of this document)
5. Select UDP protocol with port number 5060.
6. Click **Next**.

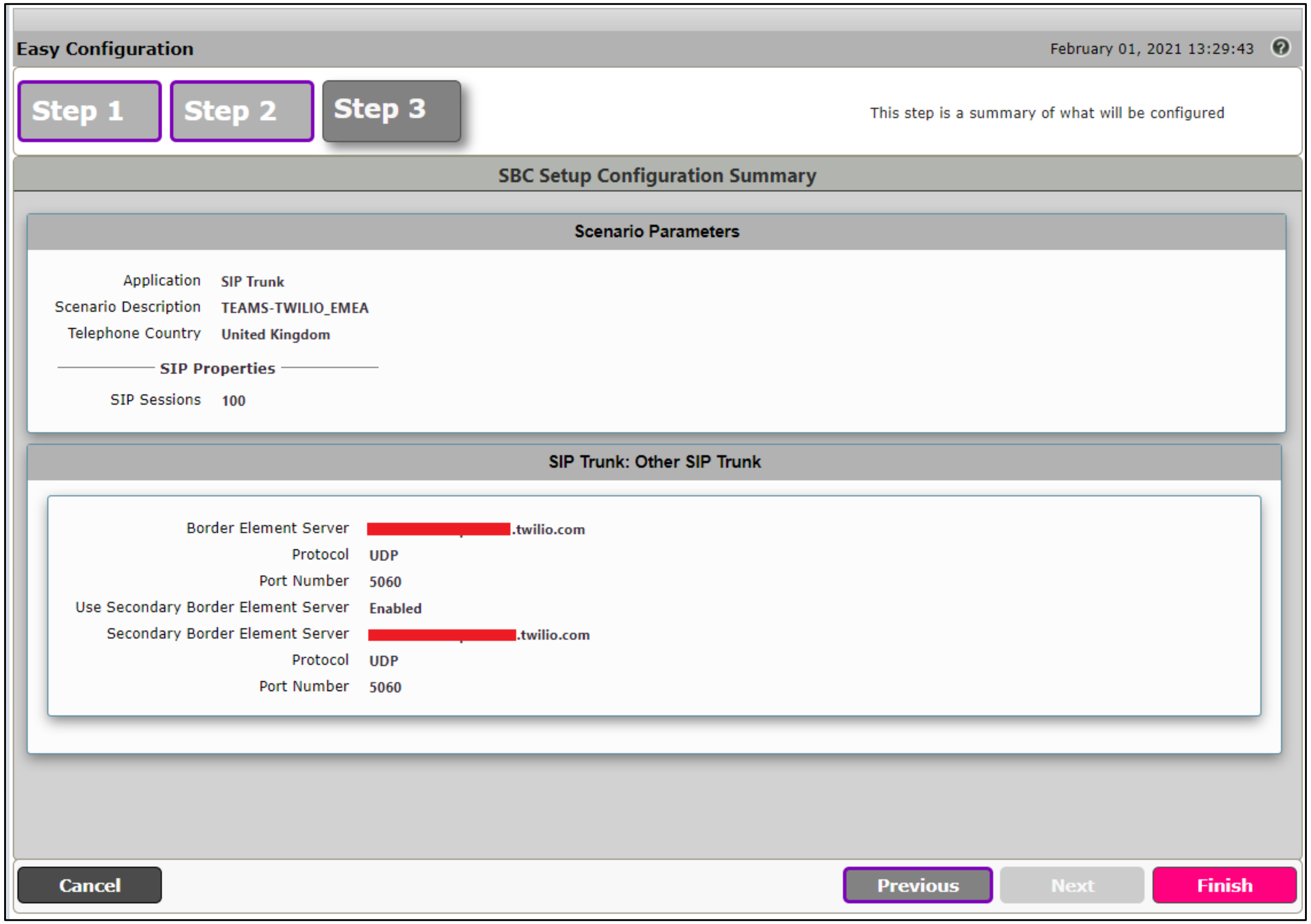


This step takes input about the Provider and User side configuration

SIP Trunk: Other SIP Trunk

Border Element Server	[redacted].twilio.cor	* FQDN or IP
Protocol	UDP	
Port Number	5060	[1024..65535]
Use Secondary Border Element Server	Enabled	
Secondary Border Element Server	[redacted].twilio.co	* FQDN or IP
Protocol	UDP	
Port Number	5060	[1024..65535]

Step 3: Re-check the configuration on the summary page and complete the configuration by clicking **Finish**.



This step is a summary of what will be configured

SBC Setup Configuration Summary

Scenario Parameters

Application SIP Trunk

Scenario Description TEAMS-TWILIO_EMEA

Telephone Country United Kingdom

SIP Properties

SIP Sessions 100

SIP Trunk: Other SIP Trunk

Border Element Server [redacted].twilio.com

Protocol UDP

Port Number 5060

Use Secondary Border Element Server Enabled

Secondary Border Element Server [redacted].twilio.com

Protocol UDP

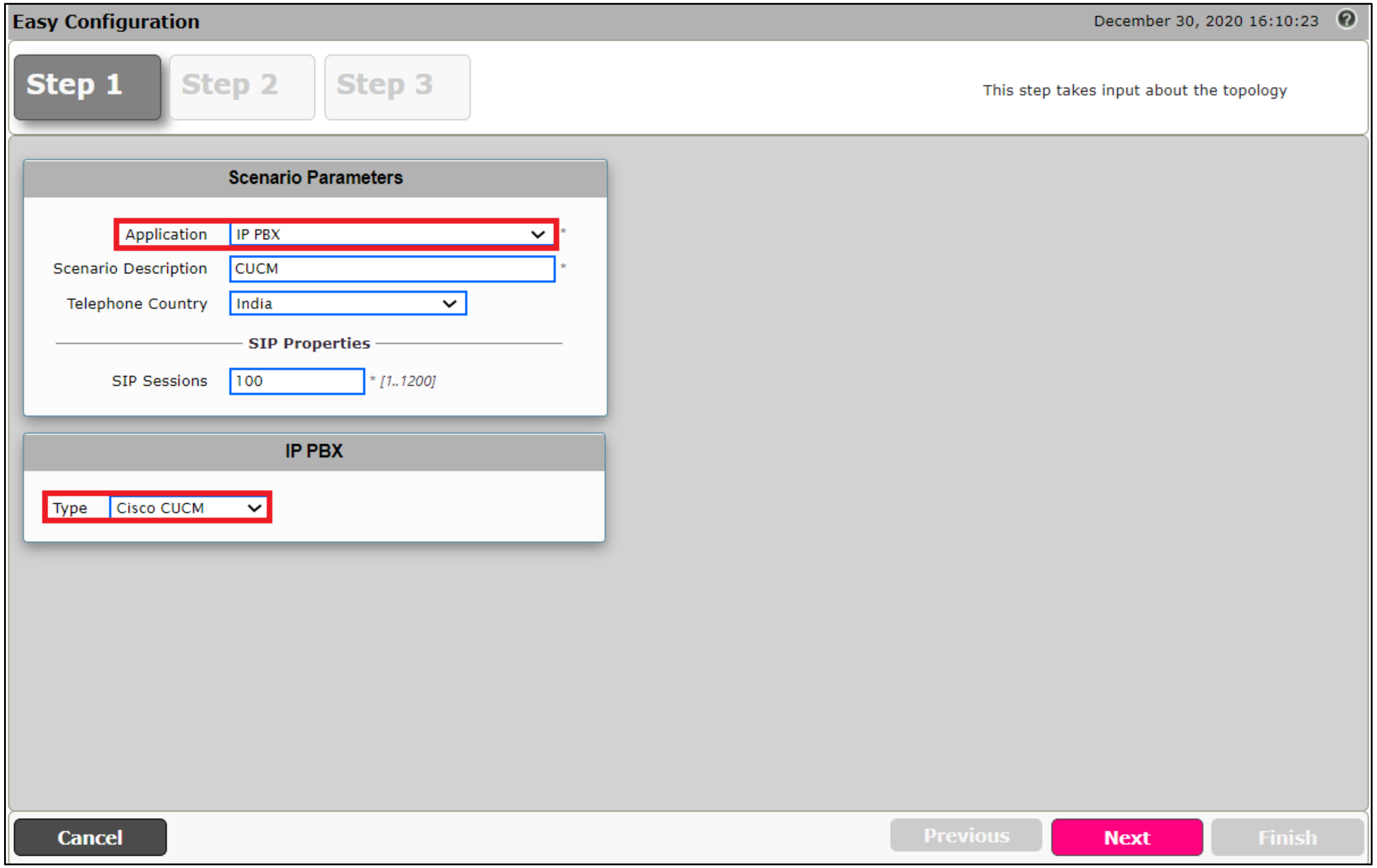
Port Number 5060

- A pop up window appears once all the 3 steps are completed. Click **OK** to continue.
- Wait for the configuration to complete and click **OK** on the next window. This will complete the configuration of Twilio EMEA Trunk.

Configure SBC SWe Lite for CUCM

Step 1: Use the Single-legged approach to configure IP PBX.

1. Click the drop-down arrow on the **Application** and select IP PBX.
2. Provide the desired description.
3. Select **Telephone Country** as India.
4. Choose from 1 to 1200 to allocate the SIP Sessions.
5. Select Cisco CUCM as **IP PBX Type.**
6. Click **Next**.



Easy Configuration

December 30, 2020 16:10:23

This step takes input about the topology

Scenario Parameters

Application: IP PBX *

Scenario Description: CUCM *

Telephone Country: India

SIP Properties

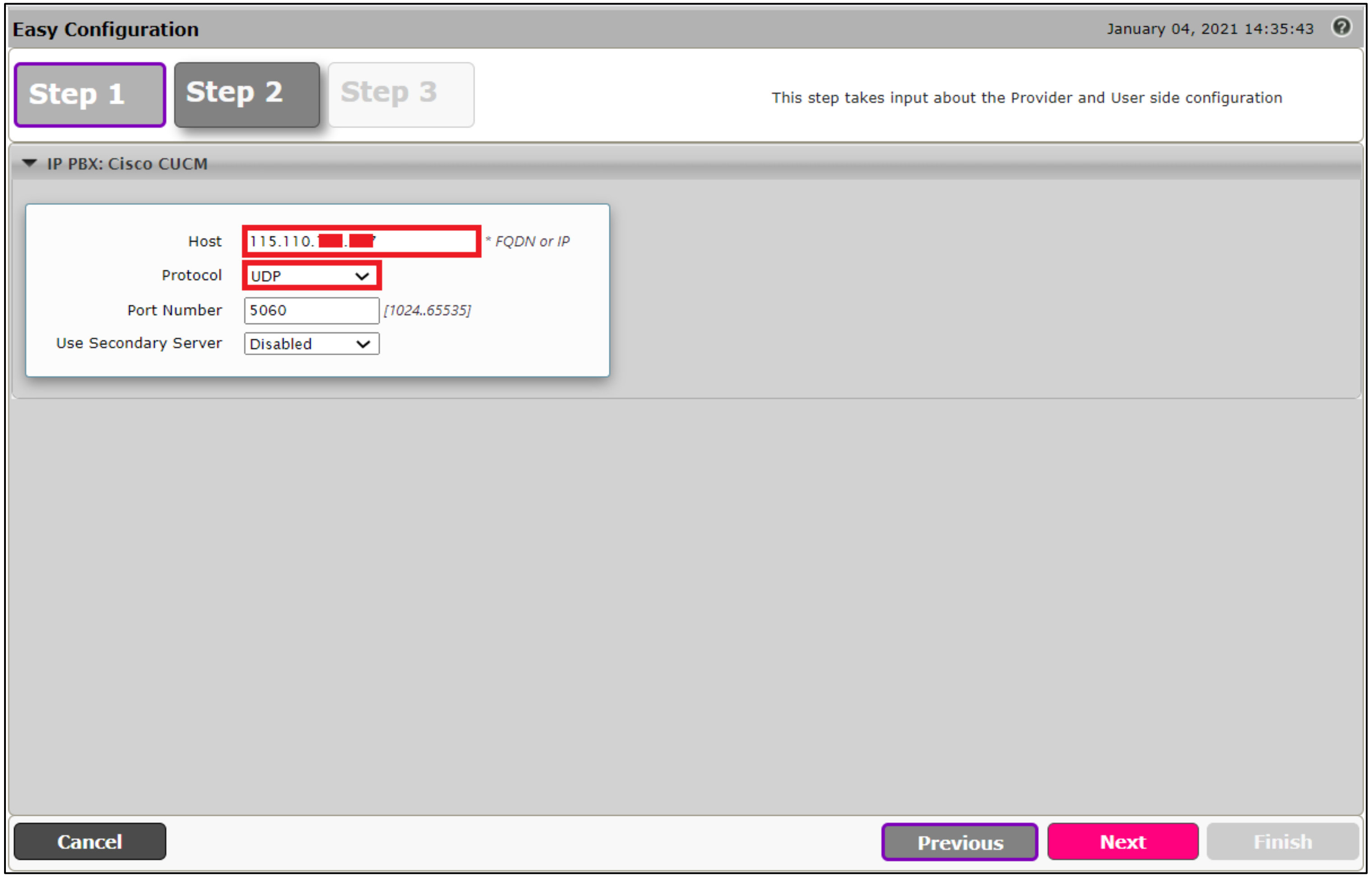
SIP Sessions: 100 * [1..1200]

IP PBX

Type: Cisco CUCM

Step 2: Follow the steps below.

1. Provide the CUCM IP Address.
2. Select **UDP** as the protocol with port 5060.
3. Click **Next**.

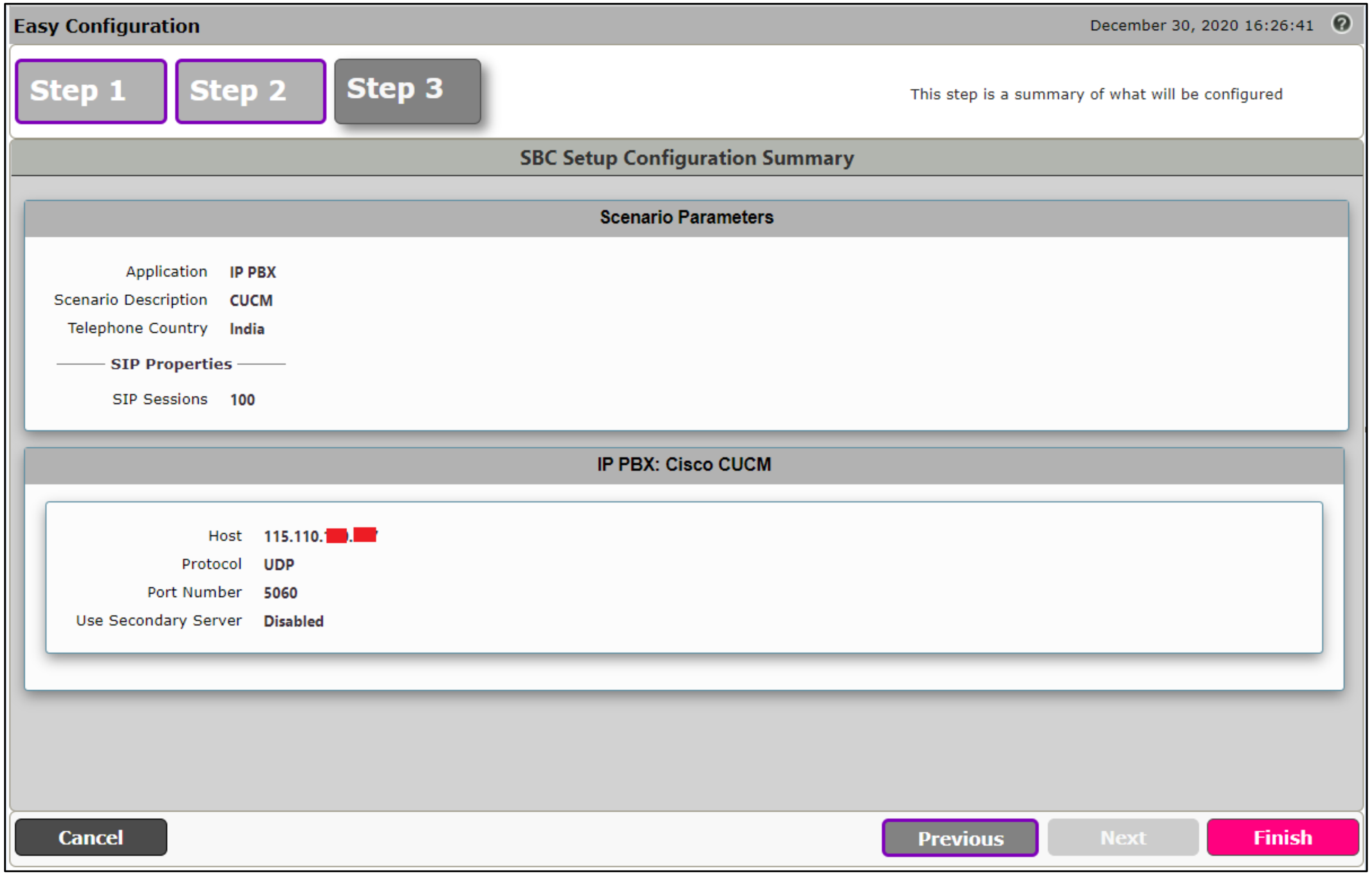


This step takes input about the Provider and User side configuration

IP PBX: Cisco CUCM

Host	115.110.[redacted].[redacted]	* FQDN or IP
Protocol	UDP	
Port Number	5060	[1024..65535]
Use Secondary Server	Disabled	

Step 3: Check the configured parameters in the summary page and click **Finish** to complete the configuration.


Easy Configuration
December 30, 2020 16:26:41
Step 1
Step 2
Step 3
This step is a summary of what will be configured
Cancel
Previous
Next
Finish

SBC Setup Configuration Summary

Scenario Parameters

Application	IP PBX
Scenario Description	CUCM
Telephone Country	India

SIP Properties

SIP Sessions	100

IP PBX: Cisco CUCM

Host	115.110.[redacted].[redacted]
Protocol	UDP
Port Number	5060
Use Secondary Server	Disabled

- A pop up window appears once all the 3 steps are completed. Click **OK** to continue.
- Wait for the configuration to complete and click **OK** on the next window. This will complete the configuration of CUCM leg on SBC SWe Lite.

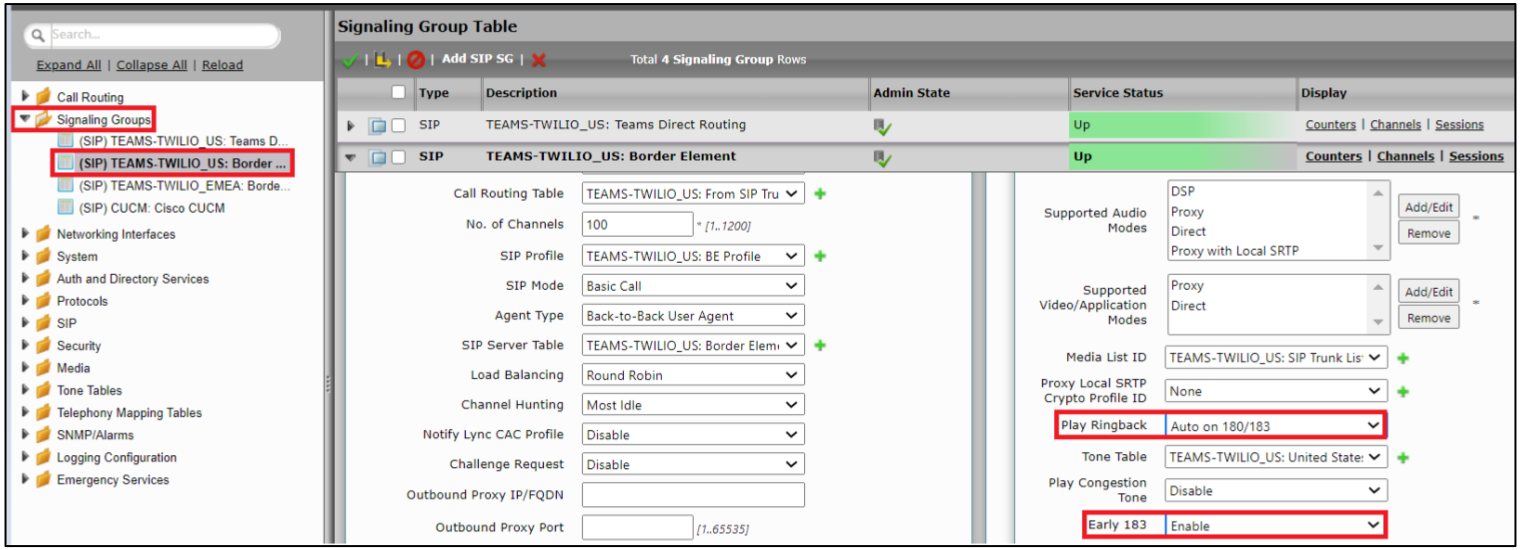
Modify SBC SWe Lite Configuration

The Easy Configuration Wizard does not currently set all Twilio applicable variables to the correct settings. This will be addressed in the subsequent SBC SWe Lite releases. Until then, please follow the procedures below.

Assign NAT Public IP

Change the settings on all the SGs as follows:

- Play Ringback - **Auto on 180/183** - Ringback is determined when processing 180 or 183.
- Early 183 - **Enable** - Specifies whether to send a SIP 183 response immediately after receiving an Invite message.



Signaling Group Table

Total 4 Signaling Group Rows

Type	Description	Admin State	Service Status	Display
SIP	TEAMS-TWILIO_US: Teams Direct Routing	✓	Up	Counters | Channels | Sessions
SIP	TEAMS-TWILIO_US: Border Element	✓	Up	Counters | Channels | Sessions

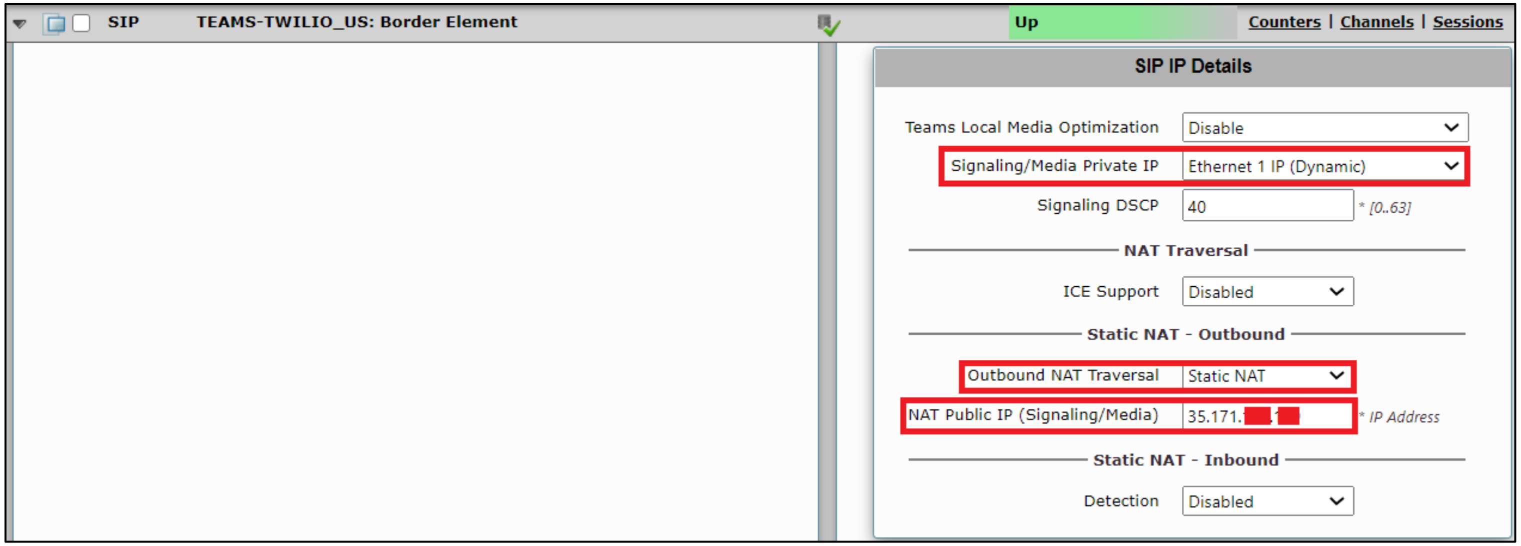
Call Routing Table	TEAMS-TWILIO_US: From SIP Tru
No. of Channels	100 * [1..1200]
SIP Profile	TEAMS-TWILIO_US: BE Profile
SIP Mode	Basic Call
Agent Type	Back-to-Back User Agent
SIP Server Table	TEAMS-TWILIO_US: Border Elem
Load Balancing	Round Robin
Channel Hunting	Most Idle
Notify Lync CAC Profile	Disable
Challenge Request	Disable
Outbound Proxy IP/FQDN	
Outbound Proxy Port	[1..65535]

Supported Audio Modes	DSP Proxy Direct Proxy with Local SRTP
Supported Video/Application Modes	Proxy Direct
Media List ID	TEAMS-TWILIO_US: SIP Trunk Lis
Proxy Local SRTP Crypto Profile ID	None
Play Ringback	Auto on 180/183
Tone Table	TEAMS-TWILIO_US: United State:
Play Congestion Tone	Disable
Early 183	Enable

Assign the interfaces for Signaling/Media Private IP to all the Signaling Groups accordingly. In this case,

- Ethernet 1 IP for TEAMS-TWILIO_US: Border Element and TEAMS-TWILIO_EMEA: Border Element Signaling Groups.
- Ethernet 2 IP for TEAMS-TWILIO_US: Teams Direct Routing and CUCM: Cisco CUCM Signaling Groups.

Enable Static NAT and map the respective IP addresses.


SIP
TEAMS-TWILIO_US: Border Element
Up
Counters | Channels | Sessions

SIP IP Details

Teams Local Media Optimization: Disable

Signaling/Media Private IP: Ethernet 1 IP (Dynamic)

Signaling DSCP: 40 * [0..63]

NAT Traversal

ICE Support: Disabled

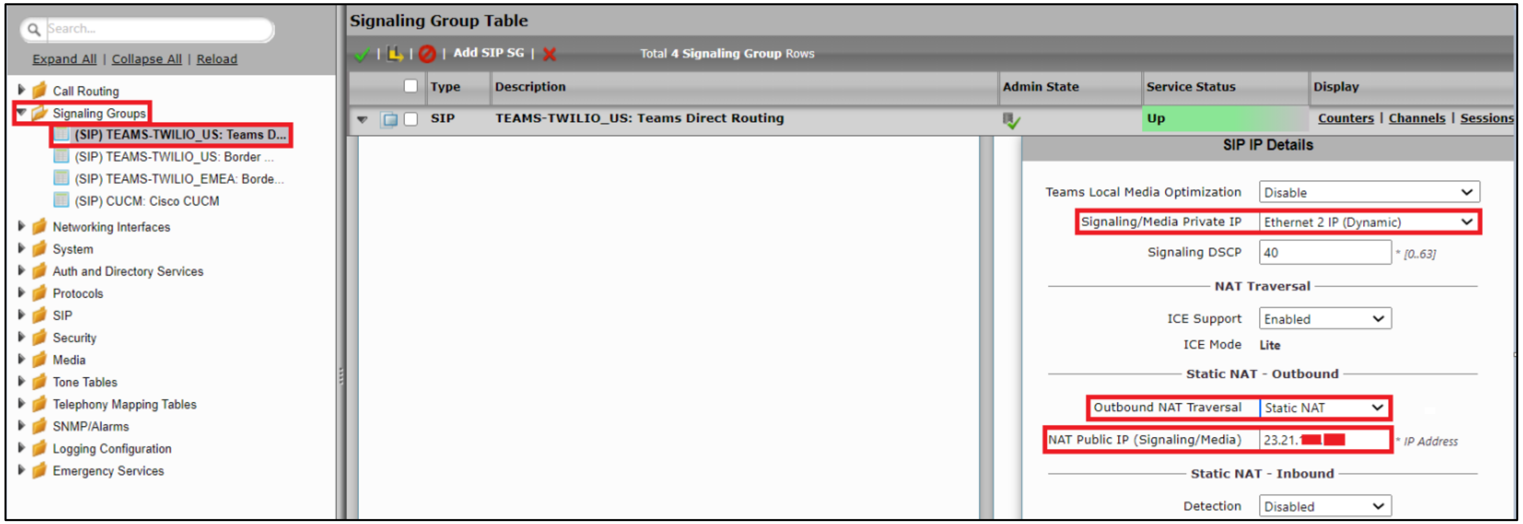
Static NAT - Outbound

Outbound NAT Traversal: Static NAT

NAT Public IP (Signaling/Media): 35.171.[redacted][redacted] * IP Address

Static NAT - Inbound

Detection: Disabled



Search...

Expand All | Collapse All | Reload

- Call Routing
- Signaling Groups
  - (SIP) TEAMS-TWILIO_US: Teams D...
  - (SIP) TEAMS-TWILIO_US: Border ...
  - (SIP) TEAMS-TWILIO_EMEA: Borde...
  - (SIP) CUCM: Cisco CUCM
- Networking Interfaces
- System
- Auth and Directory Services
- Protocols
- SIP
- Security
- Media
- Tone Tables
- Telephony Mapping Tables
- SNMP/Alarms
- Logging Configuration
- Emergency Services

Signaling Group Table

Add SIP SG | Total 4 Signaling Group Rows

Type	Description	Admin State	Service Status	Display
SIP	TEAMS-TWILIO_US: Teams Direct Routing	✓	Up	Counters | Channels | Sessions

SIP IP Details

Teams Local Media Optimization	Disable
Signaling/Media Private IP	Ethernet 2 IP (Dynamic)
Signaling DSCP	40 * [0..63]

NAT Traversal

ICE Support	Enabled
ICE Mode	Lite

Static NAT - Outbound

Outbound NAT Traversal	Static NAT
NAT Public IP (Signaling/Media)	23.21.[redacted] * IP Address

Static NAT - Inbound

Detection	Disabled

Enable OPTIONS

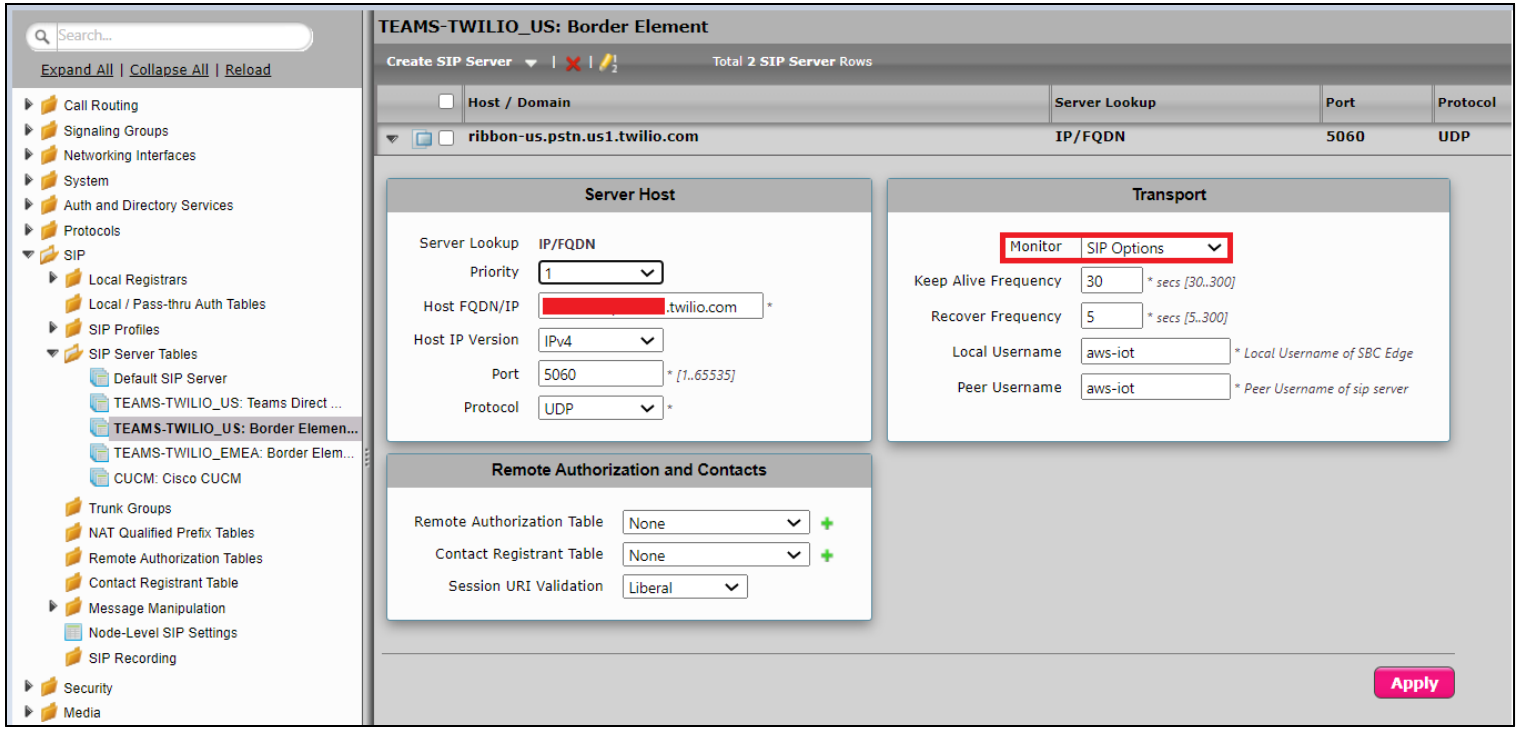
An OPTIONS message is sent to the server. When this option is selected, additional configuration items are displayed:

Keep Alive Frequency
Specifies how often, in seconds, the SBC Edge queries the server with an OPTIONS message to determine the server's availability. Visible only when SIP Options is selected from the Monitor field. If the server does not respond, the SBC Edge marks the Signaling Group as down. When the server begins to respond to the OPTIONS messages again, it is marked as up. In this case, Keep Alive Frequency is set to 30 seconds.

Recover Frequency
Specifies frequency in seconds to check server to determine whether it has become available. Recovery Frequency is set to 5 seconds for this interop.

Local Username
Local user name of the SBC Edge system. Default entry: **Anonymous**. Visible only when **SIP Options** is selected from the **Monitor** field.

Peer Username
User name of the SIP Server. Visible only when **SIP Options** is selected from the **Monitor** field. The user can change Local and Peer Usernames according to their wishes.



TEAMS-TWILIO_US: Border Element

Total 2 SIP Server Rows

Host / Domain	Server Lookup	Port	Protocol
ribbon-us.pstn.us1.twilio.com	IP/FQDN	5060	UDP

Server Host

Server Lookup IP/FQDN
Priority 1
Host FQDN/IP [redacted].twilio.com *
Host IP Version IPv4
Port 5060 * [1..65535]
Protocol UDP *

Transport

Monitor SIP Options
Keep Alive Frequency 30 * secs [30..300]
Recover Frequency 5 * secs [5..300]
Local Username aws-iot * Local Username of SBC Edge
Peer Username aws-iot * Peer Username of sip server

Remote Authorization and Contacts

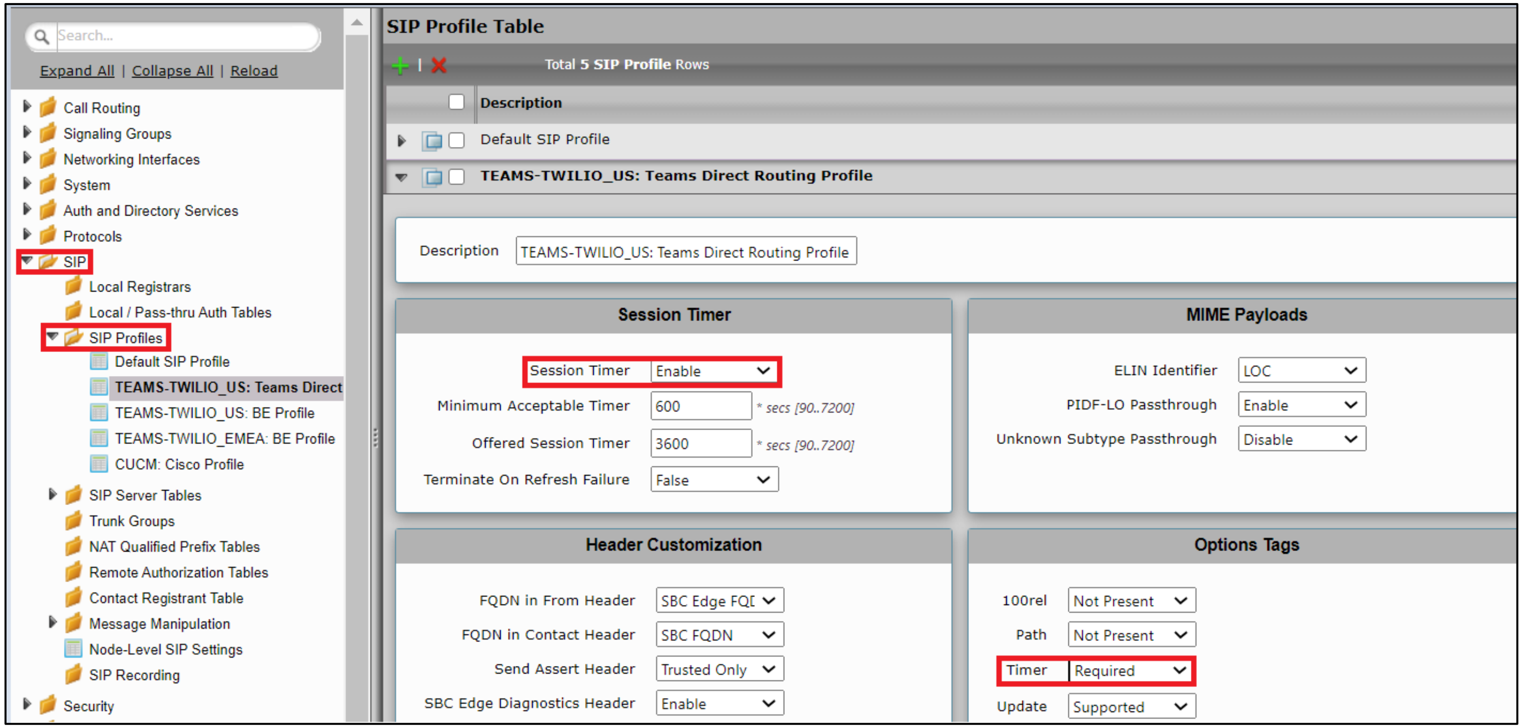
Remote Authorization Table None
Contact Registrant Table None
Session URI Validation Liberal

Note
Repeat the above steps to enable OPTIONS on all the SIP Server Tables (TEAMS-TWILIO_US: Teams Direct Routing Server, TEAMS-TWILIO_US: Border Element, TEAMS-TWILIO_EMEA: Border Element and CUCM: Cisco CUCM).

Modify SIP Profiles

Enable Session Timers

From the **Settings** tab, navigate to **SIP > SIP Profiles,** Enable Session Timers and set the Timer as Required on all the SIP Profiles.



SIP Profile Table

Total 5 SIP Profile Rows

	Description
□	Default SIP Profile
□	TEAMS-TWILIO_US: Teams Direct Routing Profile

Description: TEAMS-TWILIO_US: Teams Direct Routing Profile

Session Timer

- Session Timer: Enable
- Minimum Acceptable Timer: 600 * secs [90..7200]
- Offered Session Timer: 3600 * secs [90..7200]
- Terminate On Refresh Failure: False

MIME Payloads

- ELIN Identifier: LOC
- PIDF-LO Passthrough: Enable
- Unknown Subtype Passthrough: Disable

Header Customization

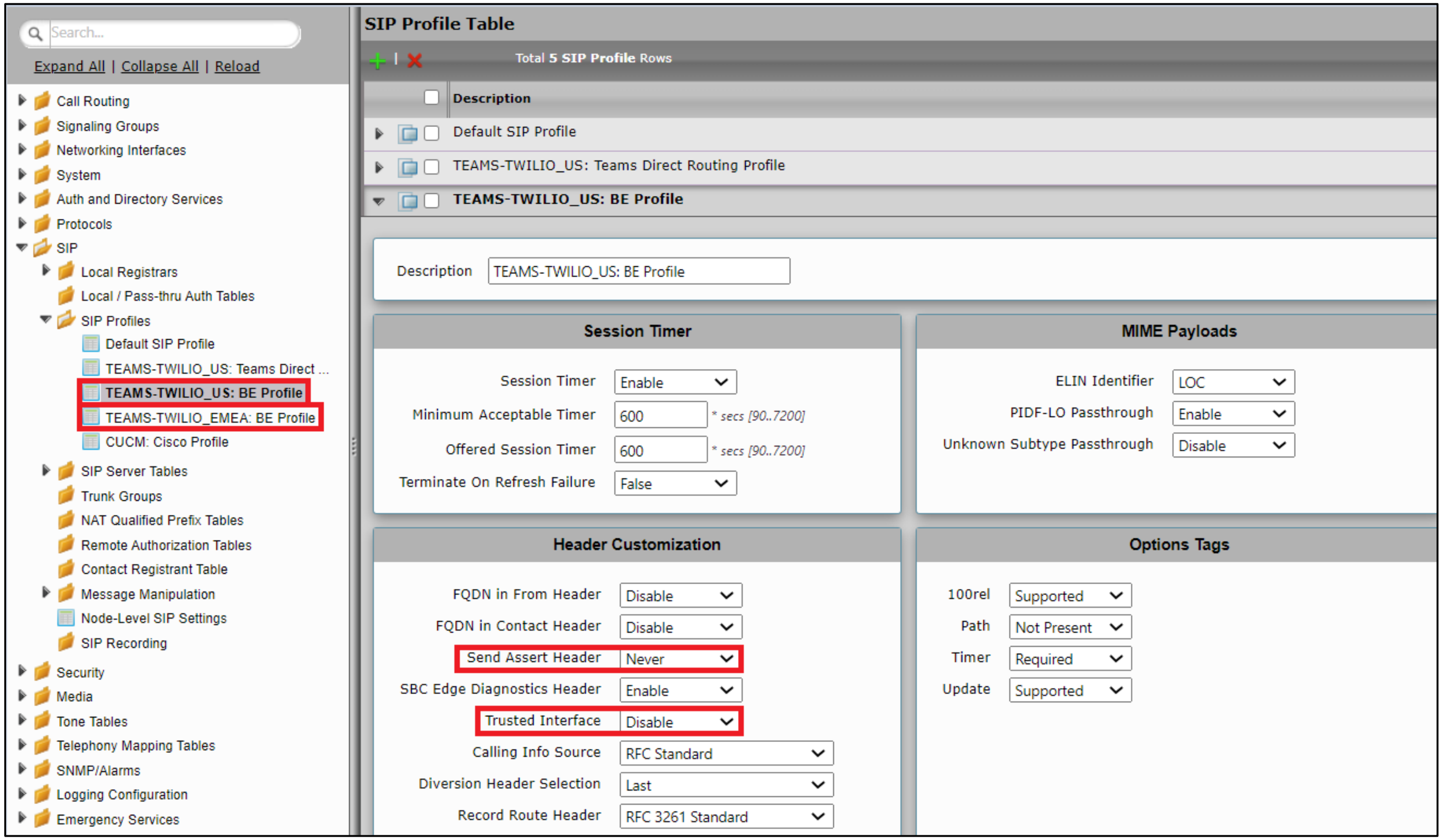
- FQDN in From Header: SBC Edge FQI
- FQDN in Contact Header: SBC FQDN
- Send Assert Header: Trusted Only
- SBC Edge Diagnostics Header: Enable

Options Tags

- 100rel: Not Present
- Path: Not Present
- Timer: Required
- Update: Supported

Change the parameters on TEAMS-TWILIO_US: BE Profile and TEAMS-TWILIO_EMEA: BE Profile SIP Profiles as follows:

- Send Assert Header - **Never**- When disabled, privacy information in the outbound INVITE is sent depending on the configuration of the Trusted Interface and the Privacy Pass-through Header.
- Trusted Interface - **Disable.**



SIP Profile Table

Total 5 SIP Profile Rows

☐	Description
☐	Default SIP Profile
☐	TEAMS-TWILIO_US: Teams Direct Routing Profile
☐	**TEAMS-TWILIO_US: BE Profile**

Description: TEAMS-TWILIO_US: BE Profile

Session Timer

Session Timer	Enable
Minimum Acceptable Timer	600 * secs [90..7200]
Offered Session Timer	600 * secs [90..7200]
Terminate On Refresh Failure	False

MIME Payloads

ELIN Identifier	LOC
PIDF-LO Passthrough	Enable
Unknown Subtype Passthrough	Disable

Header Customization

FQDN in From Header	Disable
FQDN in Contact Header	Disable
Send Assert Header	Never
SBC Edge Diagnostics Header	Enable
Trusted Interface	Disable
Calling Info Source	RFC Standard
Diversion Header Selection	Last
Record Route Header	RFC 3261 Standard

Options Tags

100rel	Supported
Path	Not Present
Timer	Required
Update	Supported

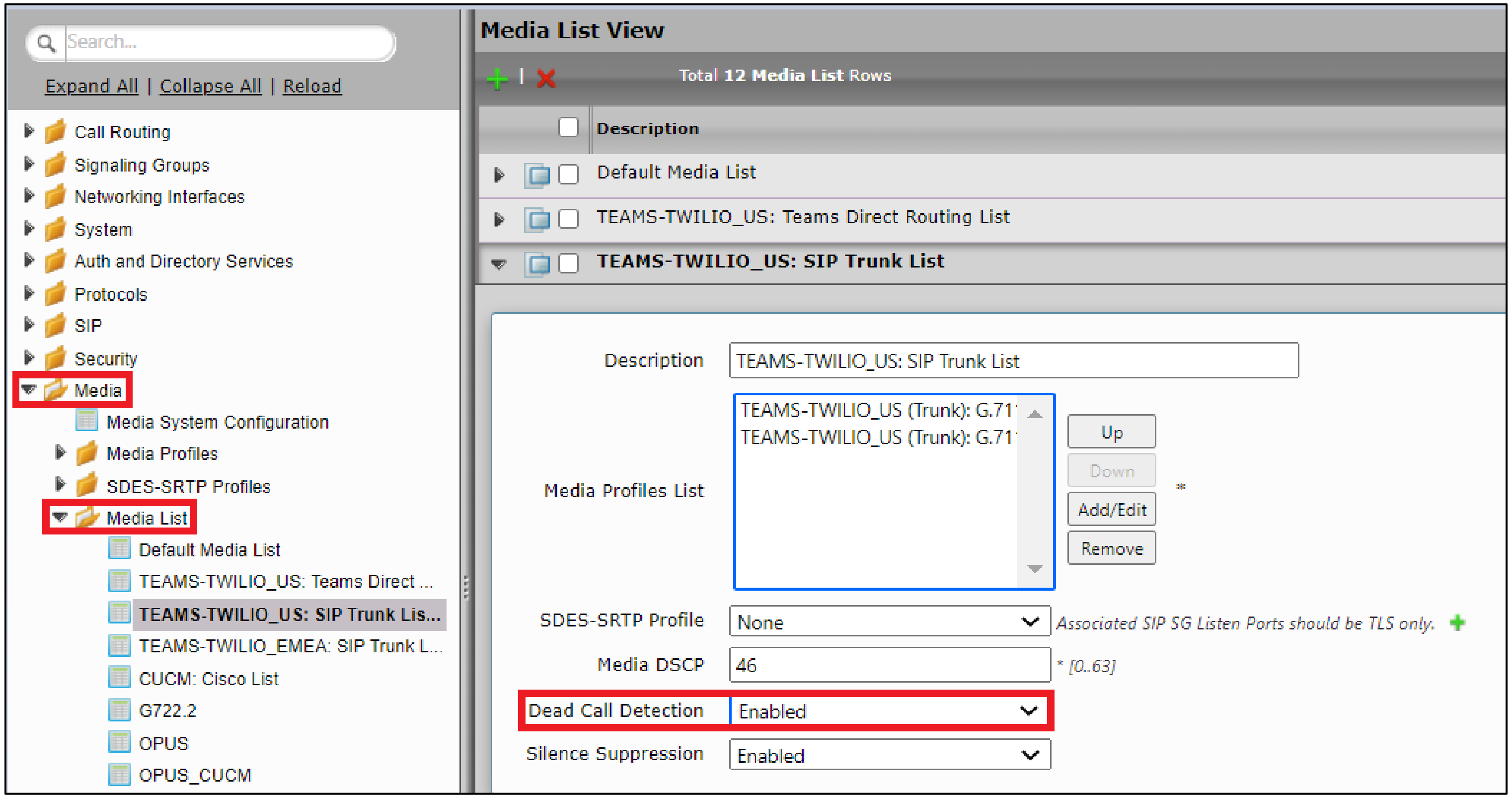
Enable Dead Call Detection

Specifies whether or not to use RTCP-based Dead Call Detection (DCD).

Dead Call Detection is accomplished by monitoring incoming RTCP packets. If this feature is enabled and no RTCP packets are received from the peer for 30 seconds, the call is considered "dead" and is disconnected. Disable DCD for any peer that does not send RTCP packets.

From the **Settings** tab, navigate to **Media > Media List.** Click the **expand** (▶) Icon next to the entry you wish to enable the feature.

- Enable DCD from the options provided in the drop-down.



Media List View

Total 12 Media List Rows

□	Description
□	Default Media List
□	TEAMS-TWILIO_US: Teams Direct Routing List
□	**TEAMS-TWILIO_US: SIP Trunk List**

Description	TEAMS-TWILIO_US: SIP Trunk List
Media Profiles List	TEAMS-TWILIO_US (Trunk): G.71 TEAMS-TWILIO_US (Trunk): G.71 *
SDES-SRTP Profile	None *Associated SIP SG Listen Ports should be TLS only.*
Media DSCP	46 * *[0..63]*
Dead Call Detection	Enabled
Silence Suppression	Enabled

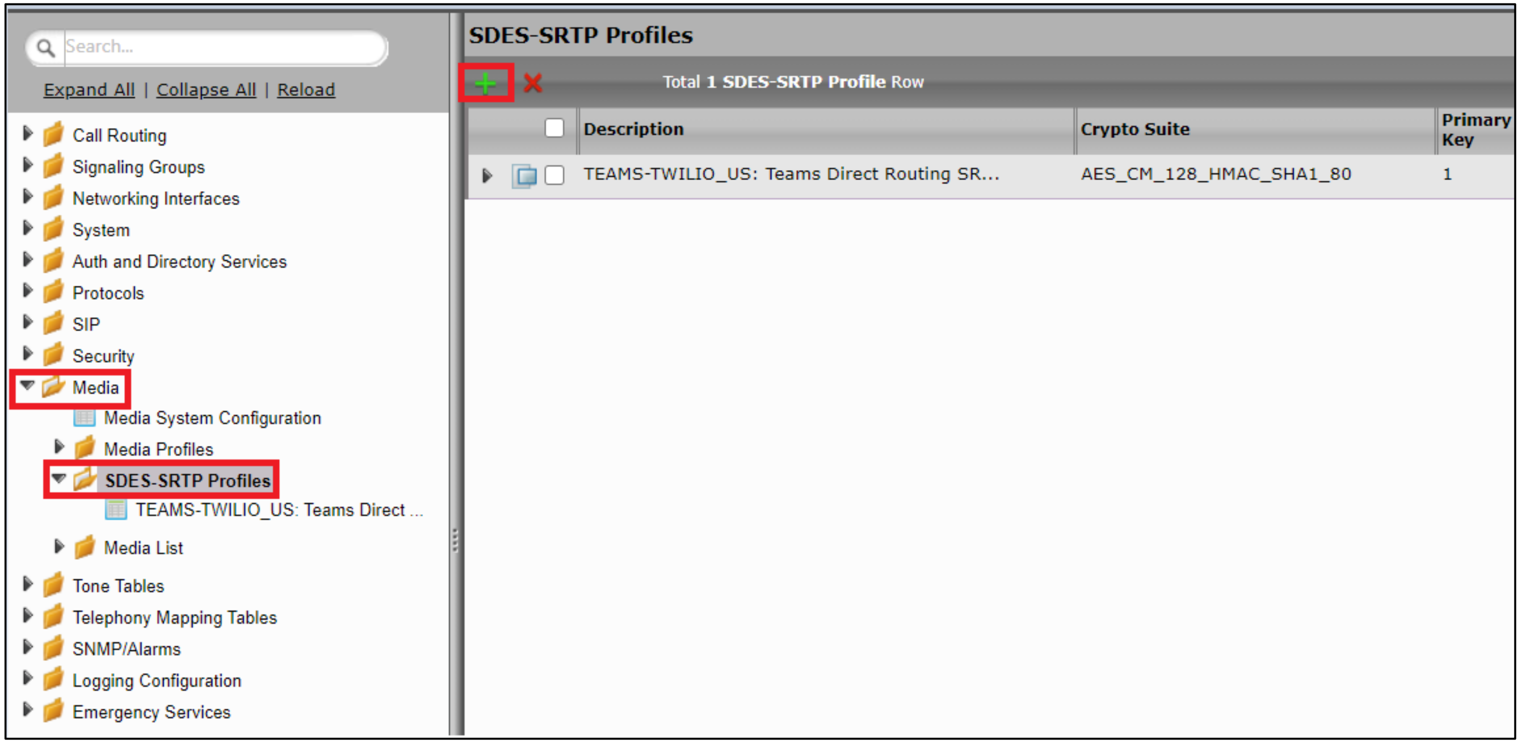
SBC SWe Lite Configuration for Twilio TLS/SRTP Trunk (Recommended)

This section describes the steps to configure SBC SWe Lite with TLS/SRTP towards Twilio SIP Trunk. Ribbon strongly recommends encrypting the connection between Twilio SIP Trunk and SBC SWe Lite.

Create SRTP profile

SDES-SRTP Profiles define a cryptographic context which 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.

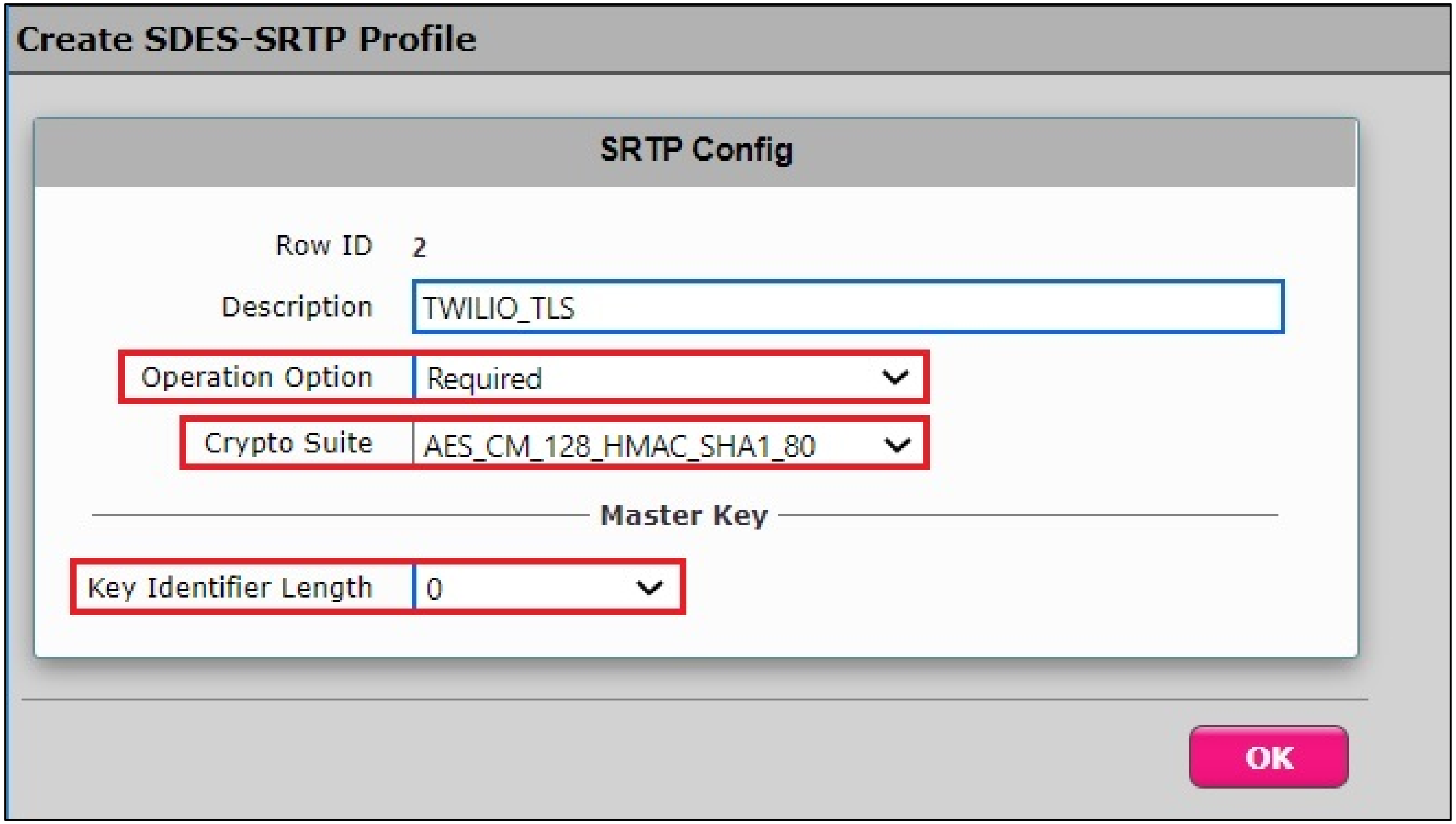
From the **Settings** tab, navigate to **Media > SDES-SRTP Profiles.** Click the ➕ icon to create a new SRTP profile.



Description	Crypto Suite	Primary Key
TEAMS-TWILIO_US: Teams Direct Routing SR...	AES_CM_128_HMAC_SHA1_80	1

Follow the steps below 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 which 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 **0** to disable the MKI in SDP.
5. Click **OK**.



Create SDES-SRTP Profile

SRTP Config

Row ID 2

Description TWILIO_TLS

Operation Option Required

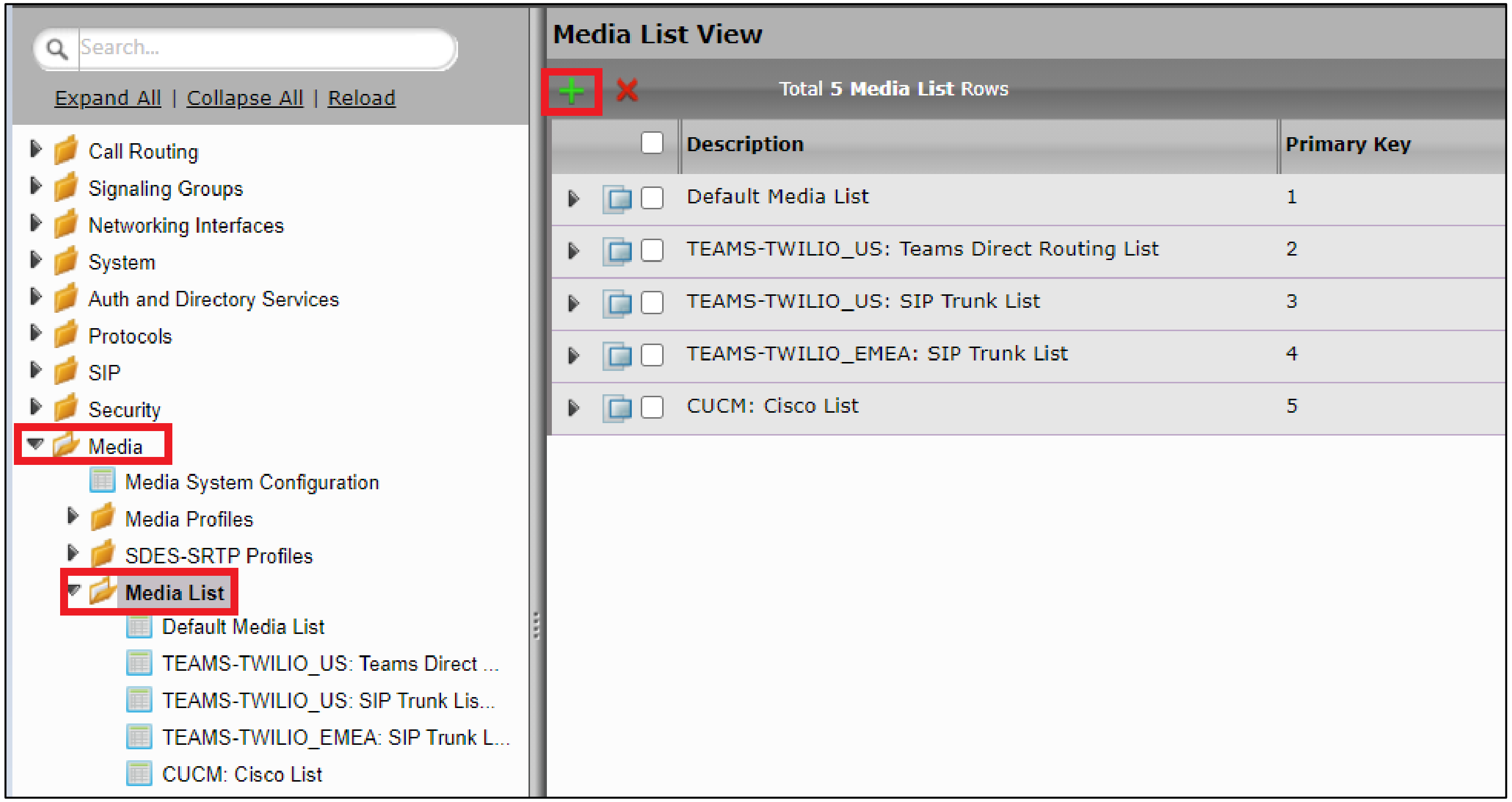
Crypto Suite AES_CM_128_HMAC_SHA1_80

Master Key

Key Identifier Length 0

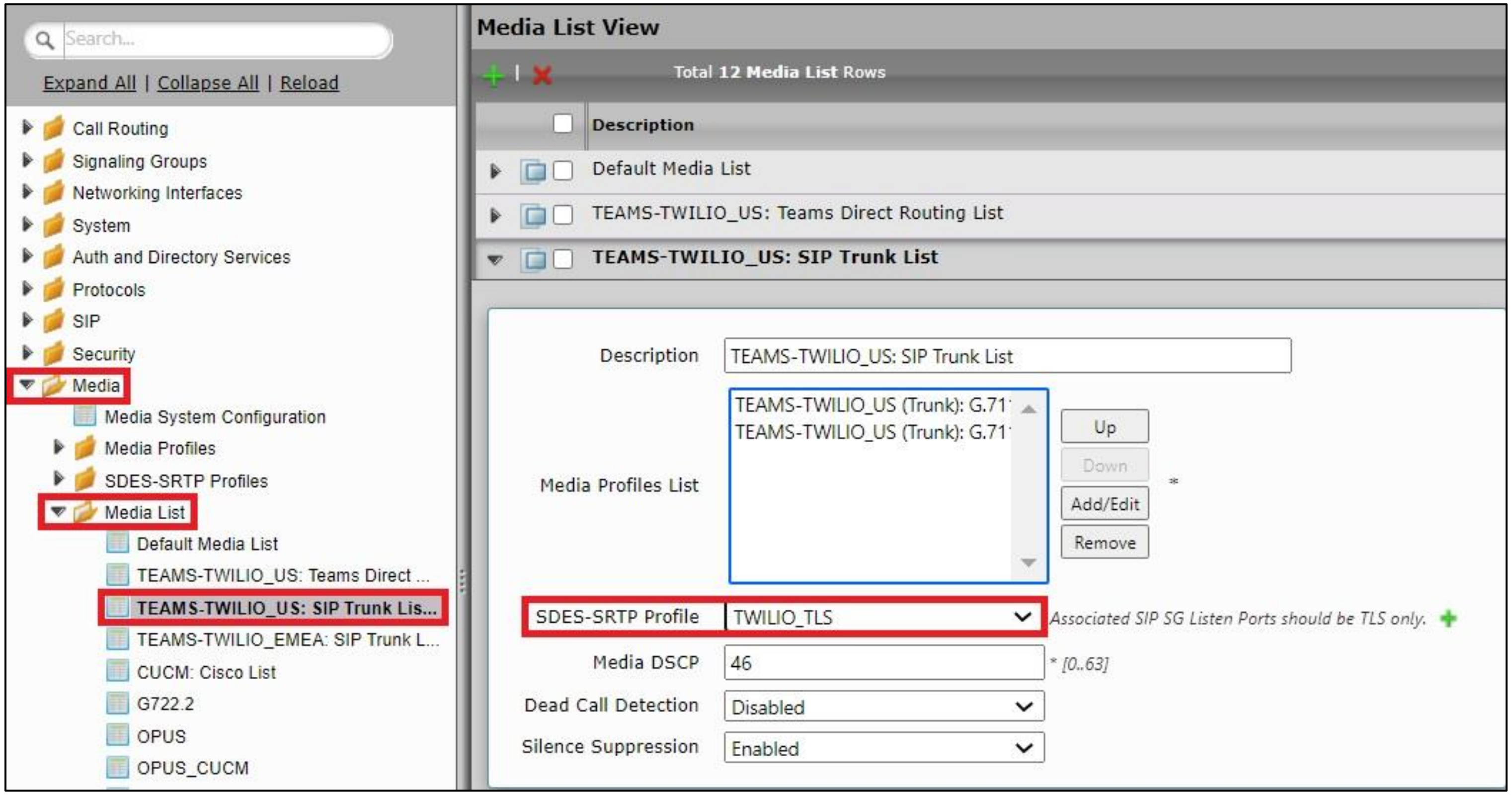
Attach SRTP Profile to the Media List

From the **Settings** tab, navigate to **Media > Media List,** Click the expand (▸) icon next to the entry.



Description	Primary Key
Default Media List	1
TEAMS-TWILIO_US: Teams Direct Routing List	2
TEAMS-TWILIO_US: SIP Trunk List	3
TEAMS-TWILIO_EMEA: SIP Trunk List	4
CUCM: Cisco List	5

1. Attach the SDES-SRTP profile (Specifies the profile for authentication/encryption protocols applied with this Media List) created in the previous step.
2. Click Apply



Media List View

Total 12 Media List Rows

□	Description
□	Default Media List
□	TEAMS-TWILIO_US: Teams Direct Routing List
□	**TEAMS-TWILIO_US: SIP Trunk List**

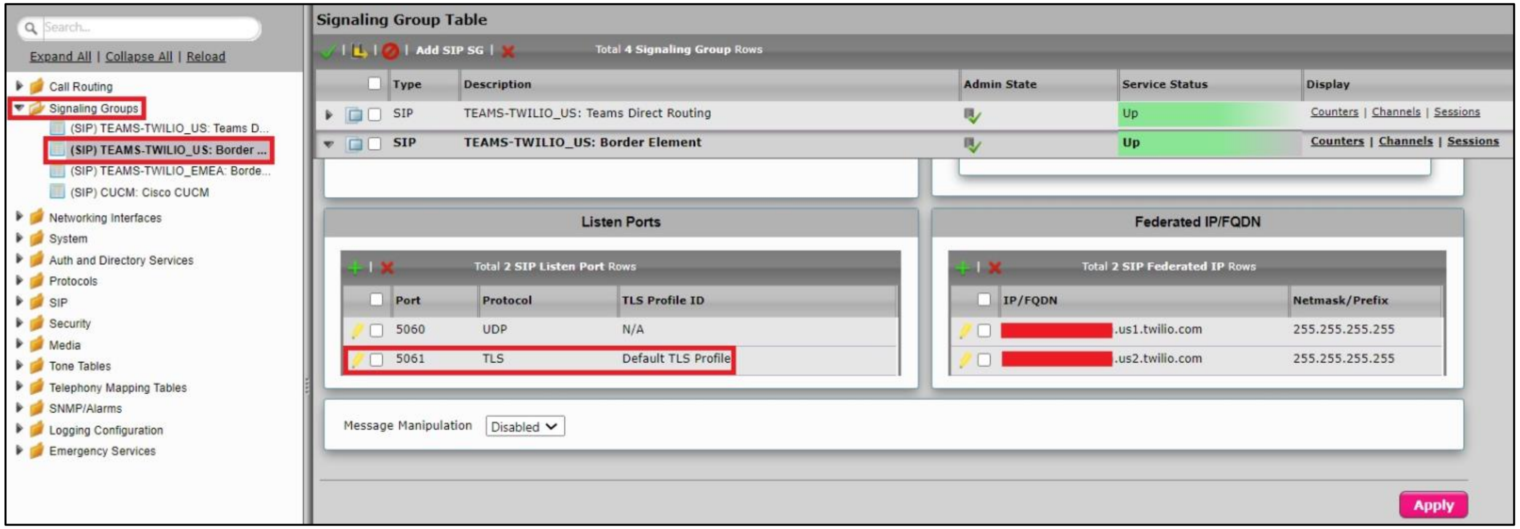
Description	TEAMS-TWILIO_US: SIP Trunk List
Media Profiles List	TEAMS-TWILIO_US (Trunk): G.71 TEAMS-TWILIO_US (Trunk): G.71
SDES-SRTP Profile	TWILIO_TLS — *Associated SIP SG Listen Ports should be TLS only.*
Media DSCP	46 * *[0..63]*
Dead Call Detection	Disabled
Silence Suppression	Enabled

Update Signaling Group

Signaling Groups allow grouping telephony channels together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected.

From the **Settings** tab, navigate to **Signaling Groups.** Click the expand (▸) icon next to the entry.

1. Update the Federated IP/FQDN (Only if the FQDNs for TLS are different). Refer to the Twilio **Create a new Trunk** → **Termination** section of this document
2. Click the ✚ icon to add Listen Ports for TLS.
3. Use TLS as the Protocol and update the Port Number provided by the Service Provider (Port Number 5061 was used during this interop).
4. Click **Apply**.



Signaling Group Table

Total 4 Signaling Group Rows

□	Type	Description	Admin State	Service Status	Display
▸ □	SIP	TEAMS-TWILIO_US: Teams Direct Routing	✓	Up	Counters | Channels | Sessions
▾ □	SIP	TEAMS-TWILIO_US: Border Element	✓	Up	Counters | Channels | Sessions

Listen Ports

Total 2 SIP Listen Port Rows

□	Port	Protocol	TLS Profile ID
□	5060	UDP	N/A
□	5061	TLS	Default TLS Profile

Federated IP/FQDN

Total 2 SIP Federated IP Rows

□	IP/FQDN	Netmask/Prefix
□	[redacted].us1.twilio.com	255.255.255.255
□	[redacted].us2.twilio.com	255.255.255.255

Message Manipulation: Disabled

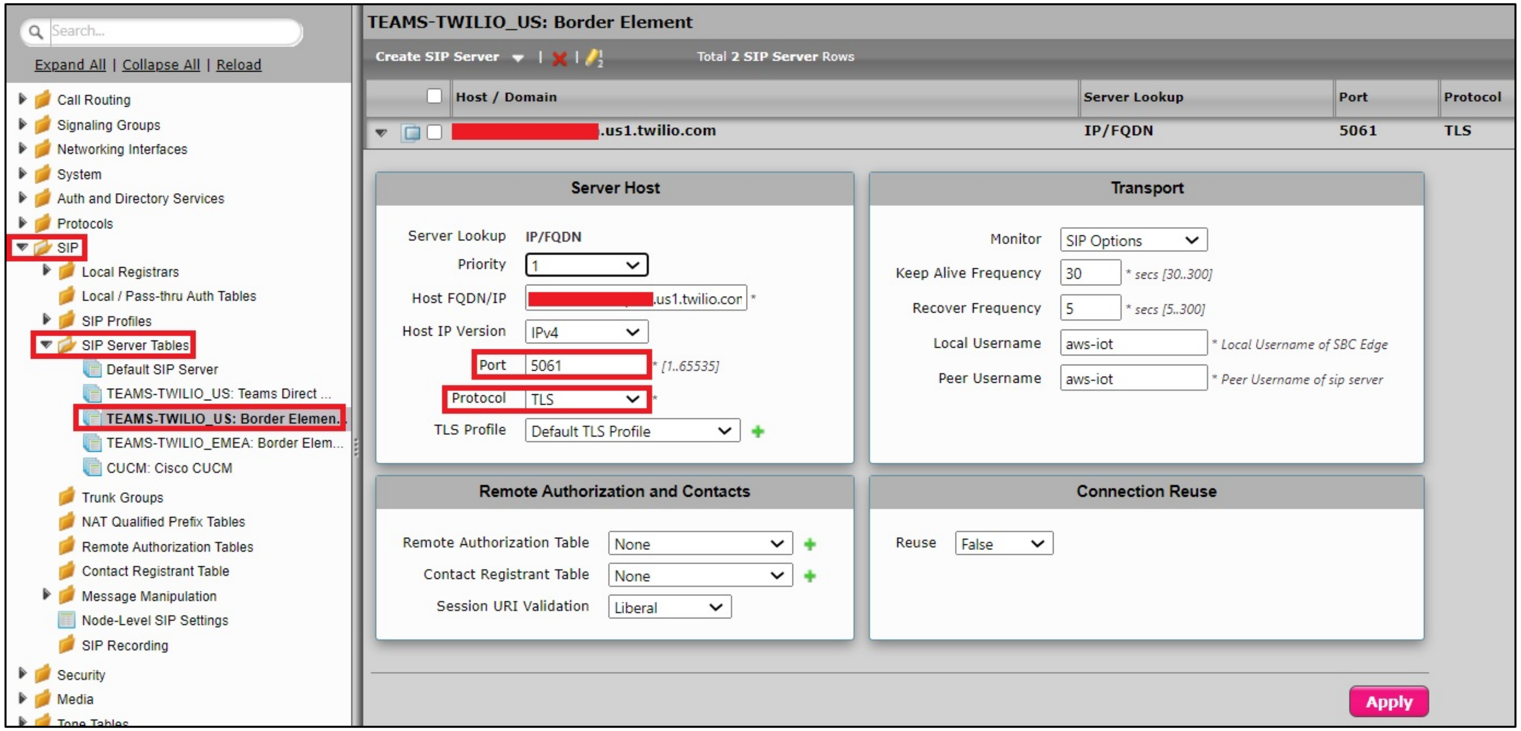
Update SIP Server Table

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 to communicate 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 > TEAMS-TWILIO_US: Border Element.** Click the expand (▸) icon next to the entry.

1. Modify the Host FQDN (Only if the FQDNs for TLS are different). Refer to the Twilio **Create a new Trunk → Termination** section of this document
2. Select TLS protocol with Port Number 5061.

Note
For this interop, the Host FQDNs were modified as a different set of FQDNs were provided for TLS. Customers can retain the FQDNs provided during the configuration of SBC SWe Lite through Easy Config Wizard in the case of no change in FQDNs.



TEAMS-TWILIO_US: Border Element

□	Host / Domain	Server Lookup	Port	Protocol
□	[redacted].us1.twilio.com	IP/FQDN	5061	TLS

Server Host

Server Lookup	IP/FQDN
Priority	1
Host FQDN/IP	[redacted].us1.twilio.cor *
Host IP Version	IPv4
Port	5061 * [1..65535]
Protocol	TLS *
TLS Profile	Default TLS Profile

Transport

Monitor	SIP Options
Keep Alive Frequency	30 * secs [30..300]
Recover Frequency	5 * secs [5..300]
Local Username	aws-iot * Local Username of SBC Edge
Peer Username	aws-iot * Peer Username of sip server

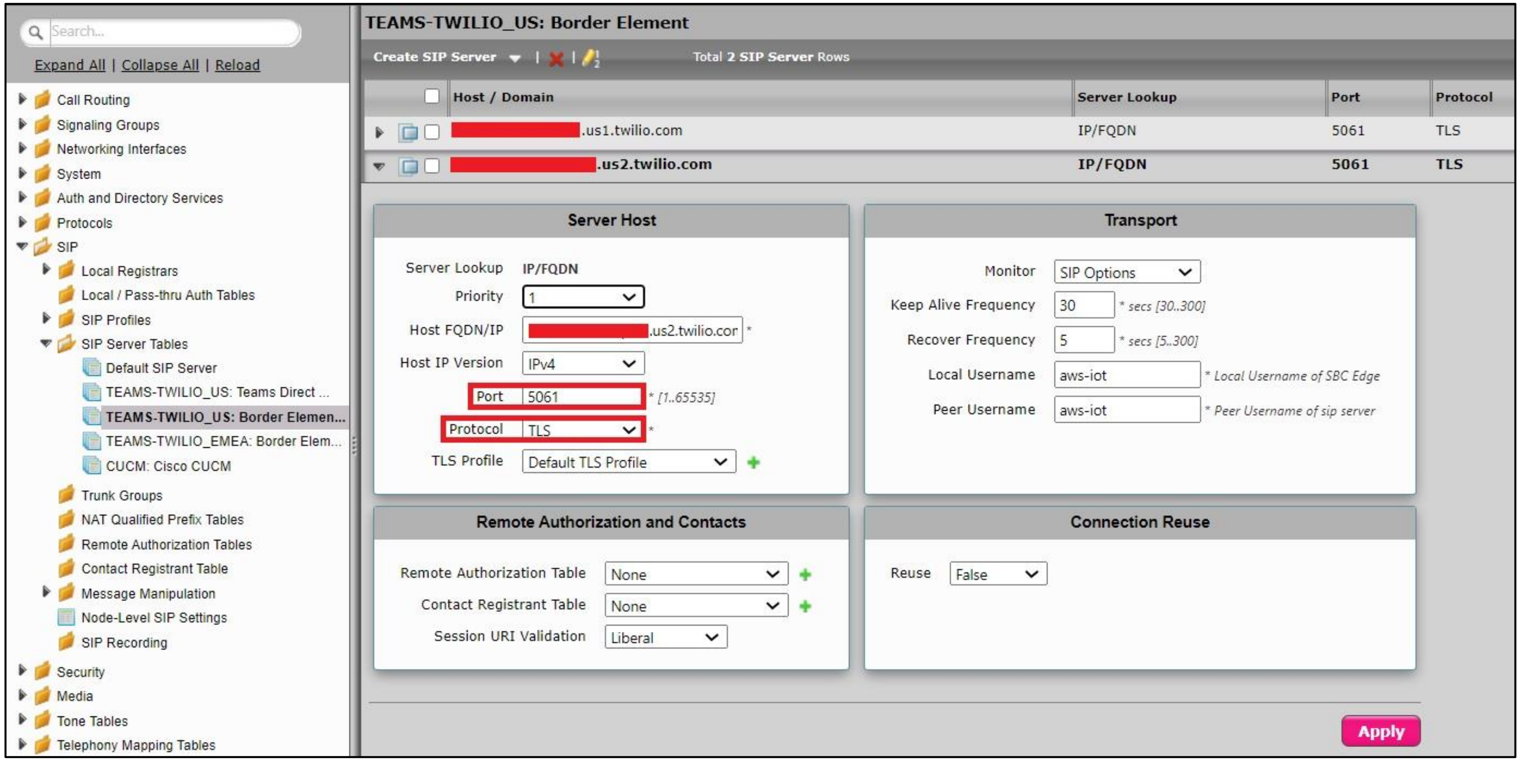
Remote Authorization and Contacts

Remote Authorization Table	None
Contact Registrant Table	None
Session URI Validation	Liberal

Connection Reuse

Reuse	False

- Modify the Secondary Border Element Server by following the same procedure.



TEAMS-TWILIO_US: Border Element

Total 2 SIP Server Rows

Host / Domain	Server Lookup	Port	Protocol
[redacted].us1.twilio.com	IP/FQDN	5061	TLS
[redacted].us2.twilio.com	IP/FQDN	5061	TLS

Server Host

Server Lookup	IP/FQDN
Priority	1
Host FQDN/IP	[redacted].us2.twilio.cor *
Host IP Version	IPv4
Port	5061 * [1..65535]
Protocol	TLS *
TLS Profile	Default TLS Profile

Transport

Monitor	SIP Options
Keep Alive Frequency	30 * secs [30..300]
Recover Frequency	5 * secs [5..300]
Local Username	aws-iot * Local Username of SBC Edge
Peer Username	aws-iot * Peer Username of sip server

Remote Authorization and Contacts

Remote Authorization Table	None
Contact Registrant Table	None
Session URI Validation	Liberal

Connection Reuse

Reuse	False

Note

Procedure and snapshots for TLS configuration are provided only for Twilio US Trunk. Follow the same procedure to modify Twilio EMEA Trunk.

Configure Transformation Tables

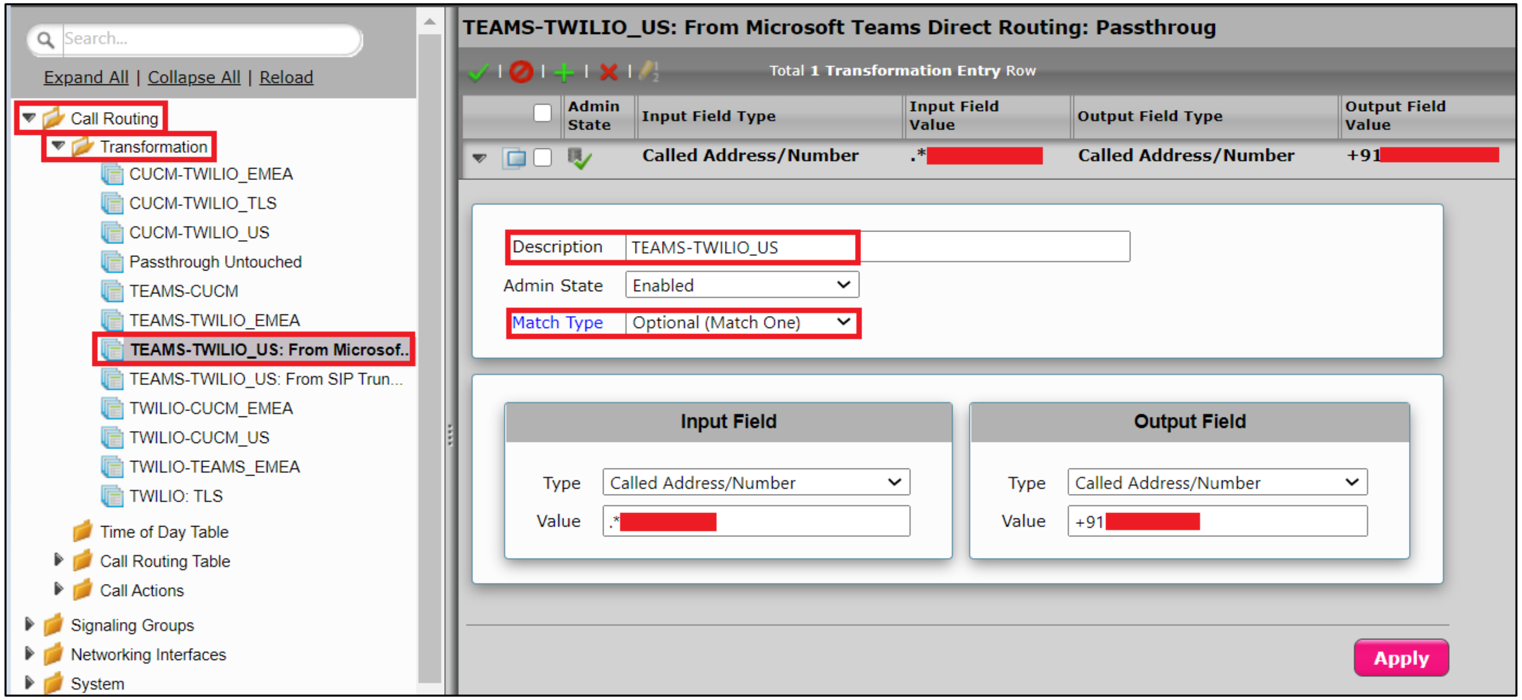
Transformation Tables facilitate the conversion of names, numbers and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table, and they are selected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

From the Settings tab, navigate to Transformation.

To Modify a Transformation Table

The Transformation Tables are created for MS Teams and Twilio US Trunk (TEAMS-TWILIO_US: From Microsoft Teams Direct Routing: Passthrough and TEAMS-TWILIO_US: From SIP Trunk: Passthrough respectively) through Easy Config Wizard. These are modified to allow specific patterns to reach the destination Signaling Group.

1. Click the **expand** (▶) icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired.
3. Modify the Values from **Input field** and **Output field** as required.
4. Set the Match Type as **Optional (Match one)**.
5. Click **OK**.



TEAMS-TWILIO_US: From Microsoft Teams Direct Routing: Passthroug

Total 1 Transformation Entry Row

	Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value
□	✓	Called Address/Number	.*[redacted]	Called Address/Number	+91[redacted]

Description	TEAMS-TWILIO_US
Admin State	Enabled
Match Type	Optional (Match One)

Input Field		Output Field	
Type	Called Address/Number	Type	Called Address/Number
Value	.*[redacted]	Value	+91[redacted]

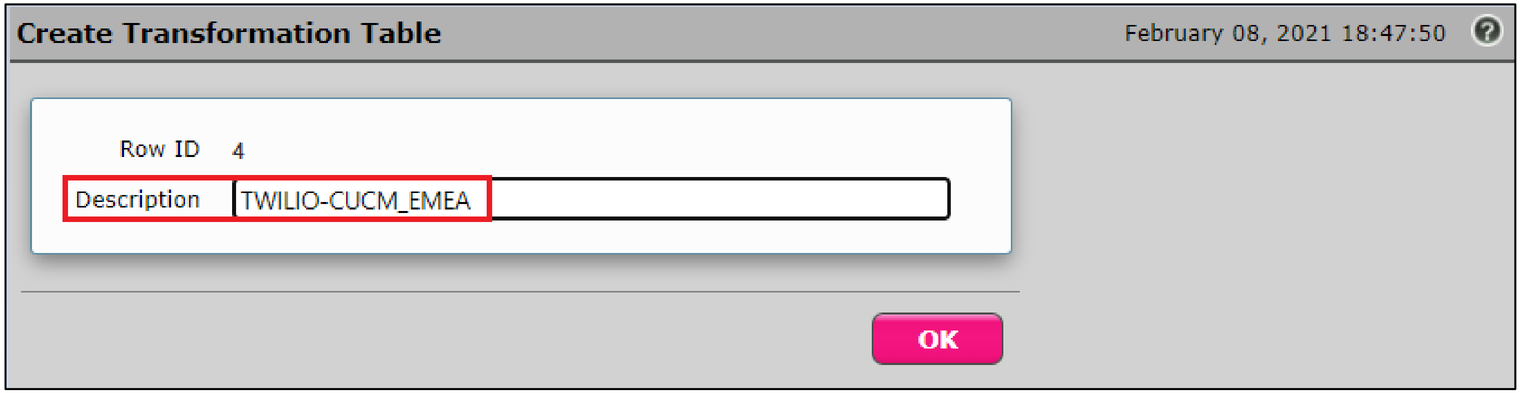
To Create a Transformation Table

Each Transformation Table contains a list of entries considered as routing rules to execute on. Each rule is executed in order until the end of the table is reached or when a Mandatory entry fails to execute.

The Single-legged wizard that was used to configure Twilio EMEA Trunk and CUCM does not create any Transformation Tables. Follow the procedure described below to configure Transformation Tables and the Entries.

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

3. Click **OK**.



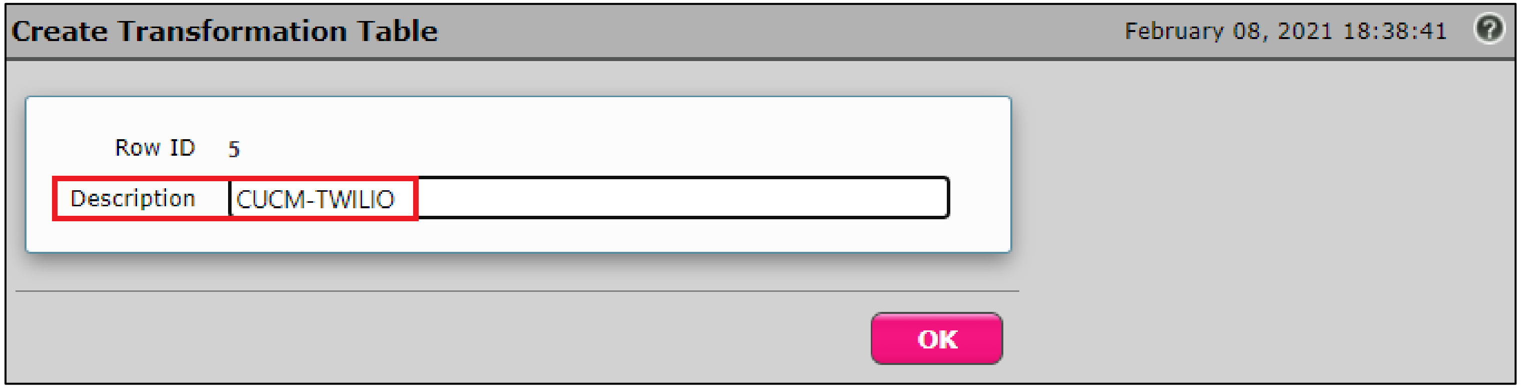
Create Transformation Table

February 08, 2021 18:47:50

Row ID 4

Description TWILIO-CUCM_EMEA

Follow the same procedure to create Transformation Tables for CUCM.



Create Transformation Table

February 08, 2021 18:38:41

Row ID 5

Description CUCM-TWILIO

Creating an Entry to a Message Transformation Table

For this interop, the entries are created based on the numbers associated with each endpoint. Users are free to select their own variables or Regular expressions.

1. Click the **Create(✚)** icon next to the table created in the previous step.
2. Provide the below details:

   Admin State:

   Enabled - The default state is Enabled.

   Match Type:

   Optional: Optional entries must match at least one of that Input Field type.

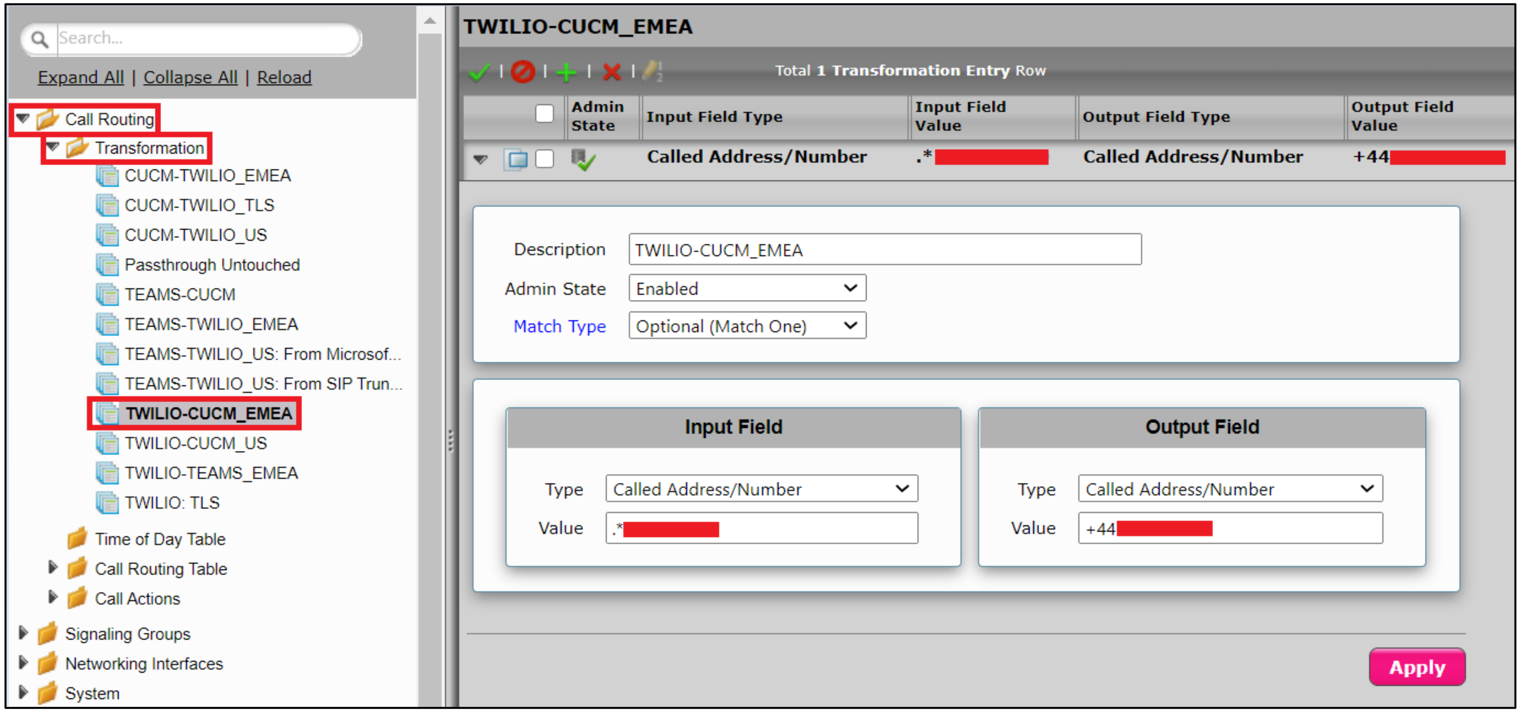
   When a call arrives at a Transformation Table, the incoming message contains a number of Informational Elements (IEs). These IEs include important call information such as: Called Address/Number, Called Extension, Calling Name, Redirecting Number and others.

   Each Informational Element is processed row by row in the Transformation Table.

   Value (Input/Output):

   Specifies the value to match against for the selected type. Depending on the type selected, values are free-form or selected from a menu.

3. Click Apply.



TWILIO-CUCM_EMEA

Total 1 Transformation Entry Row

□	Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value
□	✓	Called Address/Number	.*[redacted]	Called Address/Number	+44[redacted]

Description	TWILIO-CUCM_EMEA
Admin State	Enabled
Match Type	Optional (Match One)

Input Field

Type	Called Address/Number
Value	.*[redacted]

Output Field

Type	Called Address/Number
Value	+44[redacted]

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 allows carrying of calls between Signaling Groups. Routes are defined by Call Routing Tables, which allow for flexible configuration of which calls are carried, and how they are translated.

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

The Call Routing Tables are created to route the calls between TEAMS-TWILIO_US: Teams Direct Routing SG and TEAMS-TWILIO_US: Border Element SG through Easy Config Wizard. The user is allowed to modify these tables as per the requirement.

Modifying an Entry to 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 to 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**.

In order to route any call to or from a call system connected to 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 a 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, displays in configuration header as ✓.

   Route Priority:

   Priority of the route from 1 (highest) to 10 (lowest). Higher priority routes are matched against before lower priority routes regardless of the order of the routes in the table.

   Number/Name Transformation Table:

   Specifies the Transformation Table to use for this routing entry. This 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.

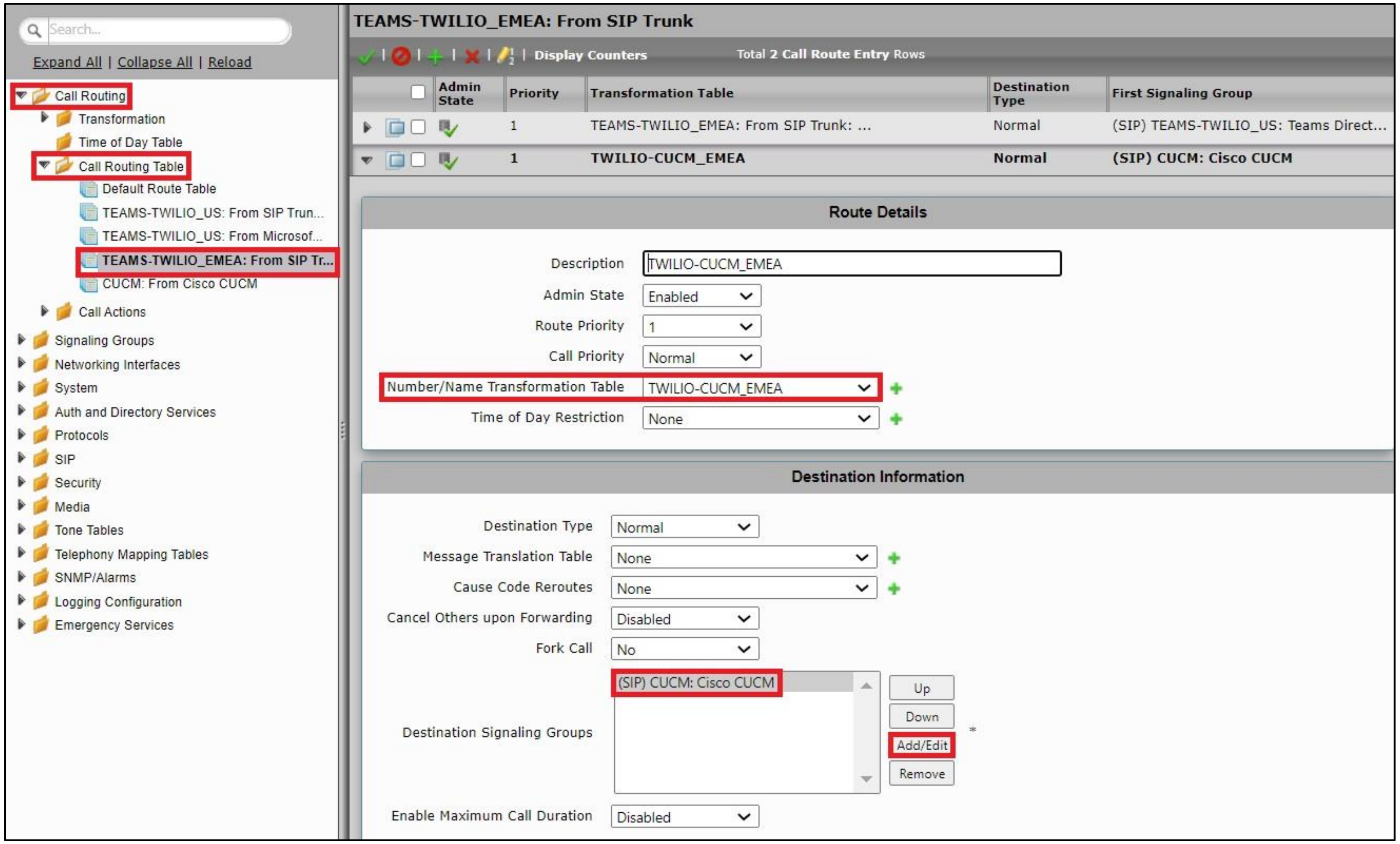
Audio Stream Mode:

DSP (default entry): The SBC uses DSP resources for media handling (transcoding) but it does not facilitate the capabilities/features between endpoints that are not supported within the SBC (codec/capability mismatch). When DSP is configured, the Signaling Groups enabled to support DSP are attempted in order.

Media Transcoding:

Enabled: Enable Transcoding on SIP-to-SIP calls.

3. Click **Apply**.



TEAMS-TWILIO_EMEA: From SIP Trunk

Total 2 Call Route Entry Rows

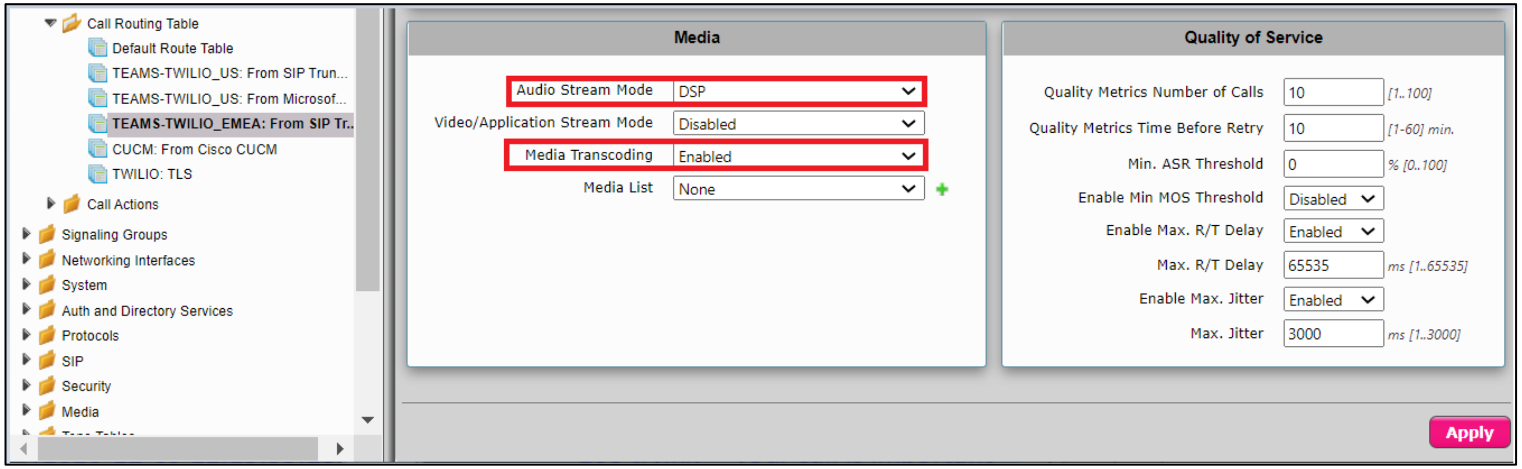
		Admin State	Priority	Transformation Table	Destination Type	First Signaling Group
▸	□	✓	1	TEAMS-TWILIO_EMEA: From SIP Trunk: ...	Normal	(SIP) TEAMS-TWILIO_US: Teams Direct...
▾	□	✓	1	TWILIO-CUCM_EMEA	Normal	(SIP) CUCM: Cisco CUCM

Route Details

Description	TWILIO-CUCM_EMEA
Admin State	Enabled
Route Priority	1
Call Priority	Normal
Number/Name Transformation Table	TWILIO-CUCM_EMEA
Time of Day Restriction	None

Destination Information

Destination Type	Normal
Message Translation Table	None
Cause Code Reroutes	None
Cancel Others upon Forwarding	Disabled
Fork Call	No
Destination Signaling Groups	(SIP) CUCM: Cisco CUCM
Enable Maximum Call Duration	Disabled



Media

Audio Stream Mode	DSP
Video/Application Stream Mode	Disabled
Media Transcoding	Enabled
Media List	None

Quality of Service

Quality Metrics Number of Calls	10	[1..100]
Quality Metrics Time Before Retry	10	[1-60] min.
Min. ASR Threshold	0	% [0..100]
Enable Min MOS Threshold	Disabled	
Enable Max. R/T Delay	Enabled	
Max. R/T Delay	65535	ms [1..65535]
Enable Max. Jitter	Enabled	
Max. Jitter	3000	ms [1..3000]

Creating Multiple Entries to a Call Routing Table

SBC SWe Lite allows the user to create multiple entries to a Call Routing table. As there are four SIP Signaling Groups in this deployment, it is required to create multiple route entries to allow the call to reach a specific destination SIP Signaling Group.

During this interop the Call Routing entries were created to route the calls:

- From TEAMS-TWILIO_US: Border Element SIP Signaling Group to TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group and CUCM: Cisco CUCM SIP Signaling Group
- From TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group to TEAMS-TWILIO_US: Teams Direct Routing and CUCM: Cisco CUCM SIP Signaling Group
- From TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group to TEAMS-TWILIO_US: Border Element SIP Signaling Group, CUCM: Cisco CUCM SIP Signaling Group and TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group
- From CUCM: Cisco CUCM SIP Signaling Group to TEAMS-TWILIO_US: Border Element SIP Signaling Group, TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group and TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group

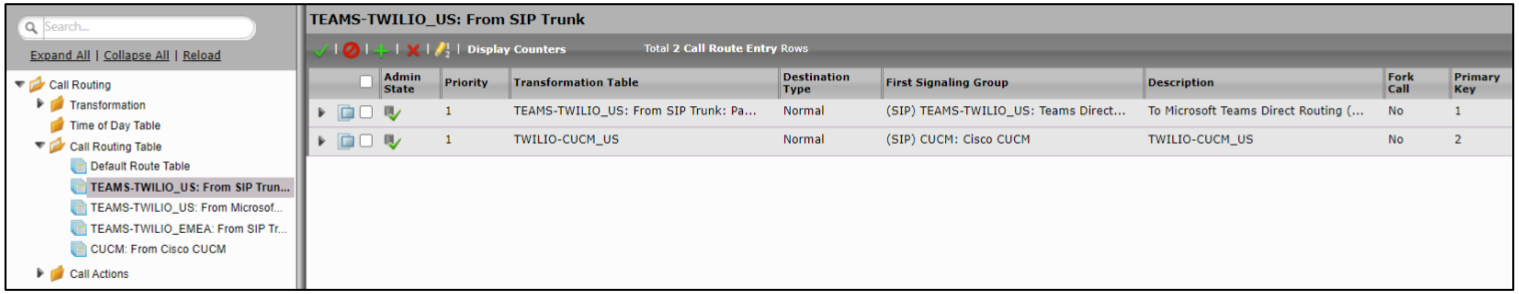
Ensure that the Transformation Tables are correctly mapped to each Call Routing Table entry.

To create multiple entries:

1. Click on the Routing Table on which multiple routing entries are required.
2. Follow the procedure described in the "Creating an Entry to a Call Routing Table" section.

The following Call Routing entries were created for the interop:

From TEAMS-TWILIO_US: Border Element SIP Signaling Group, the calls are routed to TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group or CUCM: Cisco CUCM SIP Signaling Group based on the Transformation table attached.

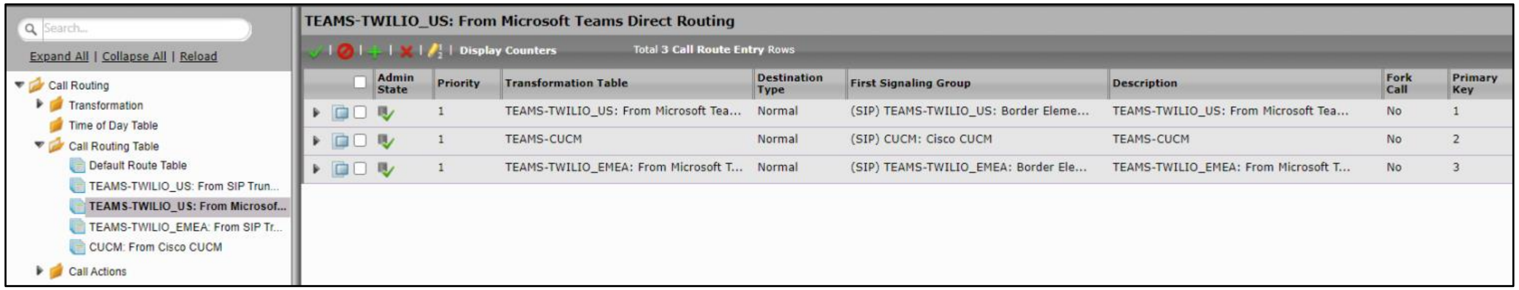


TEAMS-TWILIO_US: From SIP Trunk

Total 2 Call Route Entry Rows

Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
✓	1	TEAMS-TWILIO_US: From SIP Trunk: Pa...	Normal	(SIP) TEAMS-TWILIO_US: Teams Direct...	To Microsoft Teams Direct Routing (...	No	1
✓	1	TWILIO-CUCM_US	Normal	(SIP) CUCM: Cisco CUCM	TWILIO-CUCM_US	No	2

When the incoming call hits TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group, the call is routed to TEAMS-TWILIO_US: Border Element SIP Signaling Group, CUCM: Cisco CUCM SIP Signaling Group or TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group based on the Transformation Table associated.

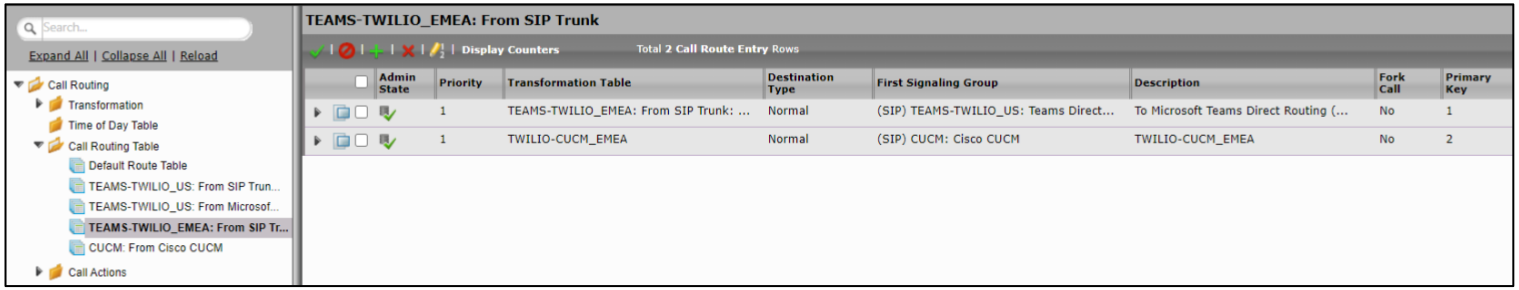


TEAMS-TWILIO_US: From Microsoft Teams Direct Routing

Total 3 Call Route Entry Rows

Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
✓	1	TEAMS-TWILIO_US: From Microsoft Tea...	Normal	(SIP) TEAMS-TWILIO_US: Border Eleme...	TEAMS-TWILIO_US: From Microsoft Tea...	No	1
✓	1	TEAMS-CUCM	Normal	(SIP) CUCM: Cisco CUCM	TEAMS-CUCM	No	2
✓	1	TEAMS-TWILIO_EMEA: From Microsoft T...	Normal	(SIP) TEAMS-TWILIO_EMEA: Border Ele...	TEAMS-TWILIO_EMEA: From Microsoft T...	No	3

When the source is TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group, the destination is either TEAMS-TWILIO_US: Teams Direct Routing or CUCM: Cisco CUCM SIP Signaling Group depending on the Transformation Table selected for the call.

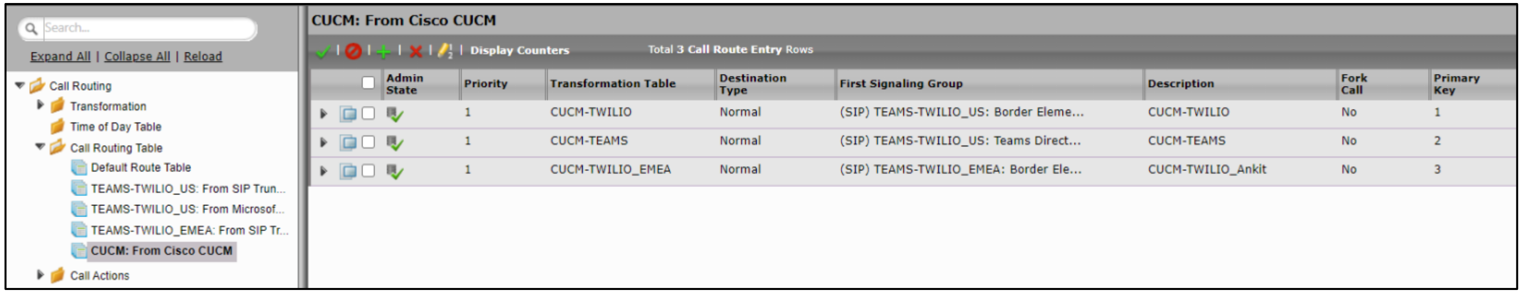


TEAMS-TWILIO_EMEA: From SIP Trunk

Total 2 Call Route Entry Rows

Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
✓	1	TEAMS-TWILIO_EMEA: From SIP Trunk: ...	Normal	(SIP) TEAMS-TWILIO_US: Teams Direct...	To Microsoft Teams Direct Routing (...	No	1
✓	1	TWILIO-CUCM_EMEA	Normal	(SIP) CUCM: Cisco CUCM	TWILIO-CUCM_EMEA	No	2

When the call is originated from CUCM: Cisco CUCM SIP Signaling Group, the Call Routing Table shown below allows the call to reach TEAMS-TWILIO_US: Border Element SIP Signaling Group, TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group or TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group based on the Transformation Table associated with the route.

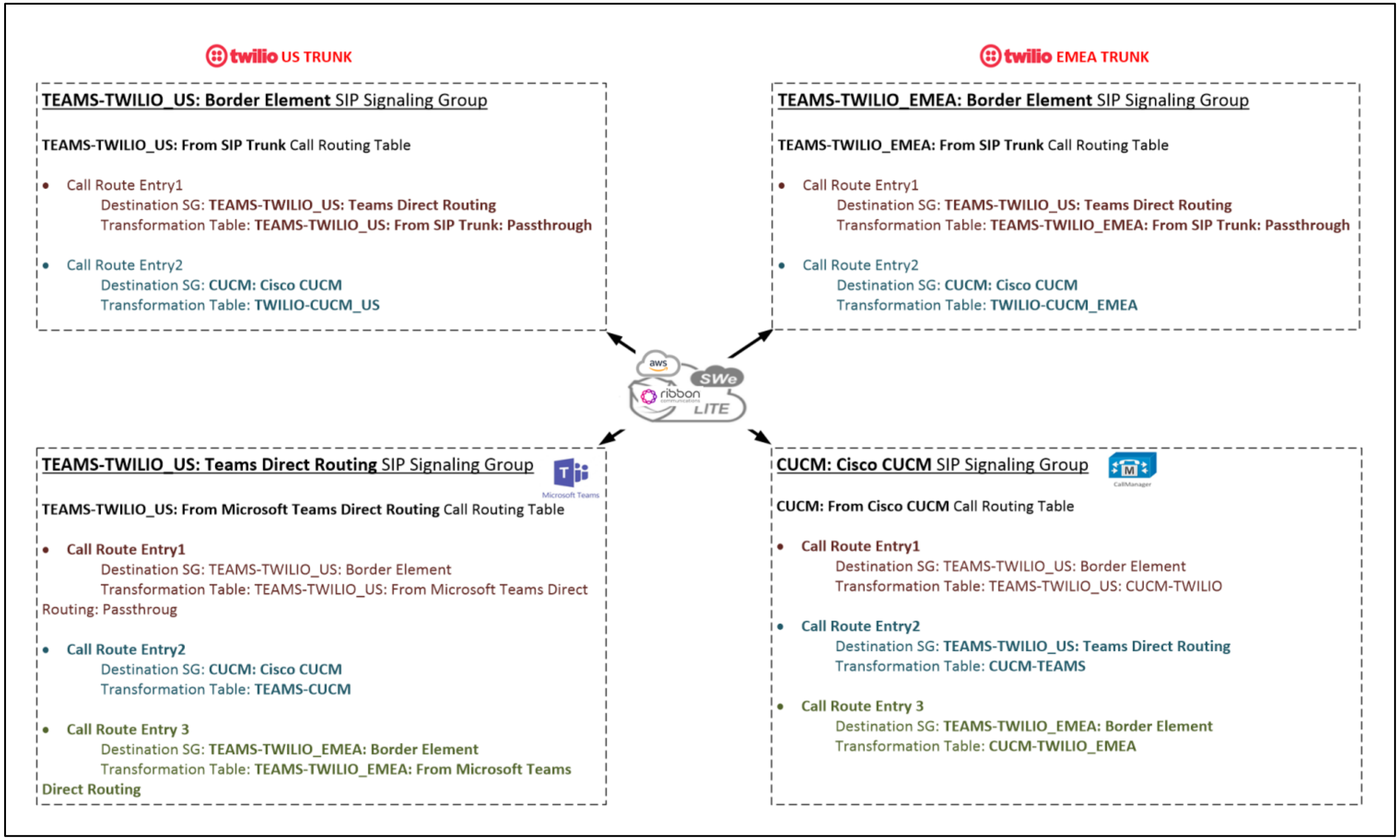


CUCM: From Cisco CUCM

Total 3 Call Route Entry Rows

Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
✓	1	CUCM-TWILIO	Normal	(SIP) TEAMS-TWILIO_US: Border Eleme...	CUCM-TWILIO	No	1
✓	1	CUCM-TEAMS	Normal	(SIP) TEAMS-TWILIO_US: Teams Direct...	CUCM-TEAMS	No	2
✓	1	CUCM-TWILIO_EMEA	Normal	(SIP) TEAMS-TWILIO_EMEA: Border Ele...	CUCM-TWILIO_Ankit	No	3

The same has been depicted in the diagram below:



twilio US TRUNK

TEAMS-TWILIO_US: Border Element SIP Signaling Group

TEAMS-TWILIO_US: From SIP Trunk Call Routing Table

- Call Route Entry1
  Destination SG: **TEAMS-TWILIO_US: Teams Direct Routing**
  Transformation Table: **TEAMS-TWILIO_US: From SIP Trunk: Passthrough**
- Call Route Entry2
  Destination SG: **CUCM: Cisco CUCM**
  Transformation Table: **TWILIO-CUCM_US**

twilio EMEA TRUNK

TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group

TEAMS-TWILIO_EMEA: From SIP Trunk Call Routing Table

- Call Route Entry1
  Destination SG: **TEAMS-TWILIO_US: Teams Direct Routing**
  Transformation Table: **TEAMS-TWILIO_EMEA: From SIP Trunk: Passthrough**
- Call Route Entry2
  Destination SG: **CUCM: Cisco CUCM**
  Transformation Table: **TWILIO-CUCM_EMEA**

TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group

TEAMS-TWILIO_US: From Microsoft Teams Direct Routing Call Routing Table

- **Call Route Entry1**
  Destination SG: TEAMS-TWILIO_US: Border Element
  Transformation Table: TEAMS-TWILIO_US: From Microsoft Teams Direct Routing: Passthroug
- **Call Route Entry2**
  Destination SG: **CUCM: Cisco CUCM**
  Transformation Table: **TEAMS-CUCM**
- **Call Route Entry 3**
  Destination SG: **TEAMS-TWILIO_EMEA: Border Element**
  Transformation Table: **TEAMS-TWILIO_EMEA: From Microsoft Teams Direct Routing**

CUCM: Cisco CUCM SIP Signaling Group

CUCM: From Cisco CUCM Call Routing Table

- **Call Route Entry1**
  Destination SG: TEAMS-TWILIO_US: Border Element
  Transformation Table: TEAMS-TWILIO_US: CUCM-TWILIO
- **Call Route Entry2**
  Destination SG: **TEAMS-TWILIO_US: Teams Direct Routing**
  Transformation Table: **CUCM-TEAMS**
- **Call Route Entry 3**
  Destination SG: **TEAMS-TWILIO_EMEA: Border Element**
  Transformation Table: **CUCM-TWILIO_EMEA**

Warning

In case of SIP URI calling, change the FQDN from sip.pstnhub.microsoft.com/sip2.pstnhub.microsoft.com/sip3.pstnhub.microsoft.com to interopdomain.com using SMM and attach it to Outbound Message Manipulation Table on TEAMS-TWILIO_US: Teams Direct Routing Signaling Group.

Message Manipulation

All the calls initiated from Teams endpoint will have "PRIVACY: id" header. As Trusted interface is disabled on Twilio (US and EMEA) SIP profiles, SWe Lite sends out all the calls as Anonymous. In order to avoid this, we have used an SMM on the Inbound Message Manipulation list of TEAMS-TWILIO_US: Teams Direct Routing SIP SG.

The SMM performs the following actions:

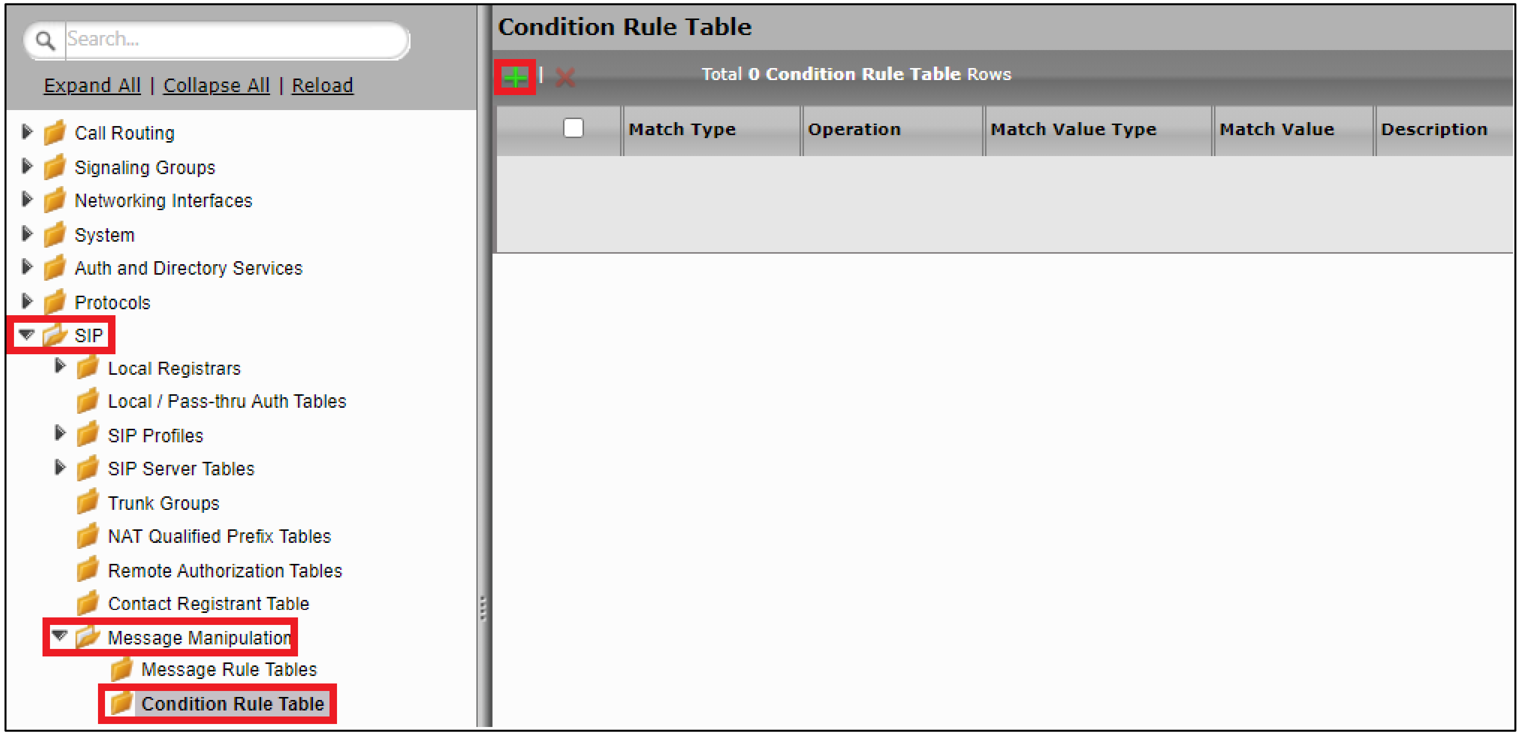
- Removes “PRIVACY: id” header when the incoming INVITE has calling party number in the From header which allows SBC SWe Lite to send the INVITE to Twilio with actual number.
- Does not perform any action when "Anonymous" is in the From header.

The Message Manipulation feature comprises two primary components that work in concert to modify SIP messages. Those component are Condition Rules and Rule Tables.

Creating a Condition Rule Table

Condition rules are simple rules that apply to a specific component of a message (e.g., diversion.uri.host, from.uri.host, etc.) the value of the field specified in the Match Type list box can match against a; literal value, token, or REGEX.

From the **Settings** tab, navigate to **SIP > Message Manipulation > Condition Rule Table.** Click the Create (➕) icon at the top of the Condition Rule Table page.

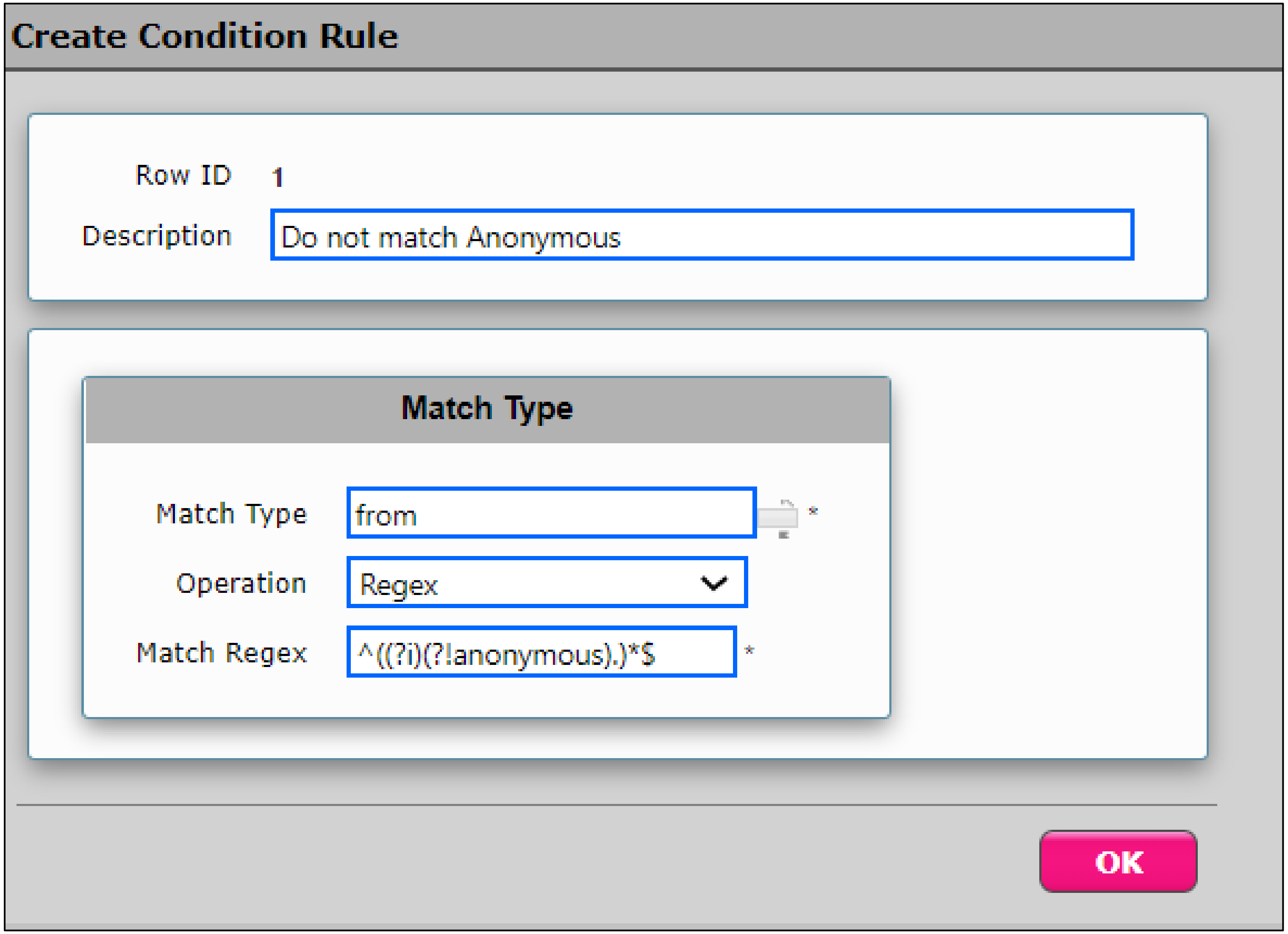


Condition Rule Table

Total 0 Condition Rule Table Rows

□	Match Type	Operation	Match Value Type	Match Value	Description

- Provide a suitable description for the rule.
- From the Match type drop-down, select "from" as we are checking if the From header has Anonymous or calling party number.
  Match type specifies the first operand for the logical condition expressed by this rule. The operand must be a parameter tree token identifier.
- Use Regex Operation.
  Operation specifies the match type for this condition.
- Write a Regular Expression to match everything but Anonymous.
- Click **OK**.



Create Condition Rule

Row ID 1

Description: Do not match Anonymous

Match Type

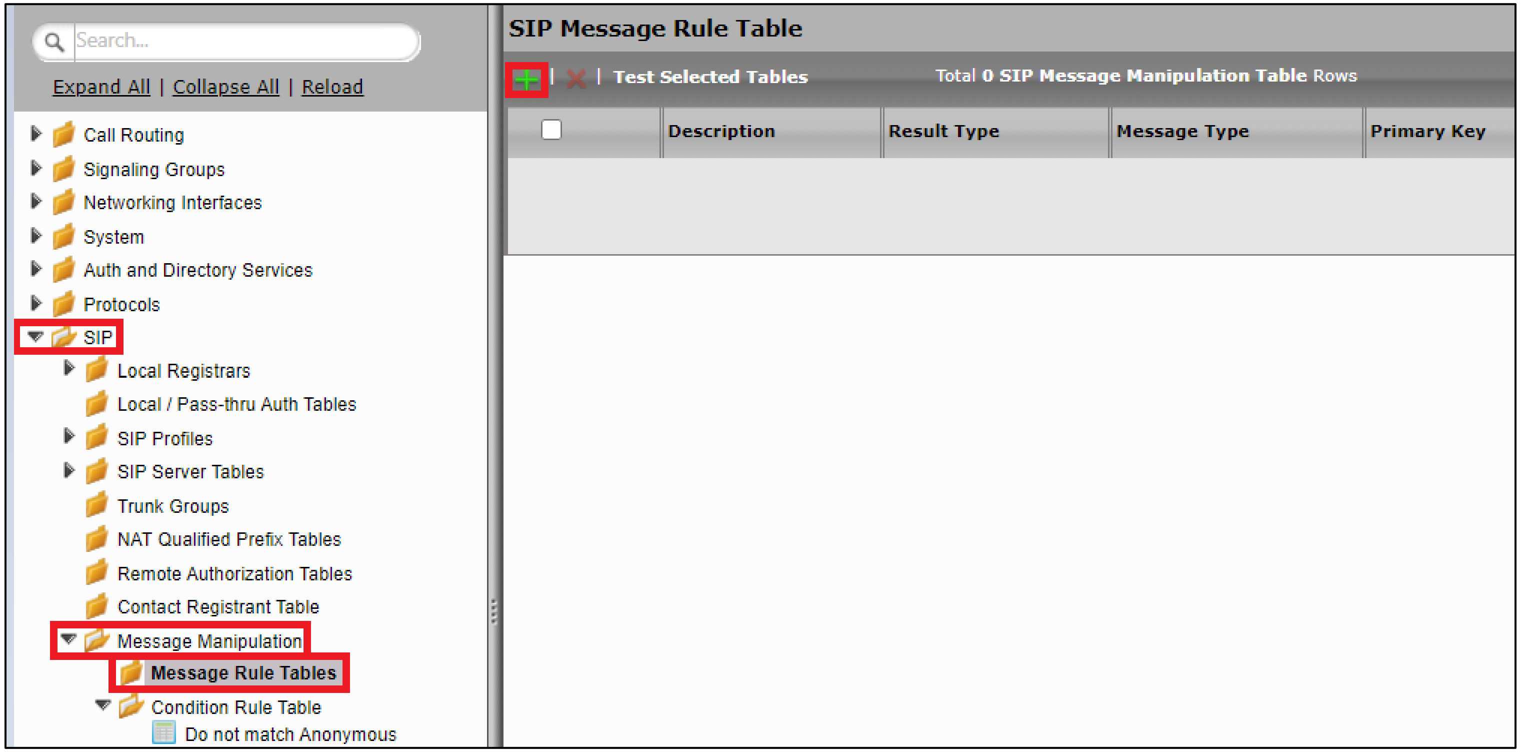
Match Type: from *

Operation: Regex

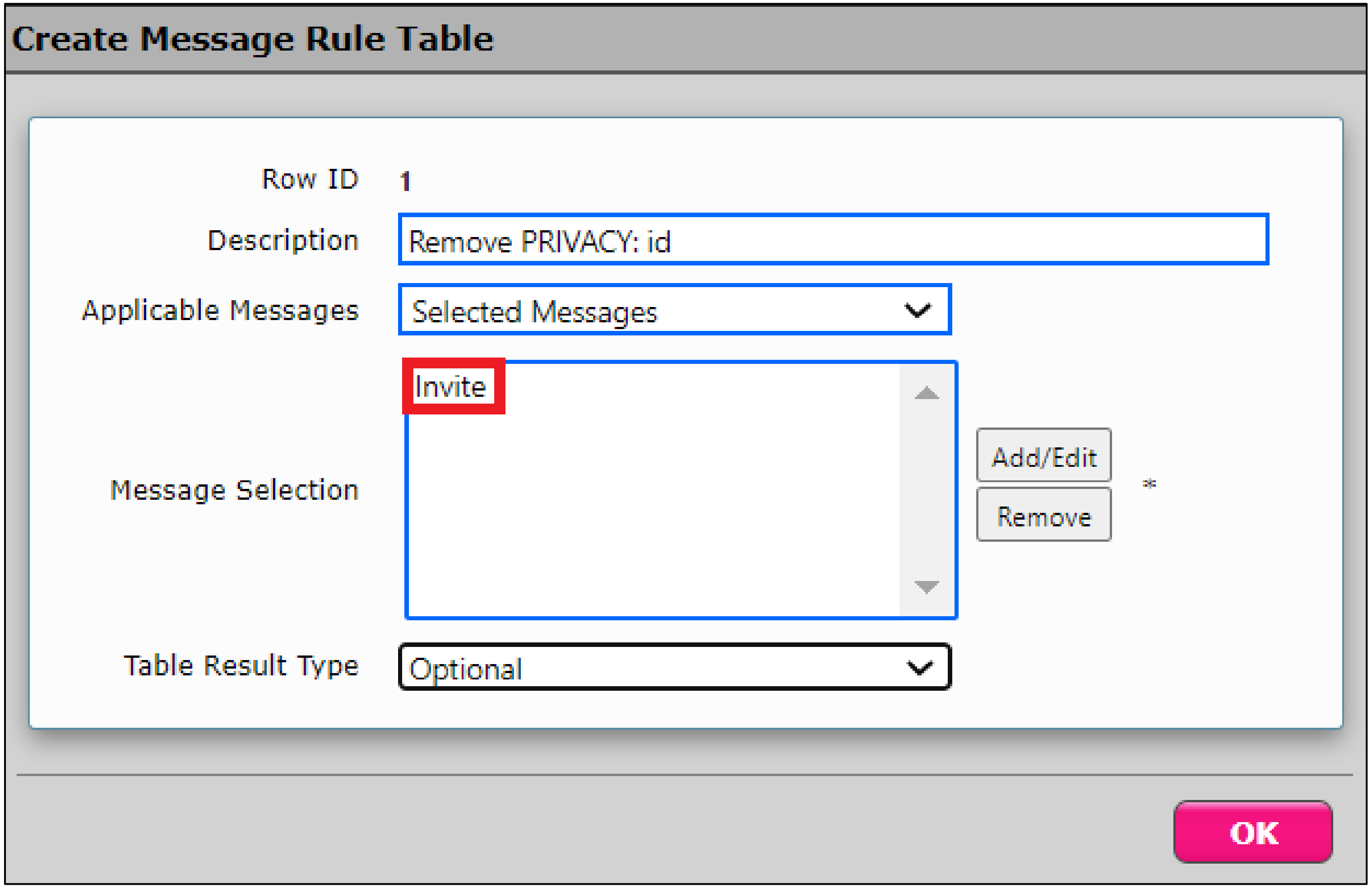
Match Regex: ^((?i)(?!anonymous).)*$ *

Creating a SIP Message Rule Table

From the **Settings** tab, navigate to **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table(+)** icon.



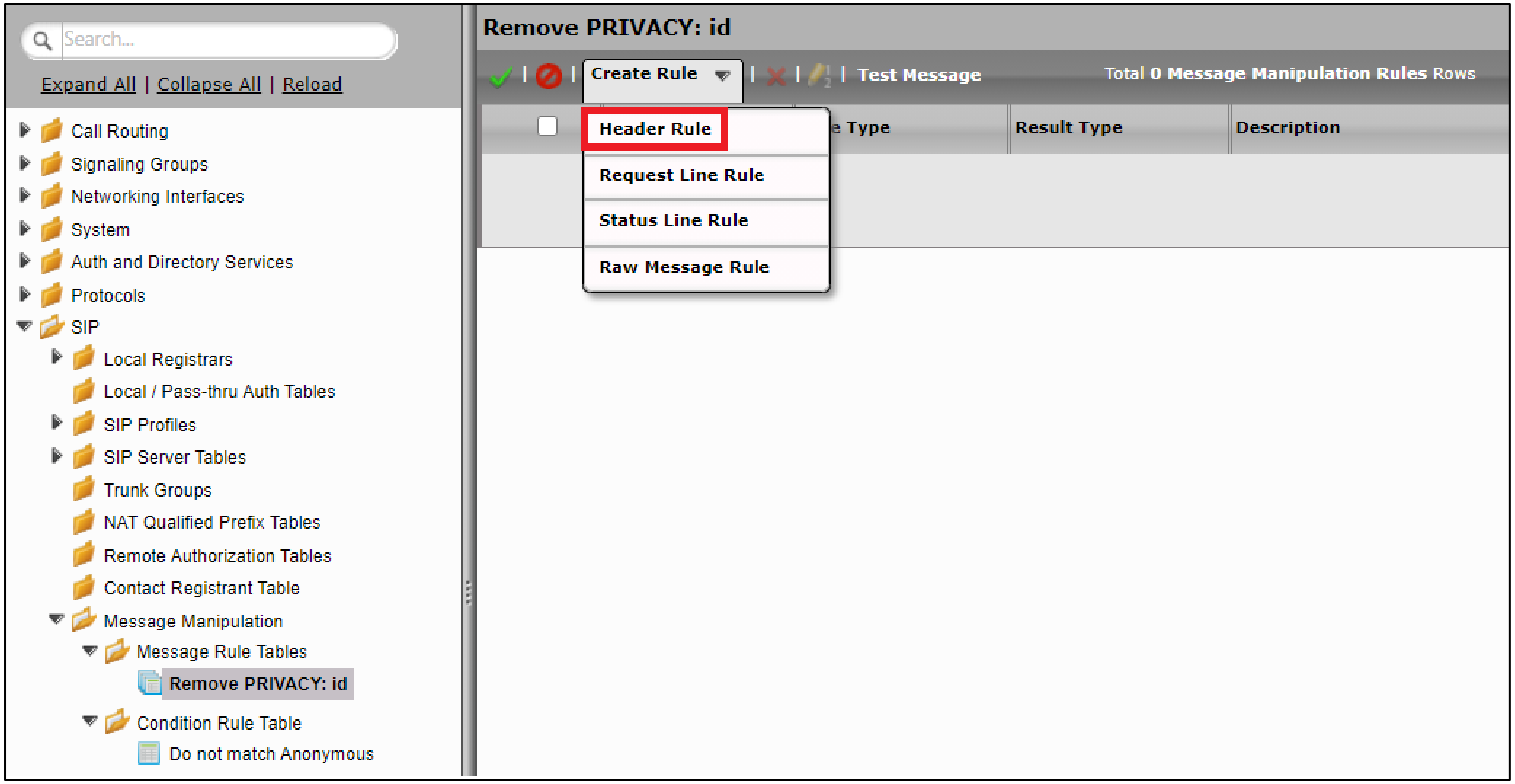
- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Invite from the Message Selection list.
- Click **OK**.



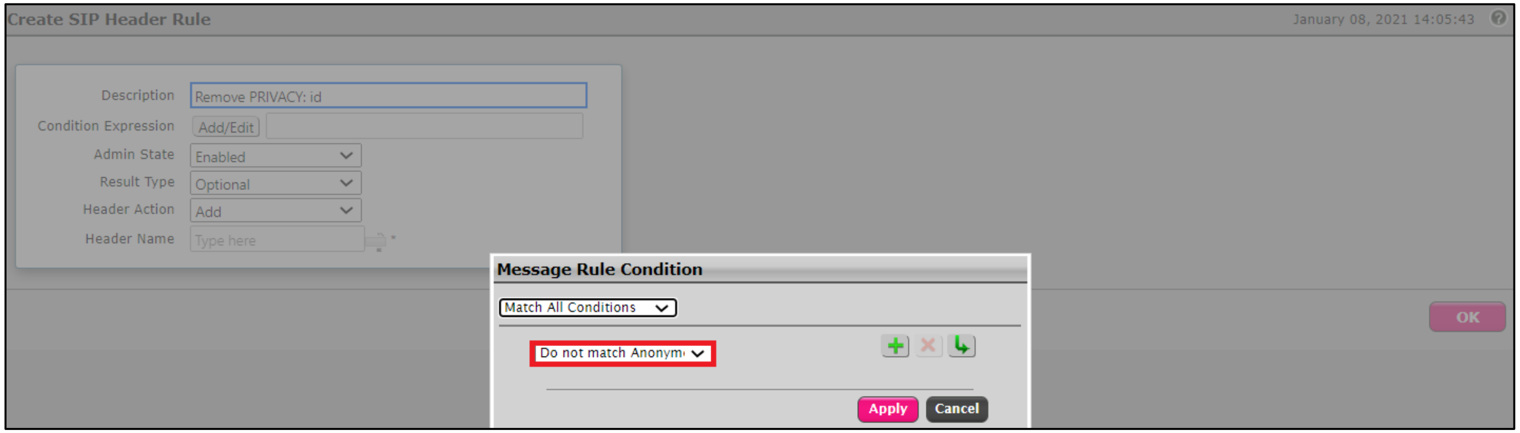
Create Message Rule Table

Row ID	1
Description	Remove PRIVACY: id
Applicable Messages	Selected Messages
Message Selection	Invite
Table Result Type	Optional

- Click the **expand** (▸) icon next to the Rule Table entry created.
- From the **Create Rule** drop down box, select **Header Rule**.



- Provide the desired description.
- Click the **Add/Edit** button to launch the Condition Expression Builder.
- Select **Match All Conditions**.
- Select the Condition Rule created in the previous step and click **Apply**.



Create SIP Header Rule

January 08, 2021 14:05:43

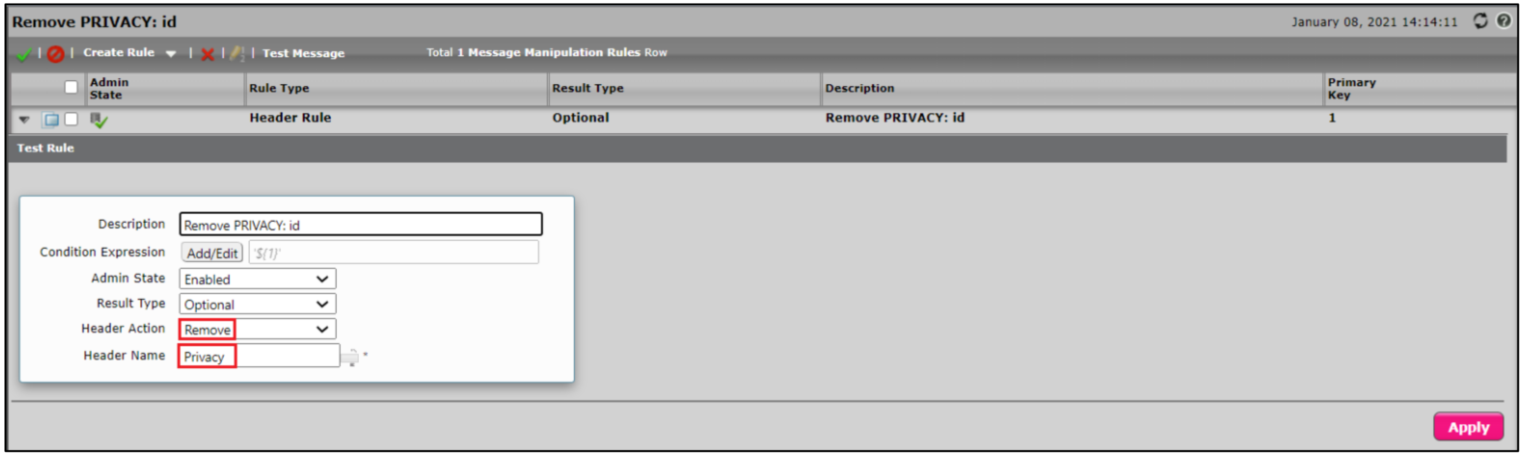
Description	Remove PRIVACY: id
Condition Expression	Add/Edit
Admin State	Enabled
Result Type	Optional
Header Action	Add
Header Name	Type here

Message Rule Condition

Match All Conditions

Do not match Anonym

- Header Action: Remove (if the header is present, it is dropped from the message).
- Header Name: Specifies the type of header referenced by this rule. In this case, Privacy header.
- Click **Apply**.



Remove PRIVACY: id

January 08, 2021 14:14:11

Total 1 Message Manipulation Rules Row

Admin State	Rule Type	Result Type	Description	Primary Key
	Header Rule	Optional	Remove PRIVACY: id	1

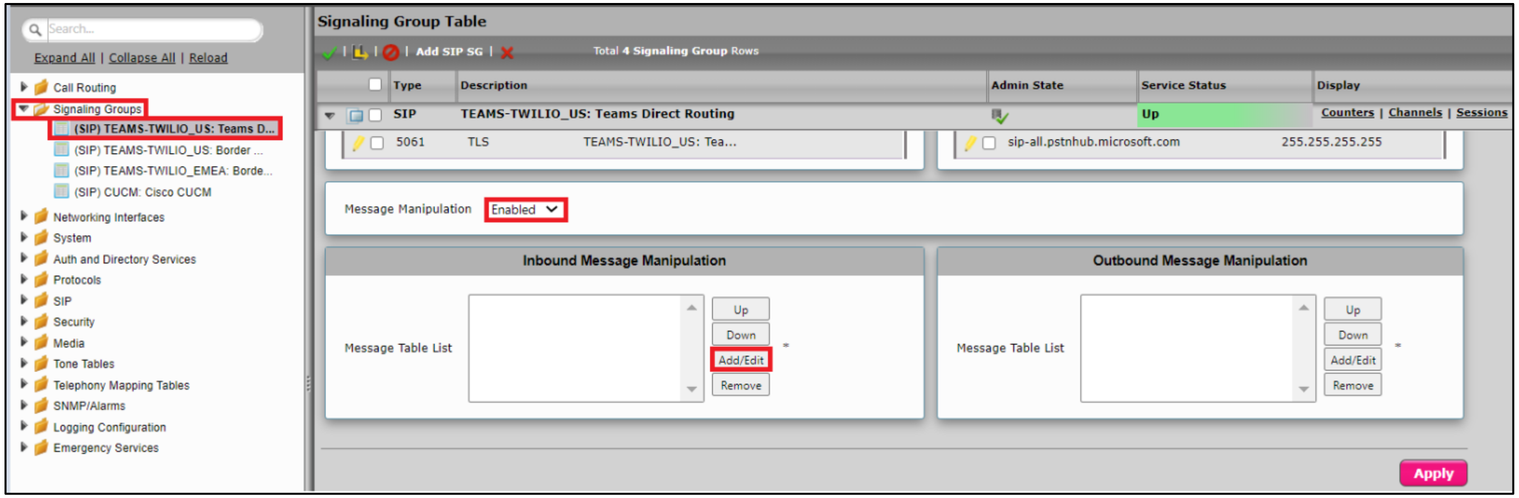
Test Rule

Description	Remove PRIVACY: id
Condition Expression	Add/Edit '$(1)'
Admin State	Enabled
Result Type	Optional
Header Action	Remove
Header Name	Privacy

Attaching the Message Table to SIP SG

From the Settings tab, navigate to Signaling Groups > TEAMS-TWILIO_US: Teams Direct Routing.

- Enable Message Manipulation.
- Click **Add/Edit** on Inbound Message Manipulation (The rules in this table are used to manipulate inbound SIP messages in the Signaling Group).



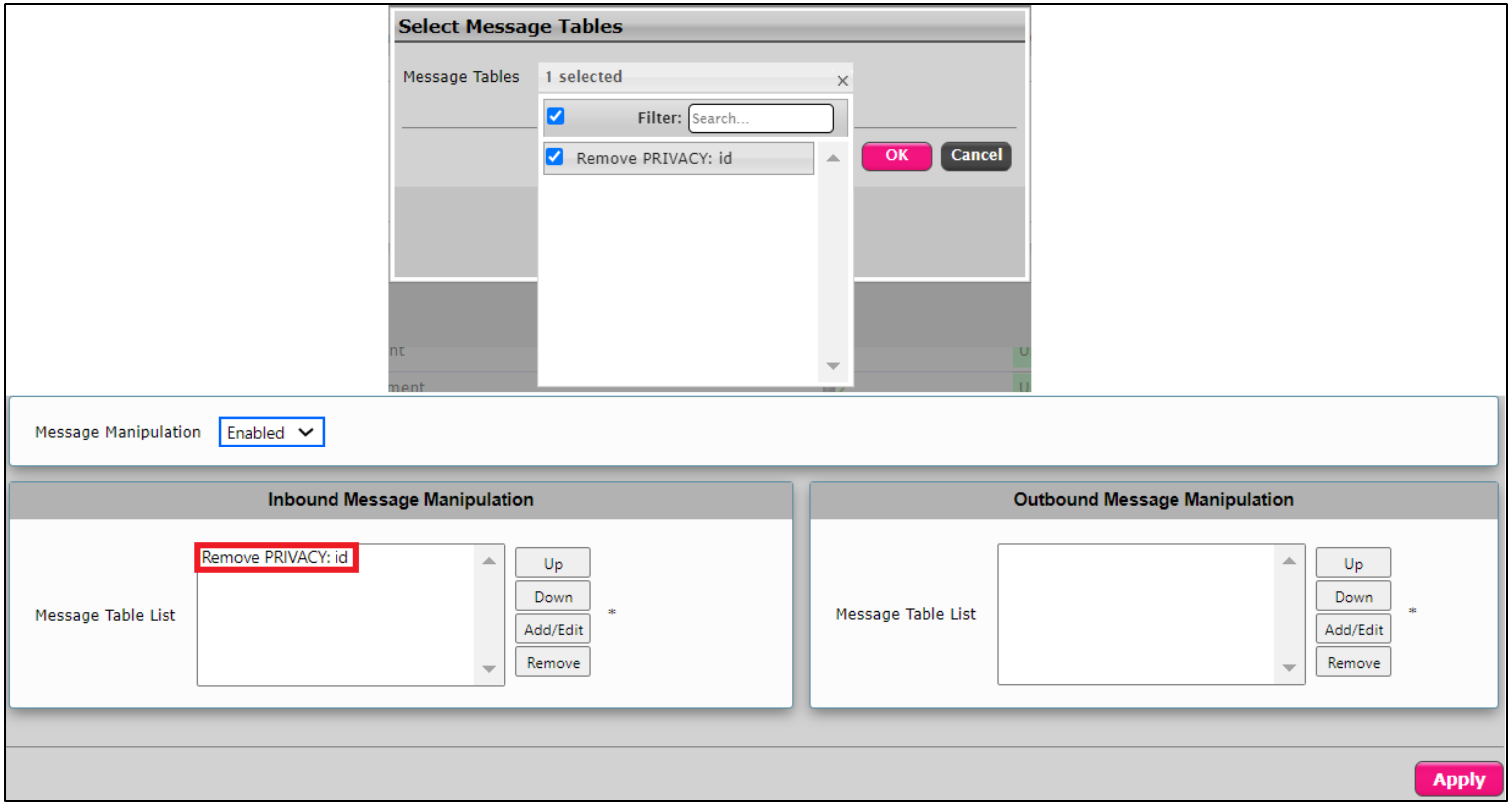
Type	Description	Admin State	Service Status	Display
SIP	TEAMS-TWILIO_US: Teams Direct Routing	✓	Up	Counters | Channels | Sessions

5061 TLS TEAMS-TWILIO_US: Tea...

sip-all.pstnhub.microsoft.com 255.255.255.255

Message Manipulation: Enabled

- This displays a drop-down list of available message tables. Select an entry and click **Apply**.



Select Message Tables

Message Tables: 1 selected

☑ Filter: Search...

☑ Remove PRIVACY: id

Message Manipulation: Enabled

Inbound Message Manipulation

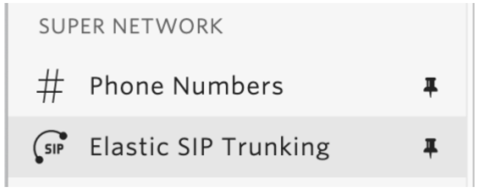
Message Table List: Remove PRIVACY: id

Outbound Message Manipulation

Message Table List

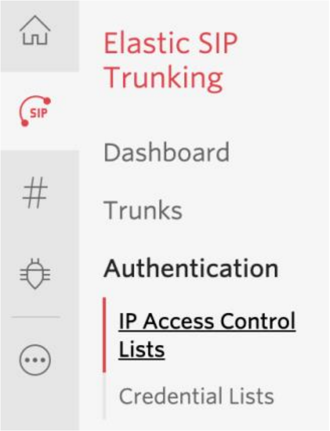
Twilio Elastic SIP Trunk Configuration

From your Twilio Console, navigate to the Elastic SIP Trunking area (or click on the SIP icon on the left vertical navigation bar).

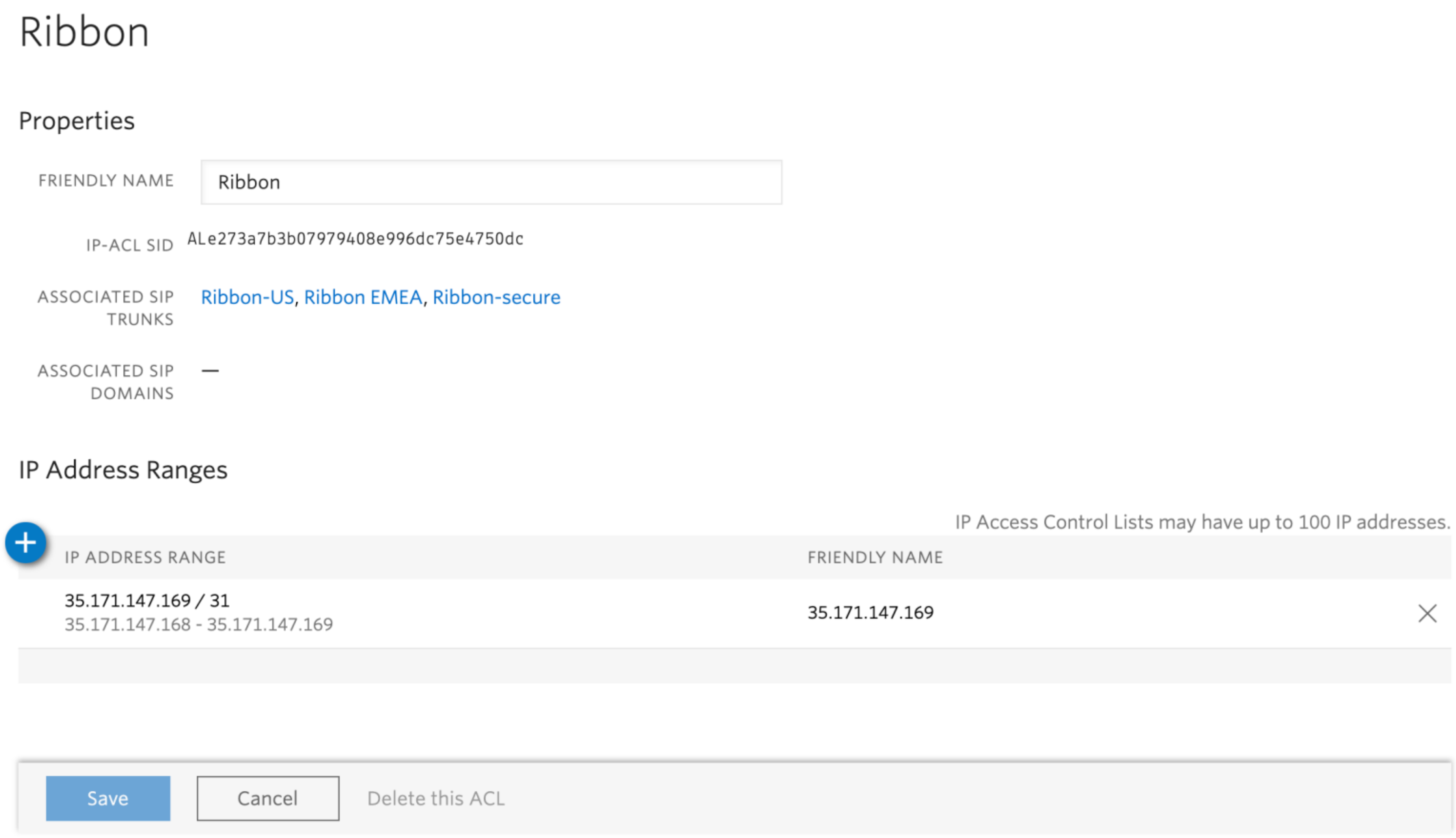


1. Create an IP-ACL rule

Click on Authentication in the left navigation, and then click on IP Access Control Lists.



Create a new IP-ACL, for example call it "Ribbon" and add your SBCs IP addresses (Kindly refer to the section Installing SBC SWe Lite on AWS)



Ribbon

Properties

FRIENDLY NAME	Ribbon
IP-ACL SID	ALe273a7b3b07979408e996dc75e4750dc
ASSOCIATED SIP TRUNKS	Ribbon-US, Ribbon EMEA, Ribbon-secure
ASSOCIATED SIP DOMAINS	—

IP Address Ranges

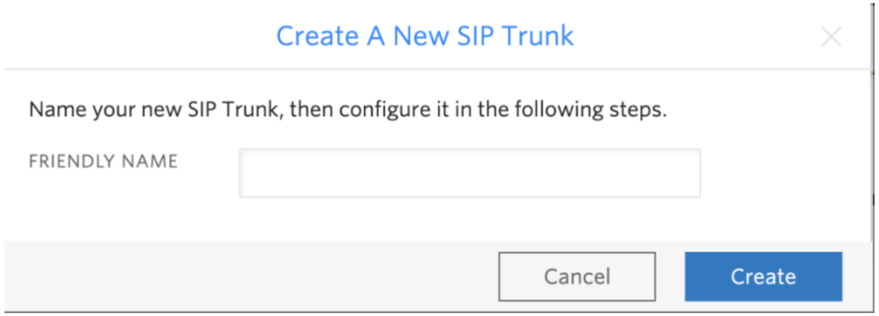
IP Access Control Lists may have up to 100 IP addresses.

IP ADDRESS RANGE	FRIENDLY NAME
35.171.147.169 / 31 35.171.147.168 - 35.171.147.169	35.171.147.169

2. Create a new Trunk

For each geographical region desired (eg. North America, Europe), create a new Elastic SIP Trunk.

To do this: From your Twilio Console, navigate to the Elastic SIP Trunking area, then click on “Trunks” on the left vertical navigation bar, and create a new Trunk.

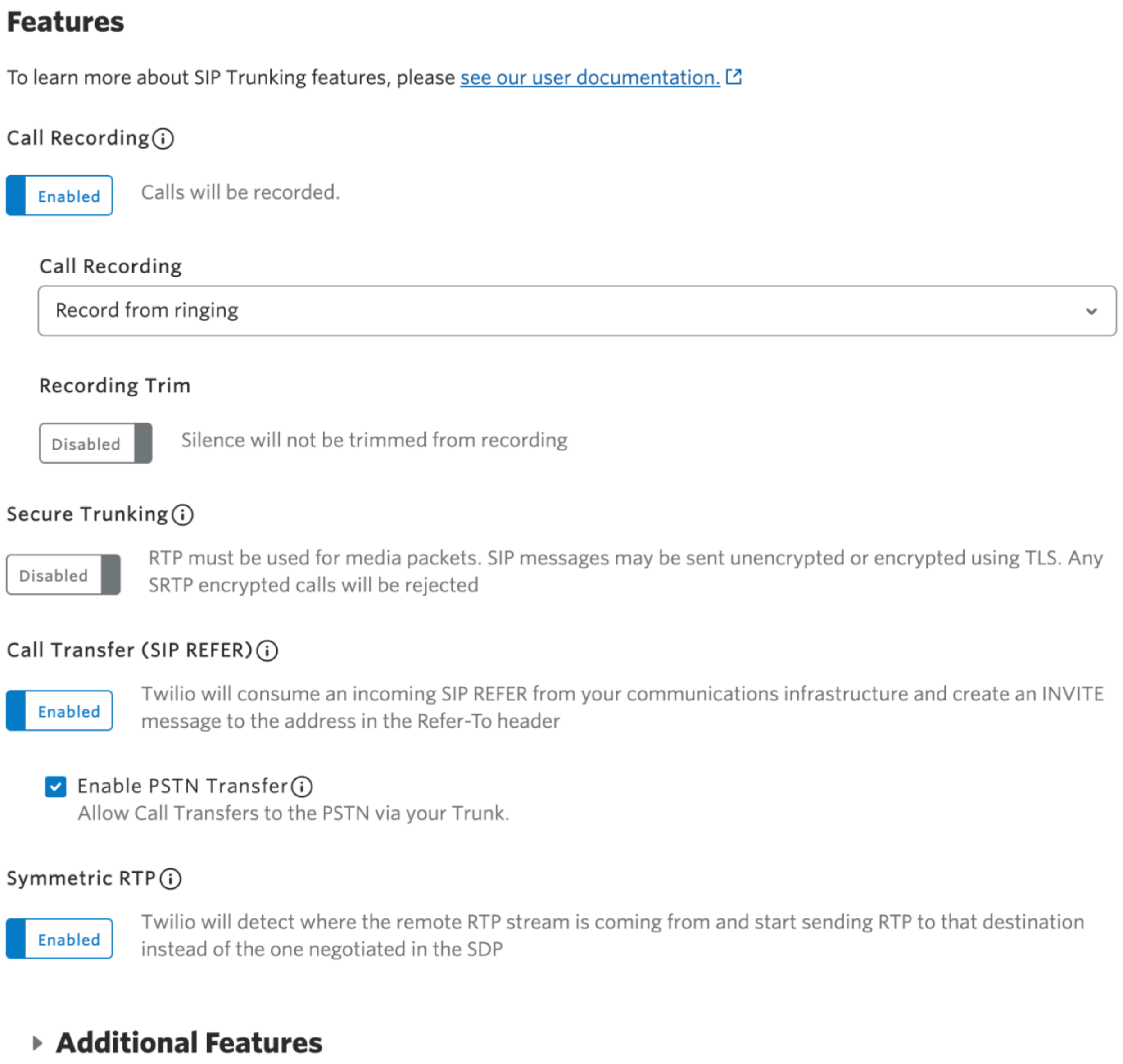

Create A New SIP Trunk

Name your new SIP Trunk, then configure it in the following steps.

FRIENDLY NAME

Under the **General Settings** you can enable different features as desired.

Note: Here is where you can enable the use of TLS & SRTP on your Trunk, learn more here.



Features

To learn more about SIP Trunking features, please see our user documentation.

Call Recording ⓘ

Enabled — Calls will be recorded.

Call Recording

Record from ringing

Recording Trim

Disabled — Silence will not be trimmed from recording

Secure Trunking ⓘ

Disabled — RTP must be used for media packets. SIP messages may be sent unencrypted or encrypted using TLS. Any SRTP encrypted calls will be rejected

Call Transfer (SIP REFER) ⓘ

Enabled — Twilio will consume an incoming SIP REFER from your communications infrastructure and create an INVITE message to the address in the Refer-To header

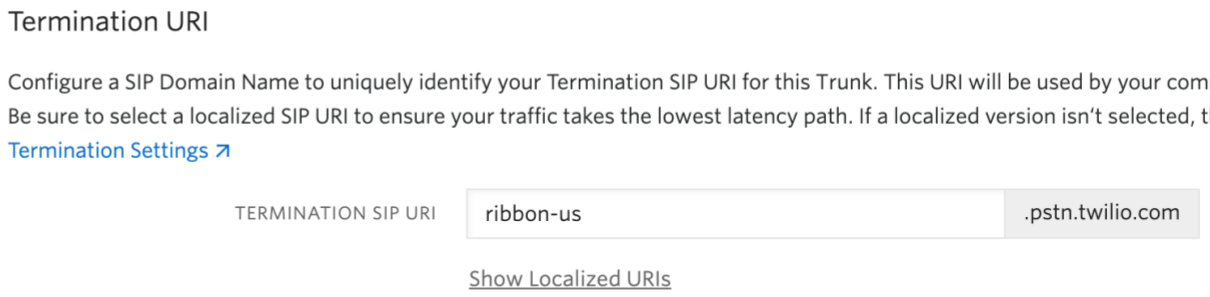
☑ Enable PSTN Transfer ⓘ
Allow Call Transfers to the PSTN via your Trunk.

Symmetric RTP ⓘ

Enabled — Twilio will detect where the remote RTP stream is coming from and start sending RTP to that destination instead of the one negotiated in the SDP

▸ **Additional Features**

In the **Termination** section, select a Termination SIP URI.

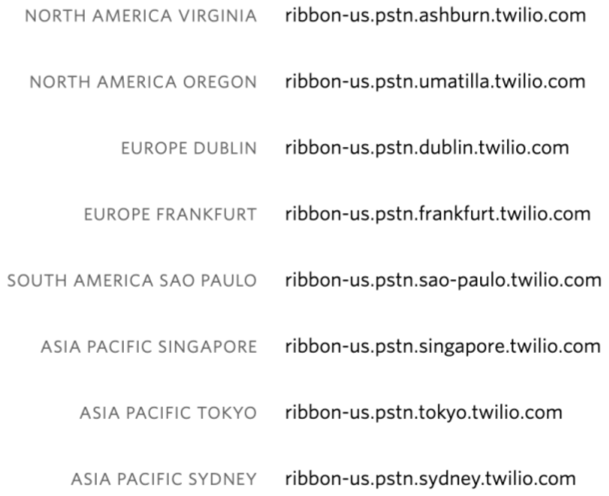


Termination URI

Configure a SIP Domain Name to uniquely identify your Termination SIP URI for this Trunk. This URI will be used by your communications infrastructure to direct SIP traffic towards Twilio. Be sure to select a localized SIP URI to ensure your traffic takes the lowest latency path. If a localized version isn't selected, then your traffic will be sent to US1. Learn more about Termination Settings ↗

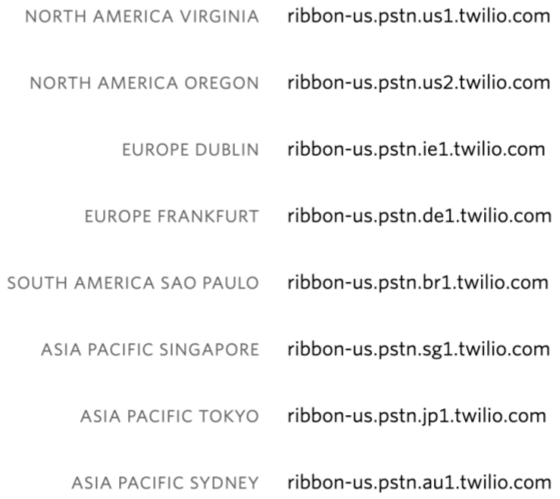
TERMINATION SIP URI: ribbon-us .pstn.twilio.com

Click on "Show localized URI's" and copy and paste this information as you will use this on your SBC to configure your Trunk.



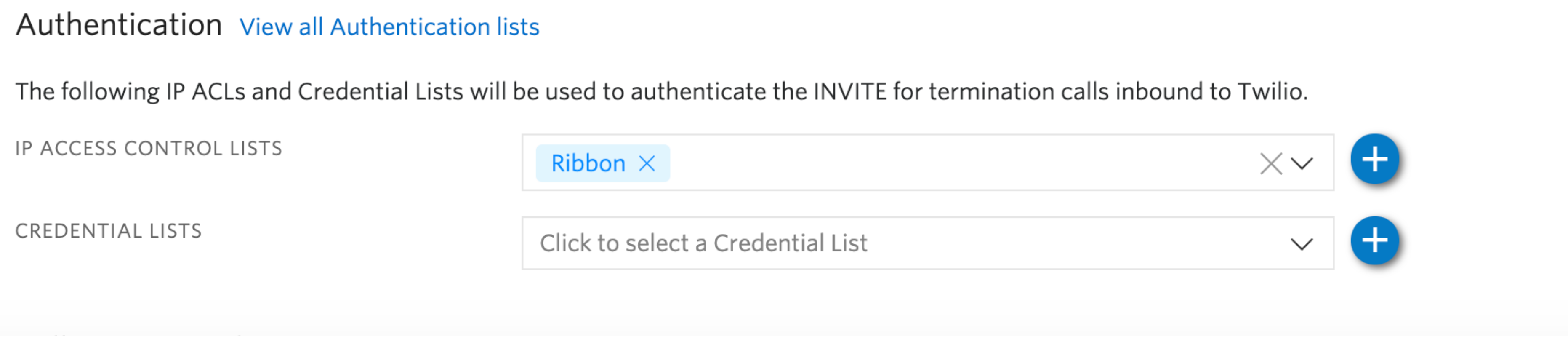
NORTH AMERICA VIRGINIA	ribbon-us.pstn.ashburn.twilio.com
NORTH AMERICA OREGON	ribbon-us.pstn.umatilla.twilio.com
EUROPE DUBLIN	ribbon-us.pstn.dublin.twilio.com
EUROPE FRANKFURT	ribbon-us.pstn.frankfurt.twilio.com
SOUTH AMERICA SAO PAULO	ribbon-us.pstn.sao-paulo.twilio.com
ASIA PACIFIC SINGAPORE	ribbon-us.pstn.singapore.twilio.com
ASIA PACIFIC TOKYO	ribbon-us.pstn.tokyo.twilio.com
ASIA PACIFIC SYDNEY	ribbon-us.pstn.sydney.twilio.com

or



NORTH AMERICA VIRGINIA	ribbon-us.pstn.us1.twilio.com
NORTH AMERICA OREGON	ribbon-us.pstn.us2.twilio.com
EUROPE DUBLIN	ribbon-us.pstn.ie1.twilio.com
EUROPE FRANKFURT	ribbon-us.pstn.de1.twilio.com
SOUTH AMERICA SAO PAULO	ribbon-us.pstn.br1.twilio.com
ASIA PACIFIC SINGAPORE	ribbon-us.pstn.sg1.twilio.com
ASIA PACIFIC TOKYO	ribbon-us.pstn.jp1.twilio.com
ASIA PACIFIC SYDNEY	ribbon-us.pstn.au1.twilio.com

Assign the IP ACL ("Ribbon") that you created in the previous step.



Authentication View all Authentication lists

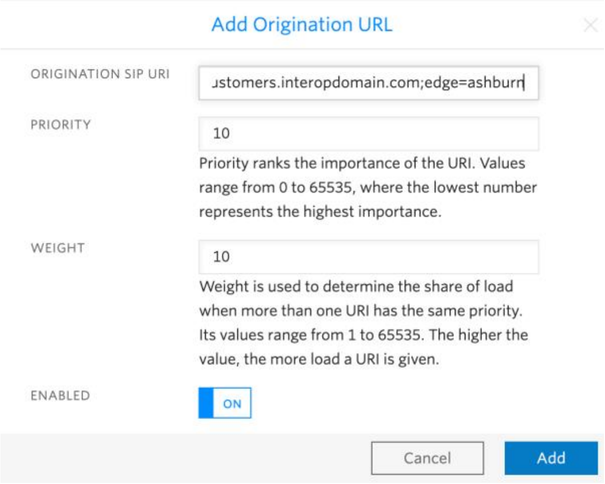
The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

IP ACCESS CONTROL LISTS: Ribbon

CREDENTIAL LISTS: Click to select a Credential List

In the **Origination** section, we'll need to add Origination URI's to route traffic towards your Ribbon SBC. The recommended practice is to configure redundant mesh per geographic region (in this context a region is one of North America, Europe, etc). In this case, we configure two Origination URIs, each egressing from a different Twilio Edge.

Click on ‘Add New Origination URI’, we'll depict the configuration for North America:

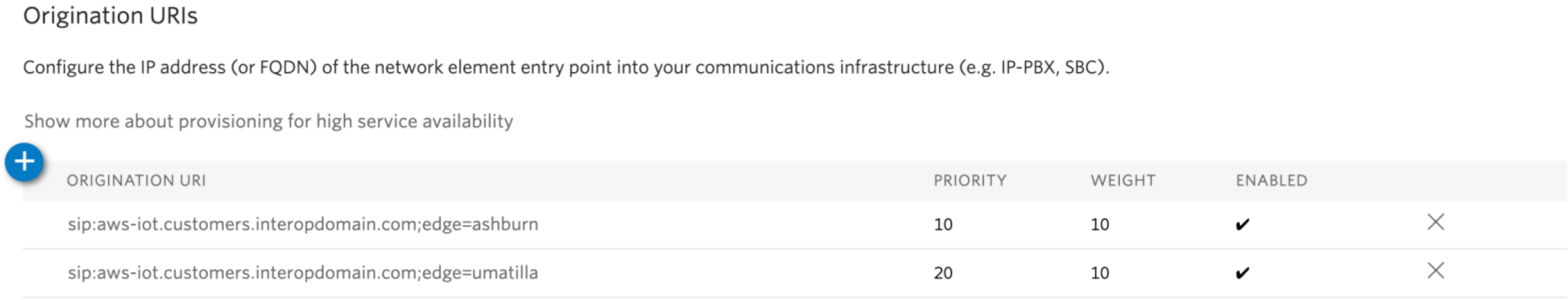


Add Origination URL

ORIGINATION SIP URI	ustomers.interopdomain.com;edge=ashburn
PRIORITY	10 Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.
WEIGHT	10 Weight is used to determine the share of load when more than one URI has the same priority. Its values range from 1 to 65535. The higher the value, the more load a URI is given.
ENABLED	ON

Note: If you enabled “Secure Trunking”, then you need to include the “transport=tls” parameter in your Origination URIs, learn more here.

Continue to add the other Origination URIs, so you have the following configuration:



Origination URIs

Configure the IP address (or FQDN) of the network element entry point into your communications infrastructure (e.g. IP-PBX, SBC).

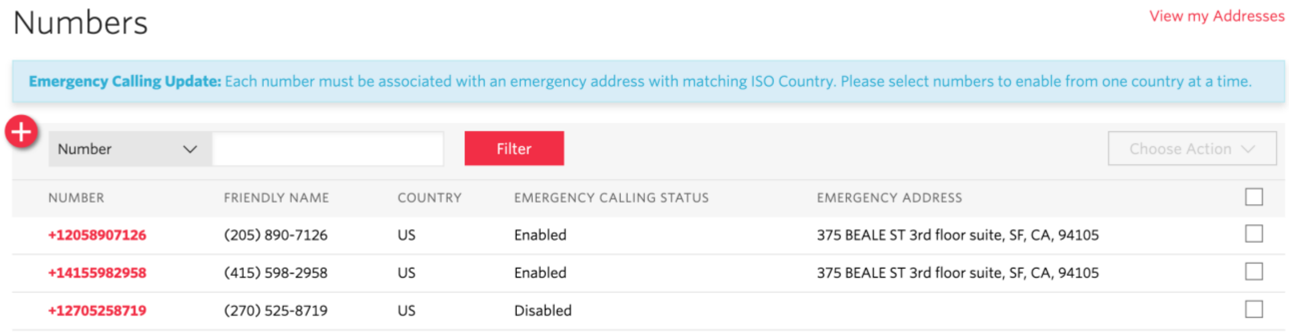
Show more about provisioning for high service availability

ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
sip:aws-iot.customers.interopdomain.com;edge=ashburn	10	10	✔	×
sip:aws-iot.customers.interopdomain.com;edge=umatilla	20	10	✔	×

In this example, Origination traffic is first routed via Twilio’s Ashburn edge, if that fails then we'll route from Twilio’s Umatilla edge.

3. Associate your Twilio Phone Numbers on your Trunk

In the **Numbers** section of your Trunk, add the Phone Numbers that you want to associate with each Trunk. Remember to associate the Numbers from a given country in the right Trunk. For example, associate US & Canada Numbers with the North American Trunk and European Numbers with the European Trunk etc.



Numbers

View my Addresses

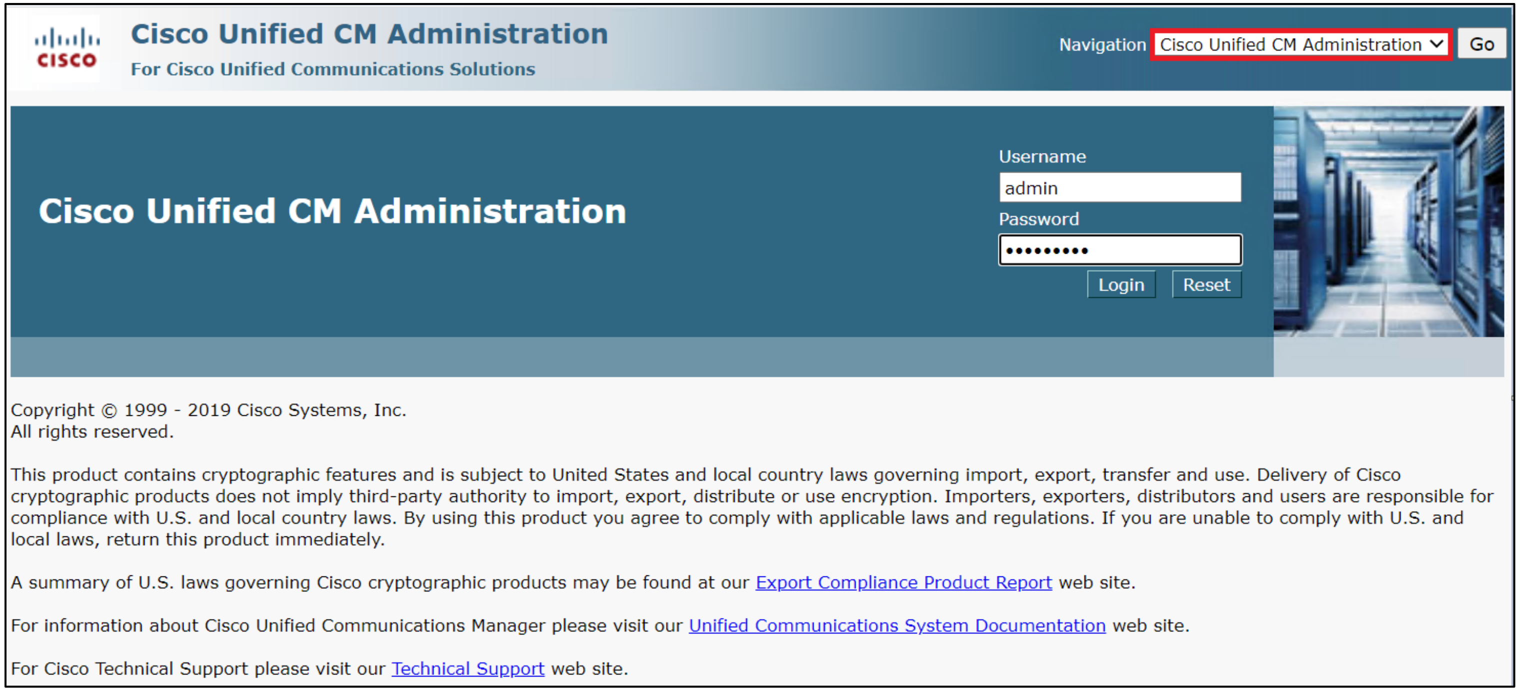
Emergency Calling Update: Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	□
+12058907126	(205) 890-7126	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	□
+14155982958	(415) 598-2958	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	□
+12705258719	(270) 525-8719	US	Disabled		□

CUCM Configuration

Accessing CUCM (Cisco Unified CM Administration)

1. Open browse and enter the CUCM IP Address.
2. Select **Cisco Unified CM Administration** from the Navigation drop-down.
3. Provide the credentials and click **Login**.



cisco
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
Cisco Unified CM Administration
Username
admin
Password
•••••••••
Login
Reset

Copyright © 1999 - 2019 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

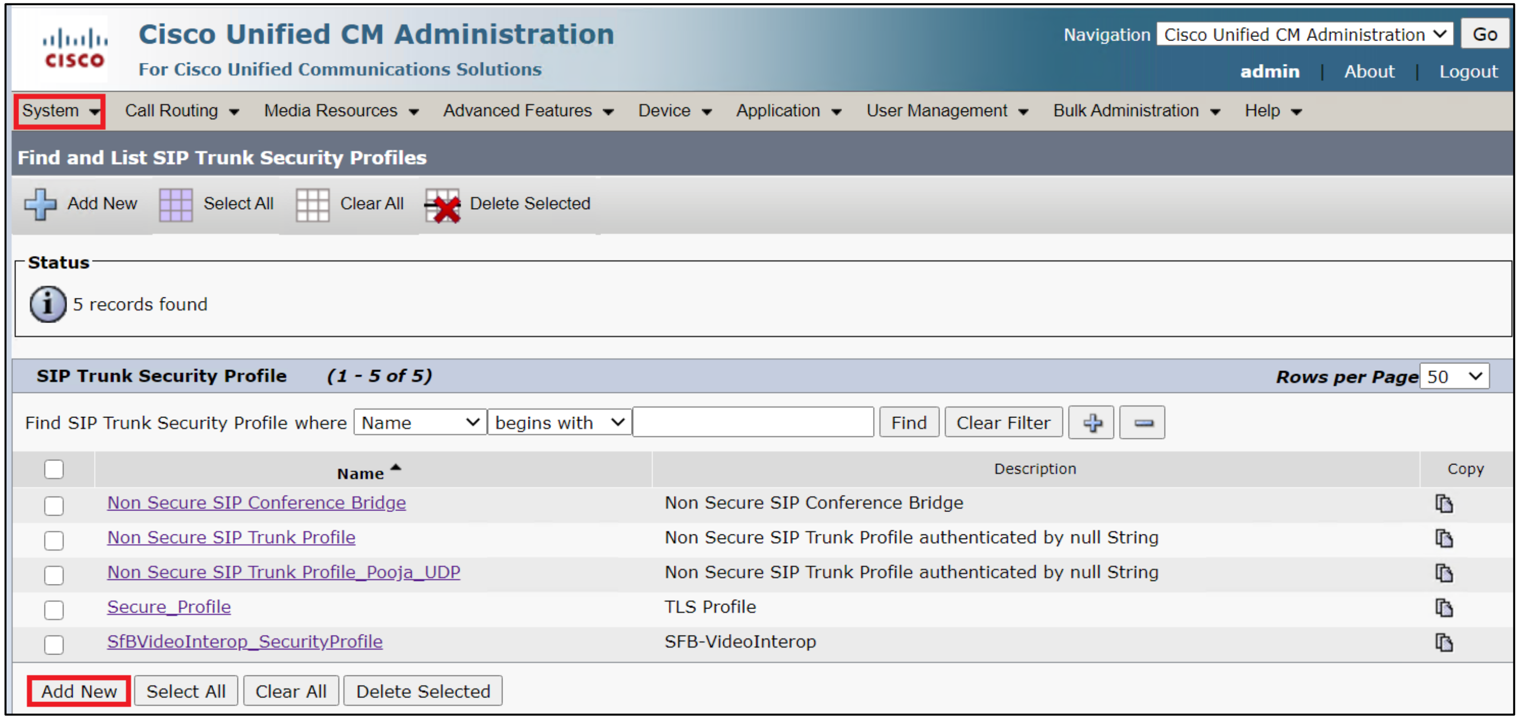
For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

Configure SIP Trunk Security Profile

Unified Communications Manager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings.

- From Cisco Unified CM Administration, navigate to **System > Security > SIP Trunk Security Profile.**
- Click **Add New**.



Find and List SIP Trunk Security Profiles

Status

5 records found

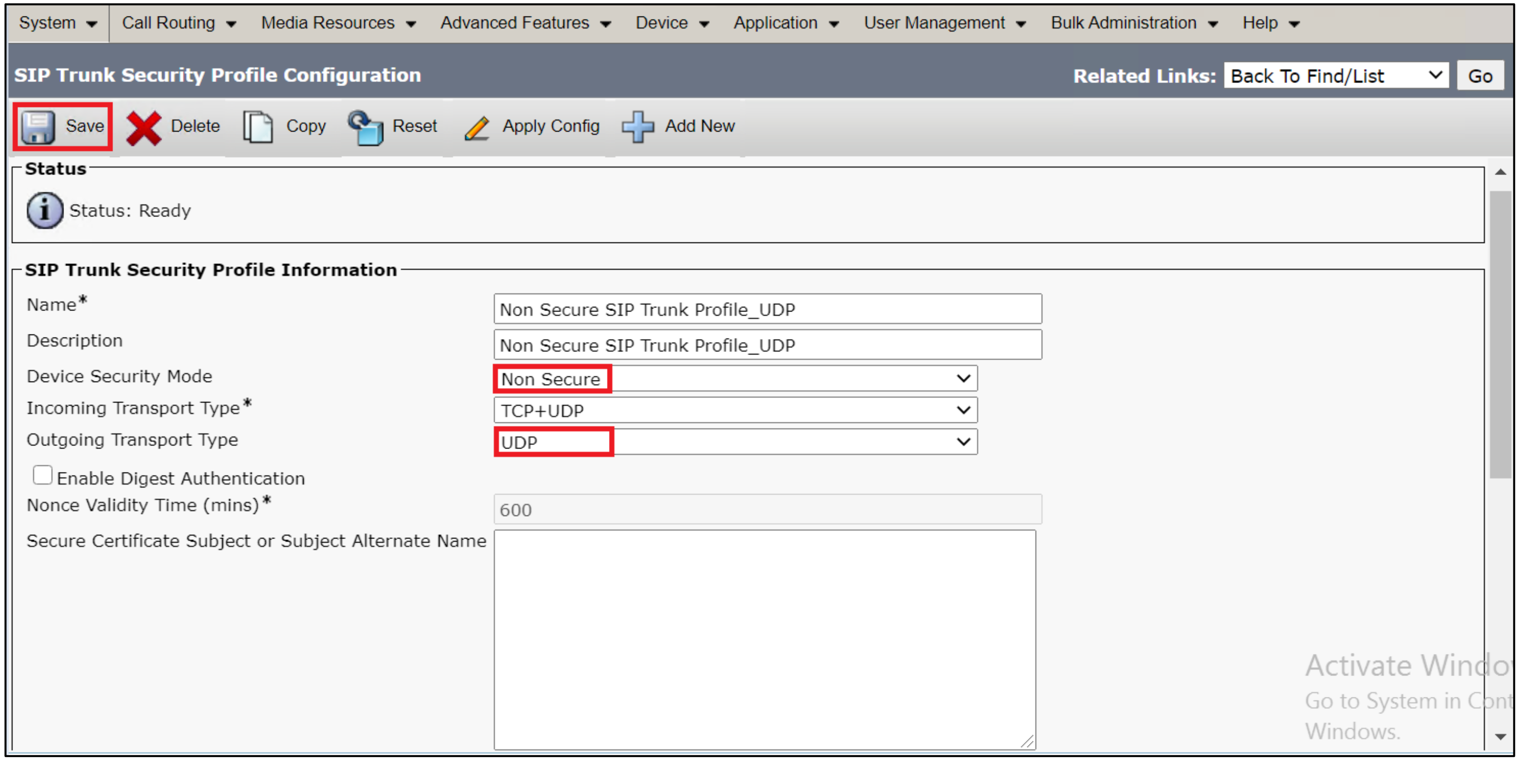
SIP Trunk Security Profile ***(1 - 5 of 5)*** ***Rows per Page*** 50

Find SIP Trunk Security Profile where Name begins with

□	Name	Description	Copy
□	Non Secure SIP Conference Bridge	Non Secure SIP Conference Bridge	
□	Non Secure SIP Trunk Profile	Non Secure SIP Trunk Profile authenticated by null String	
□	Non Secure SIP Trunk Profile_Pooja_UDP	Non Secure SIP Trunk Profile authenticated by null String	
□	Secure_Profile	TLS Profile	
□	SfBVideoInterop_SecurityProfile	SFB-VideoInterop	

- Provide the desired Name and Description.
- Choose **Non Secure** from Device Security Mode.
  - No security features except image authentication apply. A TCP or UDP connection opens to Unified Communications Manager.

- From Incoming Transport Type, select **TCP+UDP**.
  - When Device Security Mode is Non Secure, TCP+UDP specifies the transport type.
- Select Outgoing Transport Type as **UDP**.
- Click **Save**.



SIP Trunk Security Profile Configuration

Status

Status: Ready

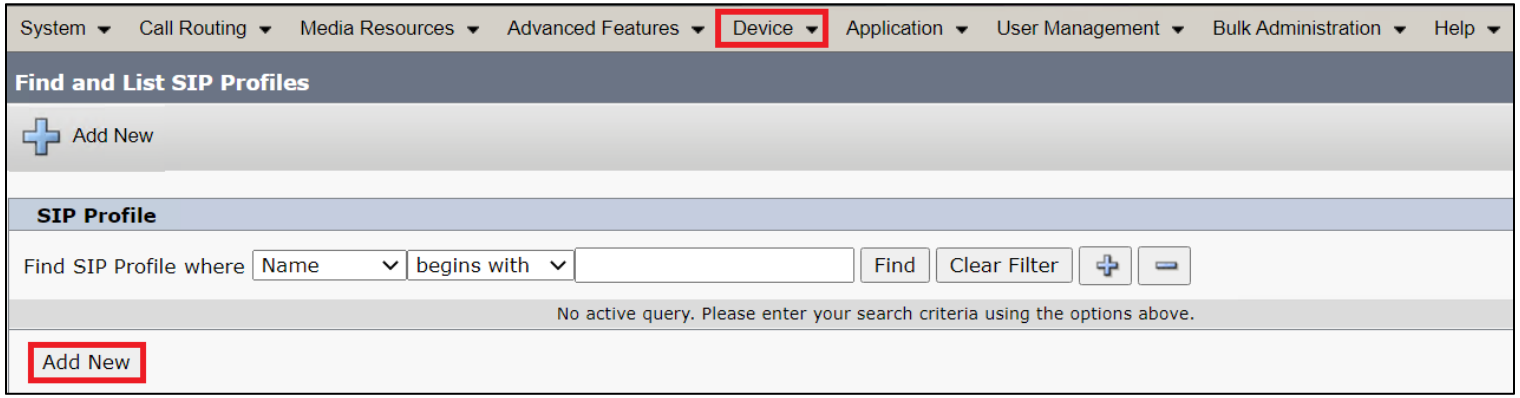
SIP Trunk Security Profile Information

Name*	Non Secure SIP Trunk Profile_UDP
Description	Non Secure SIP Trunk Profile_UDP
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	UDP
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	

Configure SIP Profiles

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that you cannot delete or change.

- From Cisco Unified CM Administration, navigate to **Device > Device Settings > SIP Profile.**
- Click **Add New**.



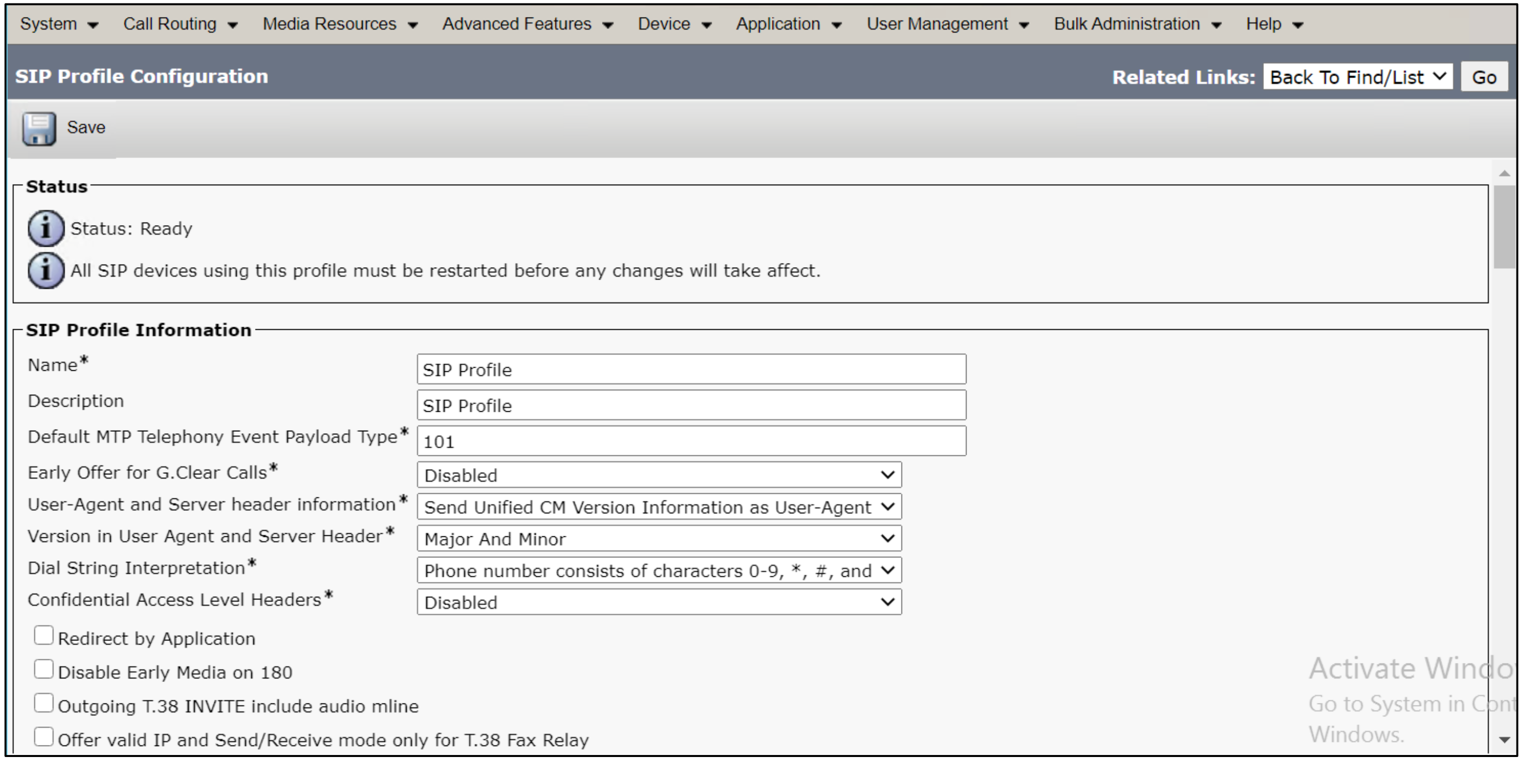
Find and List SIP Profiles

SIP Profile

Find SIP Profile where Name begins with

No active query. Please enter your search criteria using the options above.

- Enter a name to identify the SIP profile.
- Provide description to identify the purpose of the SIP profile.



SIP Profile Configuration

Status

Status: Ready

All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name*	SIP Profile
Description	SIP Profile
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
User-Agent and Server header information*	Send Unified CM Version Information as User-Agent
Version in User Agent and Server Header*	Major And Minor
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, and
Confidential Access Level Headers*	Disabled

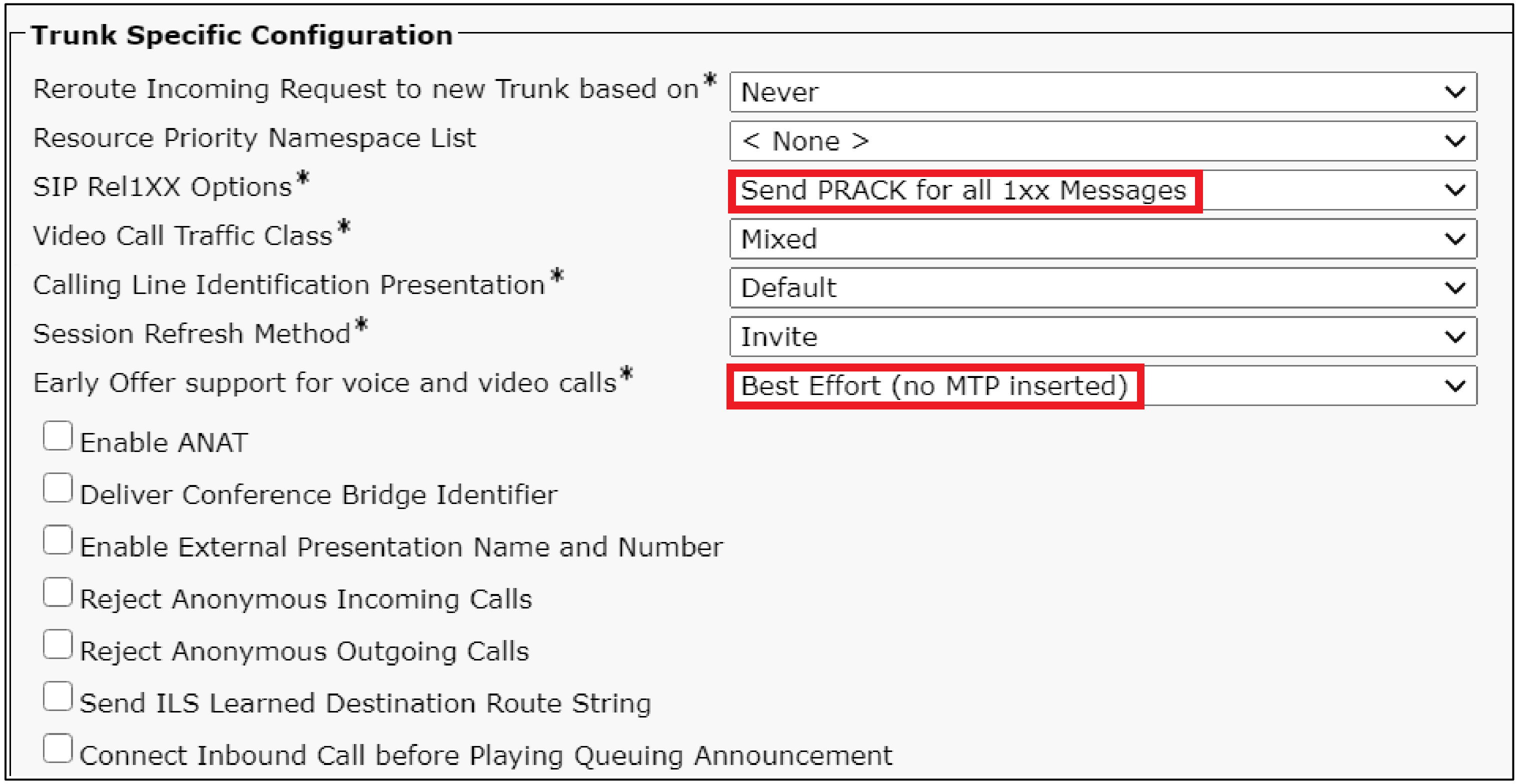
□ Redirect by Application

□ Disable Early Media on 180

□ Outgoing T.38 INVITE include audio mline

□ Offer valid IP and Send/Receive mode only for T.38 Fax Relay

- From SIP Rel1XX Options drop-down, choose **Send PRACK for all 1xx Messages**.
- From Early Offer support for voice and video calls drop-down, choose Best Effort (no MTP inserted).
  - Provide Early Offer for the outbound call only when caller side's media port, IP and codec information is available.
  - Provide Delayed Offer for the outbound call when caller side's media port, IP and codec information is not available. No MTP is inserted to provide Early Offer in this case.



Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*	Never
Resource Priority Namespace List	< None >
SIP Rel1XX Options*	Send PRACK for all 1xx Messages
Video Call Traffic Class*	Mixed
Calling Line Identification Presentation*	Default
Session Refresh Method*	Invite
Early Offer support for voice and video calls*	Best Effort (no MTP inserted)

□ Enable ANAT

□ Deliver Conference Bridge Identifier

□ Enable External Presentation Name and Number

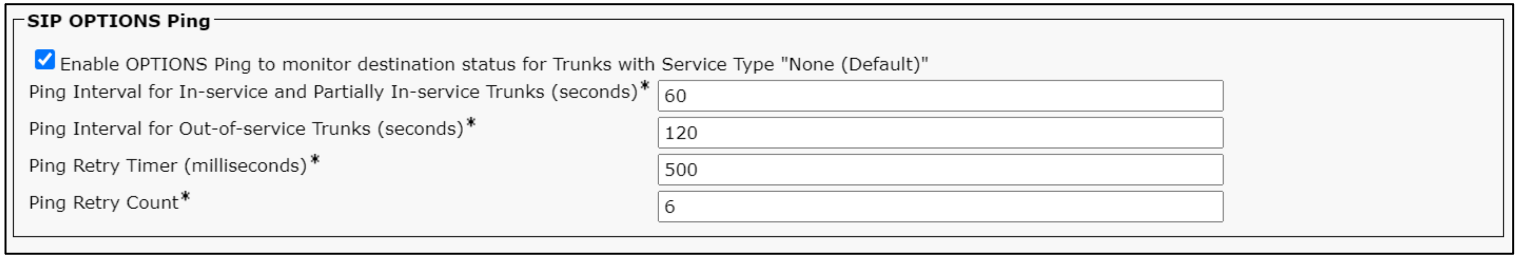
□ Reject Anonymous Incoming Calls

□ Reject Anonymous Outgoing Calls

□ Send ILS Learned Destination Route String

□ Connect Inbound Call before Playing Queuing Announcement

- Enable **SIP OPTIONS Ping**.
  - SIP OPTIONS are requests to the configured destination address on the SIP trunk.
- Click **Save**.



SIP OPTIONS Ping

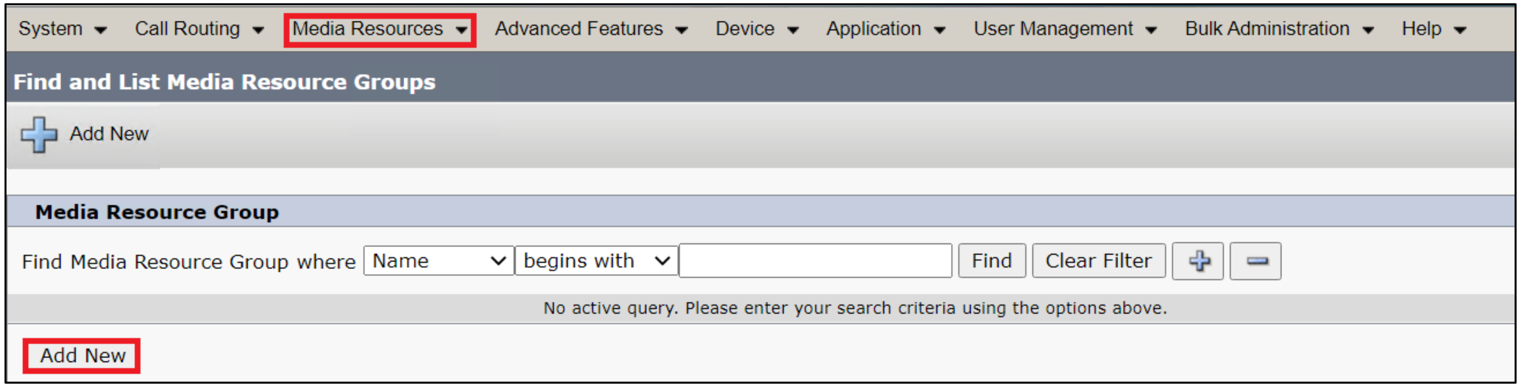
☑ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)*	60
Ping Interval for Out-of-service Trunks (seconds)*	120
Ping Retry Timer (milliseconds)*	500
Ping Retry Count*	6

Configure Media Resource Group

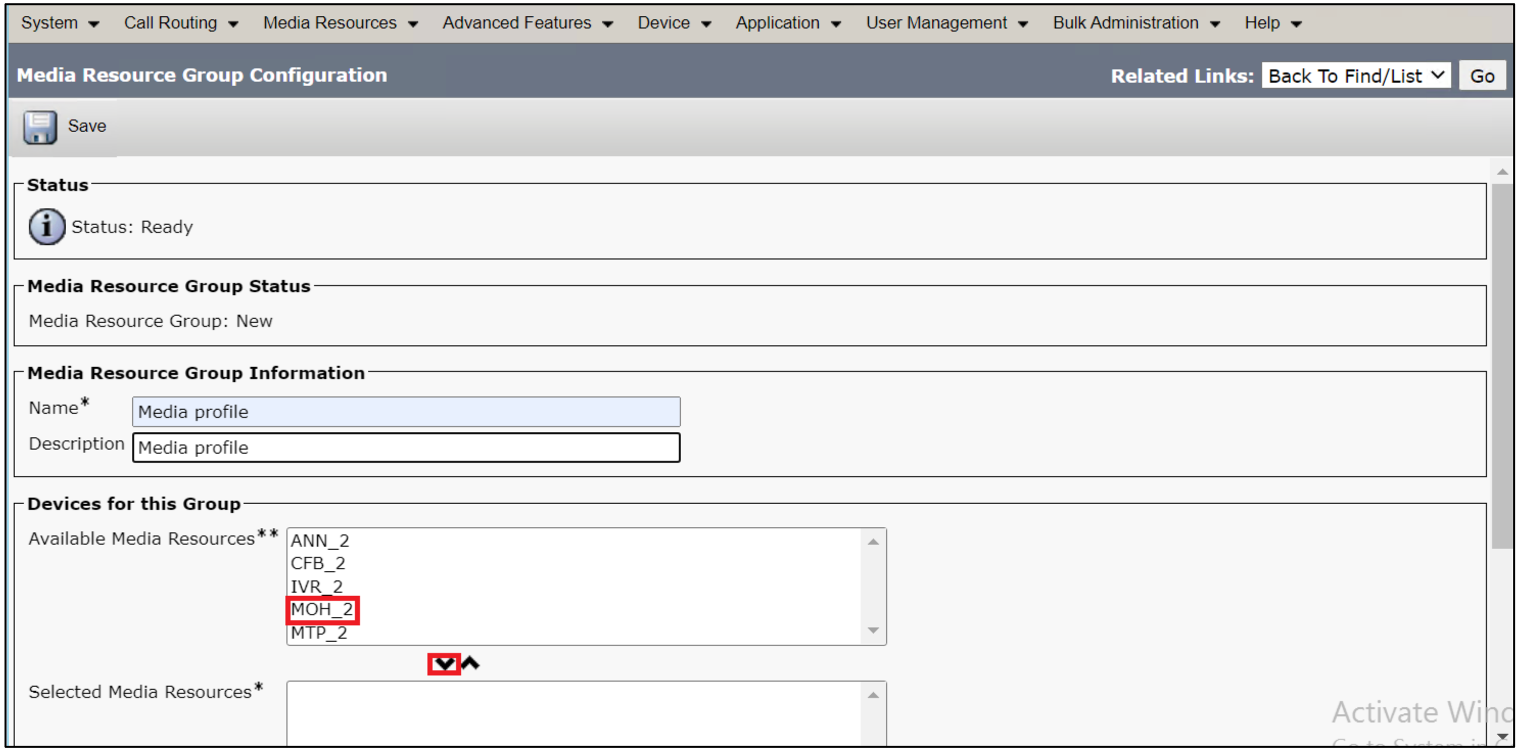
Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified Communications Managers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

- From Cisco Unified CM Administration, navigate to **Media Resources > Media Resource Group.**
- Click **Add New**.



No active query. Please enter your search criteria using the options above.

- Enter a unique name in this required field to identify the media resource group.
- Enter a description for the media resource group.
- To add a media resource for this media resource group, choose one (MoH_2 in this case) from the available Media Resources list and click the down arrow. After a media resource is added, its name moves to the Selected Media Resources pane.



Media Resource Group Configuration

Related Links: Back To Find/List Go

Save

Status

Status: Ready

Media Resource Group Status

Media Resource Group: New

Media Resource Group Information

Name* Media profile

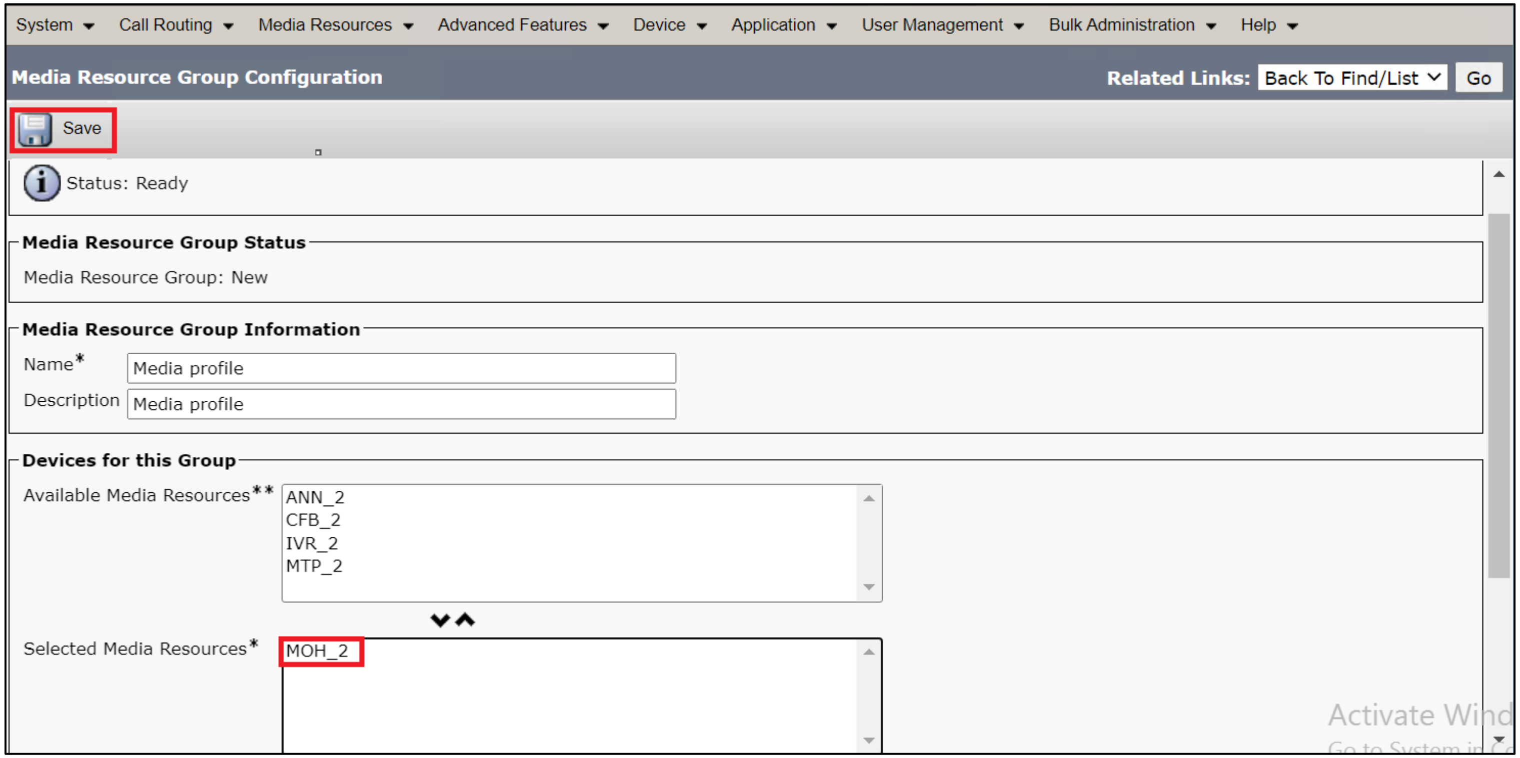
Description Media profile

Devices for this Group

Available Media Resources** ANN_2
CFB_2
IVR_2
MOH_2
MTP_2

Selected Media Resources*

- Click **Save**.



Media Resource Group Configuration

Status: Ready

Media Resource Group Status

Media Resource Group: New

Media Resource Group Information

Name* Media profile

Description Media profile

Devices for this Group

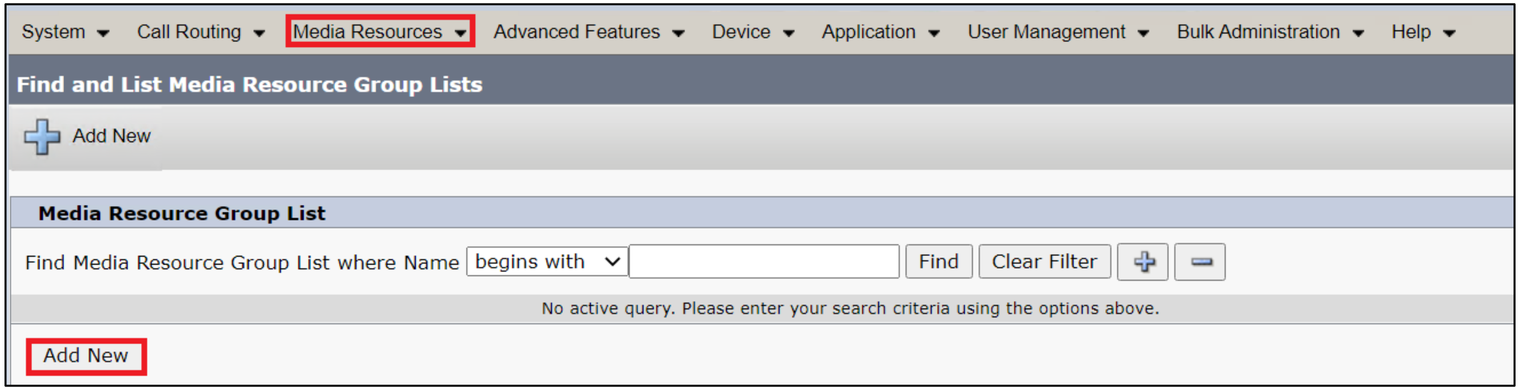
Available Media Resources** ANN_2, CFB_2, IVR_2, MTP_2

Selected Media Resources* MOH_2

Configure Media Resource Group List

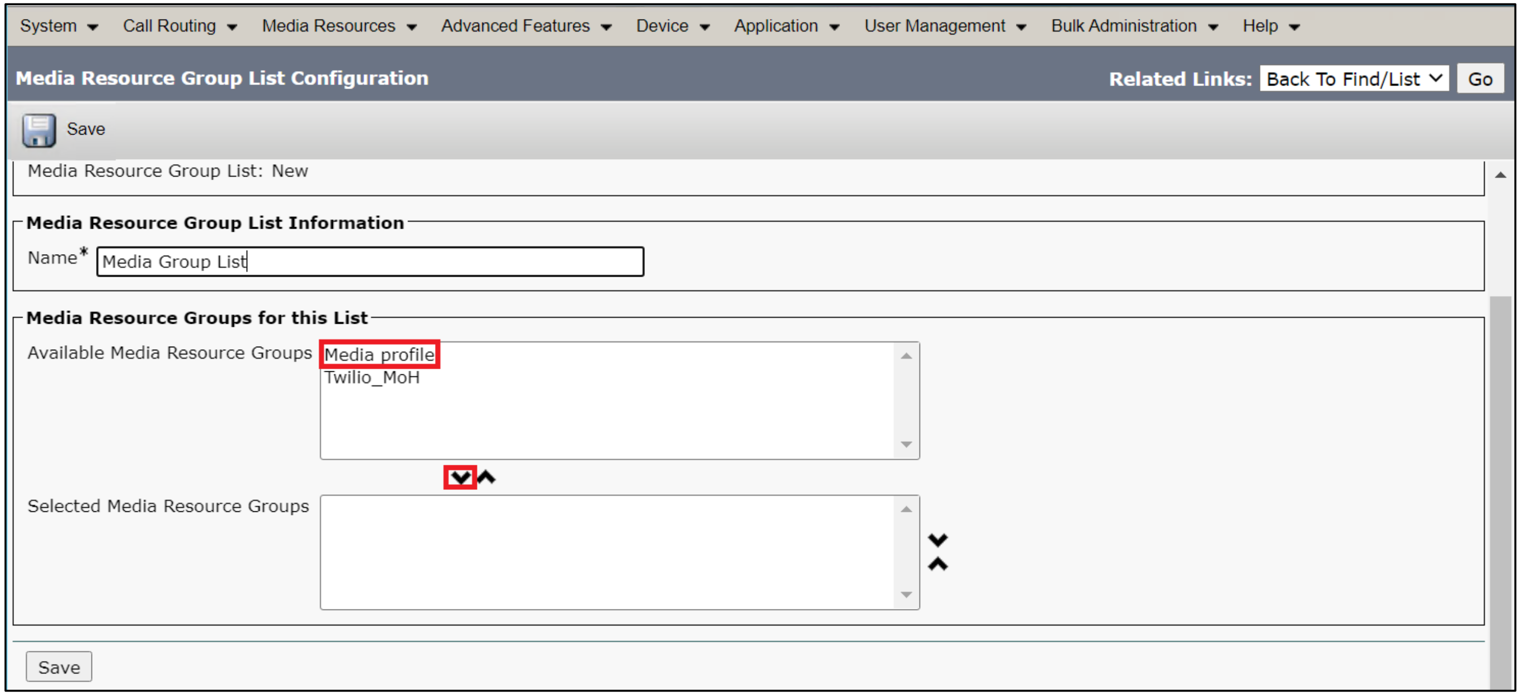
A Media Resource Group List provides a prioritized grouping of media resource groups. An application selects the required media resource, such as a music on hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

- From Cisco Unified CM Administration, navigate to **Media Resources > Media Resource Group List** menu path to configure media resource group lists.
- Click **Add New**.



No active query. Please enter your search criteria using the options above.

- Enter a unique name in this required field to identify the Media Resource Group List.
- Choose the Media Resource Group created in the previous step from the Available Media Resource Groups list and click the down arrow that is located between the two panes. After a media resource group is added, its name moves to the Selected Media Resource Groups pane.



Media Resource Group List Configuration

Media Resource Group List: New

Media Resource Group List Information

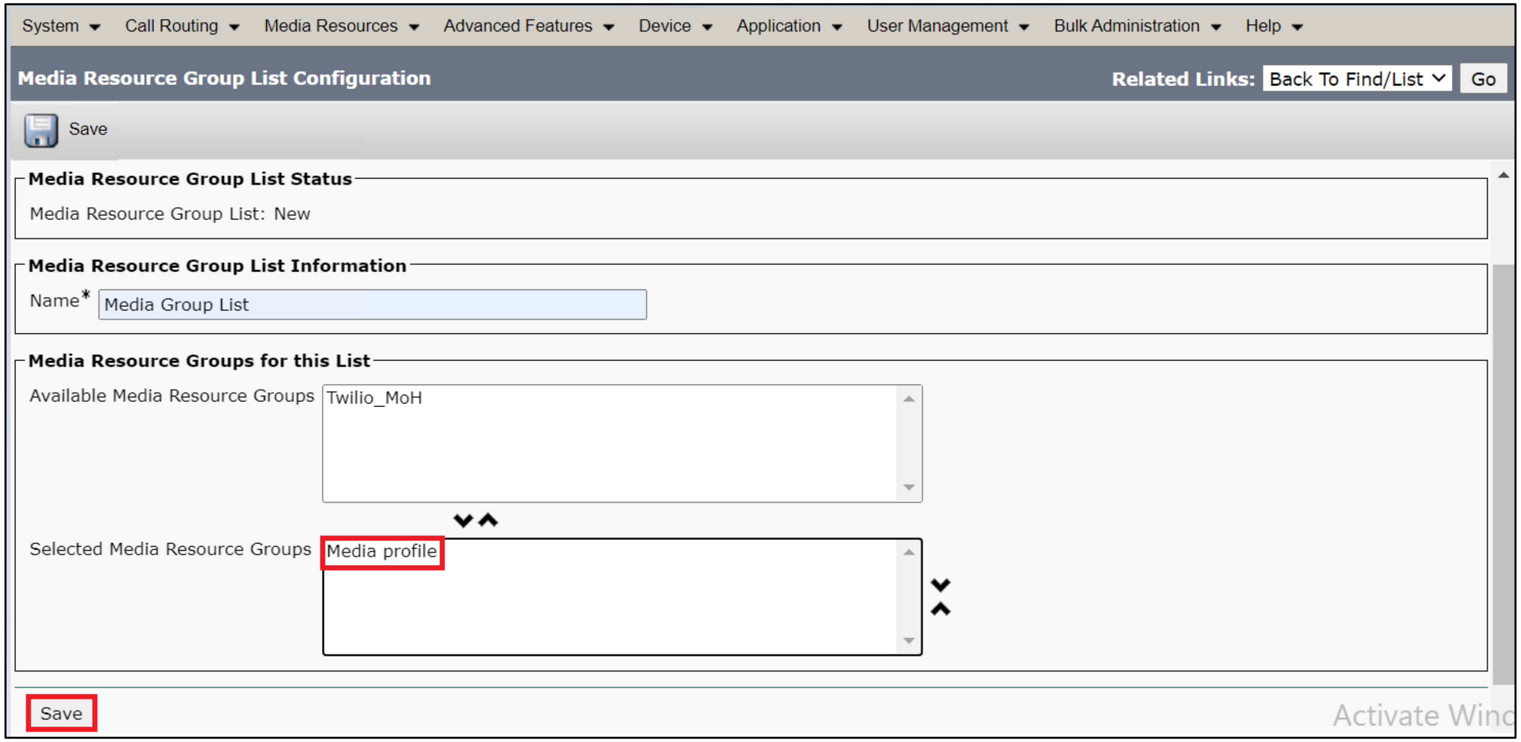
Name* Media Group List

Media Resource Groups for this List

Available Media Resource Groups: Media profile, Twilio_MoH

Selected Media Resource Groups

- Click **Save**.



Media Resource Group List Configuration

Media Resource Group List Status

Media Resource Group List: New

Media Resource Group List Information

Name* Media Group List

Media Resource Groups for this List

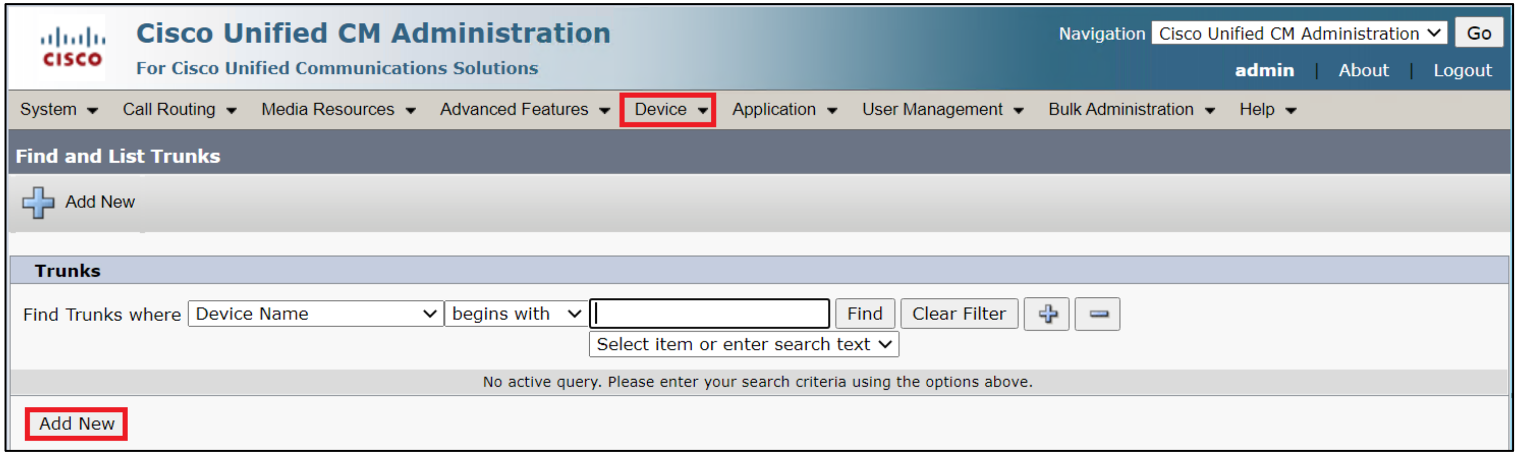
Available Media Resource Groups: Twilio_MoH

Selected Media Resource Groups: Media profile

Trunk Configuration

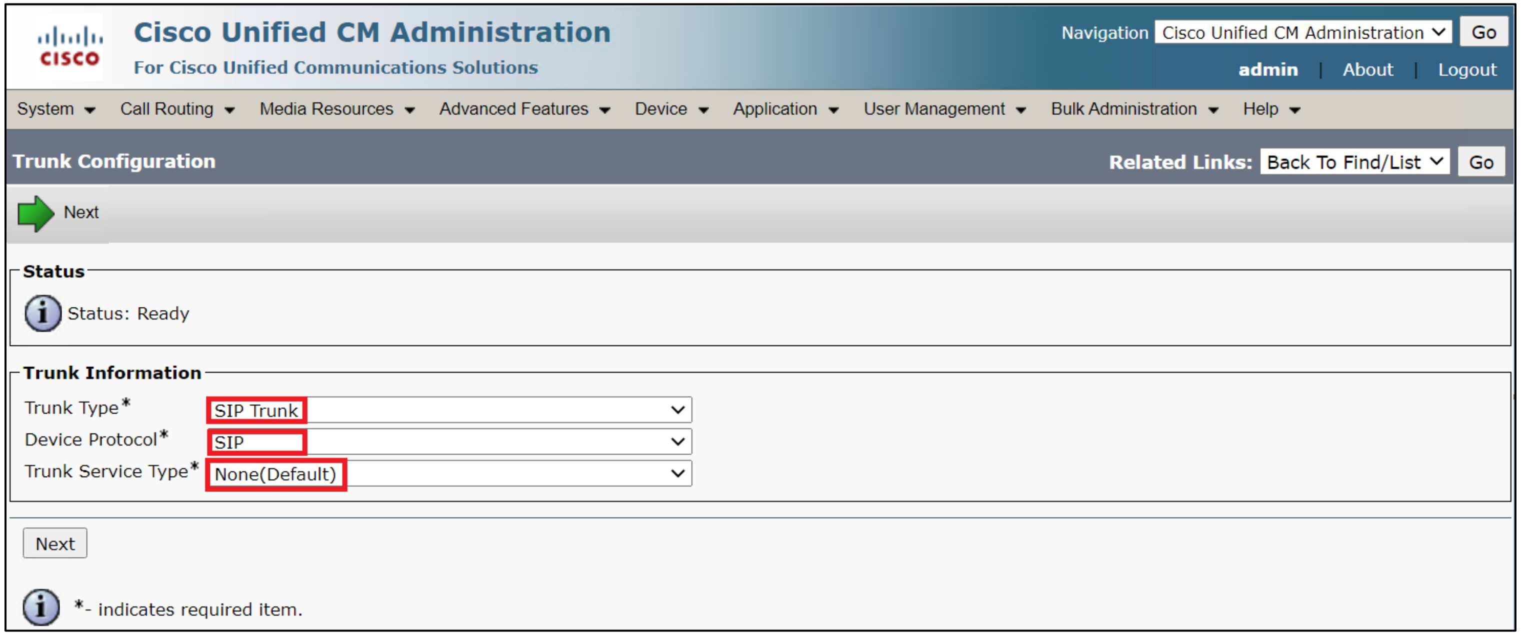
Use a trunk device to configure a logical route to a SIP network.

- From Cisco Unified CM Administration, choose **Device > Trunk.**
- Click **Add New**.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Find and List Trunks
Add New
Trunks
Find Trunks where Device Name begins with Find Clear Filter
Select item or enter search text
Add New

No active query. Please enter your search criteria using the options above.

- From the Trunk Type drop-down list, choose **SIP Trunk**.
- Choose **SIP** from Device Protocol drop-down.
- From Trunk Service Type, select the default value (None).
- Click **Next**.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | About | Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Related Links: Back To Find/List Go
Next

Trunk Configuration

Status

Status: Ready

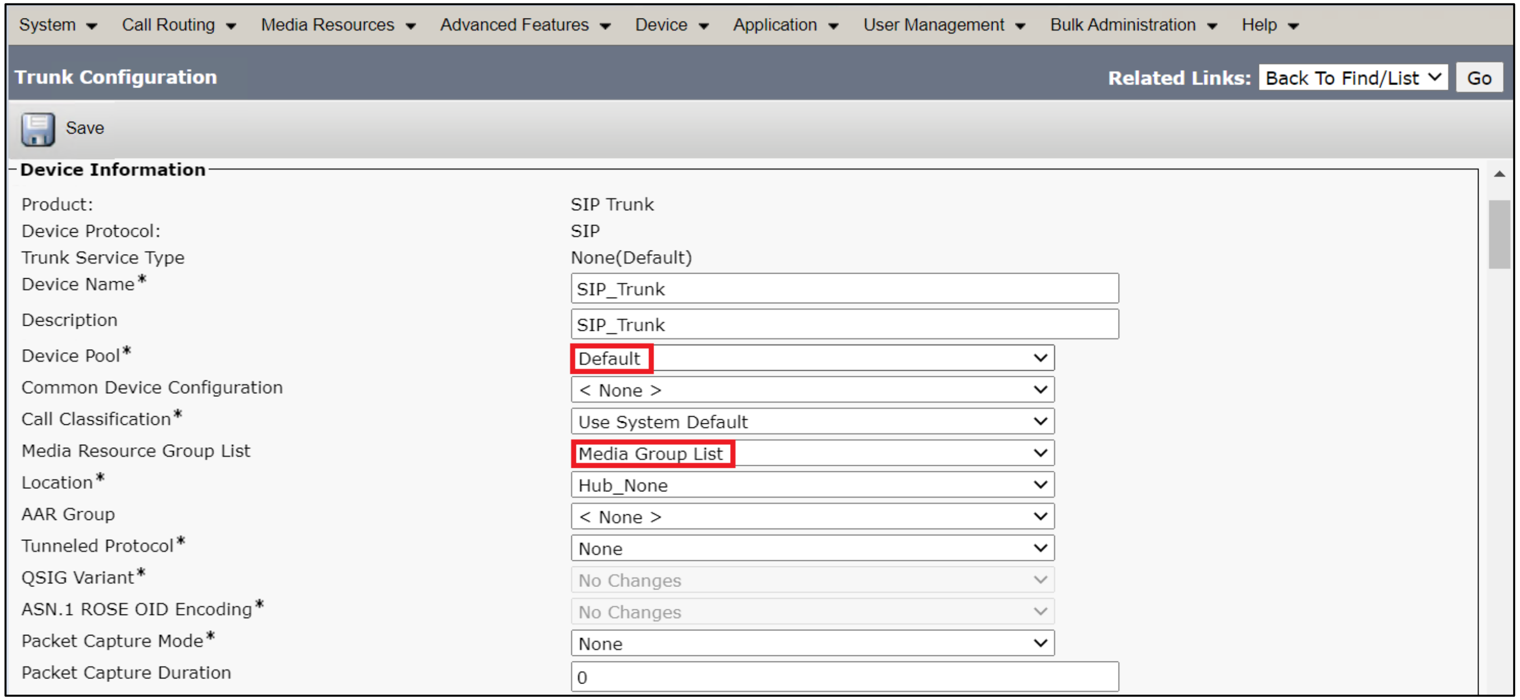
Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Next

*- indicates required item.

- Enter a unique identifier for the trunk.
- Enter a descriptive name for the trunk.
- Choose the Default Device Pool.
- Choose the Media Resource Group List created in the previous step.

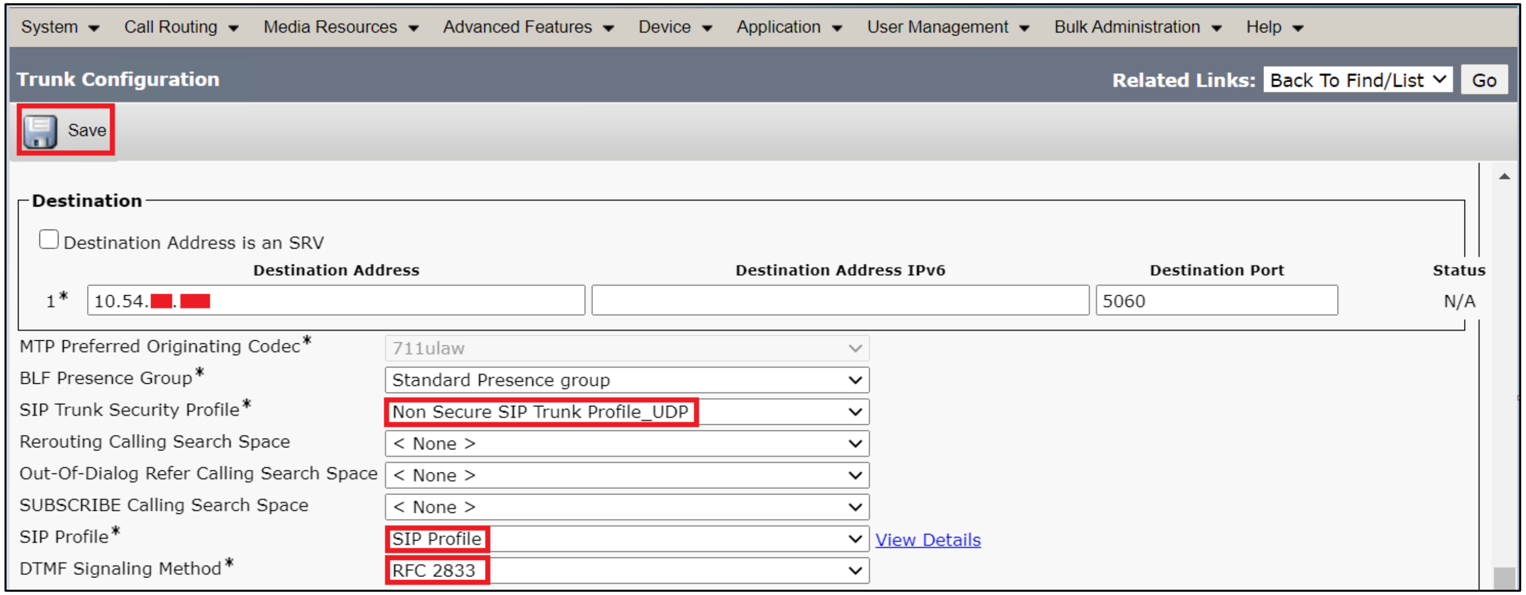


Trunk Configuration

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SIP_Trunk
Description	SIP_Trunk
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	Media Group List
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

- Provide the destination address.
  - The Destination Address represents the remote SIP peer with which this trunk will communicate.
  - SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.
- Choose the **SIP Trunk Security Profile** created to apply to the SIP trunk.
- Select the **SIP Profile** created from the list.
- Choose **RFC 2833** as DTMF Signaling Method.
- Click **Save**.



Trunk Configuration

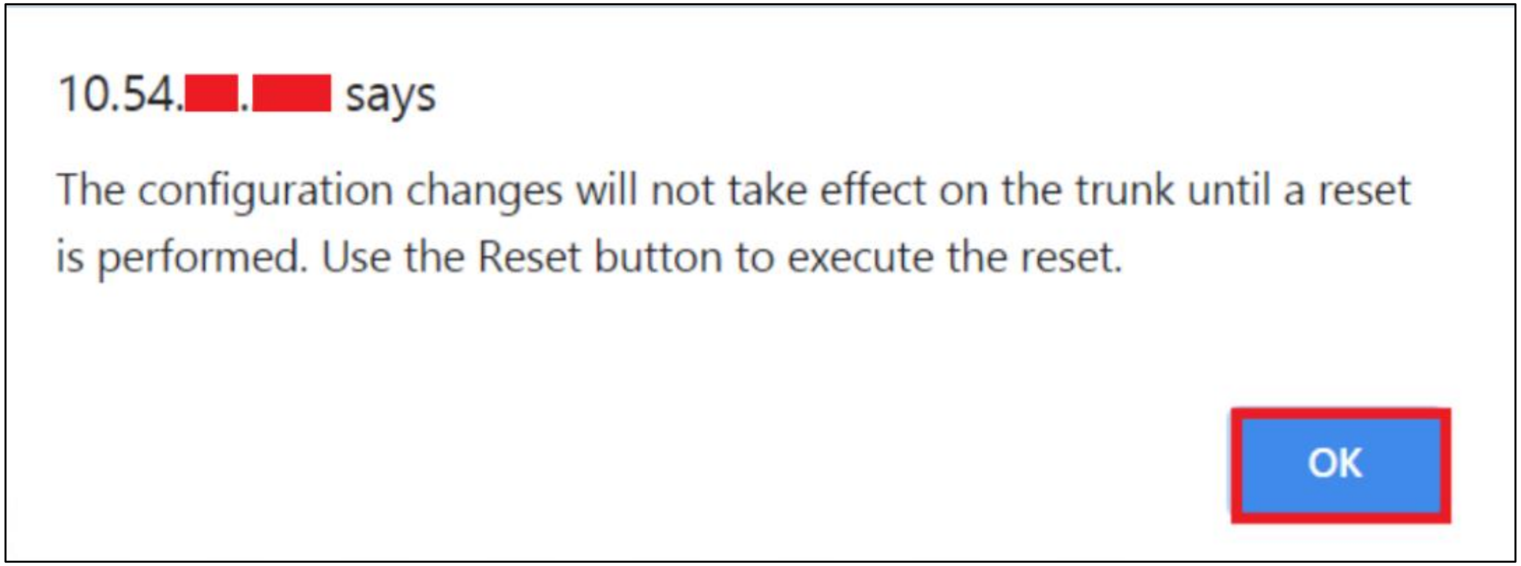
Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status
1*	10.54.[redacted].[redacted]		5060	N/A

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile_UDP
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	SIP Profile View Details
DTMF Signaling Method*	RFC 2833

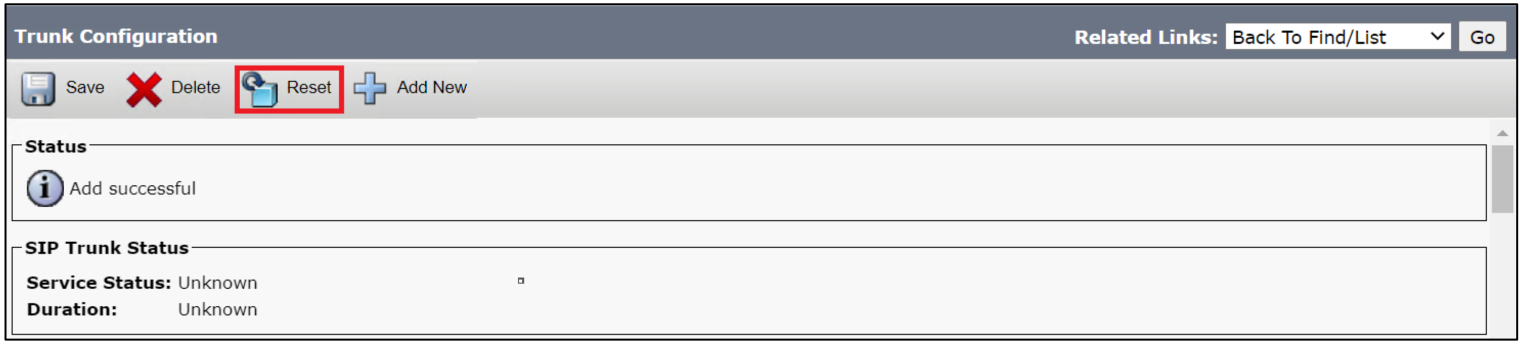
- Click **OK**.



10.54.[redacted].[redacted] says

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button to execute the reset.

- Click the **Reset** button.



Trunk Configuration

Related Links: Back To Find/List Go

Status

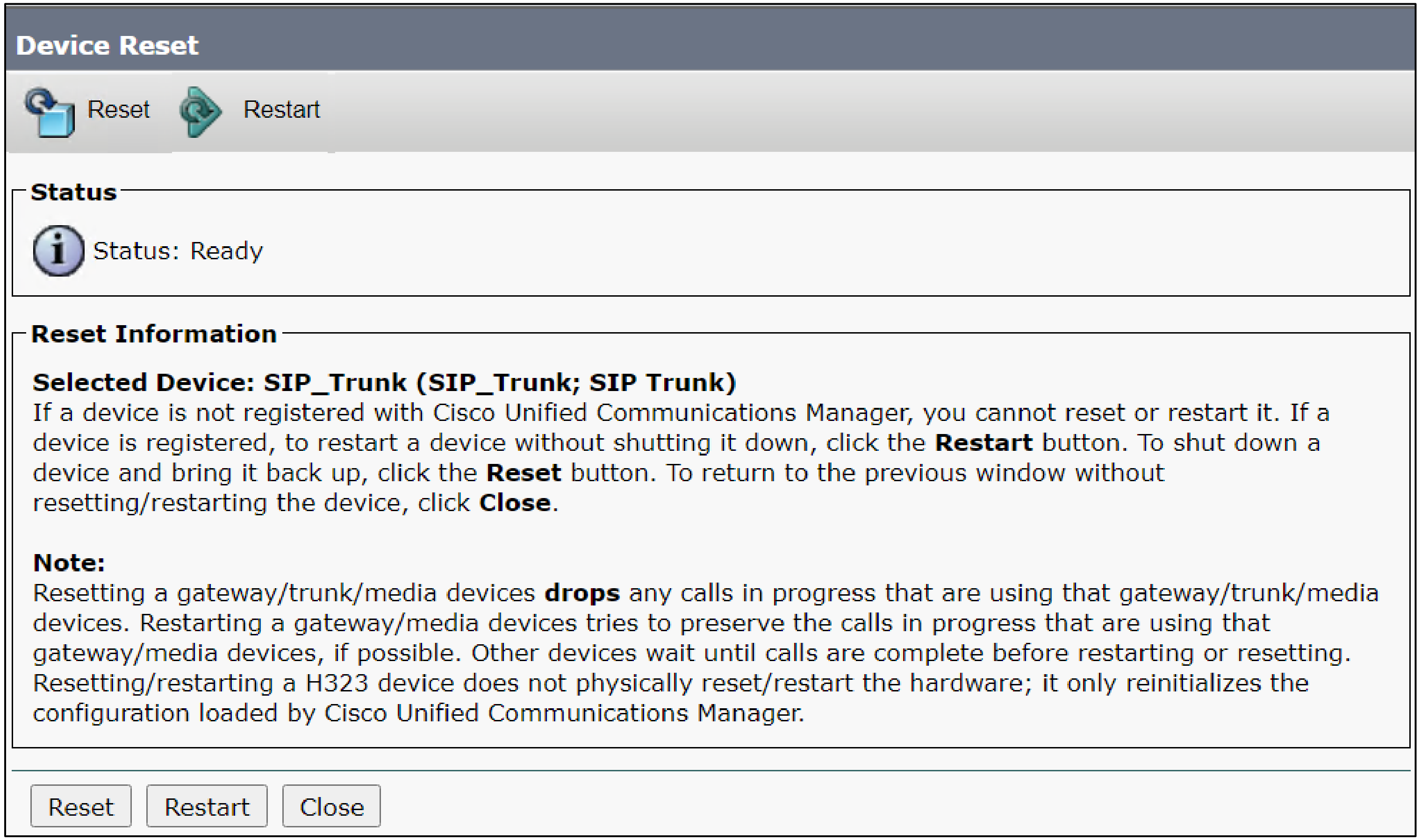
Add successful

SIP Trunk Status

Service Status: Unknown

Duration: Unknown

- Reset, Restart and Close the window. Refresh the SIP trunk page and wait until the Server status changes from Unknown to Full Service.



Status

Status: Ready

Reset Information

Selected Device: SIP_Trunk (SIP_Trunk; SIP Trunk)
If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To shut down a device and bring it back up, click the **Reset** button. To return to the previous window without resetting/restarting the device, click **Close**.

Note:
Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.

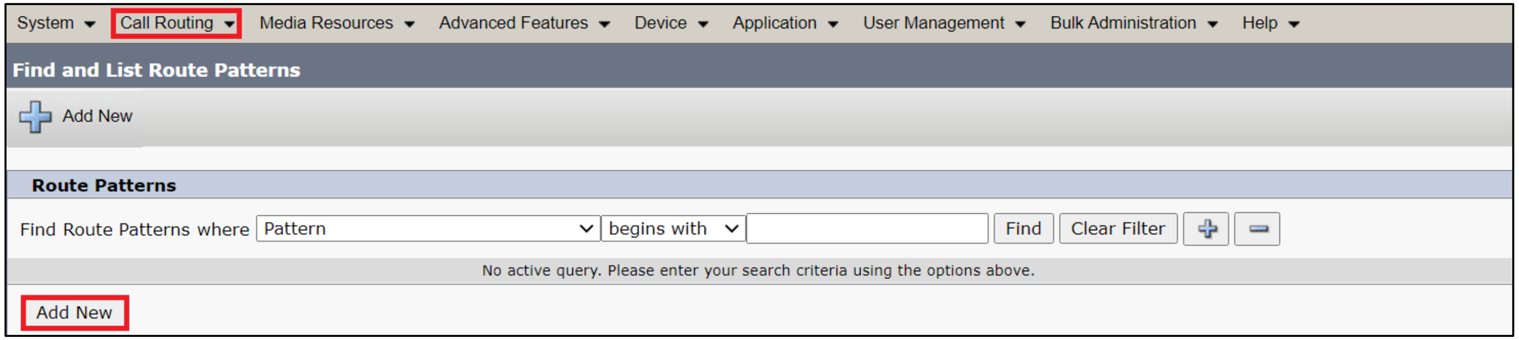
Note
Resetting/restarting a SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed.

Configure Call Routing

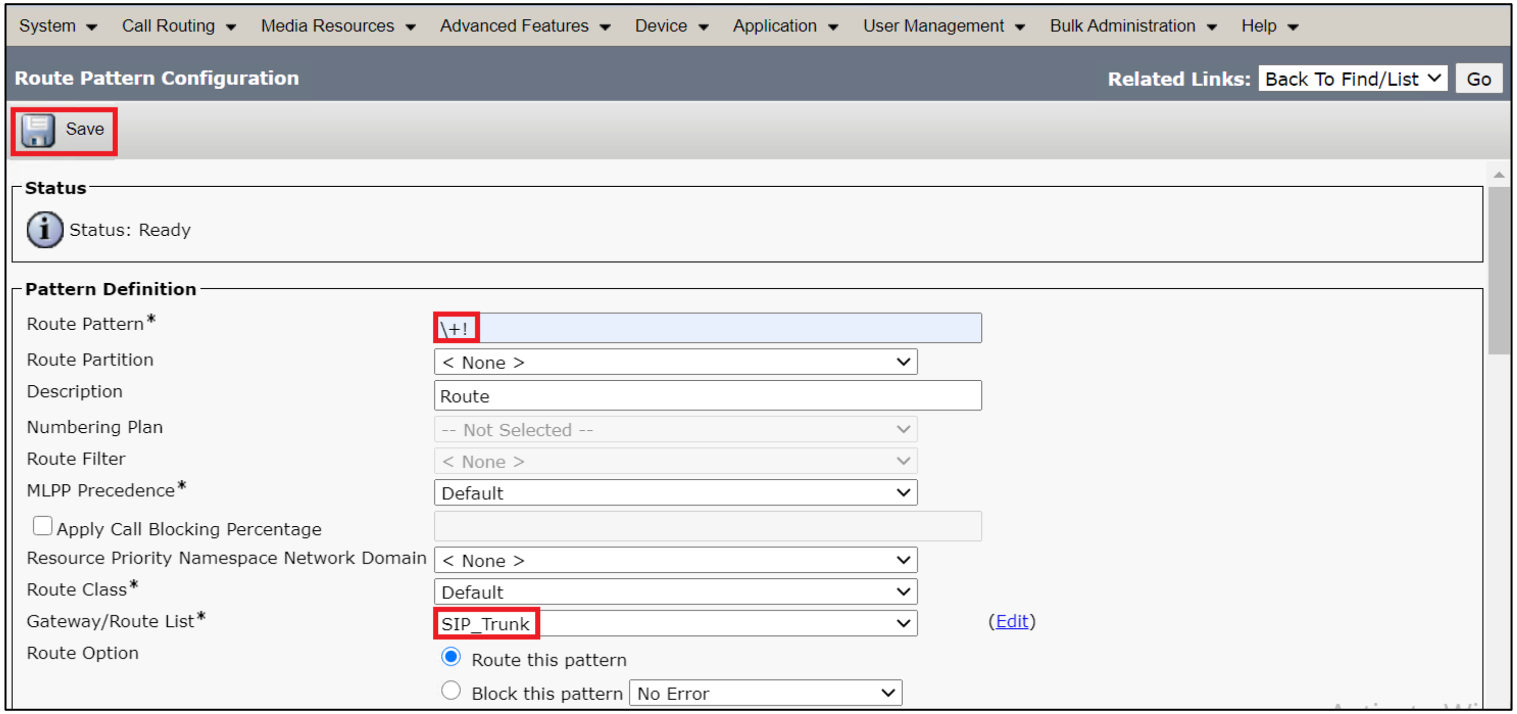
A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

- In Cisco Unified Communications Manager Administration, use the **Call Routing > Route/Hunt > Route Pattern** menu path to configure route patterns.
- Click **Add New**.



No active query. Please enter your search criteria using the options above.

- Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +.
- Configure the Route Pattern as below. This will allow all the destination numbers dialed with +.
- Choose SIP Trunk created from the gateway or route list drop-down to add the route pattern.



Route Pattern Configuration

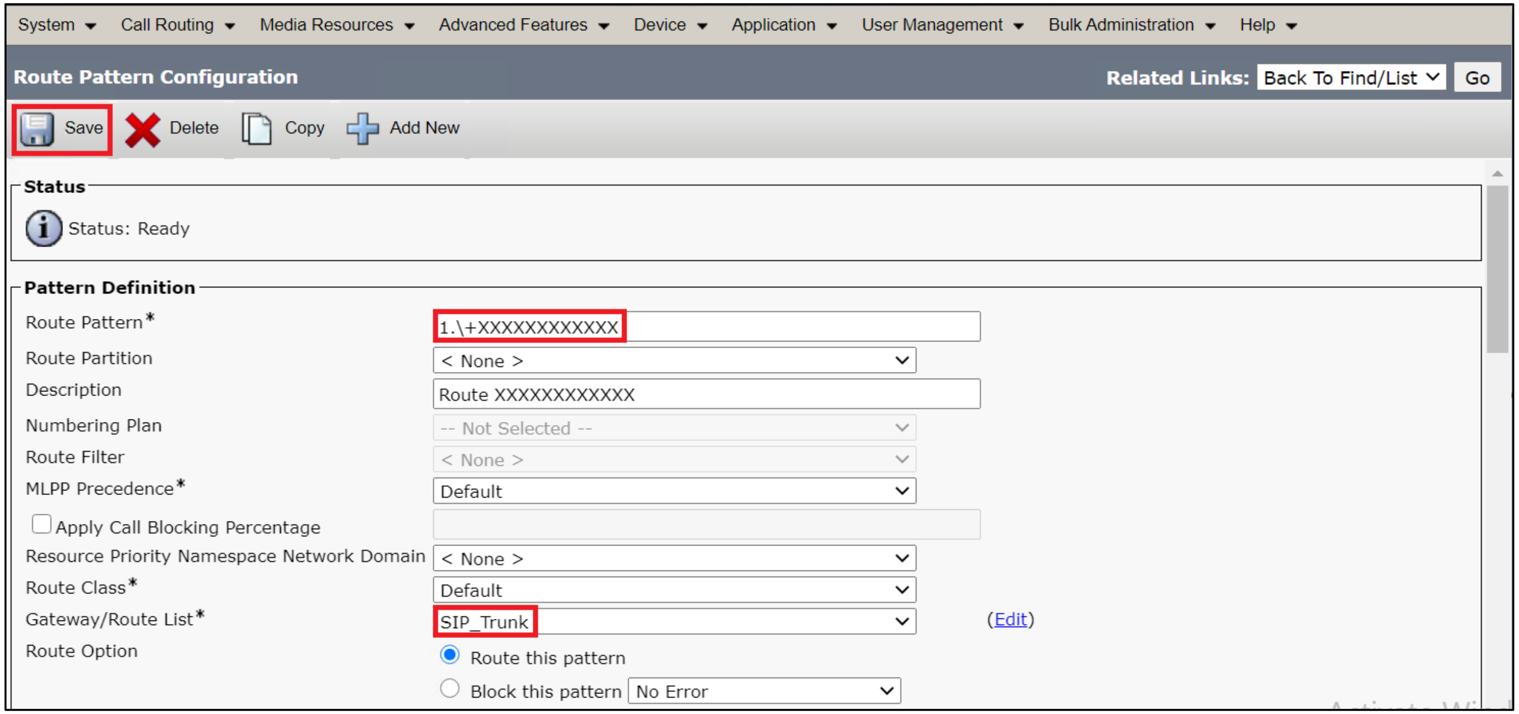
Status

Status: Ready

Pattern Definition

Route Pattern*	\+!
Route Partition	< None >
Description	Route
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	SIP_Trunk (Edit)
Route Option	● Route this pattern ○ Block this pattern No Error

- Or, Configure the pattern as 1.\+XXXXXXXXXXXX. This would require dialing the number as 1.+XXXXXXXXXXXX from the endpoint.
- Choose the **SIP Trunk** created earlier from the gateway or route list drop-down to add the route pattern.



Route Pattern Configuration

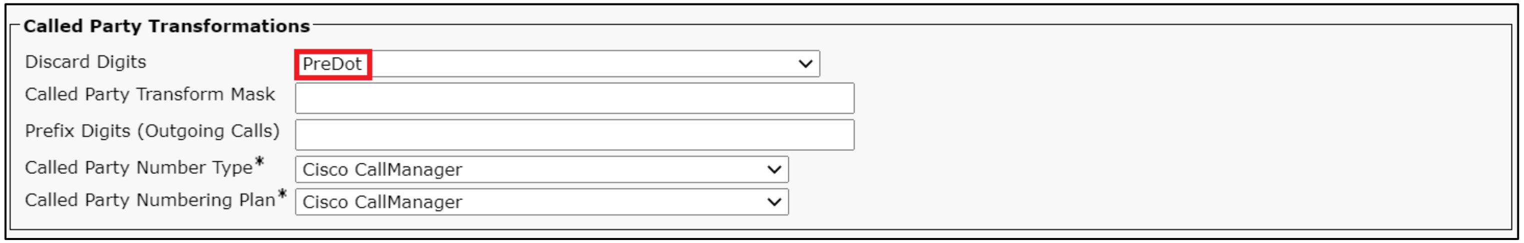
Status

Status: Ready

Pattern Definition

Route Pattern*	1.\+XXXXXXXXXXXX
Route Partition	< None >
Description	Route XXXXXXXXXXXX
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	SIP_Trunk (Edit)
Route Option	● Route this pattern ○ Block this pattern No Error

- This way of configuring Route Pattern requires additional settings to remove the digits before the Dot.
- From Discard Digits drop-down, choose **PreDot**.
  - This would remove the digits which are present before the Dot (1 in this case).



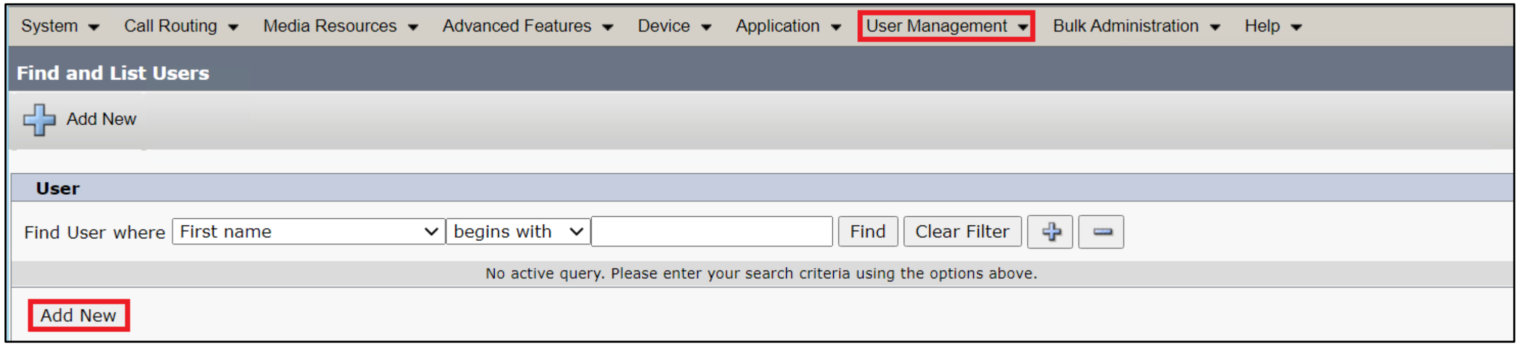
Called Party Transformations

Discard Digits	PreDot
Called Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Called Party Number Type*	Cisco CallManager
Called Party Numbering Plan*	Cisco CallManager

Configure End Users

The End User Configuration window allows you to add, search, display, and maintain information about Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window.

- In Cisco Unified CM Administration, use the **User Management > End User** menu path to configure end users.
- Click **Add New**.

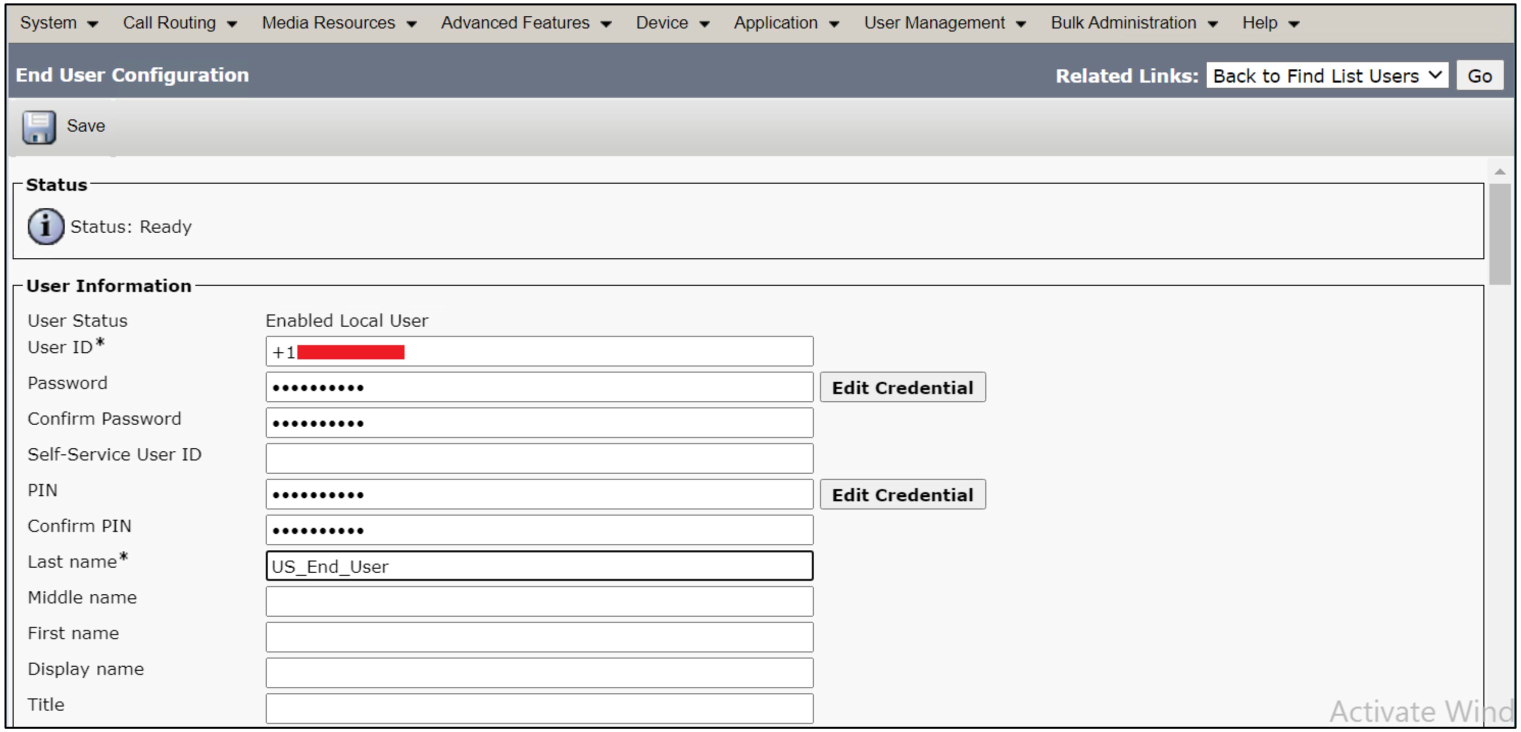


Find User where First name begins with

No active query. Please enter your search criteria using the options above.

- Enter the unique end user identification name.
- Enter alphanumeric or special characters for the end user password and confirm the same.
- Enter numeric characters for the end user PIN and confirm.
- Enter the end user last name.

- For Digest Credentials, enter a string of alphanumeric characters and confirm.



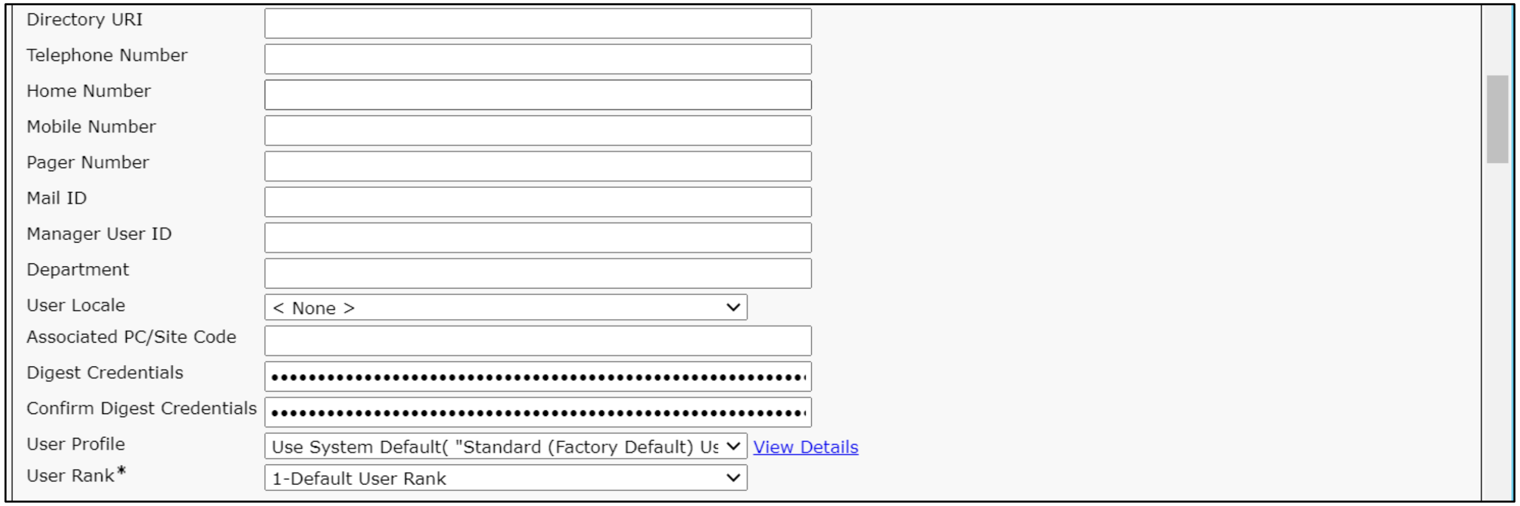
End User Configuration

Status

Status: Ready

User Information

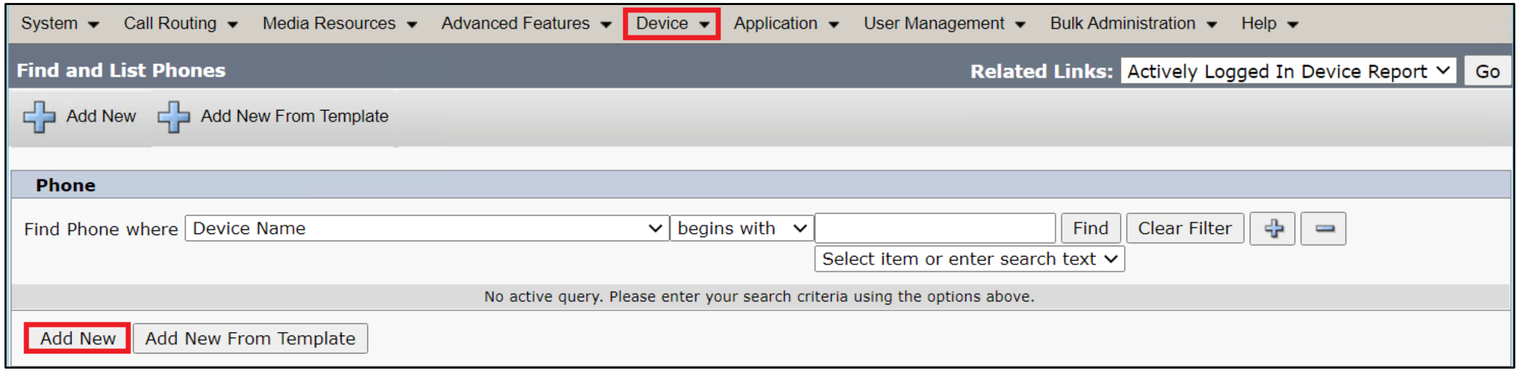
User Status	Enabled Local User
User ID*	+1[redacted]
Password	••••••••••
Confirm Password	••••••••••
Self-Service User ID	
PIN	••••••••••
Confirm PIN	••••••••••
Last name*	US_End_User
Middle name	
First name	
Display name	
Title	



Directory URI	
Telephone Number	
Home Number	
Mobile Number	
Pager Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC/Site Code	
Digest Credentials	••
Confirm Digest Credentials	••
User Profile	Use System Default("Standard (Factory Default) Us View Details
User Rank*	1-Default User Rank

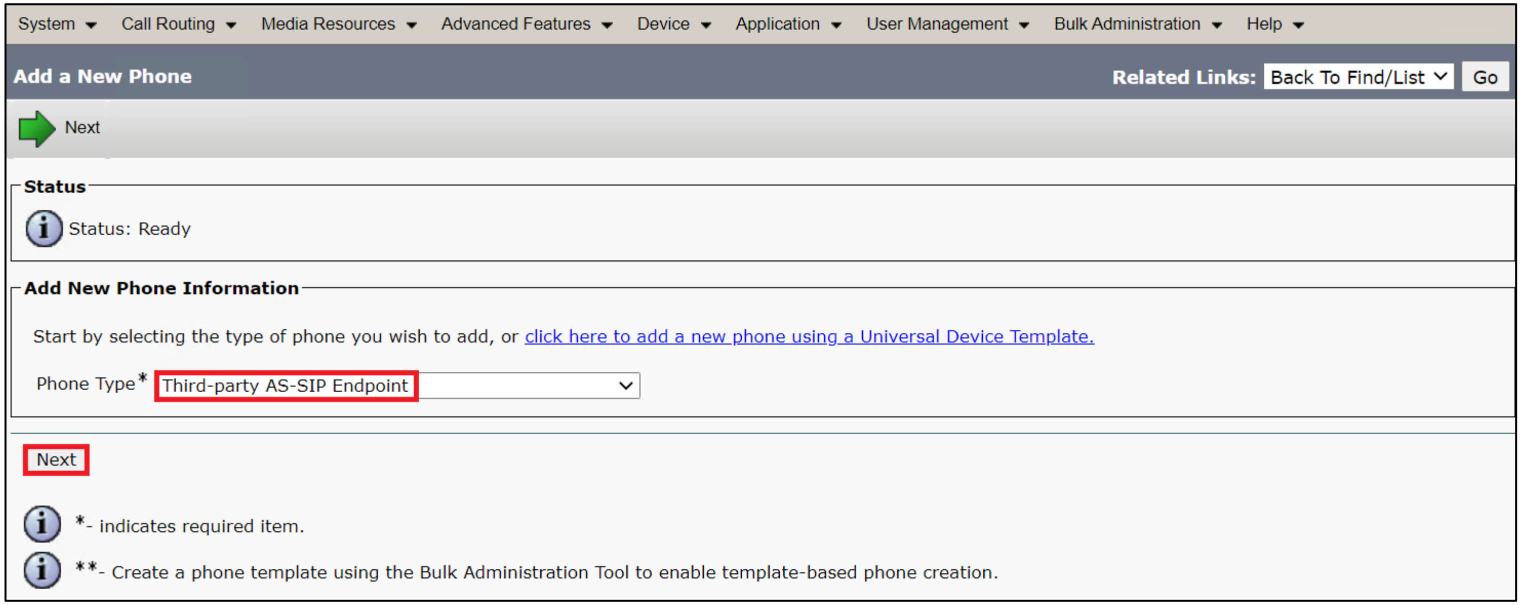
Phone Setup

- In Cisco Unified Communications Manager Administration, use the **Device > Phone** menu path to configure phones.
- Click **Add New**.



No active query. Please enter your search criteria using the options above.

- From the Phone Type drop-down, choose Third-party AS-SIP Endpoint.
- Click **Next**.



Add a New Phone

Status

Status: Ready

Add New Phone Information

Start by selecting the type of phone you wish to add, or click here to add a new phone using a Universal Device Template.

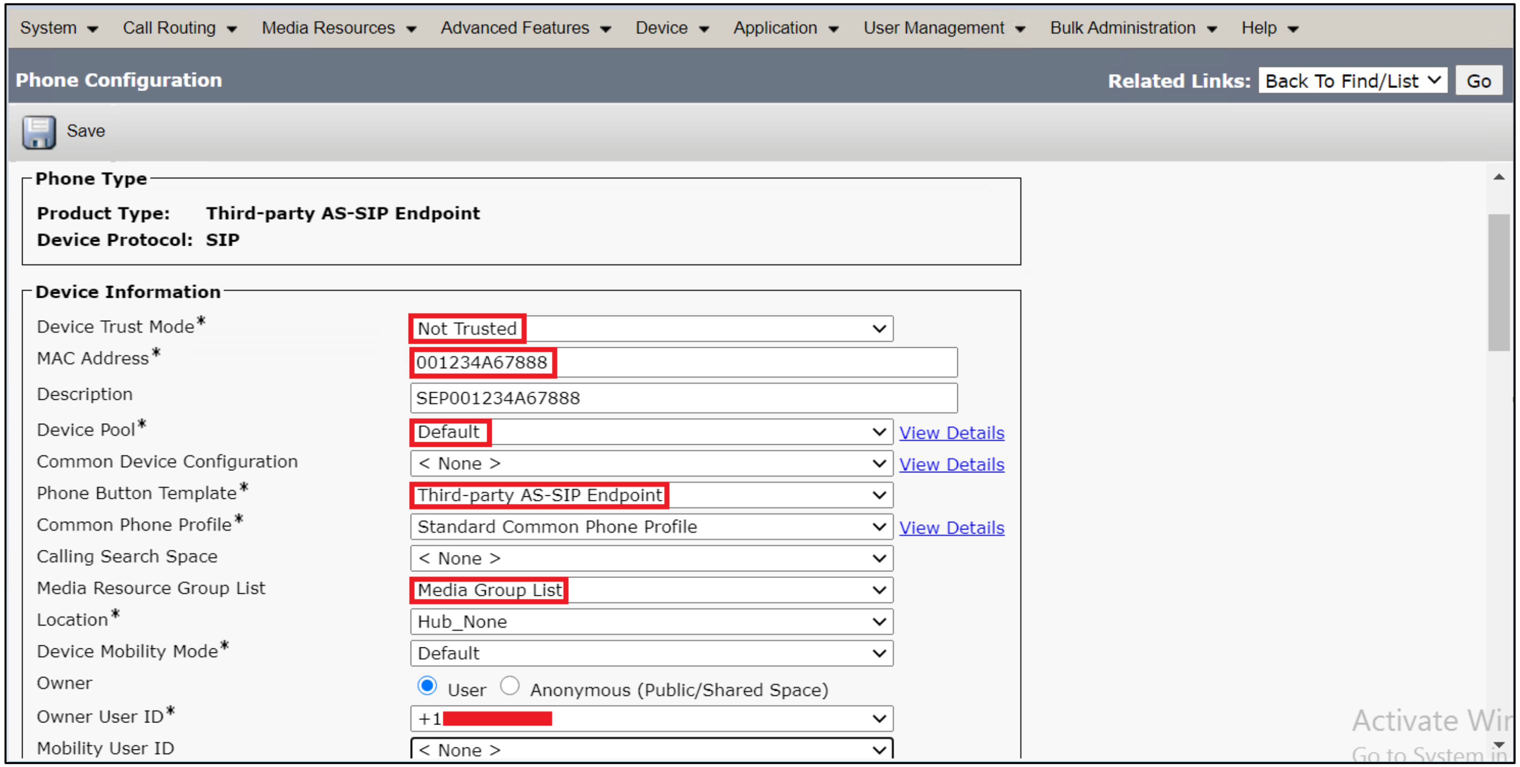
Phone Type* Third-party AS-SIP Endpoint

Next

*- indicates required item.

**- Create a phone template using the Bulk Administration Tool to enable template-based phone creation.

- Choose Device Trust Mode as **Not Trusted**.
- Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones. Make sure that the value comprises 12 hexadecimal characters.
- Choose **Default** Device pool.
  - A Device pool defines sets of common characteristics for devices, such as region, date/time group, and soft key template.
- Choose **Third-party AS-SIP Endpoint** from the phone button template drop-down.
  - The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
- Associate the Media Resource Group List created.
- Choose the user ID of the assigned phone user.



Phone Configuration

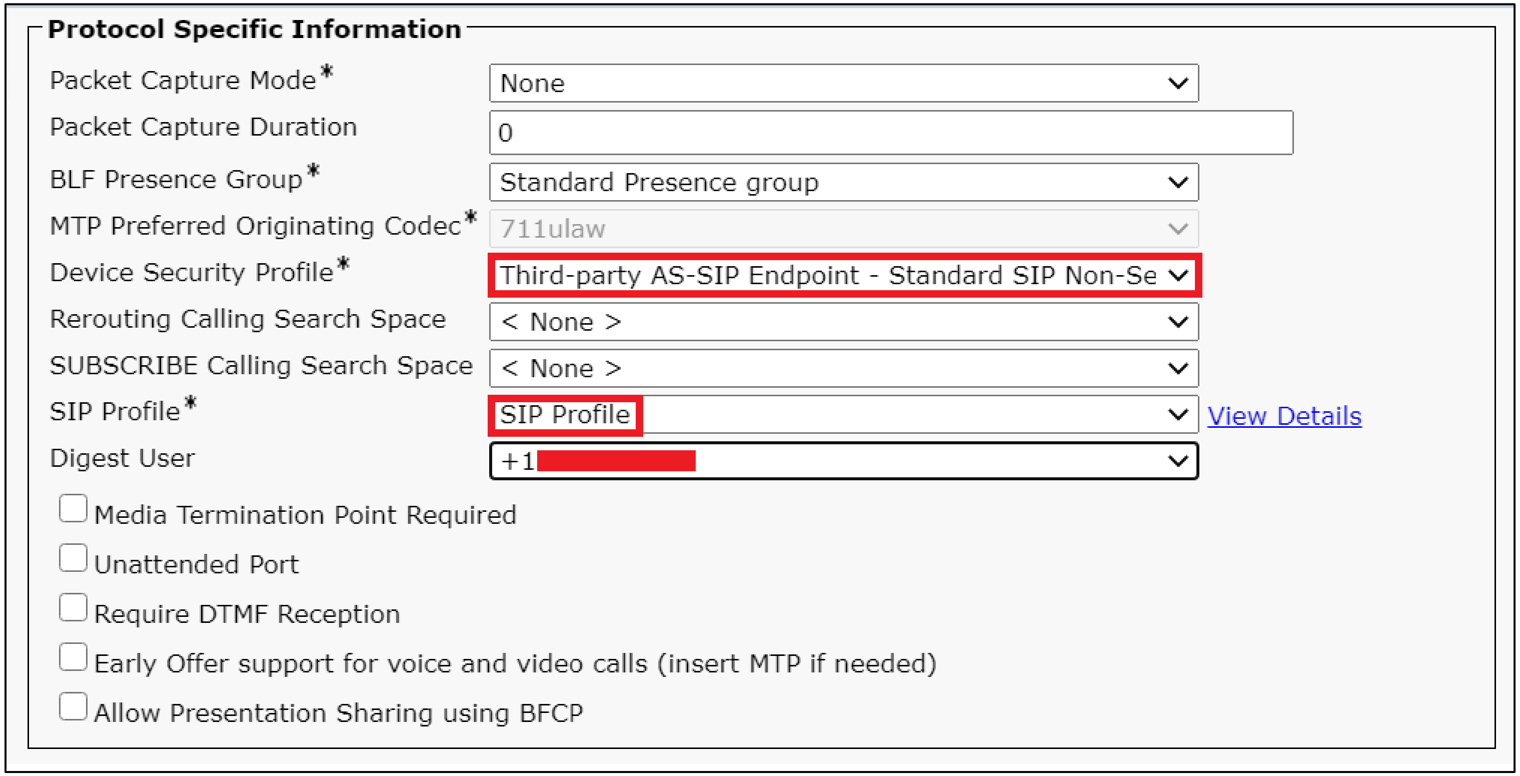
Phone Type

Product Type: **Third-party AS-SIP Endpoint**
Device Protocol: **SIP**

Device Information

Device Trust Mode*	Not Trusted
MAC Address*	001234A67888
Description	SEP001234A67888
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	Third-party AS-SIP Endpoint
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	< None >
Media Resource Group List	Media Group List
Location*	Hub_None
Device Mobility Mode*	Default
Owner	● User ○ Anonymous (Public/Shared Space)
Owner User ID*	+1[redacted]
Mobility User ID	< None >

- Choose the security profile Third-party AS-SIP Endpoint - Standard SIP Non-Secure Profile to apply to the device.
- Associate the SIP Profile created before.
  - SIP profiles provide specific SIP information for the phone such as registration and keep-alive timers, media ports, and do not disturb control.
- Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security).
- Click **Save**.



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Third-party AS-SIP Endpoint - Standard SIP Non-Se
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	SIP Profile View Details
Digest User	+1[redacted]

☐ Media Termination Point Required

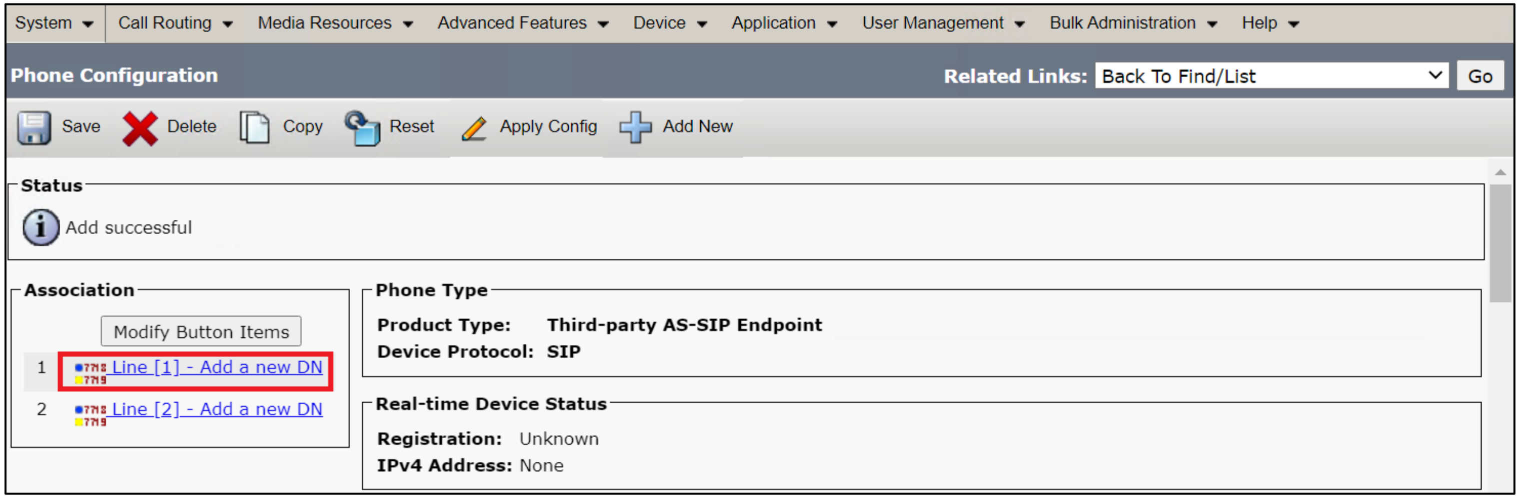
☐ Unattended Port

☐ Require DTMF Reception

☐ Early Offer support for voice and video calls (insert MTP if needed)

☐ Allow Presentation Sharing using BFCP

- Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device.



Status

Add successful

Association

1 Line [1] - Add a new DN

2 Line [2] - Add a new DN

Phone Type

Product Type: Third-party AS-SIP Endpoint

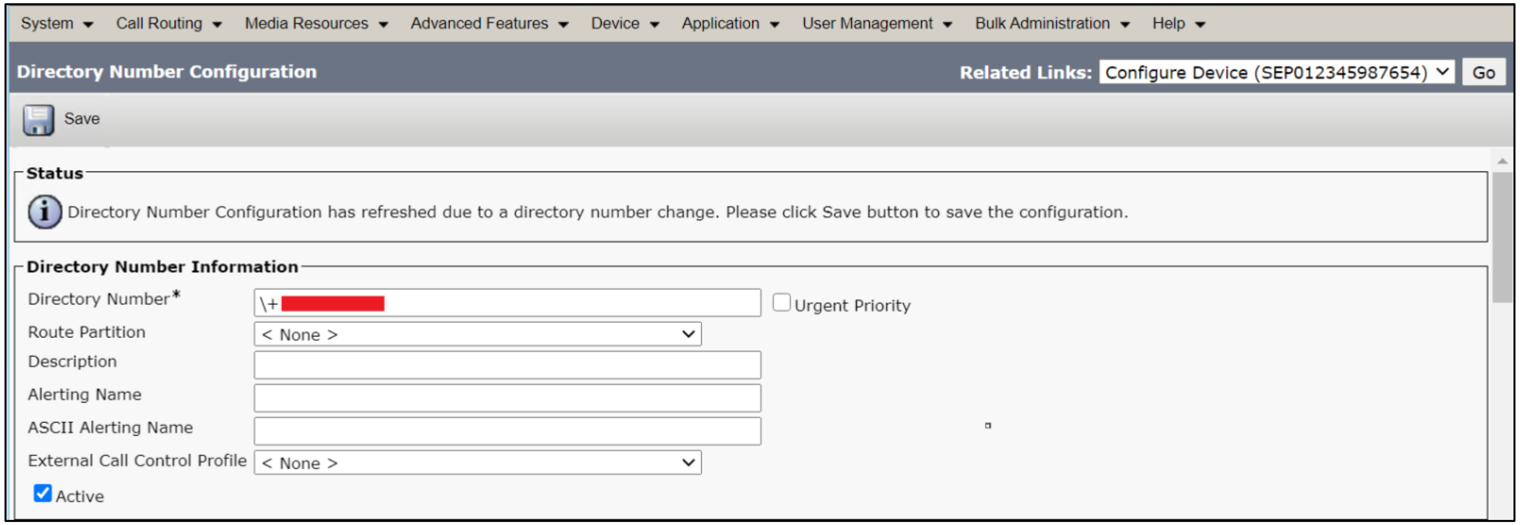
Device Protocol: SIP

Real-time Device Status

Registration: Unknown

IPv4 Address: None

- Add the Directory number.
- Click **Save**.



Directory Number Configuration

Related Links: Configure Device (SEP012345987654)

Status

Directory Number Configuration has refreshed due to a directory number change. Please click Save button to save the configuration.

Directory Number Information

Directory Number* \+[redacted] □ Urgent Priority

Route Partition < None >

Description

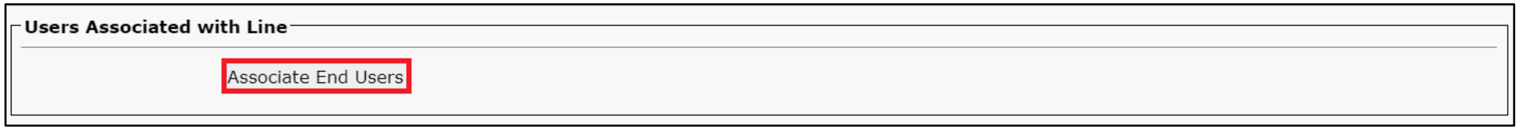
Alerting Name

ASCII Alerting Name

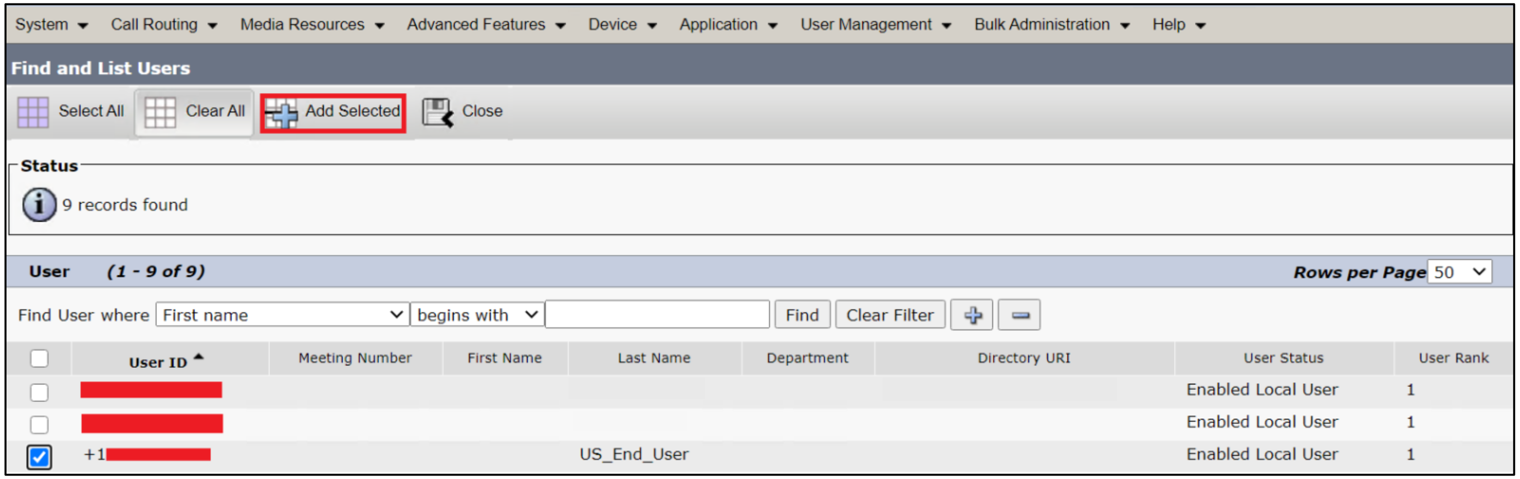
External Call Control Profile < None >

☑ Active

- Click the **Associate End User** button.


Users Associated with Line

- Select the end user created from the list and click **Add Selected**.



Find and List Users

Status

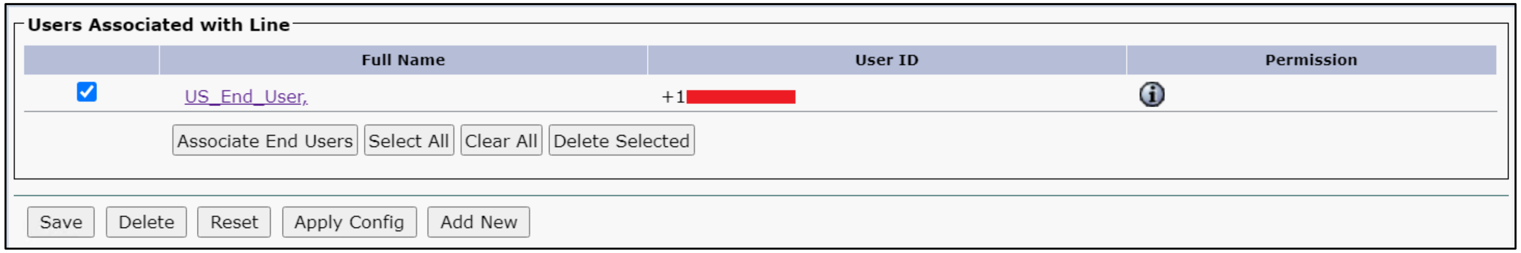
9 records found

User ***(1 - 9 of 9)*** ***Rows per Page*** 50

Find User where First name begins with

□	User ID	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
□	[redacted]						Enabled Local User	1
□	[redacted]						Enabled Local User	1
☑	+1[redacted]			US_End_User			Enabled Local User	1

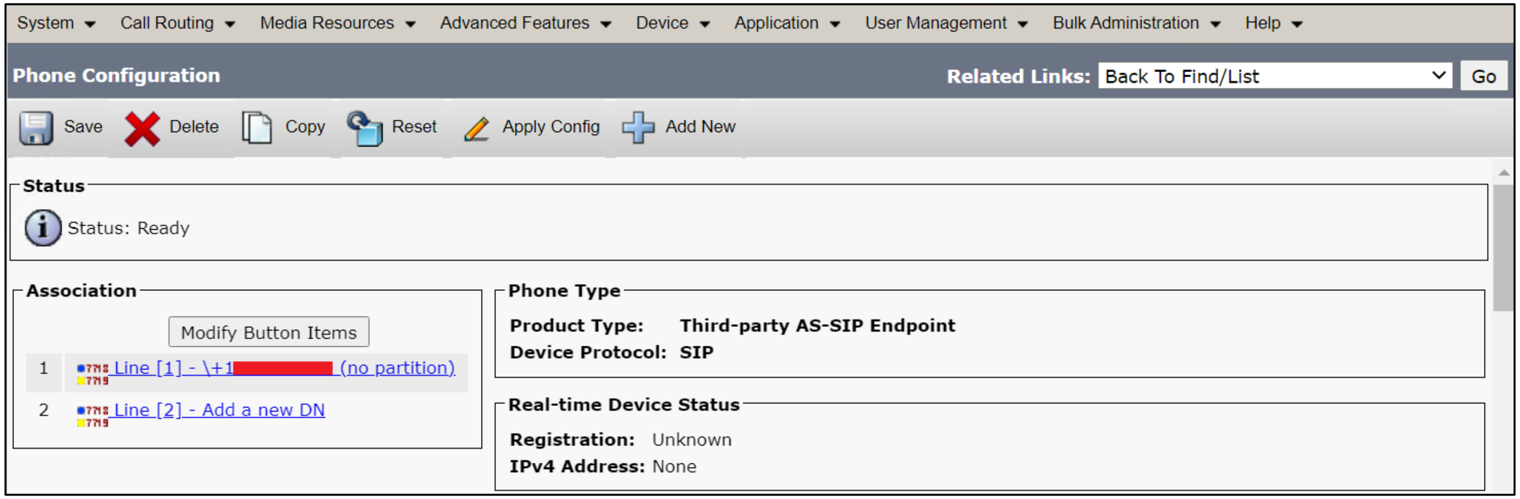
- After the above step, the user association is completed.
- Save the configuration.



Users Associated with Line

	Full Name	User ID	Permission
☑	US_End_User,	+1[redacted]	ⓘ

- Click **Apply Config** followed by the Reset button.
- Reset, Restart and Close the window.



Phone Configuration

Status

Status: Ready

Association

1 Line [1] - \+1[redacted] (no partition)

2 Line [2] - Add a new DN

Phone Type

Product Type: **Third-party AS-SIP Endpoint**

Device Protocol: **SIP**

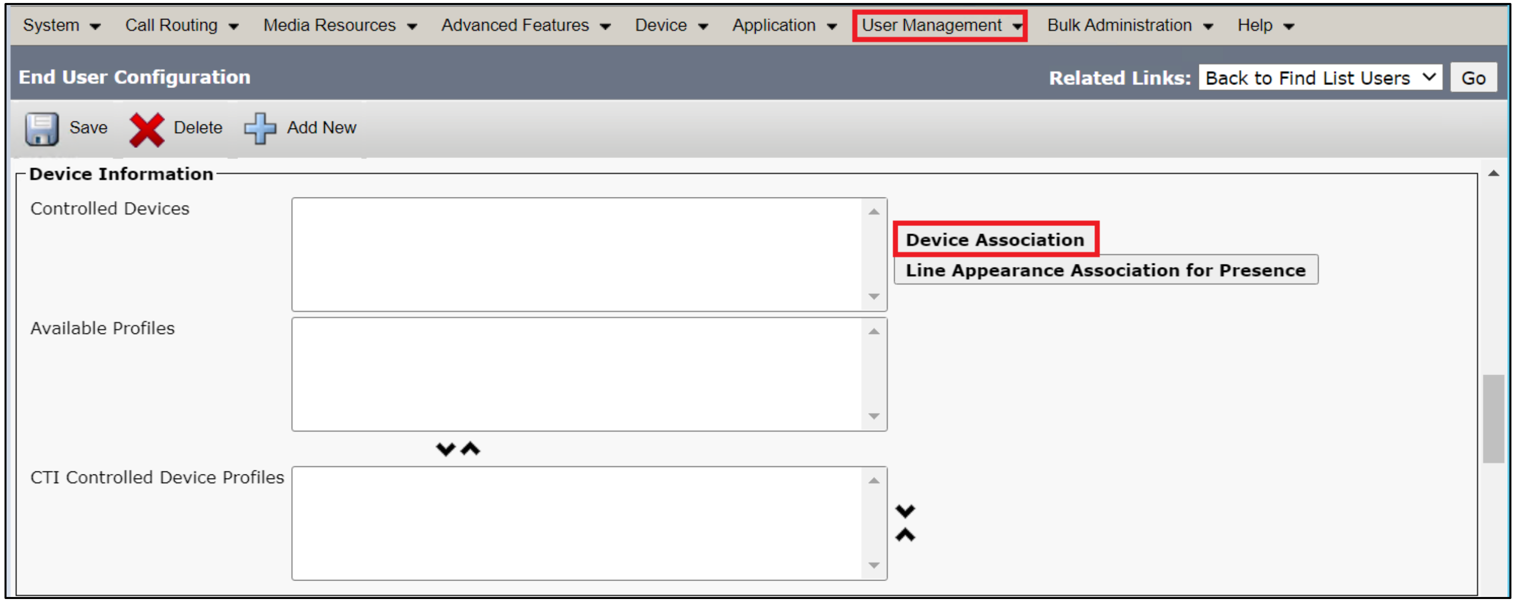
Real-time Device Status

Registration: Unknown

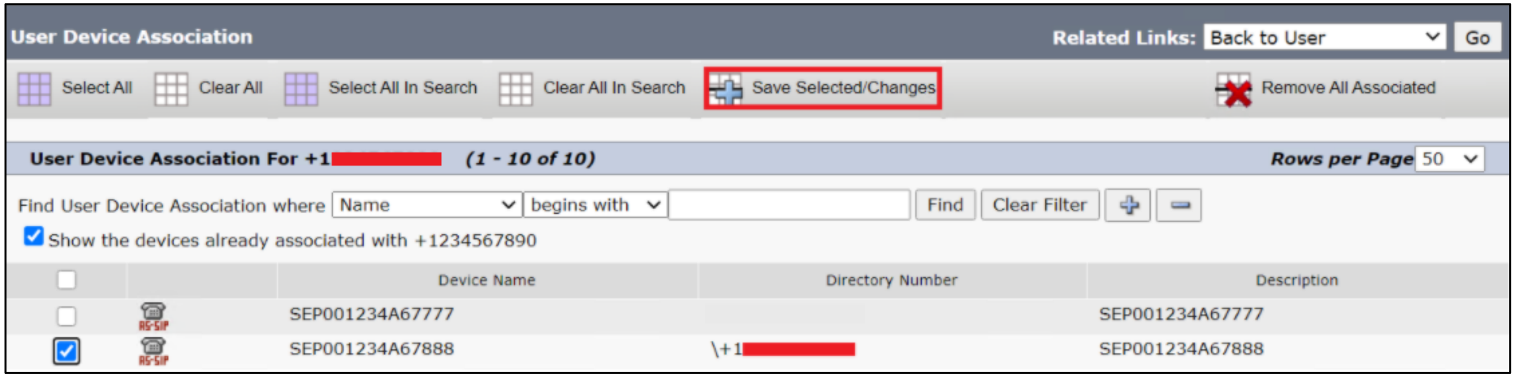
IPv4 Address: None

Device Association

- Navigate back to **User Management > End User.**
- In the Device Information field, click **Device Association**. This will display all the available devices.



- Select the device created in the previous step and save.



User Device Association

Related Links: Back to User | Go

User Device Association For +1[redacted] (1 - 10 of 10)

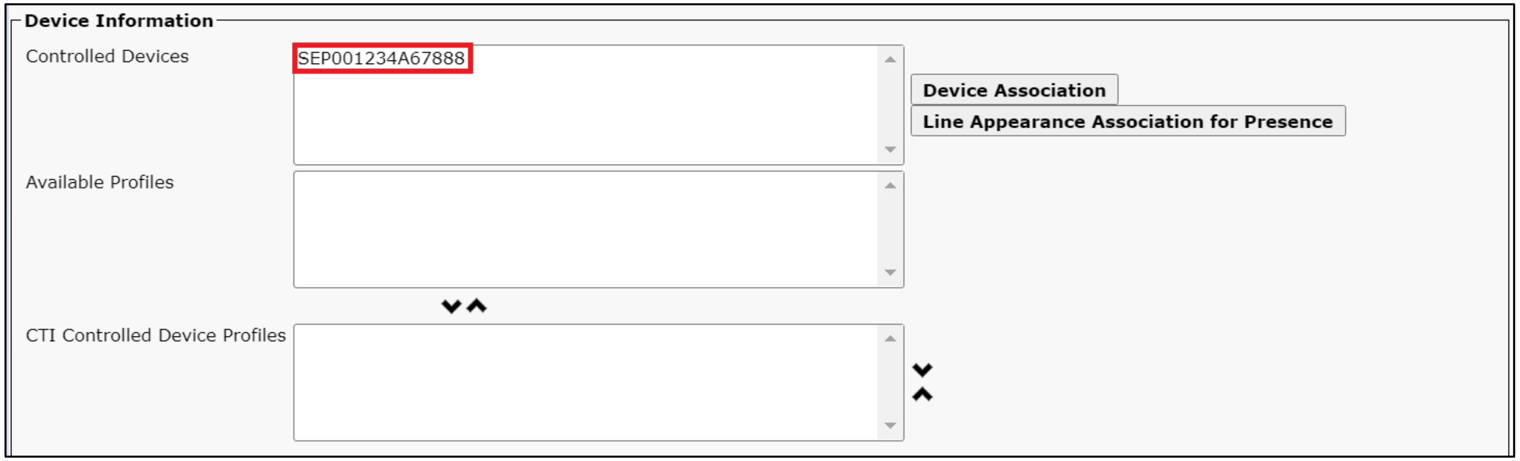
Rows per Page 50

Find User Device Association where Name begins with | Find | Clear Filter

☑ Show the devices already associated with +1234567890

☐		Device Name	Directory Number	Description
☐	☎	SEP001234A67777		SEP001234A67777
☑	☎	SEP001234A67888	\+1[redacted]	SEP001234A67888

- After selecting the appropriate device, it will appear in the Controlled Devices pane.



Device Information

Controlled Devices: SEP001234A67888

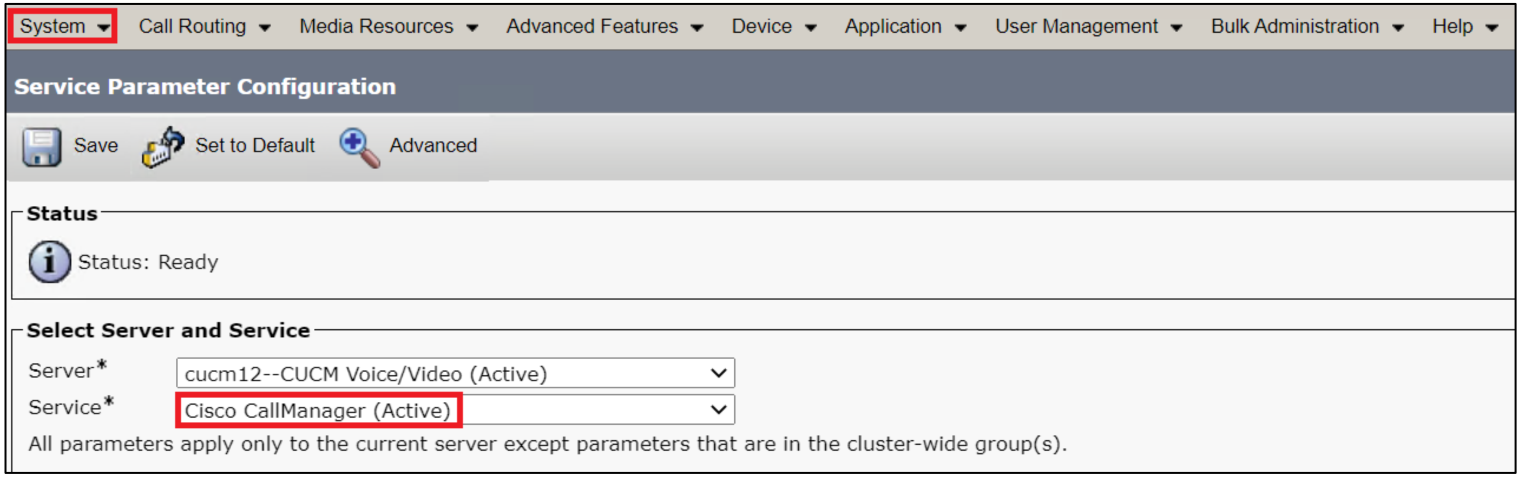
Available Profiles:

CTI Controlled Device Profiles:

Enable MoH

In Cisco Unified Communications Manager Administration, use the **System > Service Parameters** menu path to configure service parameters.

- In the Server drop-down list box in the Service Parameter Configuration window, choose the CCUCM server being used. In this case, active means that you provisioned the server in Cisco Unified Communications Manager Administration.
- From Service drop-down select Cisco CallManager. The service displays as active in the Service Parameters Configuration window.



Service Parameter Configuration

Status

Status: Ready

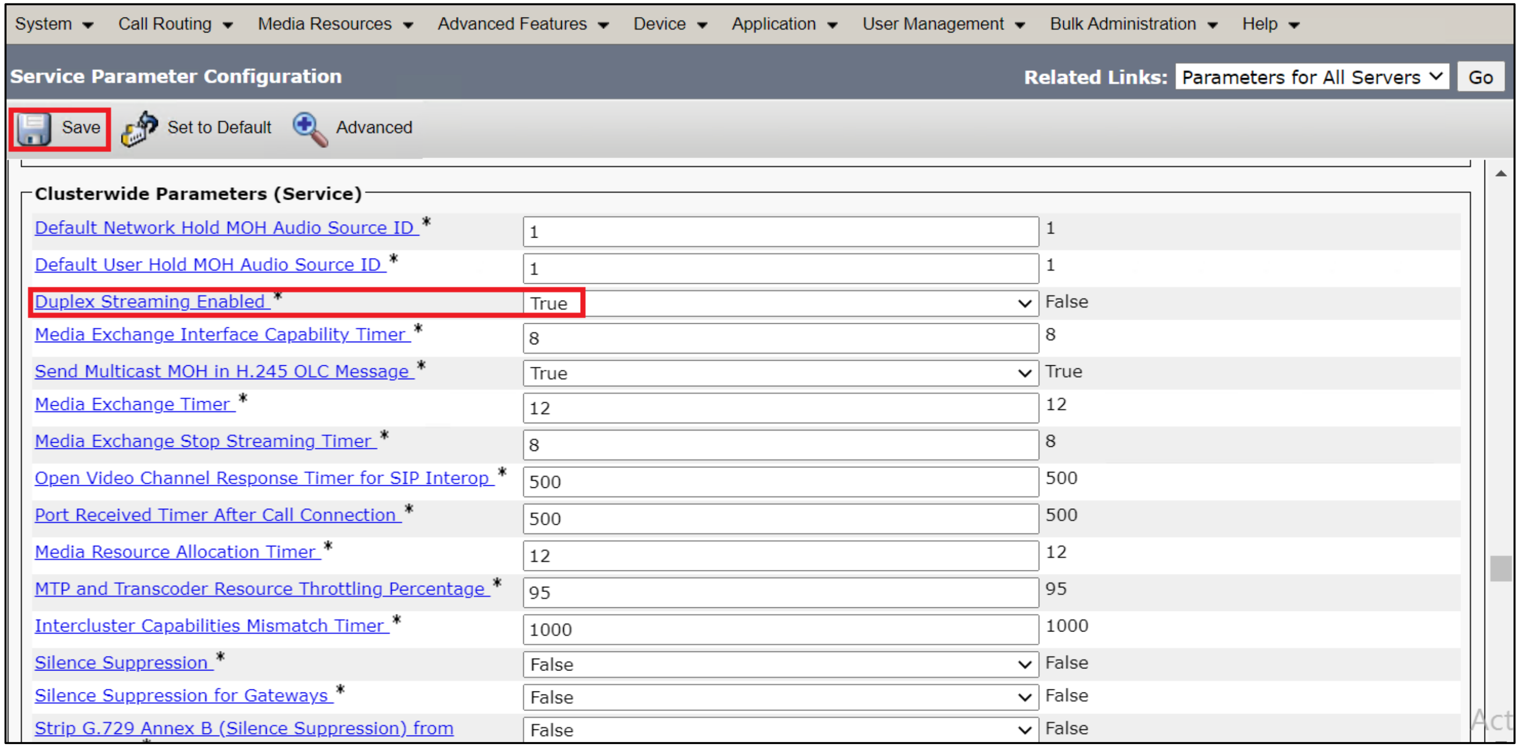
Select Server and Service

Server* cucm12--CUCM Voice/Video (Active)

Service* Cisco CallManager (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

- Set the Duplex Streaming Enabled flag to True. This parameter determines whether Music On Hold (MOH) and Annunciator use duplex streaming.
- Click **Save**.



Clusterwide Parameters (Service)

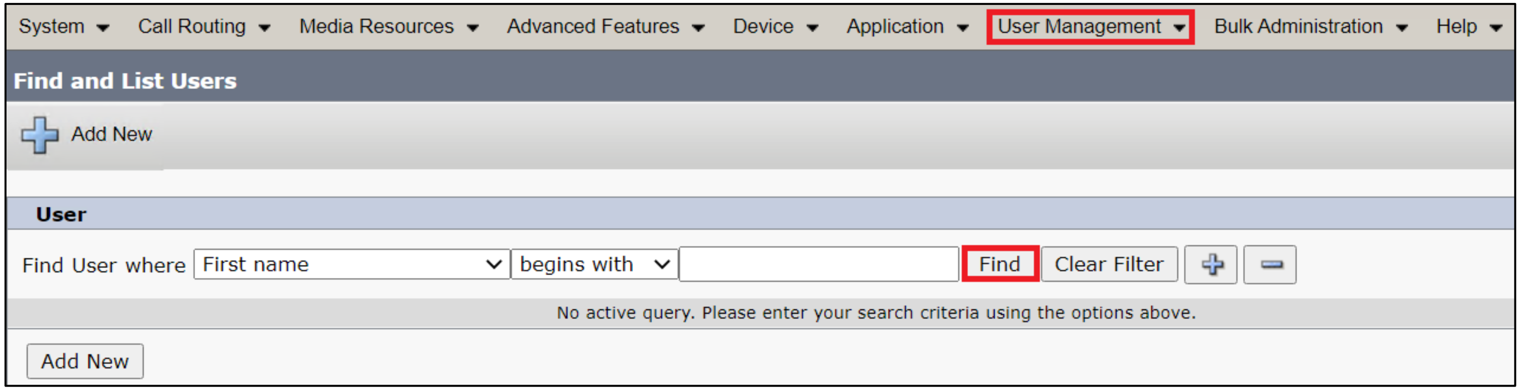
Default Network Hold MOH Audio Source ID *	1	1
Default User Hold MOH Audio Source ID *	1	1
Duplex Streaming Enabled *	True	False
Media Exchange Interface Capability Timer *	8	8
Send Multicast MOH in H.245 OLC Message *	True	True
Media Exchange Timer *	12	12
Media Exchange Stop Streaming Timer *	8	8
Open Video Channel Response Timer for SIP Interop *	500	500
Port Received Timer After Call Connection *	500	500
Media Resource Allocation Timer *	12	12
MTP and Transcoder Resource Throttling Percentage *	95	95
Intercluster Capabilities Mismatch Timer *	1000	1000
Silence Suppression *	False	False
Silence Suppression for Gateways *	False	False
Strip G.729 Annex B (Silence Suppression) from	False	False

Configuration for SIP-URI calling

The SIP URI scheme is a Uniform Resource Identifier(URI) scheme for the Session Initiation Protocol(SIP) multimedia communications protocol.

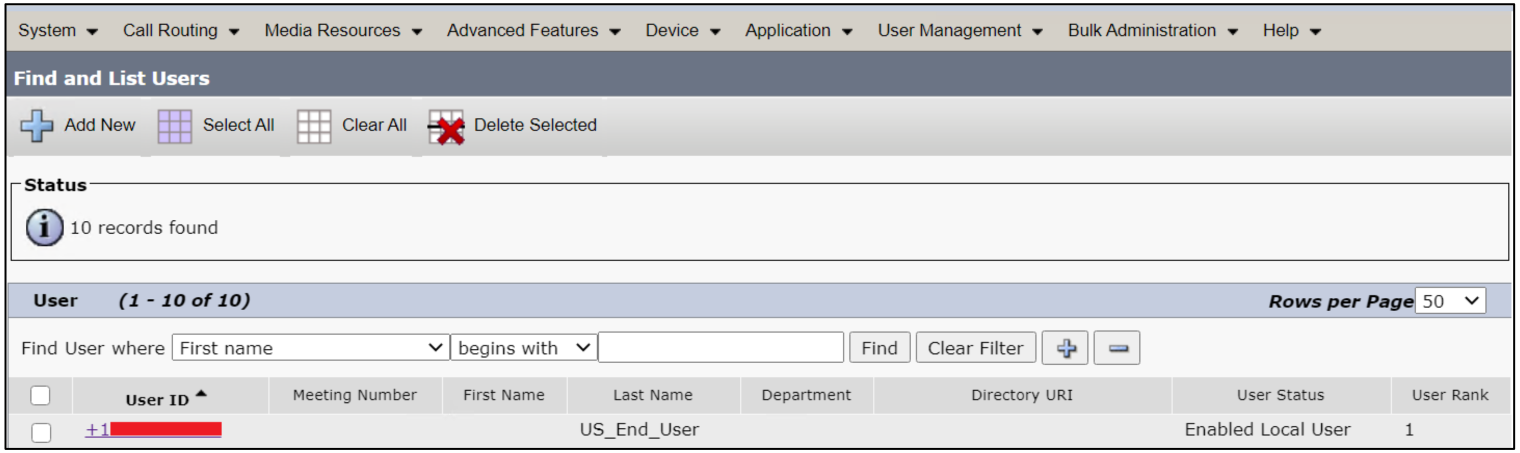
Configure End user

- In Cisco Unified CM Administration, navigate to **User Management > End User.**
- Click **Find**. This will display all the end users created.



No active query. Please enter your search criteria using the options above.

- Click on the user to configure with sip-uri.



Find and List Users

Status

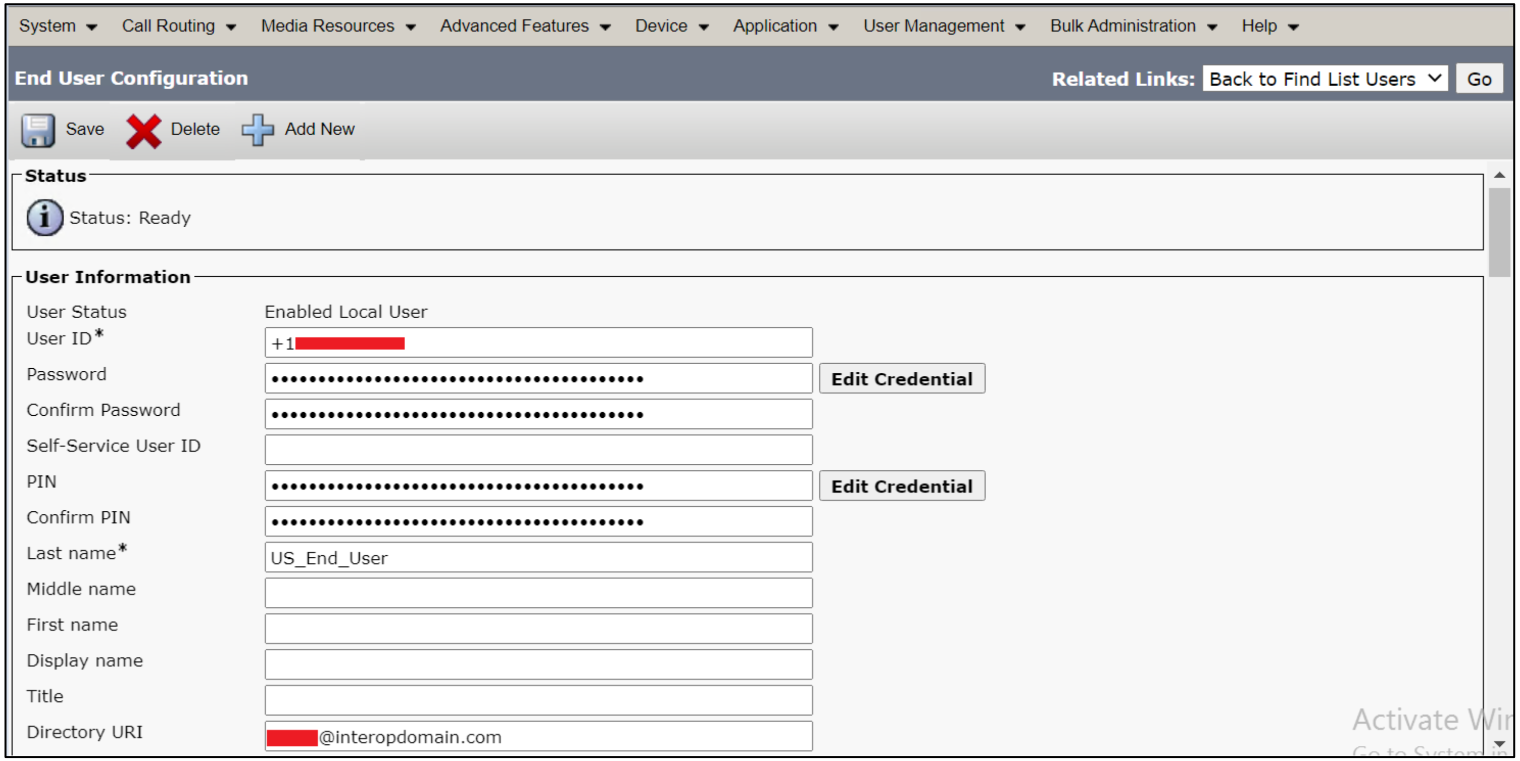
10 records found

User *(1 - 10 of 10)* — *Rows per Page* 50

Find User where First name begins with

□	User ID	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
□	+1[redacted]			US_End_User			Enabled Local User	1

- Provide a SIP address in user@domain.tld format.
- Click **Save**.



End User Configuration

Status

Status: Ready

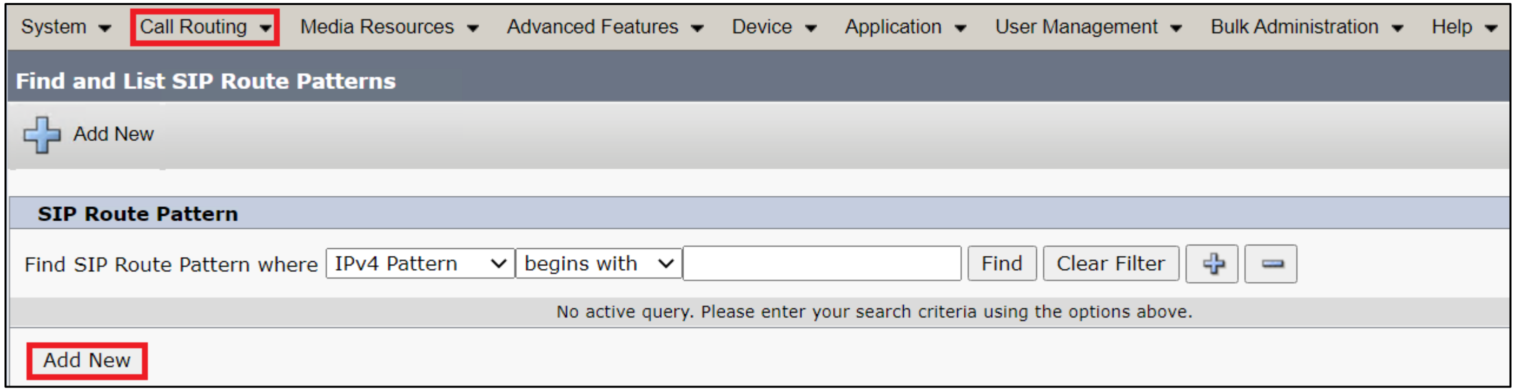
User Information

User Status	Enabled Local User
User ID*	+1[redacted]
Password	•• Edit Credential
Confirm Password	••
Self-Service User ID	
PIN	•• Edit Credential
Confirm PIN	••
Last name*	US_End_User
Middle name	
First name	
Display name	
Title	
Directory URI	[redacted]@interopdomain.com

Configure Route

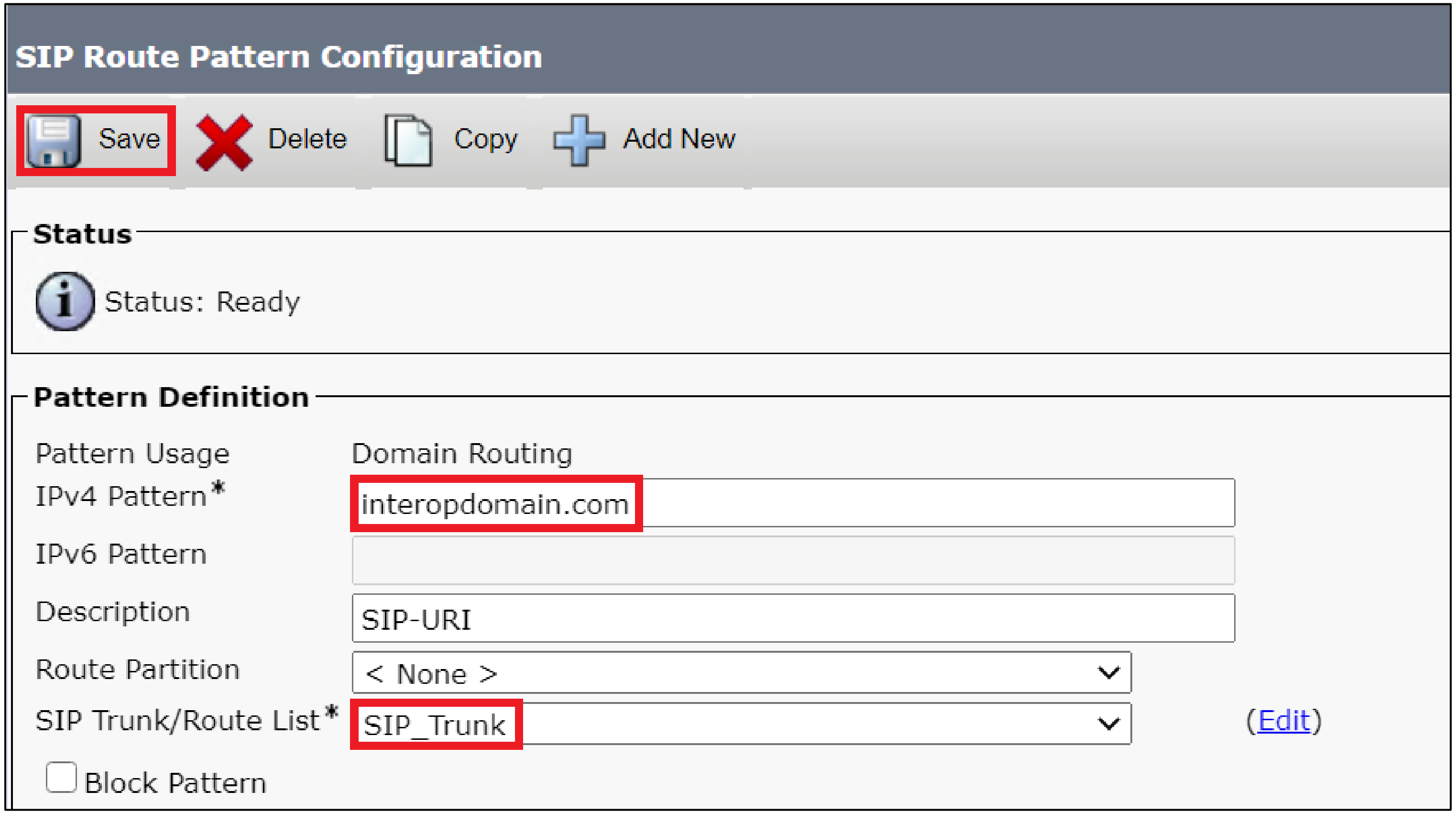
Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls.

- In Cisco Unified Communications Manager Administration, use the **Call Routing > SIP Route Pattern** menu path to configure SIP route patterns.
- Click **Add New**.



No active query. Please enter your search criteria using the options above.

- For Domain Routing pattern usage, enter a domain name(interopdmain.com in this case) IPv4 Pattern field that can resolve to an IPv4 address.
- From the drop-down list choose the SIP trunk created earlier to associate the route pattern.
- Click **Save**.



SIP Route Pattern Configuration

Status

Status: Ready

Pattern Definition

Pattern Usage	Domain Routing
IPv4 Pattern*	interopdomain.com
IPv6 Pattern	
Description	SIP-URI
Route Partition	< None >
SIP Trunk/Route List*	SIP_Trunk (Edit)

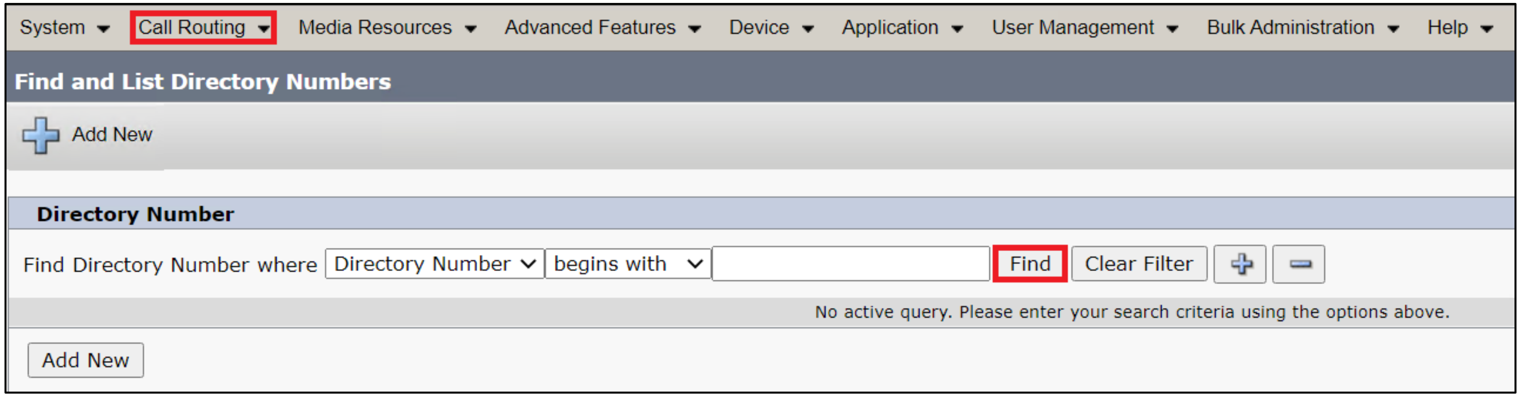
□ Block Pattern

Directory Number Information

Using Cisco Unified Communications Manager Administration, you configure and modify directory numbers (DNs) that are assigned to specific phones.

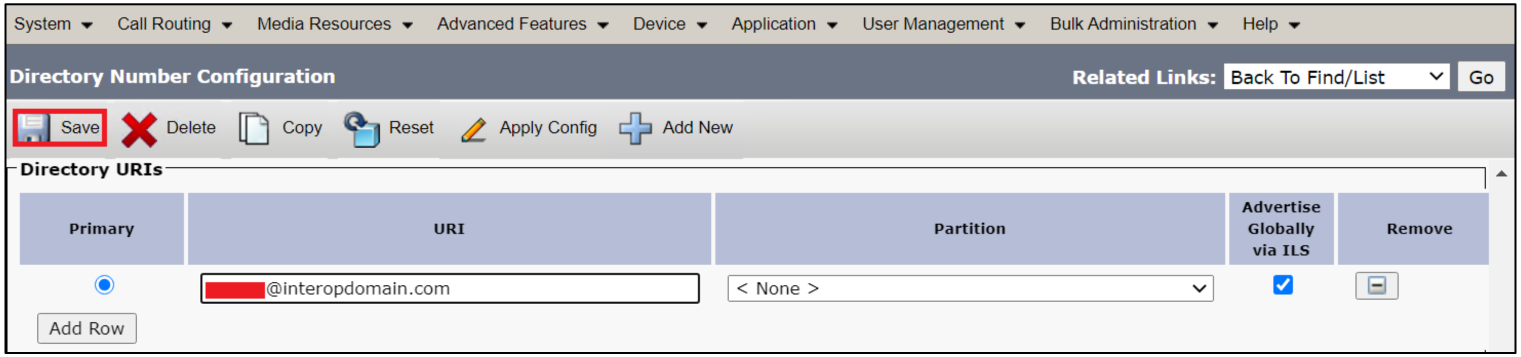
Assign Directory URIs to a Directory Number. Use the Directory Number Configuration window to associate directory URIs to a directory number. This allows Cisco Unified Communications Manager to support dialing using either the directory number or the directory URI. Each directory URI address must resolve to a single directory number in a partition.

- In Cisco Unified Communications Manager Administration, navigate to **Call Routing > Directory Number.**
- Click **Find**.



No active query. Please enter your search criteria using the options above.

- Click on the Directory number that needs a Directory URI assigned.
- Add the SIP-URI and save.
- Click **Apply Config**, Reset and Restart for the configuration to reflect.



Directory Number Configuration

Directory URIs

Primary	URI	Partition	Advertise Globally via ILS	Remove
●	[redacted]@interopdomain.com	< None >	☑	⊟

MS TEAMS Configuration

For Microsoft Teams Direct Routing configuration for SBC SWe Lite, refer to the following: Connect SBC Edge to Microsoft Teams Direct Routing

Please check the connectivity for interfacing with Microsoft Teams Direct Routing before making the calls by following the procedure provided at the following link: Working with Connectivity Check - Verifying Service and Port Requirements for CCE and Teams

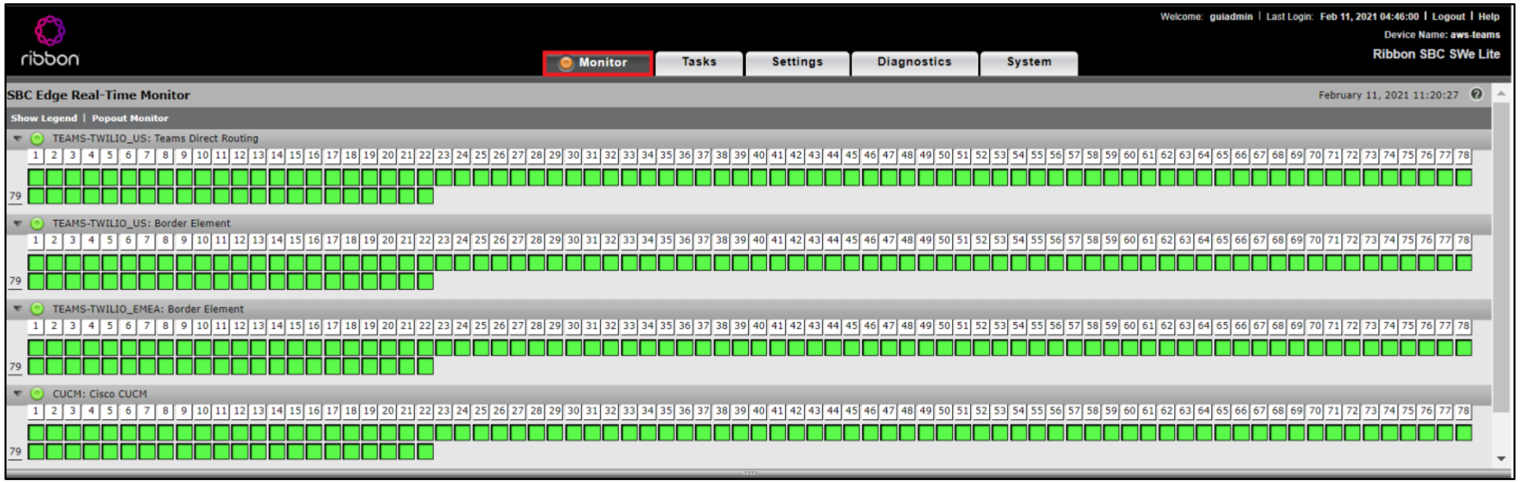
Note
This interop was performed with Media-Bypass OFF configuration on Microsoft Teams Direct Routing.

Monitor Real Time Status

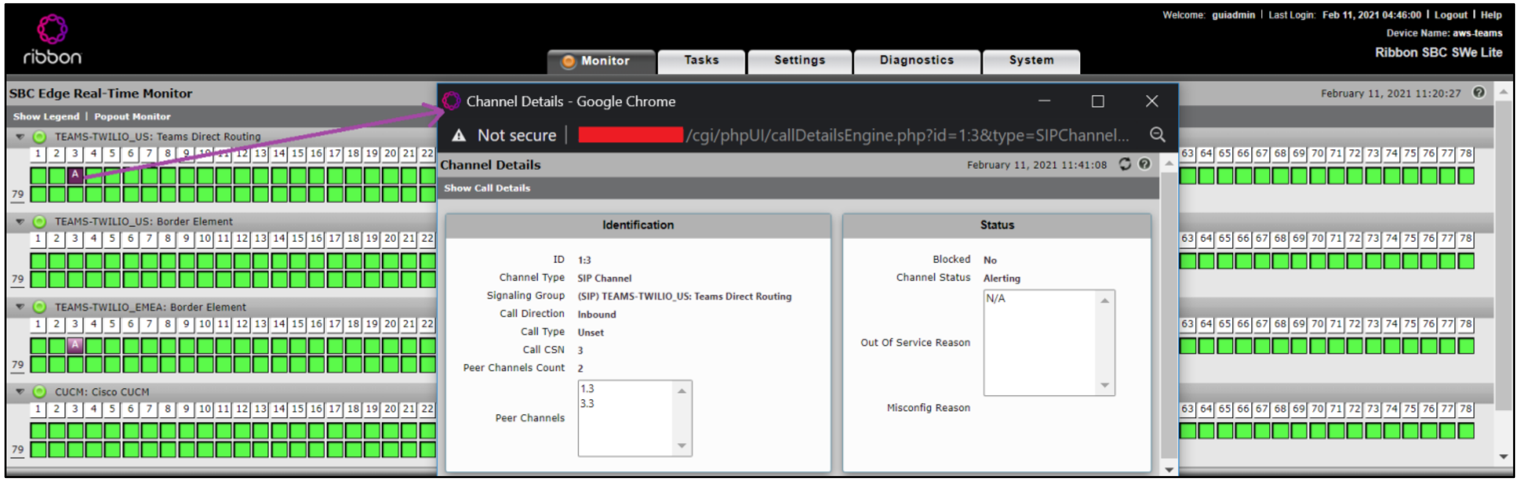
Place a Test Call

Access SBC SWe Lite's WebUI and click the **Monitor** tab. Confirm all the SIP Signaling Groups are active. This panel provides current information on the status of Ports, Channels and in-progress Calls on the Ribbon SBC SWe Lite system.

The below snapshot indicates all the SIP Signaling Groups are Active.


ribbon
Welcome: guiadmin | Last Login: Feb 11, 2021 04:46:00 | Logout | Help
Device Name: aws-teams
Ribbon SBC SWe Lite
Monitor
Tasks
Settings
Diagnostics
System
SBC Edge Real-Time Monitor
February 11, 2021 11:20:27
Show Legend | Popout Monitor
TEAMS-TWILIO_US: Teams Direct Routing
TEAMS-TWILIO_US: Border Element
TEAMS-TWILIO_EMEA: Border Element
CUCM: Cisco CUCM

- Place a test call from Microsoft Teams client to PSTN.
- Make sure the PSTN is presented with an incoming call(Phone display).
- TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group and TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group present an alerting indication (**magenta**) in the respective channels. Click on the seized channels for the details.


ribbon
Monitor
Tasks
Settings
Diagnostics
System
SBC Edge Real-Time Monitor
Show Legend | Popout Monitor
TEAMS-TWILIO_US: Teams Direct Routing
TEAMS-TWILIO_US: Border Element
TEAMS-TWILIO_EMEA: Border Element
CUCM: Cisco CUCM
February 11, 2021 11:20:27

Welcome: guiadmin | Last Login: Feb 11, 2021 04:46:00 | Logout | Help
Device Name: aws-teams
Ribbon SBC SWe Lite

Channel Details - Google Chrome

Not secure | [redacted]/cgi/phpUI/callDetailsEngine.php?id=1:3&type=SIPChannel...

Channel Details February 11, 2021 11:41:08

Show Call Details

Identification

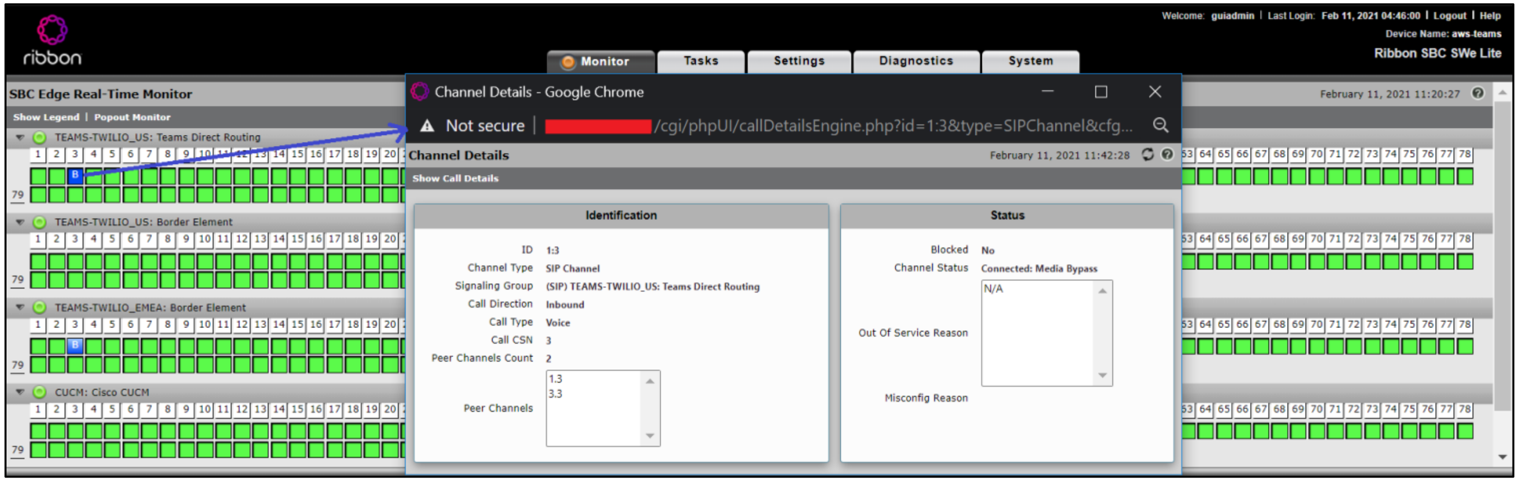
ID	1:3
Channel Type	SIP Channel
Signaling Group	(SIP) TEAMS-TWILIO_US: Teams Direct Routing
Call Direction	Inbound
Call Type	Unset
Call CSN	3
Peer Channels Count	2
Peer Channels	1.3 3.3

Status

Blocked	No
Channel Status	Alerting
Out Of Service Reason	N/A
Misconfig Reason	

Answer Call and Confirm Connection

- Answer the call on PSTN endpoint.
- TEAMS-TWILIO_US: Teams Direct Routing SIP Signaling Group and TEAMS-TWILIO_EMEA: Border Element SIP Signaling Group present a connected indication (**blue**) in the respective channels. Click on the seized channels for the details.


ribbon
Welcome: guiadmin | Last Login: Feb 11, 2021 04:46:00 | Logout | Help
Device Name: aws-teams
Ribbon SBC SWe Lite
Monitor
Tasks
Settings
Diagnostics
System
SBC Edge Real-Time Monitor
February 11, 2021 11:20:27
Show Legend | Popout Monitor
TEAMS-TWILIO_US: Teams Direct Routing
TEAMS-TWILIO_US: Border Element
TEAMS-TWILIO_EMEA: Border Element
CUCM: Cisco CUCM
B
79
Channel Details - Google Chrome
Not secure

[redacted]/cgi/phpUI/callDetailsEngine.php?id=1:3&type=SIPChannel&cfg...

Channel Details February 11, 2021 11:42:28

Show Call Details

Identification

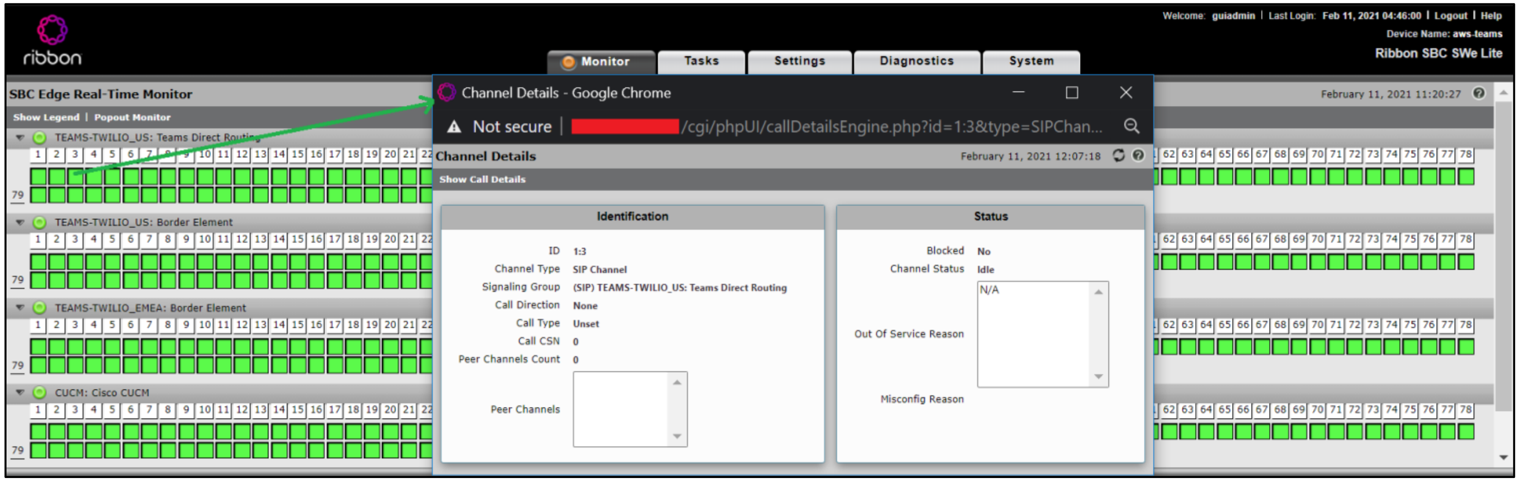
ID	1:3
Channel Type	SIP Channel
Signaling Group	(SIP) TEAMS-TWILIO_US: Teams Direct Routing
Call Direction	Inbound
Call Type	Voice
Call CSN	3
Peer Channels Count	2
Peer Channels	1.3 3.3

Status

Blocked	No
Channel Status	Connected: Media Bypass
Out Of Service Reason	N/A
Misconfig Reason	

Disconnect the Call

- Disconnect the call and ensure that the Channel Status is Idle.



ribbon
Welcome: guiadmin | Last Login: Feb 11, 2021 04:46:00 | Logout | Help
Device Name: aws-teams
Ribbon SBC SWe Lite
Monitor
Tasks
Settings
Diagnostics
System
SBC Edge Real-Time Monitor
February 11, 2021 11:20:27
Show Legend | Popout Monitor
TEAMS-TWILIO_US: Teams Direct Routing
TEAMS-TWILIO_US: Border Element
TEAMS-TWILIO_EMEA: Border Element
CUCM: Cisco CUCM
Channel Details - Google Chrome
Not secure

[redacted]/cgi/phpUI/callDetailsEngine.php?id=1:3&type=SIPChan...

Channel Details

February 11, 2021 12:07:18

Show Call Details

Identification

ID	1:3
Channel Type	SIP Channel
Signaling Group	(SIP) TEAMS-TWILIO_US: Teams Direct Routing
Call Direction	None
Call Type	Unset
Call CSN	0
Peer Channels Count	0
Peer Channels	

Status

Blocked	No
Channel Status	Idle
Out Of Service Reason	N/A
Misconfig Reason	

Note

- Click Show Legend for Channel/SG State Legend information.
- Place Test Calls between Twilio, MS Teams and Cisco endpoints to confirm the successful configuration and monitor the status.

Supplementary Services and Features Coverage

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

Sr. No	Supplementary Services/Features	Coverage
1	OPTIONS validation	✓
2	Call Setup and Termination over UDP and TLS	✓
3	Ringing and Local Ringback Tone	✓
4	Remote Ringback Tone Handling	✓
5	Cancel Call, No Answer, Busy and Call Rejection	✓
6	Basic Call with different codecs	✓
7	Voice mail	✓
8	FAX	✓
9	DTMF	✓
10	Toll Free Calls and Operator Assisted Calls	✓
11	Emergency Calls	✓

12	Anonymous Calls	✓
13	Call Hold and Resume	✓
14	Session Timers	✓
15	Call Forward - Unconditional, Busy and No Answer	✓
16	Call Transfer (Blind/Unattended)	✓
17	Call Transfer (Attended)	✓
18	Call Conference	✓
19	Route Crankback	✓
20	4xx/5xx Response Handling	✓
21	Long Duration Calls	✓
22	Early and Late Media	✓
23	Simultaneous Ringing	✓
24	Group Call Pickup	✓
25	Auto Attendant number dialing	✓

26	Call Queue	✓
27	Transcode Calls	✓
28	SIP-URI Calling	✓
29	Session Audits	✗

Legend

Supported	✓
Not Supported	✗

Caveats

Note the following items in relation to this Interop:

- OPUS codec with Asymmetric Payload negotiation is not supported. Hence, Customers are recommended to use Symmetric Payload type on both the ends.
- MS Teams does not support SIP-URI calling with Direct Routing. The SIP-URI testing has been done only from CUCM to MS Teams via SBC SWe Lite.

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/about-us

References

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

For additional information on Cisco Unified Communication Manager, please visit:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

For additional information on Ribbon SBC SWe Lite on AWS, please visit:
https://support.sonus.net/display/UXDOC90/Deploying+an+SBC+SWe+Lite+via+Amazon+Web+Services+-+AWS

For additional information on Teams, please visit:
Best Practice - Troubleshoot Issues with Microsoft Teams Direct Routing and Connect SBC Edge to Microsoft Teams Direct Routing

For detailed information about Twilio Elastic SIP Trunking and solutions, please visit:

https://www.twilio.com/sip-trunking, https://www.twilio.com/docs/sip-trunking and https://www.twilio.com/docs/sip-trunking/elastic-sip-trunking-solution-blueprints

Conclusion

This Interoperability Guide describes successful configuration for Twilio Elastic SIP Trunking interop involving Ribbon SBC SWe Lite on AWS, Cisco Unified Communication Manager and Microsoft Teams Direct Routing.

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 - additional configuration changes are possibly required to suit the exact deployment environment.