SBC Edge 1K_2K_SWe Edge R11.0 Interop with Cisco WebEx Calling : Interoperability Guide



Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
 - About Ribbon SBC Edge
 - About Cisco Webex
- Scope/Non-Goals
- Audience
- Prerequisites
- Product and Device Details
- Network Topology and E2E Flow Diagrams
 - Deployment Topology
 - Interoperability Test Lab Topology
 - Call Flow Diagram
- Document Workflow
- Installing Ribbon SBC Edge
 - Ribbon SBC Edge Configuration
 - Accessing SBC Edge
 - License and TLS Certificates
 - Installing License on SWe Edge
 - Installing license on SBC 1K/2K
 - SBC Certificate
 - Trusted CA Certificates
 - Networking Interfaces
 - Configure Static Routes
 - SBC Edge Configuration for PSTN side and Enterprise Solutions
 - Media List PSTN
 - SIP Profile PSTN
 - SIP Server Table PSTN
 - Call Routing Table PSTN
 - SIP Signaling Group PSTN
 - SIP Server Table PBX
 - Call Routing Table PBX
 - SIP Signaling Group PBX
 - SBC Edge Configuration for Cisco Webex Calling side
 - Node-Level Settings
 - TLS Profile
 - DNS Host
 - SDES-SRTP Profile Webex
 - Media Profiles Webex
 - Media List Webex
 - Message Manipulation
 - SIP Profile Webex
 - SIP Server Webex
 - Call Routing Table Webex
 - SIP Signaling Group Webex
 - Call Routing Table Entry
 - Multi-Tenant with Single IP / Multiple Port on SBC
 - TLS Certificates
 - TLS Profile
 - SIP Server Table Tenant2
 - Message Manipulation
 - Call Routing Table Tenant2 to PSTN
 - SIP Signaling Group Webex Tenant2
 - Call Routing
 - Multi-Tenant with Single IP and Port on SBC
 - TLS Certificates
 - TLS Profile
 - SIP Profile
 - Message Manipulation
 - Message Rule Table Entry for Tenant1
 - Signaling Group
 - Multi-Tenant with Multiple IP and Port on SBC
- Cisco Webex Calling Configuration
- Supplementary Services and Features Coverage
- Caveats
- Support
- References
- Conclusion

Interoperable Vendors



Copyright

© 2023 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 outlines the configuration best practices for the Ribbon SBC Edge when deployed with Cisco Webex Calling.

About Ribbon SBC Edge

The SBC Edge (SBC 1K, 2K, SWe Edge) provides best-in-class communications security with the convenience of deployment from popular virtual machine platforms as well as hosting in cloud environment. The SBC Edge dramatically simplifies the deployment of robust communications security services for SIP Trunking, Direct Routing, and Cloud UC services. SBC Edge operates natively in the Azure and AWS Cloud as well as on virtual machine platforms including Microsoft Hyper-V, VMware and Linux KVM.

About Cisco Webex

Webex Calling Cloud service (Webex Calling) supports "Bring Your Own PSTN" and Enterprise dialing using what is termed as a Local Gateway that is located at the edge of the customer's VoIP network. A local gateway is a SIP Session Border Controller that interworks with Webex Calling cloud service in specific ways. This Local gateway must operate using specified conditions with Webex Calling and this document suggests to OEM vendors the requirements to interoperate with Webex Calling Cloud services.

Scope/Non-Goals

This document provides configuration best practices for deploying Ribbon's SBC Edge for Cisco Webex Calling 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.

It is not the goal of this guide to provide detailed configurations that meet the requirements of every customer. Use this guide as a starting point, 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 the Ribbon SBC.

To perform this interop, you need to:

- use the graphical user interface (GUI) or command line interface (CLI) of the Ribbon product.
- understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- have SIP/RTP/SRTP to complete the configuration and for troubleshooting.

Note

This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this guide.

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC Edge
- Ribbon SBC Edge license
 - This interop requires the acquisition and application of SIP sessions, as documented at Working with License.
- Public IP addresses
- TLS certificates for SBC Edge
 - For more details, please visit Working with Certificates.
- Cisco Control Hub and Domain
 - Cisco Control Hub Premier license for the users.
 - For more details, contact Cisco Webex Support.

Product and Device Details

The configuration uses the following equipment and software:

Product	Appliance/ Application/ Tool	Software Version		
Ribbon SBC	SBC SWe Edge	11.0.2 build 99		
	SBC 1K/2K	11.0.1 build 634		
Cisco Webex	Cisco Control Hub	Build: 20230607-38bdcbf (mfe)		
	Cisco Webex Client	43.5.0.26155		
Third-party Equipment	Cisco Unified Communications Manager	12.5.1.11900-146		
	Poly VVX 601	5.8.2.4732		
Administration and Debugging Tools	Wireshark	3.4.9		

Network Topology and E2E Flow Diagrams

Deployment Topology

Œ

Note There can be more number of deployment topologies beyond those depicted below.

Single Webex Tenant and Single IP & Single Port on SBC



Multiple Webex Tenant and Single IP & Single Port on SBC



Multiple Webex Tenant and Multiple IPs / Ports on SBC



Interoperability Test Lab Topology



Call Flow Diagram



Document Workflow

The sections in this document follow the sequence below. Complete each section for the configuration to be successful.



Installing Ribbon SBC Edge

To deploy Ribbon SBC Edge instance, refer to Installing SBC Edge.

Ribbon SBC Edge Configuration

Accessing SBC Edge

Open any browser and enter the SBC Edge IP address.



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

00 noddin	Welcome to Ribbon SBC SWe Edge
	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 authed ingrested, and disclosed to authorized disc customer administrative, and law enforcement personnel, as well as authorized ficials 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 civili and criminal penalities. By continuing to use this system you indicate your avereness 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 admin Password] Login Cancel Copyright © 2010-2023 <u>Ribbon Communications Operating Company, Inc</u> , 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** pan el 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.

			14.1		
	Monitor Tasks	Settings	Diagnostics	System	
Current Licenses				Febr	uary 28, 20
Historical Usage Download License File		_	_		
ups License Format Version 3					
rel Settings	Fe	ature Licenses			
Total 7 Feature License Rows					
lew License Feature	Licensed	Total Licenses	Available Licenses	Feature Expiration	-
nagement SIP Signaling Sessions	₽	10	10	March 17, 2023 23:59:59	
Enhanced Media Sessions with Transc	oding 🔍	20	20	March 17, 2023 23:59:59	
Enhanced Media Sessions without Tra	nscoding 🛛	10	10	March 17, 2023 23:59:59	
SIP Registrations	₩.	10	10	March 17, 2023 23:59:59	
AMR-WB	V	Unlimited	Unlimited	March 17, 2023 23:59:59	
ping Tables SIP Recording	ų,	10	10	March 17, 2023 23:59:59	
virtual Direct Routing SBA	0	Not Licensed	Not Licensed	Not Applicable	

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

Installing License on SWe Edge

After receiving the license file, follow the below steps to apply license on SWe Edge.

- 1. From the Settings tab, navigate to System > Licensing > Install New License.
- 2. Upload the License file by selecting Choose File and click Apply.

Q Search	Install New License
Expand All Collapse All Reload	
Call Routing	License Key
Signaling Groups	
Metworking Interfaces	Select File Choose File No file chosen
🕨 🥖 Virtual DR SBA	Deboot strongly recommended following undated license installation
🔻 💋 System	Installing a license with reduced features may disrupt current configurations.
Node-Level Settings	
🔻 💋 Licensing	
Current Licenses	Decode Apply
Install New License	
🕨 📁 Software Management	

Installing license on SBC 1K/2K

Please ignore this step for SBC SWe Edge.

After receiving the license file, follow the below steps to apply license on SBC 1K/2K.

- 1. From the Settings tab, navigate to System > Licensing > Install New License.
- 2. Open the license file to get the license key and paste in the tab as shown in the snapshot.
- 3. Click Apply.

Q Search	Install New License
Expand All Collapse All Reload	
▶ 💋 Call Routing	License Key
Signaling Groups	
📁 Linked Signaling Groups	Paste license key text in the box:
Mode Interfaces	BEGIN LICENSE KEY
System	MIICWQYJKoZlhvcNAQcCoIICSjCCAkYCAQMxCzAJBgUrDgMCGgUAMIIBzwYJKoZlhvcNAQcBoIIB
Node-Level Settings	wASCAbstvQdgHEmWJSYvbcp7f0r15tfgdKElgGAIDNiQQBDswYJN5DjsHWIHIjmrKoHKZVZIXWYW ONtstphz3pwsffooL+09727b114091/21bw726FcPcSY2cmv976/four04/u+272(2H259A7vb
QoE	IOIIXidFtfzso93xzkdpvpxWs2J58dH6/Z8++Cj3+PoN04ePy+m+bLJU2q+bB69a4rPPpq37erR
USPs	3btXV1fjq3vjqr64u7ezs3v39/7i+evpPF9k28WyabPINP/lvjW7+a2PqLc0ffwsz9p1nTf8l/tb
System Timing	/3QtnM2OXp+9PHl81/3dbtKTWbnOj3Z3bBv5QAGbD2/R0dPXt+noqxfPzz64KxrTqx9WV0+On/2Q upr25auf64ft17tX11/+kLp6dfr6z0+pg5Pi19/cXG2Va9/7u5c3i2r/w6Xg2e/9+bYdPfz0gzt6
System Companding Law	+nr3Fh3tfvilXp89/2Gx+U+ePb3FmG7Zlf1LtO5jalnMivbaND5dztK72jL47vG3s3p2ITEGuzvT
Current Licenses	2c6nWf5w5+HBgwfn0/3z3enju14DfuF1XhdZ+WK9mOR19JWHDx7fDRqRDbqrRujo/wExYTBfAgED
License Keys	gBStGFB2wLG8m1GuSaAbryLtg2U6GjAJBgUrUgMCGgUAMAkGByqGSM44BAMELjAsAhQMIMbJ962j ooNEEisq1sTDE0P0OUJb5/J3AJJ1iO3iHEHbYaG+031CJEVa8sf
Install New License	END LICENSE KEY
Software Management	
Auth and Directory Services	
Protocols	
🕨 🏓 SIP	Reboot strongly recommended following updated license installation. Installing a license with reduced features may disput current configurations.
🕨 🏓 CAS	and any a neeree that readed reader of thay all appears and configurations.
Security	
🕨 🥖 Media	Decode
🕨 🧯 Tone Tables 🗸 🗸	

SBC Certificate

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

- 1. Provide the Common Name of the SBC that includes Host and Domain.
- 2. Set the Key Length to 2048 bits.
- 3. Provide the location information.
- 4. Click OK.
- 5. The CSR will be generated and displayed in the result text box.

Q Search	Generate Certificate Signing	Request						
Expand All Collapse All Reload	Subject Distinguished Name							
🕨 📁 Call Routing								
🕨 📁 Signaling Groups	Common Name	rbbn.in * Hostname or FODN						
Metworking Interfaces								
🕨 🃁 System	Subject Alternative Name DNS	comma-separated FQDN list						
Auth and Directory Services	Email Address							
🕨 🃁 Protocols								
🕨 🏓 SIP	ISO Country Code	India 🗸						
💌 🥟 Security	State/Province	Karanataka						
🕨 📁 Users								
🕨 📁 Login Messages	Locality	Bangalore e.g.: City						
▼	Organization	e.g.: Company						
Generate SBC Edge CSR								
SBC Primary Certificate	Organizational Unit	e.g.: Department						
ESBC Supplementary Certificates	Key Length	2048 bits 🗸						
Trusted CA Certificates								
TLS Profiles								
Change Password		or						
Ribbon Protect Bad Actors		OK						

After generating the CSR on Ribbon SBC, provide it to the Certificate Authority. CA would generally provide the following certificates:

- SBC CertificateCA's Root Certificate
- Intermediate Certificate



There are two ways to import SBC Primary Certificate as described below:

To import an X.509 signed certificate:

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

To import a PKCS12 Certificate and Key:

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

🔇 Import X.509 Server Certificate - Google Chrome		×		
A Not secure https://172.16.106.92/cgi/phpUl/config.php?cfg=/	views/system/uxServerCertificate	el		
Import X.509 Server Certificate	February 28, 2023 22:54:2	s 0	G Import X:509 Server Certificate - Google Chrome	X
Node Conviad Parte M			Not secure https://172.16.106.92/cgi/phpUI/config.php?cfg	=/views/system/uxServerCertificatel
			Import X.509 Server Certificate	February 28, 2023 22:54:28
			Made File Jalaad	
			Select File Chcose File No file chosen Extensions (pern der, ce	r. ber. p701 *
Paste Base64 Certificate				ОК
	// ×			
	OK			•
O Import PKCS12 S	Gerver Certificate - Google Chrome		- 🗆 ×	
A Not secure	https://172.16.106.92/cgi/php	oUI/co	fig.php?cfg=/views/system/uxServerCertificateImport	
Import PKCS12	2 Server Certificate		February 28, 2023 22:56:21 🔞	
Paseword				
Select File Choo	se File No file chosen	Extensio	s [.pfx or.p12] *	
			ОК	

Trusted CA Certificates

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

- For TLS to work, a Trusted CA (Certificate Authority) is required. For this interop, GoDaddy is used as Trusted CA.
- Add an entry in the Public DNS to resolve Ribbon SBC Edge FQDN to Public IP Address.
- Obtain Trusted Root certificate from your certification authority.
- In the trust store of the SBC, ensure you have the following certificates as part of the root certificate trust:
 - Cisco Control HUB Root R1
 - GlobalSign Root CA (if required)

Note
 Refer to Root Certificate - Cisco Webex.

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

\bigcirc							Migle	
ribbon		0	Monitor	Tasks	Settings	Diagnostics	System	se igo
Q Search	î	SBC Certificates Index						February 28, 2023 22:48:38 🔞
Expand All Collapse All Reload		Generate SBC Edge CSR						
Call Routing		SBC Primary Certificate						
 Gignaling Groups Wetworking Interfaces Metworking Interfaces 		 SBC Supplementary Certification Trusted CA Certificates 	tes					
Auth and Directory Services								
 Protocols SIP 								
V Security								
Login Messages Login Messages SBC Certificates Generate SBC Edge CSR SBC Primary Certificate SBC Supplementary Certificates								
Trusted CA Certificates								

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

- 1. To import a Trusted CA Certificate, click the Import Trusted CA Certificate (
- 2. Select File upload or copy paste for the menu listed.
- 3. If you choose File upload, browse the certificate and Click OK.

🔇 Import Trusted CA Certificate - Google Chrome	-		×	🔇 Import Trusted CA Certificate - Google Chrome	-		×
A Not secure https://172.16.106.92/cgi/phpUl/config.php?cfg=/views/sy	stem/trustedCAI	mport.x	:ml	A Not secure https://172.16.106.92/cgi/phpUl/config.php?cfg=/views/sy	stem/trustedC/	Almporta	cml
Import Trusted CA Certificate	March 01, 2023	13:23:0	7 0	Import Trusted CA Certificate	March 01, 202	3 13:23:4	5 0
Mode Copy and Paste	ОК	*		Mode File Upload V Select File Choose File No file chosen Extensions (pern, der, cer, ber, p76) * OK			

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.

Networking Interfaces

The SBC Edge 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 Edge 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 Edge 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 Edge system.

noddin		O Monitor	Tasks	Settings	Diagnostics	System		
Q Search	Logical Interfaces						February	28, 2023 23:07:49 🗘 📀
Expand All Collapse All Reload	🧹 💋 Create VLAN I/F 🗙	Total 5 Logic	calInterface Rows					
▶ 💋 Call Routing	Interface Name	IPv4 Address	1	Pv6 Address	Description	Admin State	Display	Primary Key
Signaling Groups	🕨 💼 🗖 Admin IP	172.1				Enabled	Counters	35
Vervoring menaces	Ethernet 1 IP	172.1				Enabled	Counters	36
Admin IP	Ethernet 2 IP	115.1				Enabled	Counters	37
Ethernet 2 IP	Ethernet 3 IP	10.10.10.10				Enabled	Counters	38
Ethernet 3 IP	Ethernet 4 IP	20.20.20.20				Enabled	Counters	39
Ethernet 4 IP								

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). In the default software, Ethernet 1 IP is enabled, and an IPv4 address is acquired through a connected DHCP server or you can assign a static IP as well.

\bigcirc		Help
noddin	O Monitor Tasks Settings Diagnos	stics System
Classes Al Solaces Al Reload Cal Routing Signaling Groups Classes Al Reload Cal Routing Signaling Groups Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload Classes Al Reload	Monitor Tasks Settings Diagnos Constraints Monitor Tasks Settings Diagnos Constraints Const	Enabled <u>Counters</u> 36
	Media Next Hop IP 172.1	

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. This interface will face towards Cisco Webex.

R								
	_		0					
nooon		Monitor lasks	Settings	Diagnostics	System			
Q Search Expand All Collapse All Reload	v D Ethernet 2 IP	115.1		1	Enabled	<u>Counters</u>	37	^
Excand All Collasse All Reload	Interface Name Ethernet 2 IP I/E Index 8 Alias Description Admin State Enabled MAC Address IP Addressing Mode IPv4 Informa IP Assign Method	Aentification/Status						
Emergency Services	Primary Address 115. Primary Netmask 255.255.2 Media Next Hop IP 115.	* жижи 255.192 * жижи * жижи						

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).

Destination IP

Specifies the destination IP address.

Mask

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

Gateway

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

Metric

Specifies the cost of this route and therefore indirectly specifies the preference of the route. Lower values indicate more preferred routes. The typical value is 1 for most static routes, indicating that static routes are preferred to dynamic routes.

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

Q Search	Static IP Route	Table			Marc	ch 24, 2023 20:39:31 🗘 📀
Expand All Collapse All Reload	+1 x	Total 47 IP Route Rows				Q Filter
▶ 💋 Call Routing	Row ID	Destination IP	Mask	Gateway	Metric	Primary Key
Signaling Groups	1	0.0.0.0	0.0.0.0		1	1
Virtual DR SBA	4	85	255.		1	4
🕨 🃁 System	5	85.	255.	1	1	5
Auth and Directory Services Directory Services Directory	6	128.	255.	1	1	6
🕨 📁 DNS	7	128.	255.		1	7
V IP	8	135.	255	1	1	8
Routing Table	9	135	255	1	1	9
Static ARP Access Control Lists	10	135	255		1	10
NAT	11	135.	255	1	1	11
▶ 💋 IPv6	12	135.	255.		1	12
Vetwork Monitoring SIP	13	135.	255		1	13

SBC Edge Configuration for PSTN side and Enterprise Solutions

Media List - PSTN

From the Settings tab, navigate to Media > Media List. Click the + icon at the top of the Media List View page.

- 1. Provide a name for the profile.
- 2. Attach the Media Profiles by clicking Add/Edit.
- 3. The SBC by default has G711A and G711U media profiles.
- 4. Click OK.

\bigcirc							d 1 tteip 1 met
noddin		O Monitor	Tasks	Settings	Diagnostics	System	٤
Q Search	Media List View						March 27, 2023 13:44:36 🗘 📀
Expand All Collapse All Reload	🕂 🗙 Total 3 Mee	dia List Rows					
Call Routing Signaling Groups Monorking Interfaces	Description Default Media List				Primary 1	Кеу	
Virtual DR SBA	👂 📄 🗌 Webex Media list				2		
 System Auth and Directory Services 	🔻 📋 📄 PSTN Media List				3		<u>×</u>
Protocols SIP Security	Description	PSTN Media List					
Media Media System Configuration Media Profiles SDES-STIP Profiles Media List Default Media List	Media Profiles List	G711A G711u	U Do Add, Rem	p Win Edit ove			
PSTN Media List	SDES-SRTP Profile	None	✓ Associa	ted SIP SG Listen Ports sho	uld be TLS only. 🔸		
Tone Tables	Media DSCP	46	* [063]				
Filephony Mapping Tables	Dead Call Detection	Disabled	~				
Configuration Superstand	Silence Suppression Enforce SG Codec Priority	Disabled	~		_		

SIP Profile - PSTN

SIP Profiles control how SBC Edge communicates with SIP devices. They control important characteristics, such as Session Timers, SIP Header Customization, SIP Timers, MIME Payloads, and Option Tags.

From the Settings tab, navigate to SIP > SIP Profiles. Click the + icon to create a new SIP Profile.

- 1. Provide a name for the profile in the Description field.
- 2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session.
- 3. Set Minimum Acceptable Timer to 600 and Offered Session Timer to 3600.
- 4. Click OK.

Ô						
ribbon		O Monitor Tasks	Settings	Diagnostics	System	
Q_Search Excend All Collarse All Reload > Coll Rooting > Coll Rooting > Signaling Groups	Description PSTN Session Timer Session Timer	ELIN Identifier	E Payloads	_		
	Minimum Acceptable Timer 600 * secs (80.7200) Offered Session Timer 3600 * secs (80.7200) Terminate On Refresh Falure False	PIDF-LO Passthrough Unknown Subtype Passthrough	Enable V Disable V			
Local Registrars Local Registrars Local Registrars SIR Profiles SIR Profiles Trunk Groups Nat Couling Prefit Tables Contact Registrant Table Contact Registrant Table Mode-Level SIP Settings SIP Recording SIP Recording SIP Recording SIP Recording SIP Recording SIP Recording	Header Customization FQDN in From Header Disable V FQDN in Contact Header Disable V Sand Assert Header Fuble V SBE Edge Diagnostics Header Enable V Trusted Interface Disable V Calling Info Source RFC Standard V Diversion Header Selection Last V Record Route Header RFC 3261 Standard V	Op 100rel Not Present v Path Not Present v Timer Supported v Update Supported v	ions Tags			
Tone Tables Tone Tables Telephony Mapping Tables StuffAutums Goging Configuration Emergency Services	Timers Transport Timeout Timer 5000 ms (5000.32000) Maximum Retransmissions RFC Standard V Redundancy Retry Timer Redundancy Retry Timer Redundancy Retry Timer Retransport ms (5000.160000) RFC Timers ms (100.100000) Timer T1 500 ms (100.10000) Timer T2 4000 ms (100.10000) Timer T3 5000 ms (100.10000) Timer T4 5000 ms (100.0000) Timer T4 Timer T4 5000 ms (100.0000) Timer T4 Timer T4 <td< td=""><td>SDP C Send Number of Audio Connection Info im Medja Section Origin Field Username Session Name Digit Transmission Preference SDP Handling Preference</td><td>Internation</td><td>mfouit: SBC eefouit:</td><td></td><td></td></td<>	SDP C Send Number of Audio Connection Info im Medja Section Origin Field Username Session Name Digit Transmission Preference SDP Handling Preference	Internation	mfouit: SBC eefouit:		

SIP Server Table - PSTN

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.

From the Settings tab, navigate to SIP > SIP Server Tables. Click the + icon to create a new SIP Server Table.

- 1. Provide a name for the SIP Server.
- 2. From the Type drop-down menu, choose SIP Server.
- 3. Click OK.

\bigcirc							Welcome: provin
riddon			O Monitor	Tasks	Settings	Diagnostics	System
Q Search	^	SIP Server Tables					
Expand All Collapse All Reload		🕂 🗙 Total 5 SIP Ser	ver Table Rows				
Call Routing	1	Description					Primary
Signaling Groups		Default SIP Server					1
Metworking Interfaces							2
Virtual DR SBA		PSIN					2
System							
Auth and Directory Services		Description DSTN					
Protocols		Description					
SIP		Type SIP Server 🗸					
Local / Pass-thru Auth Tables							
SIP Profiles						_	
SIP Server Tables					OK		
Trunk Groups					UN		

SIP Server Table Entry

1. Click on the SIP Server Table created in the previous step.

- 2. From the Create SIP Server drop-down menu, select IP/FQDN.
- 3. Provide IP Address and Port Number of the PSTN endpoint
- 4. Enable SIP OPTIONS by selecting SIP OPTIONS under transport section and click OK

noddin		O Monitor	Tasks	Settings	Diagnostics	System	t Login 1
Q Search Expand All Collapse All Reload Call Routing	PSTN Create SIP Server v I X 1/2 IP/FQDN	Total 1 SIP S	Server Row	Port	Protocol	Display Counters	Mar Priority
Signaling Groups Signaling Interfaces Networking Interfaces	DNS-SRV	IP/FQDN		5060	тср	Counters	1
System System Auth and Directory Services Protocols Cocal Registrars Local / Pass-thru Auth Tables SiP Profiles SiP Server Tables Default SIP Server PSTN	Server Server Lookup IP/FQDN Priority 1 Host FQDN/IP 10. Port 5060 Protocol TCP	* [1.65535] * (1.65535]		Monitor Keep Alive Frequency Recover Frequency Local Username Peer Username	SIP Options 30 * secs (30.300 5 * secs (5.300) Anonymous Anonymous	ן))* Local Username of SBC E)* Peer Username of sip ser	īdge ver
WEBEX Trunk Groups NAT Qualified Prefix Tables Remote Authorization Tables Contact Registrant Table Message Manipulation Node-Level SIP Settings Usten Port SIP Recording	Remote Authorization Table [Contact Registrant Table] Session URI Validation [tion and Contacts None Uberal	▼ + ▼ +	Reuse Tru Sockets 4 Reuse Timeout Fo	Connection Reus	e	
▶ 📁 Security							ОК

Call Routing Table - PSTN

Call Routing allows calls to be carried between Signaling Groups and 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).

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

1. Provide a name for the Routing Table and Click OK.

Q Search	Call Routing Tables
Expand All Collapse All Reload	🛶 🗙 👔 Total 4 Call Routing Table Rows
▼ 💋 Call Routing	Description
Transformation	Default Route Table
Call Routing Table Call Actions	V DSTN_TO_WEBEX
 Signaling Groups Networking Interfaces Virtual DR SBA 	Description PSTN_TO_WEBEX

SIP Signaling Group - PSTN

Signaling groups allow telephony channels to be grouped 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 Routing Tables are selected.

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

- 1. Attach the Call Routing Table CallRoutingTable-PSTN.
- 2. Attach the SIP Profile SIPProfile-PSTN.
- 3. Attach the SIP Server Table SIPServerTable-PSTN.
- 4. Attach the Media List ID MediaList-PSTN.
- 5. Configure Protocol and Listen Ports in the "Listen Ports" panel.

- 6. Associate the appropriate IP address in the "Signaling/Media Source IP" field. This address is used as the source IP for all SIP messages leaving the SBC Edge.
 - a. This specifies the Logical IP address at which SIP messages are received.
- 7. Federated IP addresses and FQDNs specified in a SIP Signaling Group are only allowed and configure the PSTN's address. The IP/FQDN specify which IP/FQDN can access the Signaling Group.

Description PSTN_SG	
Admin State Enabled Service Status Up	
SIP Channels and Routing	
	Media Information
Action Set Table None	
No. of Channels 30	DSP A
SIP Profile PSTN	Modes Direct
SIP Mode Basic Call	Proxy with Local SRTP
Agent Type Back-to-Back User Agent	Supported Proxy
SIP Server Table PSTN	Modes Viceo Application Direct
Notify Lync CAC Profile Disable	Media List ID PSTN Media List
Challenge Request Disable	Proxy Local SRTP Source Bestle ID None
Outbound Proxy IP/FQDN	Play Ringback Auto on 180
Outbound Proxy Port 5060	Tone Table Default Tone Table
Call Setup Response Timer 255	Play Congestion Disable
Call Proceeding Timer 180	Tone Each 192 Each
Forked Call Answered Too Soon Disable	Allow Refresh
	SDP Enable
SIP Recording	Music on Hold Disabled
SIP Recording Status Disabled	Multiplexing
	Media Codec Enable
	Latch
	Header Tables
	Mapping Tables
	SIP To Q.850 Override Table Default (RFC4497)
	Q.850 To SIP Override Table 503
	Pass-thru Peer SIP Response Code Enable
	SIP IP Details
	Teams Local Media Disable
	Optimization Schemet (ID
	Signaling/Media Source IP (172.16.107.92)
	Signaling DSCP 40
	NAT Traversal
	ICE Support Disabled
	Outbound NAT Traverral None
	Static NAT - Inbound
	Detection Disabled
Listen Ports	Federated IP/FQDN
779.5050	
Listen Port	Total 1 SIP Federated IP Row
· · · · ·	IP/FQDN Netmask/Prefix
	10 255.:
Message Manipulation Disabled	
Hessaye Hampulation Disabled	

(i) Note

'Proxy with local SRTP' is supported only in SBC SWe Edge, 'Proxy with Local SRTP' is used to switch the media stream between endpoints using SRTP media encryption on a call leg basis.

SIP Server Table - PBX

From the Settings tab, navigate to SIP > SIP Server Tables. Click the + icon to create a new SIP Server Table.

- 1. Provide a name for the SIP Server.
- 2. From the Type drop-down menu, choose SIP Server.
- 3. Click OK.

Q Search	SIP Server Tables
Expand All Collapse All Reload	+ X Total 4 SIP Server Table Rows
Call Routing Signaling Groups Networking Interfaces Virtual DR SBA	Description Default SIP Server PSTN
System Je Auth and Directory Services Je Protocols	WEBEX CUCM
SIP Local Registrars Local / Pass-thru Auth Tables SIP Profiles SIP Server Tables Trunk Groups Trunk Groups	Description CUCM Type SIP Server V
NAT Qualified Prefix Tables Remote Authorization Tables Contact Registrant Table	ОК

SIP Server Table Entry

- 1. From the Create SIP Server drop-down menu, select IP/FQDN.
- 2. Provide IP Address and Port Number of the PBX endpoint.

Q Search							Mar
Expand All Collapse All Reload	Create SIP Server 🔻 🗙 🥂	Total 1 SIP Server Row					
▶ 🍺 Call Routing	Host / Domain	Server Lookup		Port	Protocol	Display Counters	Priority
Signaling Groups	▼ 📋 🗌 10.54.22.250	IP/FQDN		5060	тср	Counters	1
Networking Interfaces							
Virtual DK SBA	Server Ho	ost			Transp	ort	
Auth and Directory Services							
Protocols	Server Lookup IP/FQDN			Monitor	SIP Options	~	
🔻 💋 SIP	Priority 1 🗸)	Keep Al	ve Frequency	30 * secs	(30300)	
📁 Local Registrars	Host FODN/IP 10.						
💋 Local / Pass-thru Auth Tables		1	Recov	er Frequency	5 * secs	[5=300]	
SIP Profiles	Port 5060	* [165535]	Lo	cal Username	Anonymous	* Local Username	of SBC Edge
V SIP Server Tables	Protocol TCP 🗸	•	P	eer Username	Anonymous	* Peer Username o	of sip server
E Default SIP Server							
WEREY		10			a a	B	
CUCM	Remote Authorization	h and Contacts			Connection	Reuse	
📁 Trunk Groups	Remote Authorization Table Nor	ne 🗸 +		Reuse Tru	• •		
📁 NAT Qualified Prefix Tables	Contract Desistment Table New			askata 4			
Remote Authorization Tables	Contact Registrant Table	······································		SOCKELS 4	•		
Contact Registrant Table	Session URI Validation Libe	eral 🗸	Reuse T	imeout For	ever 👻		
Message Manipulation			-	_			
Node-Level SIP Settings							
III Decording							ОК
SIP Recording							

Call Routing Table - PBX

Create a Call Routing Table to route the call from PBX to Webex.

Q Search	Call Routing Tables
Expand All Collapse All Reload	🐢 🗙 🔞 Total 4 Call Routing Table Rows
▼ 💋 Call Routing	Description
Transformation	👂 📋 🗋 Default Route Table
Time of Day Table	PSTN TO WEBEX
Call Actions	
Signaling Groups	V COCM_IO_WEBEX
Metworking Interfaces	
🕨 📁 Virtual DR SBA	Description CUCM_TO_WEBEX
🕨 📁 System	
Auth and Directory Services	
Protocols	
🕨 🃁 SIP	OK

SIP Signaling Group - PBX

SIP Profile and Media List which created for PSTN can be attached in the PBX Signaling group as well.

- 1. Attach the SIP Server Table SIPServerTable-PBX.
- 2. Attach the Call Routing Table CallRoutingTable-PBX.
- 3. Federated IP/FQDN should be configured with PBX's address.

Description CUCM Admin State Enabled Service Status Up	
SIP Channels and Routing	
Arias Cat Table - Name	Media Information
Call Routing Table CUCM_TO_WEBEX No. of Channels 30 SIP Profile PSTN SIP Mode Basic Call	Supported Audio Modes DSP * * Proxy Direct Proxy with Local SRTP *
Agent Type Back-to-Back User Agent SIP Server Table CUCM Load Balancing Round Robin Netic Luce CAC Particle Disable	Supported Video/Application Modes Proxy *
Challenge Request Disable Outbound Proxy IP/FQDN Outbound Proxy Port 5060	Proxy Local SRTP Crypto Profile ID Play Ringback Auto on 180 Tone Table Default Tone Table
Call Setup Response Timer 255 Call Proceeding Timer 180 Use Register as Keep Alive Enable	Play Congestion Tone Early 183 Disable
Forked Call Answered Too Soon Disable SIP Recording	Allow Refresh SDP Enable Music on Hold Disabled
SIP Recording Status Disabled	Multiplexing Disable Media Codec Latch Enable
	Mapping Tables SIP To Q.850 Override Table Default (RFC4497) Q.850 To SIP Override Table Default (RFC4497) Pass-thru Peer SIP Response Code Enable
	SIP IP Details
	Teams Local Media Optimization Disable Signaling/Media Source IP Ethernet 1 IP (172.16.107.92) Signaling DSCP 40 MAT Traversal ICE Support ICE Support Disabled Outbound None Outbound NAT ICE Static NAT - Inbound Detection Disabled Information
Listen Ports	Federated IP/FQDN
TCP-5080	Total 1 SIP Federated IP Row
· · · · · · · · · · · · · · · · · · ·	IP/FQDN Netmask/Prefix 10.: 255.
Message Manipulation Disabled	

Note

'Proxy with local SRTP' is supported only in SBC SWe Edge, Proxy with Local SRTP is used to switch the media stream between endpoints using SRTP media encryption on a call leg basis.

SBC Edge Configuration for Cisco Webex Calling side

Node-Level Settings

From the Settings tab, navigate to System > Node-Level Settings.

- 1. From the Use Primary DNS drop-down menu, select Yes.
- 2. Provide the Primary DNS IP address and select the Ethernet pointing towards the Cisco Webex.
- 3. Configure the Host name and Domain name based on the name of the tenant1's FQDN.
- 4. Provide the desire NTP (Network Time Protocol) server, used for clock synchronization.

For SBC SWe Edge, refer to the snapshot below.

Ô		Contraction of the second s
noddin	💿 Monitor 🛛 Tasks 🛛 Se	ettings Diagnostics System
Q Search	Set Date/Time Backup Config Restore Config Clear DNS Cache	
Expand All Collapse All Reload	Host Information	Domain Name Service
Call Routing Call Routing Call Routing Call Routing Networking Interfaces System Call Route-Level Settings Call Route-Lev	Host Name t Domain Name rbbn.in System Information System Location System Contact	Use Primary DNS Yes Primary Server IP S.8.8.8 Primary Server IP Primary Server Ethernet 2 IP (115. (V) Use Secondary DNS No V
Protock December Ventres Protock SiP Security Media Tone Tables Shift Airms Source Ventres Source Ventres Source Ventres Emergency Services	Time Management Time Zone (GMT-5:30) India, Sri Lanka Network Time Protocol Use NTP VE V NTP Server 172. NTP Server Authentication Disabled NTP Server 2 V Use NTP Server 2 No	Ribbon Application Management Platform (RAMP) Connect to RAMP No
	Country Level Information Country Code United States	
		Apply

For SBC 1K/2K, refer to the snapshot below.

Q Search.	Node-Level Settings	
Expand All Collapse All Reload	Set Date/Time Backup Config Restore Config Clear DNS Cache	
Call Routing	Host Information	Domain Name Service
Signang Groups Groups Groups Groups Googlanding Groups	Host Name t ribbn.in Domain Name ribbn.in 	Use Primary DNS Yes Primary Server IP 88.8.8 Occur or sector Primary Source Ethernet 2 IP (115. Use Secondary DNS No
System Timing System Companding Law System Companding Law Software Management	System Location	Enable DNS Service No V
	Time Management Time Zone ((SIMT+5:30) India, Sri Lanka Network Time Protocol Use NTP Yes NTP Server 172. NTP Server 172. NTP Server 4uthentication Disabled NTP Server 2 Use NTP Server 2 No	Ribbon Application Management Platform (RAMP) Connect to RAMP No
	System LEDs	DHCP Server
	Power LED Green Alarm LED Blinking Red Ready LED Green Locator LED On Green	Enable DHCP Server No 🗸
	Country Level Information	
	Country Code None	

TLS Profile

The TLS profile defines the crypto parameters for the SIP protocol.

TLS Profiles are used by SIP Signaling Groups when the TLS transport type is selected for incoming and outgoing SIP trunks (Listen Ports), and in SI P Server Tables when TLS is selected as the Server Host protocol.

From the Settings tab, navigate to Security > TLS Profiles. Click the + icon to create a new TLS profile.

- 1. From the TLS Protocol drop-down menu, select TLS 1.0-1.2.
- 2. Attach the certificate which is uploaded in the SBC Certificate.
- 3. Add the cipher suites that are supported on Cisco Webex.
- 4. Enable the Validate Server and Client FQDN fields to validate the CN and SAN name in the certificate send by Server and Client.
- 5. Click OK.

Q Search	TLS Profile	
Expand All Collapse All Reload	🕂 🗙 Total 2 TLS Profile Rows	
Call Routing	Description	
Signaling Groups	Default TLS Profile	
Virtual DR SBA	v 📋 🗋 Webex_TLS	
🕨 💋 System	TLS Parameters	
 Auth and Directory Services Protocols 	Common Attailudes	
SIP	TLS Protocol TLS 1.2 Only V Mutual Authentication Enabled V	
🕨 📁 Login Messages	Handshake Inactivity Timeout 10 secs (1.30)	
SBC Certificates	Certificate SBC Edge Certificate	
Default TLS Profile Webex_TLS Change Password Ribbon Protect Bad Actors Media Media Media Media Media Media Media Logging Configuration Media M	Client Attributes	
	Validate Server FQDN Enabled	
	Server Attribute	
	Validate Client FQDN Enabled	

Note

The SBC doesn't support tracking active/closed TLS connections.

DNS Host

To Validate the Client FQDN, add the FQDN entries and corresponding IPs that are resolved from the Cisco Webex SRV under the Host section on the SBC.

DNS host on SBC SWe Edge:

Q Search	Hosts Table	
Expand All Collapse All Reload	Total 4 Host Entry Rows	
🕨 🃁 Call Routing	FQDN/Host Name	IP Address
Signaling Groups		139.
Networking Interfaces		139.
Virtual DR SBA		120
Auth and Directory Services		135.
Vertical Protocols	i	139.
V DNS		
Hosts		

DNS host on SBC 1K/2K:

Please ignore this step for SBC SWe Edge. In SBC 1K/2K, the Dynamic Refresh should be configured as No.

 System 	🕂 🗙 Total 4 Host Entry Rows			
Auth and Directory Services	EQDN/Host Name 🔻	IP Address	Dynamic Refresh	Primary Key
V V DNS	C	139.	No	3
Hosts		139.17	No	5
DNS Table		139.	No	4
🕨 🏓 IP		139.	No	1

SDES-SRTP Profile - Webex

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

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

- 1. Provide a name for the profile in the Description field.
- 2. 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.
- 3. Operation Option should be **Required**.
- 4. Set the Key Identifier Length to 0 to disable the MKI in SDP.
- 5. Click OK.

For SBC SWe Edge, refer to the snapshot below.

noddin		O Monitor	Tasks	Settings	Dia
Q Search	SDES-SRTP Profiles				
Expand All Collapse All Reload	🚽 I 🗙 Total :	1 SDES-SRTP Profile Row		_	
▶ 🥖 Call Routing	Description		Crypto Suite		
Signaling Groups	v 📄 🗌 Webex_Cryp	to	AES_CM_12	8_HMAC_SHA1_80	
Virtual DR SBA					
System		SRTP Confi	g		
Auth and Directory Services					
Protocols	Description	Webex_Crypto			
🕨 📁 SIP	Operation Option	Required	~		
Security		AES_CM_128_HMAC_SHA1_80	*		
Media System Configuration			Add/Edit		
Media Profiles	Crypto Suite		Remove		
SDES-SRTP Profiles			-		
Webex_Crypto					
🕨 📁 Media List		Master Key			
🕨 🃁 Tone Tables	Key Identifier Length	0 🗸			
Telephony Mapping Tables					
🕨 📁 SNMP/Alarms					
[] Logging Configuration []					
Emergency Services				0	



E in Call Routing	Description		Crypto Suite
Signaling Groups	webex Crypt	0	AES_CM_128_HMAC_SHA1_80
📁 Linked Signaling Groups			
Mode Interfaces		CDTD Confi	-
🕨 📁 System		SKIPCONI	9
Auth and Directory Services			
Protocols	Description	Webex Crypto	
🕨 🃁 SIP	Operation Option	Required	~
🕨 🥩 CAS	Crynto Suite	AFS CM 128 HMAC SHA1	80 ×
Security	crypto Suite	Ac5_CM_120_NMAC_SHAT	
💌 🥪 Media		Master Key	
Media System Configuration	Master Key Lifetime	Set 🗸	
🕨 📁 Media Profiles		231	
SDES-SRTP Profiles	Lifetime Value	2	
Webex Crypto	Derivation Rate	0 ~	
DTLS-SRTP Profiles	Key Identifier Length	0 ~	
🕨 📁 Media List			
Jone Tables			
Telephony Mapping Tables			
▶ 💋 SNMP/Alarms			ОК

Media Profiles - Webex

Media Profiles allow you to specify the individual voice and fax compression codecs and their associated settings, for inclusion in a Media List.

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

ç) ribbon		O Monitor	Tasks	Settings	Diagnostics	System		rta a A Edge
Q Search	Media Profiles						March 01, 2023 11:33:30	00
Expand All Collapse All Reload	Create Media Profile 🔻 🛛 🗙	Total 4 Media	Profile Rows					_
Call Routing	Voice Codec Profile			Description			Primary Key	
Signaling Groups	Fax Codec Profile			Default G711A			1	
▶ j System	G.711 μ-Law			Default G711u			2	
Auth and Directory Services	▶ 💼 🗆 G.722 WB			G.722			3	
Protocois Ø SIP	🕨 📋 🗌 Opus			OPUS			4	
Security Security Media System Configuration Media Profiles Media Profiles Orball 0711A Defaul 0711u								
G.722								

For G.711U-Law and G.711A-Law, the SBC Edge has default profiles.

For G722:

- 1. Provide the profile's description.
- 2. Select G.722 from the Codec drop-down menu.
- 3. Click OK.

Vo	ice Codec Configuration	
escription	G.722	
Codec	G.722 🗸	
Rate	64000 b/s	
yload Size	20 ms	
	escription Codec Rate yload Size	escription G.722 Codec G.722 Rate 64000 b/s yload Size 20 ms

Media List - Webex

Media Profiles specify the individual voice and fax compression codecs and their associated settings for inclusion into a Media List. Different codecs provide varying levels of compression, allowing the reduction of bandwidth requirements.

- Select Settings > Media > Media List.
- Create a media list with desired descriptions "Webex Media List", add the media profile List, and attach the SDES-SRTP Profile "Webex_Cr ypto".

Q Search	Media List View	
Expand All Collapse All Reload	💠 🗙 Total 3 Media List Rows	
Call Routing Signaling Groups Networking Interfaces Virtual DR SBA	Description Default Media List Webex Media list	Primary 1 2
System System Auth and Directory Services Protocols SIP Security Media Media System Configuration Media System Configuration SDES-SRTP Profiles SDES-SRTP Profiles	Description Webex Media list G711A G711U G.722 Up Down Add/Edit Remove	
Default Media List Webex Media List PSTN Media List PSTN Media List Tone Tables STRP/Alarms Coging Configuration	SDES-SRTP Profile Webex_Crypto Associated SIP SG Listen Ports should be TLS only. Media DSCP 46 * [0.63] Dead Call Detection Disabled * Silence Suppression Disabled * Enforce SG Codec Priority Disabled *	

Message Manipulation

a) IP to FQDN Conversion in P-Asserted-Identity

The Message Manipulation is used convert IP to tenant1's FQDN in the P-Asserted-Identity.

Condition Rule Table

Condition Rule Tables are used to apply the Message Manipulation only if the provided conditions are matched.

Here, the Condition Rule Table is used to match Tenant1 Cisco Webex's number.

From the Settings tab, navigate to SIP > Message Manipulation > Condition Rule Table. Click the + icon to create a new Condition Rule Table.

- 1. Provide a name for the Rule table.
- 2. From the Match Type drop-down menu, select to.uri.userinfo.user.
- 3. Under Operation, select Regex.
- 4. Under Match Regex, enter Tenant1's number.
- 5. Click OK.

System Auth and Directory Services	-	Condition Rule Table		
Protocols		Total 2 Condition Rule 1	able Rows	
V SIP		Match Type	Operation	Match Value Type
 Local / Pass-thru Auth Table SIP Profiles SIP Server Tables 	s	v i to.uri.userinfo.user	Regex	N/A
 Trunk Groups NAT Qualified Prefix Tables Remote Authorization Table Contact Registrant Table Message Manipulation 	5	Description Tenant1 Num Match Type		
 Message Rule Tables Condition Rule Table Tenant1 Num 408 to 503 		Match Type to.uri.userinfo.user Operation Regex		
 Node-Level SIP Settings Multiple Listen Port SIP Recording 		Match Regex 18919122452	¥	
 ▶				ОК

Message Rule Table

From the Settings tab, navigate to SIP > Message Manipulation > Message Rule Table. Click the + icon to create a Message Rule Table.

- 1. Provide a description for the Rule Table.
- 2. Apply the message rule to All Messages, since the P-Asserted-Identity has to be changed on all the messages.
- 3. Click OK.

Q Search	^ !	SIP Message Rule Table		
Expand All Collapse All Reload		🕴 🗙 Test Selected Tables	Total 2 SIP Message Manipu	lation Table Rows
Call Routing		Description		Result Type
 Signaling Groups Networking Interfaces 		V 📄 🗌 PAI IP to FQDN		Mandatory
▶ 💋 Virtual DR SBA ▶ 💋 System	10	Test Message		
 Auth and Directory Services Protocols 		Description PAI IP to FD	QN	
SIP		Applicable Messages All Message	s 🗸	
 Local Registrars Local / Pass-thru Auth Tables SIP Profiles SIP Server Tables 	-	Table Result Type Mandatory	v	
Trunk Groups NAT Qualified Prefix Tables Remote Authorization Tables	1111			ОК
Contact Registrant Table Contact Registrant Table Condition Contact Registrant Table Condition Rule Table Condition Rule Table		408 to 503		Mandatory

Message Rule Table Entry

Header Rule:

- 1. Select Message Rule Tables > PAI IP to FQDN.
- 2. From the Create Rule drop-down menu, select Header Rule.
- Under Condition Expression> Add/Edit and select Message Rule Condition > Match all Condition and from the drop-down menu, select the condition rule as Tenant1 Num.
- 4. Select Header Action as Modify and Header Name as P-Preferrred-Identity.
- 5. Under Header Value > URI Host, select Modify.
- 6. Click on Add/Edit. Under the Edit Message Field, set Type of Value as Literal and Value as Tenant1's FQDN.
- 7. Click OK and Apply.

O Search	PAI IP to	FDON						
Expand All I Collapse All I Reload	101	Create Rule 💌 🔀	/ Test Mess	age	Total 1 Message	Manipulation Rules R	ow	
		Handes Dala	Pule Type			Result Type		Description
Call Routing		Header Kule	cule Type			Result Type		Description
Signaling Groups	🔻 🛄 🗆	Request Line Rule	Header Rule			Mandatory		PPI IP to F
Vidual DB SBA		Status Line Rule						
System			-					
Auth and Directory Services		Raw Message Rule	FQDN					
Protocols	Con	dition Expression Add	'Edit] '\${1}'					
V 🖉 SIP		Admin State Enab	ed	~				
🥖 Local Registrars		Result Type Man	latory	~				_
📁 Local / Pass-thru Auth Tables		Header Action Mod	fv	~	Edit Message Field	1		
🕨 🃁 SIP Profiles		Header Name P.As	erted-Identity					
🕨 🃁 SIP Server Tables	Handar	Ordinal Number 1st		v *				
Dirunk Groups	Header	ordinal Number		•	Type of Value	teral	v	
NAT Qualified Prefix Tables					Value S			
Remote Authorization Tables	🔻 Hea	der Value						
Contact Registrant Table							_	
Vessage Manipulation	D	isplay Name Ignore	~					
Message Rule Tables PAUR to EDON	• •	P URI					OK	Canad
408 to 502		URI Scheme	lanore	×			UK	Cancer
		k URT User Tofo	Ignore					
Condition Rule Table		p ond oser into	ignore	•				
Node-Level SIP Settings		URI Host	Modify	~	Add/Edit is			
Listen Port		URI Port	Ignore	~				
SIP Recording			4 1×		Total O SPRUriParam Roy	15		
Security			T 10					
Media		LIPI Parameters		Name	Value	•	Action	
Tone Tables		ond Parameters						
Telephony Mapping Tables					Table	e is empty		

b) 408 Request Time-Out to 503 Service Unavailable

 Note 	
	 The SBC doesn't generate an alarm and the inactive node is not removed from call routing when a 408 response is received from the Webex node for SIP OPTIONS. It is recommended to use the SMM given below to convert 408 Request Time-out to 503 Service Unavailable.

Condition Rule Table

The Condition Rule Table is here to match the 408 response that is coming only for SIP OPTIONS.

From the Settings tab, navigate to SIP > Message Manipulation > Condition Rule Table. Click the + icon to create a new Condition Rule Table.

- 1. Provide a name to Rule table.
- 2. From the Match Type drop-down menu, select CSeq.
- 3. Under Operation, select Regex.
- 4. Under Match Regex, give the regular expression as [0-9] OPTIONS.
- 5. Click OK.

Q Search	Condition Rule Table		
Expand All Collapse All Reload	Total 2 Condition Rule	Table Rows	
▶ 🥬 Call Routing	Match Type	Operation	Match Value Type
Signaling Groups	to.uri.userinfo.user	Regex	N/A
Virtual DR SBA	🔻 📋 🗌 cseq	Regex	N/A
▶ 🥖 System			
Auth and Directory Services	Description 400 to 502		
Protocols	Description 408 to 505		
 SIP Local Registrars Local / Pass-thru Auth Tables SIP Profiles SIP Server Tables Trunk Groups NAT Qualified Prefix Tables Remote Authorization Tables Contact Registrant Table Contact Registrant Table Message Manipulation Message Rule Tables Condition Rule Table 	Match Type Match Type Operation Match Regex [0-9] OPTIONS		
Tenant1 Num 408 to 503			ОК

Message Rule Table

From the Settings tab, navigate to SIP > Message Manipulation > Message Rule Table. Click the + icon to create a Message Rule Table.

- 1. Provide a description for the Rule Table.
- 2. Apply the message rule to Selected Messages.
- 3. Under Message Selection, click on Add/Edit and select 408 Request Timeout.
- 4. Click OK.

Q Search	-	SIP Message Rule Table	
Expand All Collapse All Reload		💠 🗙 Test Selected Tables Total 2 SIP Message I	Manipulation Table Rows
Call Routing		Description	Result Type
Signaling Groups Networking Interfaces		PAI IP to FQDN	Mandatory
▶ 📁 Virtual DR SBA ▶ 📁 System		V 0 10 303	Handatory
Auth and Directory Services protocols		Description 408 to 503 Applicable Messages Selected Messages	1
V Coral Registrars		408 Request Timeout	
 Local / Pass-thru Auth Tables SIP Profiles SIP Server Tables 		Message Selection	Add/Edit Remove
 Trunk Groups NAT Qualified Prefix Tables 		Table Result Type Mandatory	-
Remote Authorization Tables Contact Registrant Table		Honorory -	<u>,</u>
Message Rule Tables PAI IP to FQDN			
e 408 to 503			

Message Rule Table Entry

Status Line Rule:

- 1. Click on the Message Rule Table 408 to 503.
- 2. From the Create Rule drop-down menu, select Status Line Rule.

- Under Condition Expression> Add/Edit, select Message Rule Condition > Match all Condition, and from the drop-down menu, select the condition rule as 408 to 503.
- 4. Under Status Line Value > Modify > Add/Edit, set Type of Value as Literal and Value as 503 Service Unavailable.
- 5. Click OK.

Q Search	4	408 to 503	
Expand All Collapse All Reload	F	🗸 🔗 Create Rule 🔻 🗶 🥂 Test Message 🛛 🛛 Total 1 Message	Manipulation Rule
Call Routing	F	Admin State Rule Type	Result Type
🕨 📁 Signaling Groups		▼ 📋 🗍 🖳 Status Line Rule	Mandatory
Metworking Interfaces			
Virtual DR SBA		Test Kule	
System			
Auth and Directory Services		Message Rule Condition	
Protocols		Description 408 to 503 Match all Conditions	
T 💋 SIP		Condition Expression Add/Edit (5/2)	
📁 Local Registrars		408 to 503	+ × 4
📁 Local / Pass-thru Auth Tables		Admin State Enabled	
SIP Profiles		Result Type Mandatory 🗸	
SIP Server Tables			Apply Cancel
Dirunk Groups			
NAT Qualified Prefix Tables		♦ Status Line Value Modify ✓ Add/Edit 'SIP/2.0 503 Service Units	vailable
prote Authorization Tables		Edit Message Field	
💋 Contact Registrant Table			
▼		Type of Value Literal	
Message Rule Tables		Value SIP/2.0 S03 Service Unavai	
PPI IP to FDQN	11		
(a) 408 to 503		OK Cancel	

SIP Profile - Webex

From the Settings tab, navigate to SIP > SIP Profiles. Click the + icon to create a new SIP Profile.

- 1. Provide a name for the profile in the Description field.
- 2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session.
- 3. Set Minimum Acceptable Timer to 600 and Offered Session Timer to 3600.
- 4. From the FQDN in From Header drop-down menu, select SBC Edge FQDN, so that sip Messages from SBC Edge to Webex will have SBC FQDN in From header
- 5. From the FQDN in Contact Header drop-down menu, select SBC FQDN, so that sip Messages from SBC Edge to Webex will have SBC FQDN in Contact header.
- 6. Click OK.



SIP Server - Webex

From the Settings tab, navigate to SIP > SIP Server Tables. Click the + icon to create a new SIP Server Table.

- 1. Provide a name for the SIP Server.
- 2. From the Type drop-down menu, select SIP Server.
- 3. Click OK.

Q Search	SIP Server Tables
Expand All Collapse All Reload	+ X Total 3 SIP Server Table Rows
Call Routing Signaling Groups Networking Interfaces Virtual DR SBA	Description Default SIP Server PSTN
 System Auth and Directory Services Protocols Cocal Registrars Local / Pass-thru Auth Tables SIP Profiles SIP Profiles Default SIP Server Tables PSTN WEBEX 	VEBEX Description WEBEX Type SIP Server OK

SIP Server Table Entry

- 1. Click on the SIP Server Table created in the previous step.
- 2. From the Create SIP Server drop-down menu, select DNS-SRV.
- 3. Provide the SRV of the Cisco Webex and service of the SRV as sips.
- 4. Select the Protocol as TLS and attach the TLS profile which was created previously.
- 5. Under the Transport section, enable sip OPTIONS by selecting SIP OPTIONS from the Monitor drop-down menu, and set the Local username as SBC host name and the Peer Username as Webex.
- 6. Click OK.

Q Search	WEBEX					Ma
Expand All Collapse All Reload	Create SIP Server 🔻	X 1 🖉 Total 1 SIP Server Row				
▶ 💋 Call Routing	IP/FQDN		Server Lookup	Port	Protocol	Display Counters
Signaling Groups	DNS-SRV	ect.bcld.webex.com	DNS SRV	N/A	TLS	Counters
Metworking Interfaces						
Virtual DR SBA		Server Host		Transpo	ort	
V System						
Auth and Directory Services	Server Lookup	DNS SRV	Monitor SIP C	Options	~	
	Host IP Version	IPv4 V	Kana Aliva Francisco 20		20. 2001	
Docal Registrars	Demais Name/FODN		Keep Alive Frequency	^ secs (:	30300/	
📁 Local / Pass-thru Auth Tables	Domain Name/PQDN	.webex.com	Recover Frequency 5	* secs (5300]	
SIP Profiles	Service Name	sips *	Local Username t		* Local Usern	ame of SBC Edge
V SIP Server Tables	Protocol	TLS 🗸 *	Dens Hannan and Invelo			
C Default SIP Server	TI S Profile	Default TIS Profile 🛛 🖌 📥	Peer Username Web	ex	 Peer Userno 	ame of sip server
E PSTN	res Frome					
C WEBEX						
Dirunk Groups	Remote A	Authorization and Contacts	Co	nnection	Reuse	
NAT Qualified Prefix Tables				_		
Remote Authorization Tables	Remote Authorization	Table None 👻 🕇	Reuse True	~		
Contact Registrant Table	Contact Registrant	Table None 💙 🕇	Sockets 4	~		
Message Manipulation	Section UPI Valid	dation Liberal	Pauce Timeout Ecrever			
Node-Level SIP Settings	Session ORI Vallo		Reuse rimeout Forever	•		
Listen Port						

Call Routing Table - Webex

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

- 1. Provide a name for the Routing Table.
- 2. Click OK.

Q Search	Call Routing Tables
Expand All Collapse All Reload	Total 4 Call Routing Table Rows
Call Routing	Description
Figure Transformation	🕨 📋 🗋 Default Route Table
Call Routing Table	PSTN_TO_WEBEX
C Default Route Table	CUCM_TO_WEBEX
	WEBEX_TO_PSTN&CUCM
WEBEX_TO_PSTN&CUCM	
Call Actions	
🕨 🥖 Signaling Groups	Description WEBEX_TO_PSTN&COCM
Metworking Interfaces	
🕨 🥩 Virtual DR SBA	
🕨 🧊 System	ОК
Auth and Directory Services	

SIP Signaling Group - Webex

From the Settings tab, navigate to Signaling Groups. Click Add SIP SG.

- 1. Attach the Call Routing Table (CallRoutingTable-Webex).
- 2. Attach the Sip Profile (SipProfile-Webex).
- 3. Attach the SIP Server Table (SIPServerTable-PSTN).
- 4. Attach the SDES-SRTP Profile (SDES-SRTPProfile-Webex).

- 5. Attach the Media List (MediaList-Webex).
- 6. Associate the appropriate IP address in the "Signaling/Media Source IP" field.
- 7. Configure Protocol and Listen Ports in the "Listen Ports" panel.
- 8. Create an entry in the Federated IP/FQDN panel.
- 9. Enable Message Manipulation and attach the profile "PAI IP to FQDN" and "408 to 503" in the outbound Message Manipulation Table List.

10. Click OK.

Description WEBEX_SG	
Admin State Enabled	
Service Status Up	
SIP Channels and Routing	
on channels and routing	Hadia Information
Action Set Table None	weda information
Call Routing Table WEBEX TO PSTN&CUCM	
No. of Channels 30	DSP A
STD Drofile Webey	Modes Direct
STO Made Basis Call	Proxy with Local SRTP 🔍
SIP Model Basic Call	Council Dama
Agent Type Back-to-back Oser Agent	Video/Application Direct
SIP Server lable WEEK	Modes 👻
Load Balancing Priority: Register All	Media List ID Webex Media list
Notify Lync CAC Profile Disable	Proxy Local SRTP
Challenge Request Disable	Crypto Profile ID Webex_Crypto
Outbound Proxy IP/FQDN	Play Ringback Auto on 180
Outbound Proxy Port 5060	Tone Table Default Tone Table
Call Setup Response Timer 255	Play Congestion Disable
Call Proceeding Timer 180	Tone
Use Register as Keep Alive Enable	Early 183 Disable
Forked Call Answered Too Soon Disable	Allow Refresh
SIP Recording	SUP
Sir Recording	Music on Hold Disabled
SIP Recording Status Disabled	Multiplexing Disable
our recording status inserted	Media Codec
	Latch Enable
	Hanalas Tablas
	Mapping Tables
	CID To O SEO Oversida Table - Default (RECUMPT)
	0 850 To CID Quantida Table CO2
	Greate to ath overlige rapie and
	Deve about David CID Devenues Code - Family
	Pass-thru Peer SIP Response Code Enable
	Pass-thru Peer SIP Response Code Enable
	Pass-thru Peer SIP Response Code Enable SIP IP Details
	Pass-thru Peer SIP Response Code Enable SIP IP Details
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Disable
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Disable Signaling/Media Source IP Ethernet 2 IP (115)
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115, Signaling DSCP, 40, Signaling DSCP, 40, Signaling D
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 Ethernet 2 IP (115. Signaling DSCP (115. Signaling DSC
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Static NAT - Outbound
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Static NAT - Outbound Outbound NAT Traversal None
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Static NAT - Outbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Disabled
	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Disabled
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 -NAT Traversal ICE Support Disabled -Static NAT - Outbound Outbound NAT Traversal None -Static NAT - Inbound Detection Disabled Federated IP/FQDN
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Disable Signaling/Media Source IP Ethernet 2 IP (115. Signaling/Media Source IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Outbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Signaling/Media Source IP Signaling/Media Source IP Signaling/Media Source IP Signaling DSCP NAT Traversal ICE Support Outbound NAT Traversal Outbound NAT Traversal Outbound NAT Traversal Detection Disabled Detection Disabled
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN Total 1 SIP Federated IP Row IP/FQDN Netmask/Prefix
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN Total 1 SIP Federated IP Row IP/FQDN Netmask/Prefix
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Outbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN Federated IP/FQDN Total 1 SIP Federated IP Row IP/FQDN Netmask/Prefix 85. 255.
Listen Ports	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115. Signaling/Media Source IP Ethernet 2 IP (115. Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40
Listen Ports Listen Port	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Disable Signaling/Media Source IP Ethernet 2 IP (115, Signaling DSCP 40 NAT Traversal ICE Support ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Detection Disabled Federated IP/FQDN Federated IP/FQDN IP/FQDN Netmask/Prefix Static Detection Disabled
Listen Ports Listen Port	Pass-thru Peer SIP Response Code Enable SIP IP Details Disable Optimization Disable Signaling/Media Source 1P Ethernet 2 IP Signaling DSCP 40 -NAT Traversal ICE Support ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Detection Disabled Federated IP/FQDN Netmask/Prefix 85. 255.
Listen Ports Listen Port Listen Port Message Manipulation Enabled Inbound Message Manipulation	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Disable Signaling/Media Source IP Ethernet 2 IP (115. Signaling DSCP 40 MAT Traversal ICE Support ICE Support Disabled Outbound NAT Traversal None Static NAT - Outbound Outbound Detection Disabled Pederated IP/FQDN Federated IP/FQDN IP/FQDN Netmask/Prefix 85.: 255.:*****
Listen Ports Listen Port Liste	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115, Signaling DSCP 40 -NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN Total 1 SIP Pederated IP Row IP/FQON Netmask/Prefix 85
Listen Ports Listen Port Listen Port Listen Port II.S-5001	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Optimization Signaling/Media Source IP Signaling/Media Source IP Signaling/Media Source IP Signaling DSCP 40 -NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN Total 1 SIP Federated IP Row IP/FQDN Netmask/Prefix B3: Outbound Message Manipulation
Listen Ports Listen Port Listen Port Listen Port Message Manipulation Enabled Inbound Message Manipulation	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Disable Optimization Signaling/Media Source IP Ethernet 2 IP (115, Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Federated IP/FQDN Federated IP/FQDN Fotal 1 SIP Federated IP Row IP/FQDN Netmask/Prefix 85::::::::::::::::::::::::::::::::::::
Listen Ports Listen Port Message Manipulation Inbound Message Manipulation Message Table List	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Disable Signaling/Media Source IP Ethernet 2 IP (115, Signaling DSCP 40 NAT Traversal ICE Support Disabled Outbound NAT Traversal None Static NAT - Outbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Utbound INAT Traversal None Static NAT - Inbound Outbound NAT Traversal None Static NAT - Inbound Detection Disabled Vector Disabled Static NAT - Static NAT - Inbound Detection Detection Disabled
Listen Ports Listen Port Listen Port Message Manipulation Enabled Inbound Message Manipulation Message Table List	Pass-thru Peer SIP Response Code Enable SIP IP Details Teams Local Media Optimization Disable Signaling/Media Source IP Ethernet 2 IP (115, Signaling DSCP 40 NAT Traversal ICE Support ICE Support Disabled Outbound NAT Traversal None Static NAT - Inbound Detection Detection Disabled Static NAT - Inbound Detection Detection Disabled Outbound Mat Traversal None Static NAT - Inbound Detection Disabled Outbound Mat Traversal None Static NAT - Inbound Detection Disabled Outbound Message Manipulation DP/FQDN Netmask/Prefix 85. 255. Manipulation Message Table List *

0

Note 'Proxy Local SRTP Crypto Profile ID' is available for SBC SWe Edge only. This field is available only when 'Proxy with Local SRTP' (Supported only in SWe Edge) is included in the 'Supported Audio modes'.

Call Routing Table Entry

Call Routing entries must to be created after creating SIP Signaling Groups as Destination SGs need to be attached to these entries.

Transformation Table

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

Transformation Table Webex to PBX

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

- 1. Provide a desired name for the transformation table.
- 2. Click OK.

Q Search	Transformation
Expand All Collapse All Reload	I 🗙 🖺 Total 3 Transformation Table Rows
Call Routing	Description
Transformation	The state of
WEBEX_CUCM	V BEX_CUCM
WEBEX_PSTN	
Time of Day Table Call Routing Table	Description WEBEX_CUCM
Call Actions	
Signaling Groups	
Metworking Interfaces	ок
🕨 🥟 Virtual DR SBA	

Transformation Table Entry PBX

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

- 1. Under Input Field, enter the PBX number that is dialed from the Webex.
- 2. Click OK.

Q Search	WEBEX_CUCM			
Expand All Collapse All Reload	🗸 l 🥝 l 🕂 l 🗙 l 🥂 Total 1 Transform	nation Entry Row		
▼ 💋 Call Routing	Admin State Input Field Type	Input Field Value	Output Field Type	Output Fi Value
Transformation Passtbrough Untouched	v 🗀 🛛 🎼 Called Address/Number	(.*7353662224)	Called Address/Number	\1
WEBEX_CUCM				
WEBEX_PSTN	Description WEBEX_CUCM			
Time of Day Table Call Routing Table	Admin State Enabled			
Call Actions	Match Type Optional (Match One)			
🕨 📁 Signaling Groups				
Virtual DB SBA				
 Virtual DR SBA System 	Input Field		Output Field	
Auth and Directory Services	Type Called Address/Number	Type Ca	lled Address/Number	1
Protocols	Value (*7353662224)	Value \1		
Security				
Media				
 Ione Tables Telephony Mapping Tables 				
🕨 📁 SNMP/Alarms				ОК

Transformation Table Webex to PSTN

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

- 1. Provide a desired name for the transformation table.
- 2. Click OK.

Q Search	Transformation
Expand All Collapse All Reload	Total 3 Transformation Table Rows
Call Routing	Description
Transformation	Passthrough Untouched
	V D WEBEX_CUCM
WEBEX_PSTN	
Day Table	Description WEBEX_PSTN
Call Routing Table	
Signaling Groups	
Metworking Interfaces	ОК
Virtual DR SBA	

Transformation Table Entry PSTN

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

- 1. Under Input Field, enter the PSTN number that is dialed from the Webex.
- 2. Click OK.

Q Search	WEBEX_PSTN	
Expand All Collapse All Reload	🧹 ⊘ 👆 🗙 🥂 Total 1 Transforma	ation Entry Row
Call Routing	Admin State Input Field Type	Input Field Output Field Type Output Value
Transformation	▼ 📄 🛛 🍕 Called Address/Number	\+18919122453 Called Address/Number \1
WEBEX_CUCM		
WEBEX_PSTN	Description CISCO_PSTN	
 Time of Day Table Call Routing Table 	Admin State Enabled 🗸	
🕨 📁 Call Actions	Match Type Optional (Match One) 💙	
Signaling Groups		
Metworking Interfaces		
Virtual DR SBA	Input Field	Output Field
🕨 🧊 System	input riola	oupurried
Auth and Directory Services	Ture Celled Address (Number 1	Tura Called Address (Number 1
Protocols	Type Called Address/Number V	Type Called Address/Number V
🕨 🣁 SIP	Value \+18919122453	Value \1
🕨 📁 Security		
🕨 📁 Media		
🕨 📁 Tone Tables		
Telephony Mapping Tables		
🕨 🃁 SNMP/Alarms		ок

Transformation Table PSTN to Webex Tenant1

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

- 1. Provide a desired name for the transformation table.
- 2. Click OK.

Q Search	Transformation
Expand All Collapse All Reload	Total 7 Transformation Table Rows
▼ 💋 Call Routing	Description
Transformation	E PBX to Webex
Passthrough Untouched	Passthrough Untouched
PSTN to Tenant 2	PSTN to Tenant 2
PSTN to Webex	V PSTN to Webex
Webex to E PBX	
Webex to PSTN	Description DCTM to Websy
Day Table	
Call Routing Table	
Gall Actions Gall Actions Gall Actions	
d Linked Signaling Oroung	

Transformation Table Entry

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

- 1. Under Input Field, enter the Webex Tenant1 number that is dialed from the PSTN.
- 2. Click OK.

PST	N to Webe	ĸ				
\checkmark	0 + ×	🥖 Total 4 Tran	sformation Entry Ro)WS		
-	Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Mat Typ
~	🗀 🗆 🐶	Called Address/Number	(.*9725980076)	Called Address/Number	+19725980076	Ма
						_
	Description	Called Address/Number				
	Admin State	Enabled 🗸				
	Match Type	Mandatory (Must Match) 🗸				
		Input Field		Output Field		
	Туре 🔇	Called Address/Number	▼ 1	/pe Called Address/Number	· ·	
	Value (.*9725980076)	Va	lue +19725980076		
				L		
	_				_	
—						
					ок	

Note
 The

The same Transformation Table can be used for PBX Call Routing also because here, we only check the Webex Tenant1 number.

Call Routing Table Entry

PSTN to Webex

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

- 1. Attach the PSTN to Webex Transformation Table, which is present in the SBC Edge by default.
- 2. Click on $\mbox{Add/Edit}$ under Destination Signaling Groups, and select Webex_SG.
- 3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
- 4. Click OK.

0 Search	PSTN_TO_WEBEX				
Expand All Collapse All Reload	🥪 🧭 📑 🗙 🥂 Display C	ounters	Total 1 Call Route Entry Row		
▼ 龙 Call Routing	Admin Pr	riority	Transformation Table		Destination Type
Transformation			Passthrough Untouche	d	Normal
🥑 Time of Day Table			-		
Call Routing Table	Descrip	ption PSIN_to_Cisco)		
Default Route Table	Admin S	State Enabled	~		
CUCM TO WEBEX	Route Pric	ority 1	~		
WEBEX TO PSTN&CUCM	Call Pric	ority Normal	~		
Call Actions	Number/Name Transformation T	Table PSTN to WEBE	x 🗸 🖌		
Signaling Groups	Time of Day Restric	ction None	* +		
Metworking Interfaces					
Virtual DR SBA			Destination Infor	mation	
🕨 🥬 System			Destinution mon		
Auth and Directory Services	Destination Type	Normal	~		
Protocols	Message Translation Table	None			
SIP	message mansiación nable	None	·		
Security	Cause Code Reroutes	None	• •		
Tone Tables	Cancel Others upon Forwarding	Disabled	~		
Telephony Mapping Tables	Fork Call	No	~		
MP/Alarms		(SIP) WEBEX SG	A .		
Logging Configuration				Jp	
Emergency Services	Destination Signaling Groups		De	*	
			Add	d/Edit	
			Rer	nove	
	Enable Maximum Call Duration	Disabled	v		
		Media		Quality of S	Service
	Audio Stream Mode	DSP	~	Quality Metrics Number of Calls	10 [1100]
	Video/Application Stream Mode	Proxy	~	Quality Metrics Time Before Retry	10 [1-60] min.
	Media Transcoding	Enabled	~	Min ASR Threshold	
	Media List	None	v +	Fachle Min MOS Threshold	Dirabled
				Enable Max, R/T Dalay	Enabled
				May, P/T Dalay	65525 mr (1 655251
				Fachie Marchiele	Enabled
				Enable Max. Jitter	
				Max. Jitter	3000 ms [13000]
				L	

PBX to Webex

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

- 1. Attach the PSTN to Webex Transformation Table, which is present in the SBC Edge by default.
- 2. Click on Add/Edit under Destination Signaling Group and select Webex_SG.
- 3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
- 4. Click OK.

Q Search	CUCM_TO_WEBEX				
Expand All Collapse All Reload	🗸 🥥 📑 🗙 🥂 Display	Counters	Total 1 Call Route Entry Rov	*	
Call Routing	Admin State	Priority	Transformation Table		Destination Type
Transformation	▼ 🔲 🗋 🦞	1	Passthrough Untouched	I	Normal
Call Routing Table	Des	ription CUCM_TO_W	EBEX		
e Default Route Table	Admi	n State Enabled	~		
PSTN_TO_WEBEX	Route	Priority 1	~		
CUCM_TO_WEBEX	Call	Priority Normal	~		
	Number/Name Transformatio	n Table PSTN to WEB	EX 🖌 🖌		
Signalina Groups	Time of Day Res	triction None	× +	 • 	
Gignaling Groups Metworking Interfaces		Little			
Virtual DR SBA			Doctination Infor	mation	
🕨 🃁 System			Destination infor	mation	
Auth and Directory Services	Destination Ty	pe Normal	~		
Protocols	Message Translation Tab	le None	× •		
Security	Cause Code Resout	as None	~		
Media	Cause Code Reload	es Disabled	· · ·		
🕨 🏓 Tone Tables	Cancel Others upon Forward	ng Disabled	•		
Telephony Mapping Tables	Fork C	all No	~		
SNMP/Alarms		(SIP) WEBEX_SG	A .	Up	
Logging Configuration			D	own	
Emergency Services	Destination Signaling Grou	ps	Ad	d/Edit	
			Re	move	
	Enable Maximum Call Durati	on Disabled	~		
		Media		Quality of S	Service
	Audio Stream Mo	de DSP	~	Quality Metrics Number of Calls	10 [1100]
	Video/Application Stream Mo	de Proxy	~	Quality Metrics Time Before Retry	10 [1-60] min.
	Media Transcodi	ng Enabled	~	Min, ASR Threshold	96 10, 1001
	Media L	ist None	* +	Enable Min MOS Threshold	Disabled V
				Enable Max. R/T Delay	Enabled ¥
				Max. R/T Delay	65535 ms [165535]
				Enable Max. Jitter	Enabled 💙
				Max. Jitter	3000 ms [13000]

Note

0

For Passthrough calls, 'Audio Stream Mode' can be set to 'Proxy preferred over DSP' and enable SRTP on PBX leg.

Webex to PSTN

From the Settings tab, navigate to Call Routing > Call Routing Table > Webex_TO_PSTN&CUCM. Click the + icon to create a Call Routing Table.

- 1. Attach the Webex_PSTN Transformation Table to the match the PSTN's number.
- 2. Click on Add/Edit under Destination Signaling Groups, and select PSTN_SG.
- 3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
- 4. Click OK.

Q Search	WEBEX_TO_PSTN&CUCM	
Expand All Collapse All Reload	VI 🖉 🚛 🗶 🎢 Display Counters Total 2 Call Route Entry Rows	
Call Routing	Admin Priority Transformation Table	Destination Type
🕨 🥖 Transformation	V 1 WEBEX_PSTN	Normal
Time of Day Table		
Call Routing Table	Description WEBEX_PSTN	
PSTN_TO_WEBEX	Admin State Enabled 🗸	
CUCM_TO_WEBEX	Route Priority 1	
WEBEX_TO_PSTN&CUCM	Call Priority Normal	
🕨 🥖 Call Actions	Number/Name Transformation Table WEBEX_PSTN 🛩 🕂	
Signaling Groups	Time of Day Restriction None 🗸 🕈	
Metworking Interfaces		
Virtual DR SBA	Destination Information	
System System Auth and Directory Services		
🕨 🏓 Protocols	Destination Type Normal	
🕨 🃁 SIP	Message Translation Table None 🗸 🕇	
Security	Cause Code Reroutes None 👻 🔶	
Media	Cancel Others upon Forwarding Disabled	
F ione rables F ione rables	Fork Call No	
🕨 🍺 SNMP/Alarms		
Logging Configuration	Up	
🕨 🃁 Emergency Services	Destination Signaling Groups	
	Add/Edit	
	Remove	
	Enable Maximum Call Duration Disabled	
	Modia Ouality of S	nuico
	Quality of St	SI VICE
	Audio Stream Mode DSP V Quality Metrics Number of Calls	10 [1., 100]
	Video/Application Stream Mode Proxy V Ouality Metrics Time Before Retry	10 (1-60) min
	Media Transcoding Enabled	
	Media List None V	Dischlard and
	Enable Min MOS Threshold	
	Enable Max. R/T Delay	
	Max. R/T Delay	65535 ms [165535]
	Enable Max. Jitter	Enabled V
	Max. Jitter	3000 ms [13000]

Webex to PBX

From the Settings tab, navigate to Call Routing > Call Routing Table > Webex_TO_PSTN&CUCM. Click the + icon to create a Call Routing Table.

- 1. Attach the Webex_CUCM Transformation Table to the match the PBX's number.
- 2. Click on Add/Edit under Destination Signaling Groups, and select CUCM_SG.
- 3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
- 4. Click OK.



Multi-Tenant with Single IP / Multiple Port on SBC

For Multi-Tenant deployment, refer to SBCEdgeConfigurationforCiscoWebexCallingside for Tenant1. Refer to the following configuration for Tenant 2.

TLS Certificates

CN-based TLS Certificate for Multiple Tenants

Create the certificate for Ribbon SBC with the CN containing the SBC's FQDN for Tenant 2.

Generating CSR Key for Tenant2 Certificate

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

- 1. Provide the Common Name of the Tenant2 that includes Host and Domain.
- 2. Set the Key Length to 2048 bits.
- 3. Provide the location information.
- 4. Click OK.
- 5. The CSR will be generated and displayed in the result text box.

Q Search	Generate Certificate Signing	Request	
Expand All Collapse All Reload		Subject Distinguished Nan	ne
Call Routing			
Signaling Groups	Common Name	.rbbn.info	* Hostname or FQDN
Virtual DR SRA	Subject Alternative Name DNS		comma-separated FQDN list
▶ j System	Email Address		
Auth and Directory Services definition	ISO Country Code	India	✓ .
🕨 🧰 SIP	State/Province	Karanataka	
Security Josephine General General	Locality	Bangalore	e.g.: City
🕨 🥖 Login Messages	Organization		e.g.: Company
V SBC Certificates	Organizational Unit		e.g.: Department
SBC Primary Certificate	Key Length	2048 bits 🗸	
E SBC Supplementary Certificates			
Trusted CA Certificates			
TLS Profiles			ОК
Change Password			

After generating the certificate, import the Tenant2 certificate under Settings tab, navigate to Security > SBC Certificates > SBC Supplementary Certificate.

Q Search	SBC Certificates Index
Q. Search Expand All Collapse All Reload Call Routing Call Routing Signaling Groups Networking Interfaces Virtual DR SBA System Auth and Directory Services Protocols SIP Security Login Messages	SBC Certificates Index Generate SBC Edge CSR SBC Primary Certificate SBC Supplementary Certificates Trusted CA Certificates
SBC Certificates	
Trusted CA Certificates	

Upload the certificate in the SBC certificate (Refer to SBC Certificate).

Info The SAN/CN name for the TLS establishment with Webex is CASE SENSITIVE on the Cisco Webex side.

TLS Profile

From the Settings tab, navigate to Security > TLS Profiles. Click the + icon to create a new TLS profile.

- 1. From the TLS Protocol drop-down menu, select TLS 1.0-1.2.
- 2. Attach the certificate which is uploaded in the supplementary certificate.
- 3. Add the cipher suites that are supported on Cisco Webex.
- 4. Enable the Validate Server and Client FQDN fields to validate the CN and SAN name in the certificate send by Server and Client.

5. Click OK.



SIP Server Table Tenant2

Create a sip server table similar to the one created before.

- 1. From the Create SIP Server drop-down menu, select DNS-SRV.
- 2. Provide the SRV of the Cisco Webex and set the service of the SRV as sips.
- 3. Select the Protocol as TLS and attach the TLS profile which was created using the Tenant2 certificate.
- 4. Under the Transport section, enable sip OPTIONS by selecting SIP OPTIONS from the Monitor drop-down menu, and set the Local username as the SBC host name and the Peer Username as Webex.
- 5. Click OK.

Q Search	Tenant 2	Tenant 2 A						
Expand All Collapse All Reload	Create SIP Server ▼	X 1 🖉 Total 1 SIP Server Row						
▶ 💋 Call Routing	IP/FQDN		Server Lookup	Port	Protocol	Display Counters		
Signaling Groups	DNS-SRV	ect.bcld.webex.com	DNS SRV	N/A	TLS	Counters		
Linked Signaling Groups								
Weight Green		Server Host		Transpo	ort			
Could with and Directory Services Protocols Coal / Pass-thru Auth Tables SIP Profiles SIP Profiles SIP Server Tables Grauf SIP Server PSTN	Server Lookup Host IP Version Domain Name/FQDN Service Name Protocol TLS Profile	DNS SRV	Monitor SIP O Keep Alive Frequency 45 Recover Frequency 5 Local Username 3 Peer Username Webe	ptions * secs [* secs x_	(30300) [5300] * Local Userr * Peer Userri	iame of SBC Edge ame of sip server		
E PBX	Remote A	uthorization and Contacts	Cor	nnection	Reuse			
 ✓ Trunk Groups ✓ NAT Qualified Prefix Tables ✓ Remote Authorization Tables ✓ Contacl Registrant Table ✓ Message Manjoulation 	Remote Authorization Contact Registrant Session URI Vali	Table None	Reuse True Sockets 4	• •				

Message Manipulation

IP to FQDN Conversion in P-Asserted-Identity

The Message Manipulation is used to convert IP to tenant2's FQDN in the P-Asserted-Identity.

Condition Rule Table for Tenant2

The Condition Rule Table mentioned below is used to match Tenant2 Cisco Webex's number.

From the Settings tab, navigate to SIP > Message Manipulation > Condition Rule Table. Click the + icon to create a new Condition Rule Table.

- 1. Provide a name to Rule table.
- 2. From the Match Type drop-down menu, select to.uri.userinfo.user.
- 3. Under Operation, select Regex.
- 4. Under Match Regex, enter Tenant2's number.
- 5. Click OK.

Metworking Interfaces	^	Condition Rule Table		
Virtual DR SBA	. 1	Total 3 Condition Rule Table Roy	NS	
🕨 📁 System	. 1			
Auth and Directory Services	. 1	Match Type	Operation	Match Value Type
Protocols		to.uri.userinfo.user	Regex	N/A
V 🖾 SIP	11		-	
Local Registrars	11	🕨 🛄 🗌 cseq	Regex	N/A
Local / Pass-thru Auth Tables	11	🔻 📋 📄 to.uri.userinfo.user	Regex	N/A
SIP Profiles	11			
Figure SiP Server Tables	11			
NAT Qualified Deafer Tables	11	Description Tenant2		
Pamata Authorization Tables	11			
Contact Registrant Table	11			
Message Manipulation		Match Type		
Message Rule Tables	11	materi type		
Condition Rule Table	11	Notes Trans. In universitate una	1	
Tenant1 Num	11	Match Type to.un.userhito.user		
408 to 503	11	Operation Regex 🗸	·	
Tenant2	11	Match Regex 1888997772	*	
Node Level SIR Settings	11		,	
listen Port				
SIP Recording				
A d Casultu				
Security				ок
🖻 📁 Media				

Message Rule Table for Tenant2

From the Settings tab, navigate to SIP > Message Manipulation > Message Rule Table. Click the + icon to create a Message Rule Table.

- 1. Provide a description for the Rule Table.
- 2. Apply the message rule to All Messages, since the P-Asserted-Identity has to be changed on all the messages.
- 3. Click Ok.

Auth and Directory Services	1	SIP Message Rule Ta	ble	
Protocols SIP		🕂 🗙 Test Selected T	ables Total 3 SIP Message Mar	ipulation Table Rows
Local Registrars		Description		Result Type
SIP Profiles		🔻 📋 🗌 Towards Ten	nant2	Optional
SIP Server Tables		Test Message		
📁 Trunk Groups				
📁 NAT Qualified Prefix Tables				
📁 Remote Authorization Tables		Description	Towards Tenant2	
📁 Contact Registrant Table		Applicable Messages		
Verse Manipulation		Applicable Hessages	Air Messages	
Message Rule Tables		Table Result Type	Optional 🗸	
Towards Tenant2				
PAI IP to FDQN	1			
(iii) 408 to 503				
Condition Rule Table				ОК

Message Rule Table Entry for Tenant2

Header Rule:

- 1. Select Message Rule Tables > Towards Tenant2.
- 2. From the Create Rule drop-down menu, select Header Rule.
- Under Condition Expression> Add/Edit and select Message Rule Condition > Match all Condition and from the drop-down menu, select the condition rule as Tenant2.
- 4. Select Header Action as Modify and Header Name as P-Preferrred-Identity.
- 5. Under Header Value > URI Host select Modify.
- 6. Click on Add/Edit. Under the Edit Message Field, set Type of Value as Literal and Value as Tenant2's FQDN.
- 7. Click OK and Apply.

Signaling Groups	Towards Tenant2					
Metworking Interfaces	Towards renance					
Virtual DR SBA	🧹 🕗 Create Rule 🔻	🗙 🥂 Test Message	Total 1 Me	essage Manipulation I	Rules Row	
🕨 🃁 System	Admin	Rule Type		Result Type		Description
Auth and Directory Services	State	Kule type		Result type		Description
🕨 🃁 Protocols	🔻 🗀 🗋 🦞	Header Rule		Optional		Towards Ten
V 🖉 SIP		-				
📁 Local Registrars	Description	Towards Tenant2				
📁 Local / Pass-thru Auth Tables	Condition Expression	Add/Edit '\${3}'				
SIP Profiles	Admin State	Enabled 🗸				
SIP Server Tables	Result Type	Optional 🗸	Edit Massage	Field		
💋 Trunk Groups	Header Action	Modify 🗸	Edit Message	s Field		
📁 NAT Qualified Prefix Tables	Header Name	P.Asserted.Identity	-			
p Remote Authorization Tables	Handar Ordinal Number	14				
🥬 Contact Registrant Table	Header Ordinal Number	ist 🗣	Type of Valu	ue Literai	V	
Vessage Manipulation			Valu	Je S		
Vessage Rule Tables	▼ Header Value					
Towards Tenant2						
PAI IP to FDQN	Display Name Ign	iore 🗸				
(= 408 to 503	🔻 URI					OK Cancel
🕨 📁 Condition Rule Table						
Node-Level SIP Settings	URI S	icheme Ignore	~			
🕨 🃁 Listen Port	URI Us	er Info Ignore	~			
📁 SIP Recording		RT Host Modify	➤ Add/Edit ::			
Security		RI Dert Lesers				
🕨 🧯 Media		RI Port Ignore	•			
🕨 🏓 Tone Tables		+ 1 ×	Total 0 SPRUriPara	am Rows		
Telephony Mapping Tables				Value	Antion	
SNMP/Alarms	URI Para	meters	e	value	Action	
Logging Configuration						
Emergency Services			-	 Table is empty 		
· · · · · · · · · · · · · · · · · · ·						

SIP Profile Webex Tenant2

From the Settings tab, navigate to SIP > SIP Profiles. Click the + icon to create a new SIP Profile.

- 1. Provide a name for the profile in the Description field.
- 2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session.
- 3. Set Minimum Acceptable Timer to 600 and Offered Session Timer to 3600.
- 4. From the drop-down menus of both FQDN in From Header and FQDN in Contact Header, select **Static** and enter the Tenant2 FQDN in the Static Host FQDN/IP.
- 5. Webex is case-sensitive for FQDN in the contact header.
- 6. Click OK.



Call Routing Table Tenant2 to PSTN

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

- 1. Provide a name for the Routing Table.
- 2. Click OK.

Q Search	Call Routing Tables
Expand All Collapse All Reload	Total 6 Call Routing Table Rows
Call Routing	Description
Transformation	Tenant2 to PSTN
📁 Time of Day Table	
🔻 💋 Call Routing Table	
Tenant2 to PSTN	Description Transf2 to DSTN
PSTN_To_Webex	
Webex_To_PSTN	
E PBX to Webex	
Webex to E PBX	ОК
PSTN to Tenant2	
🕨 📁 Call Actions	

SIP Signaling Group - Webex Tenant2

From the Settings tab, navigate to Signaling Groups. Click Add SIP SG.

- 1. Attach the Call Routing Table (CallRoutingTableTenant2toPSTN).
- 2. Attach the Sip Profile (SipProfile).
- 3. Attach the SIP Server Table (SipServerTableTenant2).
- 4. Attach the SDES-SRTP Profile which is used for Tenant1 (SDES-SRTPProfile-Webex).
- 5. Attach the Media List which is used for Tenant1 (MediaList-Webex).
- 6. Associate the appropriate IP address in the "Signaling/Media Source IP" field which is used for Tenant1.
- 7. Configure Protocol and Listen Ports in the "Listen Ports" panel.
- 8. Create an entry in the Federated IP/FQDN panel.
- 9. Enable Message Manipulation and attach the profile "Towards Tenant2" and "408 to 503" in the outbound Message Manipulation Table List.
- 10. Click OK.



O Note

Proxy Local SRTP Crypto Profile ID is available for SBC SWe Edge only. This field is available only when **Proxy with Local SRTP** (Support ed only in SWe Edge) is included in the Supported Audio mode list.

Call Routing

Create Transformation Table from Tenant2 to PSTN and PSTN to Tenant2.

Transformation Table

Tenant2 to PSTN

Create a Transformation Table similar to the one for Tenant1.

From the Settings tab, navigate to Call Routing > Transformation > click on the new table created. Click the + icon to create a Transformation Table Entry.

- 1. Under Input Field give the PSTN number that is dialed from the Webex or Passthrough can be used since we are creating a separate Call Routing for Tenant2 to Webex.
- 2. Click Ok.

v 🔲 🗌 🗤	Called Address/Number	(.*)	Called Address/Number	\1
Description	Tenant2 to PSTN			
Admin State	Enabled 🗸			
Match Type	Optional (Match One) 🗸			
	Input Field		Output Field	
Туре	Called Address/Number	•	Type Called Address/Number	~
Value	(*)		Value \1	
		_		
				Or
				UK

PSTN to Tenant2

Create a Transformation Table.

From the Settings tab, navigate to Call Routing > Transformation > click on the new table created. Click the + icon to create a Transformation Table Entry.

- 1. Under Input Field, enter the Tenant2 number of Webex that is dialed from the PSTN.
- 2. Click OK.

State	Input Field Type	Input Value	Field	Output Field Type	Output Field Value
	Called Address/Number	r (.*97	25980078)	Called Address/Number	+197259800
Description	Called number				
Admin State	Enabled 🗸]			
Match Type	Optional (Match One) 🗸]			
	Input Field			Output Field	
Type [Input Field Called Address/Number	~	Туре	Output Field Called Address/Number	
Type [Input Field Called Address/Number		Type	Output Field Called Address/Number + 19725980078	
Type [Value [Input Field Called Address/Number (.*9725980078)	>	Type Value	Output Field Called Address/Number +19725980078	

Call Routing Table

Webex Tenant2 to PSTN

From the Settings tab, navigate to Call Routing > Call Routing Table > Tenant2 to PSTN. Click the + icon to create a Call Routing Table.

- 1. Attach the Tenant2 to PSTN Table.
- 2. Click on Add/Edit under Destination Signaling Group and select PSTN_SG.
- 3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
- 4. Click OK.



PSTN to Tenant2

In the existing Call Routing table which is created for Tenant1, add another Call Routing Table by clicking on 🕇.

- 1. Attach the PSTN to Tenant2 Table.
- 2. Click on Add/Edit under Destination Signaling Group and select Tenant 2 SG.
- 3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
- 4. Click OK.



Multi-Tenant with Single IP and Port on SBC

For Multi-Tenant deployment with a single IP/Port, refer to SBCEdgeConfigurationforCiscoWebexCallingside with some changes in the following profiles.

TLS Certificates

SAN-based TLS Certificate for Multiple Tenants

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

- 1. Provide the Tenant1's FQDN in the Common Name and Tenant2's FQDN in the Subject Name Alternative.
- 2. Set the Key Length to 2048 bits.
- 3. Provide the location information.
- 4. Click OK.
- 5. The CSR will be generated and displayed in the result text box.

Q Search	Generate Certificate Signing	Request	
Expand All Collapse All Reload		Subject Distinguished Nar	ne
🖻 📁 Call Routing		, ,	
Signaling Groups	Common Name	.rbbn.in	* Hostname or FQDN
Virtual DR SBA	Subject Alternative Name DNS	rbbn.info	comma-separated FQDN list
▶ 🥖 System	Email Address		
Auth and Directory Services	ISO Country Code	India	~
► D Protocois	State/Province	Karanataka	1
V Security	Locality	Bangalore	e.a.: City
Users I Jogin Messages	Organization		e.a.: Company
V 🗇 SBC Certificates	Organizational Unit		e a : Department
Generate SBC Edge CSR	Viganizational Onic	2048 bits	e.y Deputitient
SBC Primary Certificates	Key Length	2046 DIts 👻	
Trusted CA Certificates			
🕨 📁 TLS Profiles			ОК
Change Password			

After generating the CSR on Ribbon SBC, provide it to the Certificate Authority and get the SBC certificate.

Upload the certificate in the SBC certificate (Refer SBC Certificate).

TLS Profile

From the Settings tab, navigate to Security > TLS Profiles. Click the + icon to create a new TLS profile.

- 1. From the TLS Protocol drop-down menu, select TLS 1.0-1.2.
- 2. Attach the certificate which is uploaded in the SBC certificate.
- 3. Add the cipher suites that are supported on Cisco Webex.
- 4. Enable the Validate Server and Client FQDN fields to the validate the CN and SAN name in the certificate sent by Server and Client.
- 5. Click OK.

Q Search	TLS Profile				
Expand All Collapse All Reload	+ X Total 2 TLS Profile Rows				
E pail Routing	Description				
Signaling Groups	[i] Default TLS Profile				
Virtual DR SBA	v 📋 🗋 Webex_TLS				
🕨 🏓 System	TLS Parameters				
 Auth and Directory Services Protocols 	Common Attributes				
SIP	TLS Protocol TLS 1.2 Only V				
🕨 📁 Users	Mutual Authentication Enabled V				
Login Messages SBC Certificates	Handshake Inactivity Timeout 10 secs [1.30]				
TLS Profiles	Certificate SBC Edge Certificate				
Default TLS Profile	Client Attributes				
Change Password Change Password Ribbon Protect Bad Actors Media Tone Tables Telephony Mapping Tables SNMP/Alarms Expanding Configuration Emergency Services	TLS_ECOHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECOHE_RSA_WITH_AES_128_GCM_SHA3256 TLS_ECOHE_RSA_WITH_AES_128_GCS_SHA3256 TLS_ECOHE_RSA_WITH_AES_128_GCS_SHA3256 TLS_ECOHE_RSA_WITH_AES_128_GCS_SHA3256 TLS_ECOHE_RSA_WITH_AES_256_CCS_SHA356 TLS_RSA_WITH_AES_128_GCS_SHA356 TLS_RSA_WITH_AES_128_GCS_SHA356 TLS_RSA_WITH_AES_128_GCS_SHA356				
	Validate Server FQDN Enabled V				
	Server Attribute				
	Validate Client FQDN Enabled				

SIP Profile

In the existing sip profile which is created in the single tenant, **Disable** the FQDN in **From Header and Contact header**.



Message Manipulation

Condition Rule Table

Create 2 condition Rule Tables for matching the Tenant1 and Tenant2 Number each as shown in the snapshot below.



Message Table

From the Settings tab, navigate to SIP > Message Manipulation > Message Rule Table. Click the + icon to create a Message Rule Table.

- 1. Provide a description for the Rule Table.
- 2. Apply the message rule to All Messages, since the P-Asserted-Identity has to be changed on all the messages.
- 3. Click OK.

Signaling Groups	SIP Message Rule Table		
Linked Signaling Groups	L M Test Colorted Tables Table (STD Message	e Manipulation Table Pour	
Mode Interfaces	The selected rables total 4 SIP Plessag	e Planipulation Table Rows	
🕨 📁 System	Description	Result Type	
Auth and Directory Services		Mandatan	
Protocols		Mandatory	
🔻 🚧 SIP	🔻 📋 🗌 Towards Webex	Mandatory	
💋 Local Registrars	Test Message		
📁 Local / Pass-thru Auth Tables	Test message		
🕨 🃁 SIP Profiles			
🕨 🃁 SIP Server Tables	Description Towards Webey		
📁 Trunk Groups	Iowards Webex		
📁 NAT Qualified Prefix Tables	Applicable Messages All Messages	~	
prote Authorization Tables	Table Result Type Mandatory	~	
💋 Contact Registrant Table			
Message Manipulation			
V Wessage Rule Tables			
C Message Rule Table #1		ОК	
Towards Webex			

Message Rule Table Entry for Tenant1

P-Preferrred-Identity Header IP to FQDN

- 1. Click on the Message Rule Table Towards Webex.
- 2. From the Create Rule drop-down menu, select Header Rule.
- Under Condition Expression> Add/Edit and select Message Rule Condition > Match all Condition and from the drop-down menu, select the condition rule as Tenant1.
- 4. Select Header Action as Modify and Header Name as P-Preferrred-Identity.
- 5. Under Header Value > URI Host select Modify.
- 6. Click on Add/Edit. Under Edit Message Field, set Type of Value as Literal and Value as Tenant1's FQDN.
- 7. Click OK and Apply.

🤜 ⊘ Create Rule 🔻 🗙 /	/] Test Message	Total 1 Message Manipulation Rules Row
Header Rule	tule Type	Result Type Description
🔻 🛄 🗌 Request Line Rule	Header Rule	Mandatory
Status Line Rule		
Raw Message Rule	FQDN	
Condition Expression Add/E	dit 'S(1)'	
Admin State Enable	d 🗸	
Result Type Manda	story 🗸	Edit Maccana Field
Header Action Modify	v ~	
Header Name P-Asse	arted-Identity	
Header Ordinal Number 1st	~	Type of Value Literal 🗸
		Value S
▼ Header Value		
Display Name Ignore	~	
VRI URI		
URI Scheme		OK Cancel
▶ URI User Info	Ignore 🗸	
URI Host	Modify 🗸	Add/Edit 's
URI Port	Ignore 🗸	
	+1×	Total O SPRUriParam Rows
	- Norma	Value
URI Parameters	ivame	Value
		Table is empty

Contact Header IP to FQDN

- 1. Click on the Message Rule Table Towards Webex.
- 2. From the Create Rule drop-down menu, select Header Rule.
- Under Condition Expression> Add/Edit and select Message Rule Condition > Match all Condition and from the drop-down menu, select the condition rule as Tenant1.
- 4. Select Header Action as Modify and Header Name as Contact.
- 5. Under Header Value > URI Host, select **Modify**.
- 6. Click on Add/Edit. Under Edit Message Field, set Type of Value as Literal and Value as Tenant1's FQDN.
- 7. Click OK and Apply.

VIOI Create	e Rule 🔻 🛛 🗙 🕅	Test Message	Total 1 Message Ma	nipulation Rules Row	
Head	ler Rule	tule Type	Re	esult Type	Description
🔻 🛄 🗌 Requ	est Line Rule	Header Rule	м	andatory	PPI IP to F
Statu	us Line Rule				
Raw	Message Rule	FQDN			
Condition I	Expression Add/E	dit '\$(1)'			
Ad	dmin State Enabled	d 🗸			
R	esult Type Manda	tory 🗸	Edit Message Field		
Hea	der Action Modify	~	Luit Hessage Heid		
Hea	der Name Conta	ct 🔤			
Header Ordin	al Number Ist	Ť	Type of Value Litera	al 👻	
			Value S		
▼ Header Va	lue				
Display I	Name Ignore	~			
1 T 2	URI				OV Cancel
	URI Scheme	Ignore 🗸			UN Cancer
	URI User Info	Ignore 🗸			
	URI Host	Modify 🗸	Add/Edit 's		
	URI Port	Ignore 🗸			
		+1×	Total O SPRUriParam Rows		
		Name	Value	Action	
	URI Parameters		1.100	riction .	
			Table is	empty	

From Header IP to FQDN

- 1. Click on the Message Rule Table Towards Webex.
- 2. From the Create Rule drop-down menu, select Header Rule.
- Under Condition Expression> Add/Edit and select Message Rule Condition > Match all Condition and from the drop-down menu, select the condition rule as Tenant1.
- 4. Select Header Action as Modify and Header Name as From.
- 5. Under Header Value > URI Host, select **Modify**.
- 6. Click on Add/Edit. Under Edit Message Field, set Type of Value as Literal and Value as Tenant1's FQDN.
- 7. Click OK and Apply.

🗸 🖉 Create Rule 🔻 🗙	/] Test Message	Total 1 Message Manipulation Rules Row	
Header Rule	tule Type	Result Type	Description
🔻 🔲 🗌 Request Line Rule	Header Rule	Mandatory	PPI IP to F
Status Line Rule			
Raw Message Rule	FQDN		
Condition Expression Add/	Edit : \$(1)"		
Admin State Enable	ed 🗸		
Result Type Mand	atory 🗸	Edit Message Field	
Header Action Modif	y v		
Header Name From			
Header Ordinal Number 1st	~	Type of Value Literal 🗸	
		Value	
▼ Header Value			-
Diselective lines			
Visplay Name Ignore			
			OK Cancel
URI Scheme	Ignore 🗸		
URI User Info	Ignore 🗸		
URI Host	Modify 🗸	Add/Edit 's	
URI Port	Ignore 🗸		
	+1×	Total O SPRUriParam Rows	
	Name	Value	tion
URI Parameters		Table is empty	

Note Message Rule Table Entry for Tenant2:

- 1. Attach the Tenant2 Condition Rule Table.
- 2. Edit Message Field, set Type of Value as Literal and Value as Tenant2's FQDN.

Signaling Group

0

- The same Signaling Group can be used by attaching the newly created SIP Profile and Message manipulation.
- Attach the newly created TLS profile in the existing sip server table which is used for single tenant configuration.
- The same Call Routing Table can be used which is used for single tenant configuration.
- Both Tenant FQDN will be using the same listen port.

Description Webex	
Admin State Enabled	
Service Status Unknown ()	
SIP Channels and Routing	
	Media Information
Action Set Table None	
Call Routing Table WEBEX_TO_PSTN_CUCM	Supported Proxy
No. of Channels 60	Audio/Fax Modes
SID Mode - Paris Call	Supported
Agent Type Back-to-Back User Agent	Video/Application Disabled
Interop Mode Standard	Modes
SIP Server Table Webex	Alley Refeet
Load Balancing Priority: Register All	SDP Enable
Channel Hunting Round Robin	RTCP Disable
Notify Lync CAC Profile Disable	Multiplexing
Challenge Request Disable	
Outbound Proxy IP/FQDN	Mapping Tables
Outbound Proxy Port	
Call Setup Response Timer 255	SIP To Q.850 Override Table Default (RFC4497)
Call Proceeding Timer 180	Q.850 To SIP Override Table Default (KFC4497)
Use Register as Keep Alive Enable	
Forked Call Answered Too Soon Disable	
	SIP IP Details
	Teams Local Media
	Optimization
	Signaling/Media Source IP Ethernet 2 (192 65 79 122)
	Signaling DSCP 40
	NAT Travercal
	ICE Support Disabled
	Static NAT - Outbound
	Outbound NAT Traversal None
	Static NAT - Inbound
	Detection Disabled
Listen Ports	Federated IP/FQDN
Total 1 SIP Listen Port Row	Total 1 SIP Federated IP Row
Port Protocol TLS Profile ID	IP/FQDN Netmask/Prefix
5061 TLS Webex_TLS_Profile	255.255.255.255
Message Manipulation Enabled	
Labourd Manage Mariaulation	Outbound Manager Manipulation
inbound message Manipulation	Outbound message Manipulation
	Towards Webex
Message Table List *	Message Table List *
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

Note

The same Call Routing can be used which is used in the Single Tenant Configuration by adding an Transformation table entry in PSTN and PBX towards Webex to match the Tenant2 number.

Multi-Tenant with Multiple IP and Port on SBC

- For Multi-Tenant deployment with Multiple IP and Port, you can refer to SBCEdgeConfigurationforCiscoWebexCallingside for Tenant1. For Tenant 2, refer to Multi-TenantwithSingleIP/MultiplePortonSBC.
- For Multi-Tenant with Multiple IP and Port, the same configuration above can be used by changing the signaling/media Source IP on 'SIP Signaling Group Webex Tenant2'.
- If multiple Webex tenants are in same 'Webex control hub location' and when the SBC's source ethernet IPs are in different networks, it is recommended to configure the static route using 'different netmasks' for the same destination (Location).

For configuration on Cisco Webex, visit https://help.Webex.com/.

Supplementary Services and Features Coverage

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

Sr. No.	Supplementary Services/ Features	Coverage
1	Basic Call Setup & Termination	✓
2	Call Transfer (Attended/ Consultative)	✓
3	Call Transfer (Unattended/ Blind)	✓
4	TLS trunk connections	✓
5	Load Balancing (SRV based)	\checkmark
6	Trunk Monitoring	✓
7	Media encryption	✓
8	Voice Transcoding	✓
9	Multi-tenancy	✓
10	Call Park/Retrieve	✓
11	Video Calls	✓
12	Fax	✓
13	Calling Line ID	✓
14	DTMF	✓
15	Session Audit	✓
16	Call Diversion	\checkmark

Legend



Caveats

Note the following items in relation to this Interop - these are either limitations, untested elements or useful information pertaining to the interoperability.

STUN packets (ICE) not received from Webex during the Ringback stage

- For Webex to PSTN calls with the ICE mode enabled, the SBC doesn't receive any STUN packets from Webex. Due to this, the SBC rejects
 the call with 5XX response.
- As a workaround solution, it is recommended to enable 'static NAT' on the Webex signaling group.

Not blocklisting the Webex node when the SBC receives 503 for the INVITE

- When PSTN calls Webex client and the Webex node sends a 503 response, the INVITE goes to the next available Webex node but the SBC does not blocklist the Webex node. But this status will be for a short period only till OPTIONS is sent.
- This issue does not have any impact on calls.

Displaying the status/history of the nodes

- When the SBC receives 503/408/no response for SIP Options from Webex, the SBC generates an alarm in the Monitor tab but there is no status (up/down) displayed for that particular node.
- Functionality is working fine but from a serviceability perspective, the SBC is unable to display the node status/history.

TTL issue

- The SBC is not adhering to the Time To Live (TTL) for sending the SRV query.
- This issue is observed only in SBC 1K/2K and not observed in SWe Edge.

SBC response to OPTIONS during drain mode

- When the SIP signaling group is in drain mode, the SBC is not responding with 503 Service Unavailable for incoming SIP OPTIONS.
- This issue is observed only in SBC 1K/2K and not observed in SWe Edge.

SBC supports only Proxy mode for Video calls

- The SBC supports only Proxy mode for Video calls, so the SBC relays Crypto lines without decrypting or encrypting.
- As a workaround, it is suggested to use SRTP on the Enterprise network.

These issues will be addressed by Ribbon in their upcoming releases.

Support

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

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

References

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

For detailed information about Cisco Webex, visit: https://www.Webex.com/.

Conclusion

This Interoperability Guide describes successful configuration for Ribbon SBC Edge interop involving Cisco Webex Calling for customer deployments.

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

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

© 2023 Ribbon Communications Operating Company, Inc. © 2023 ECI Telecom Ltd. All rights reserved.