Amazon Chime Voice Connector

SIP Trunk Configuration Guide:

Fonality and Ribbon SWe

May 2021

Document History

Rev. No.	Date	Description
1.0	May-25-2021	Draft SIP Trunk Configuration Guide

Table of Contents

Table of Figures

1 Audience

This document is intended for technical staff and Value Added Resellers (VAR) with installation and operational responsibilities. This configuration guide provides steps for configuring SIP Trunk using **Fonality** and **Ribbon SWe** to connect to **Amazon Chime Voice Connector** for inbound and/or outbound telephony capabilities.

The information in this document is for informational purposes only. AWS does not guarantee the accuracy of this document and AWS has no responsibility or liability for errors or omissions related to this document. The document is subject to change without notice, and should not be construed as a commitment by AWS.

1.1 Amazon Chime Voice Connector

Amazon Chime Voice Connector is a pay-as-you-go service that enables companies to make or receive secure phone calls over the internet or AWS Direct Connect using their existing telephone system or session border controller (SBC). The service has no upfront fees, elastically scales based on demand, supports calling both landline and mobile phone numbers in over 100 countries, and gives customers the option to enable inbound calling, outbound calling, or both.

Amazon Chime Voice Connector uses the industry-standard Session Initiation Protocol (SIP). Amazon Chime Voice Connector does not require dedicated data circuits. A company can use their existing Internet connection or AWS Direct Connect public virtual interface for SIP connectivity to AWS. Voice connectors can be configured in minutes using the AWS Management Console or Amazon Chime API. Amazon Chime Voice Connector offers cost-effective rates for inbound and outbound calls. Calls into Amazon Chime meetings, as well as calls to other Amazon Chime Voice Connector customers are at no additional cost. With Amazon Chime Voice Connector, companies can reduce their voice calling costs without having to replace their on-premises phone system.

2 SIP Trunking Network Components

The network for SIP Trunk reference configuration is illustrated below and is representative of **Fonality** using **Ribbon SWe** with **Amazon Chime Voice Connector**

IP PBX is used as a secondary PBX in the topology to perform call failover and call distribution

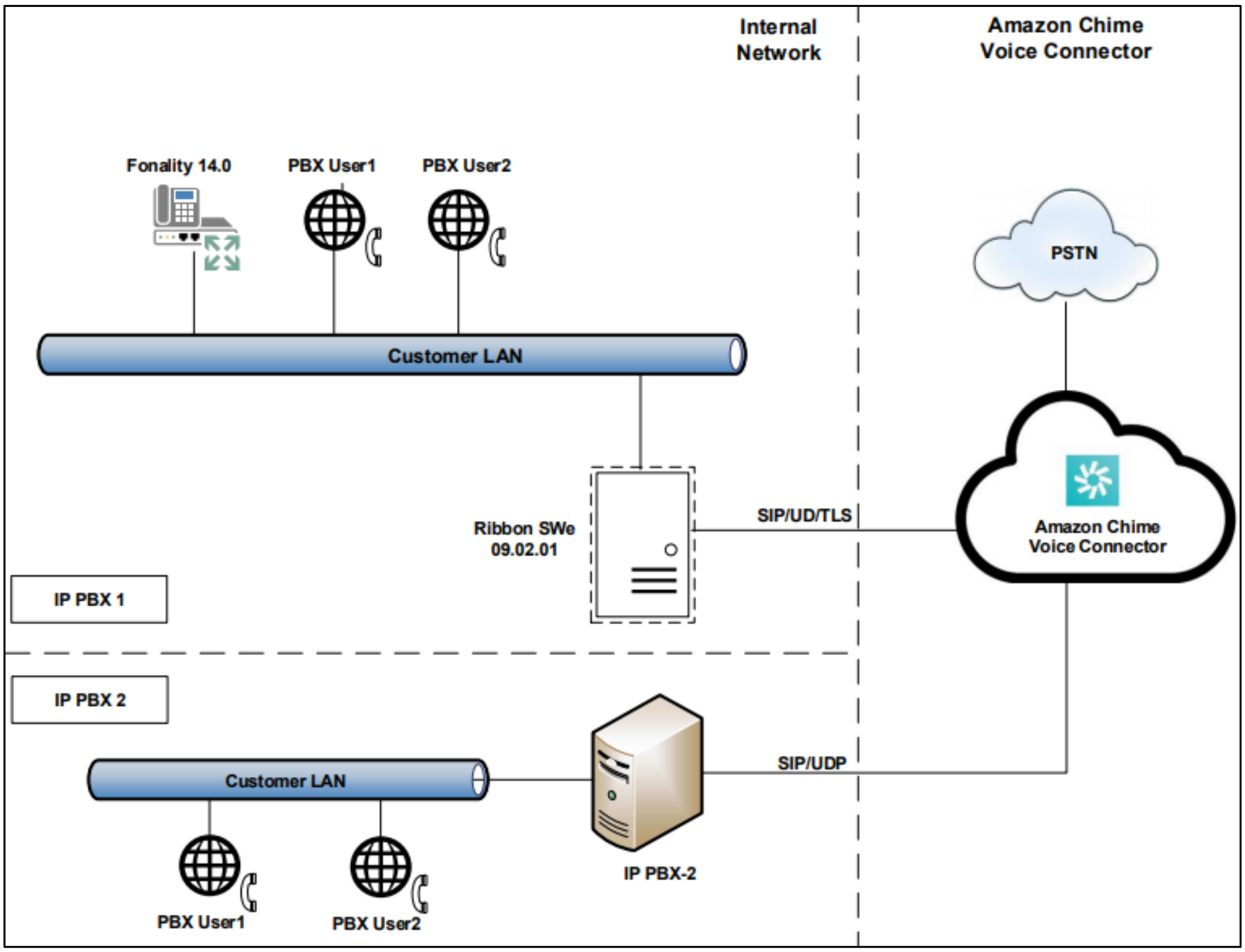

Figure 1 Network Topology

2.1 Hardware Components

- Fonality
- UCS-C240 VMWare server running ESXi 6.7 or later used for the following virtual machines
    - Ribbon SWe

2.2 Software Requirements

- Fonality – 14.0
- Ribbon SWe – V09.02.01-R000

3 Features

3.1 Features Supported

- Calls to and from non-Toll-Free number
- Calls to Toll Free number
- Calls to Premium Telephone number
- Calling Party Number Presentation
- Calling Party Number Restriction
- Inbound Calls to an IVR
- International Calls
- Anonymous call
- DTMF-RFC 2833
- Long duration calls
- Calls to conference scheduled by Amazon Chime user
- Calls to Amazon Chime Business number
- Call Distribution
- Call Failover

3.2 Features Not Supported

- Amazon Chime Voice Connector responds to OPTIONS and TCP Keep Alive messages received from customer equipment, but does not send OPTIONS or TCP Keep Alive messages to customer equipment

3.3 Features Not Tested

- None

3.4 Caveats and Limitations

- Amazon Chime Voice Connector,
  - does not support SIP NOTIFY or SIP INFO for DTMF
  - does not send SIP session refresher for long duration calls
- When the WAN link is down and a call is in progress, the PSTN call leg is not disconnected automatically after a period of inactivity. The call must be cleared manually
- Ribbon SWe process the inbound calls when the incoming INVITE from Amazon Chime Voice Connector contains only the Crypto attributes AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32. When the Incoming INVITE from Amazon Chime Voice Connector contains the following Crypto attributes in addition to AES_CM_128 then Ribbon SWe rejects the call with “501 Not Implemented” due to Crypto errors. If you remove the following crypto attributes using SIP Manipulations in Ribbon SWe then the Inbound call from Amazon Chime Voice Connector to Ribbon SWe should work as expected
  - AES_192_CM_HMAC_SHA1_80
  - AES_192_CM_HMAC_SHA1_32
  - AES_256_CM_HMAC_SHA1_80
  - AES_256_CM_HMAC_SHA1_32

4 Configuration

The specific values listed in this guide are used in the lab configuration described in this document and are for illustrative purposes only. You must obtain and use the appropriate values for your deployment. Encryption is always recommended if supported.

4.1 Configuration Checklist

In this section we present an overview of the steps that are required to **Fonality** and **Ribbon SWe** for SIP Trunking with **Amazon Chime Voice Connector.**

Table 1 – PBX Configuration Steps

Steps	Description	Reference
Step 1	Fonality Configuration	Section 4.2
Step 2	Ribbon SWe Configuration	Section 4.3
Step 3	Amazon Chime Voice Connector Configuration	Amazon Chime Voice Connector

4.2 Fonality Configuration

This section with screen shots taken from Fonality used for the interoperability testing gives a general overview of the Fonality configuration.

4.2.1 Fonality PBX Login and Version

1. Access Fonality Server URL and enter the credentials to perform the configuration in Fonality

Figure 2: Fonality PBX Login

2. After logging in, the screen that appears first contains the version as shown below,

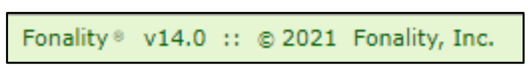

Figure 3: Fonality PBX Version

4.2.1 Add Phone

1. Click on **Users / Extensions** and choose **Phones**
2. Enter the **MAC** address of the Phone, Choose the **Vendor** from one of the available lists and enter a **Description**
3. Click on **Add Device**

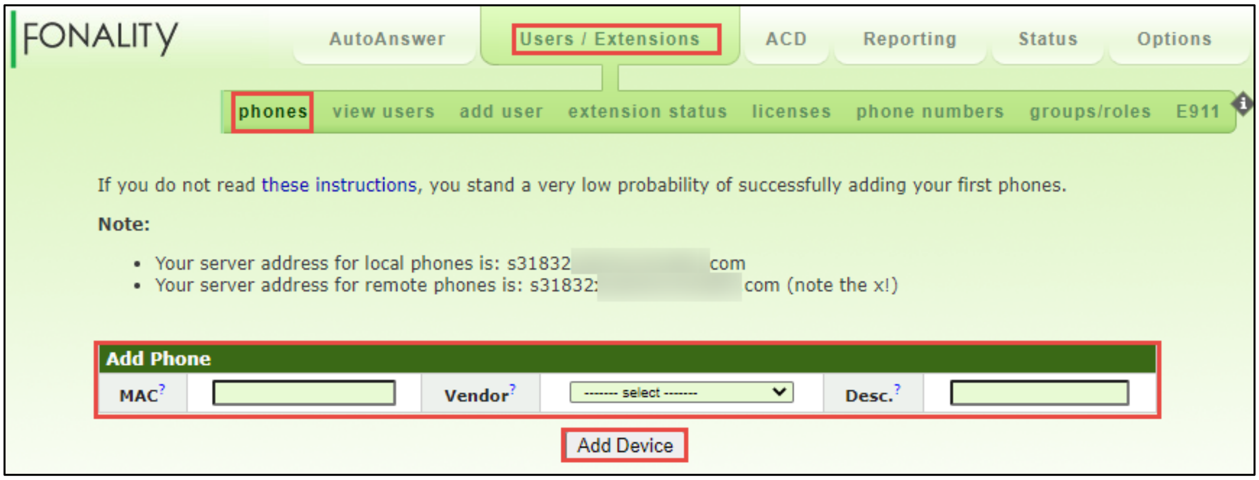

Figure 4: Add Phone

4.2.2 Add Phone Numbers

1. Click on **Users / Extensions** and choose **Phone Numbers**
2. In the **Add Phone Number** section, enter the DID Number obtained from Amazon Chime Voice Connector in **Number** field, **Type** as **VOIP** and enter the **Description**
3. Click on **Add Phone Number**

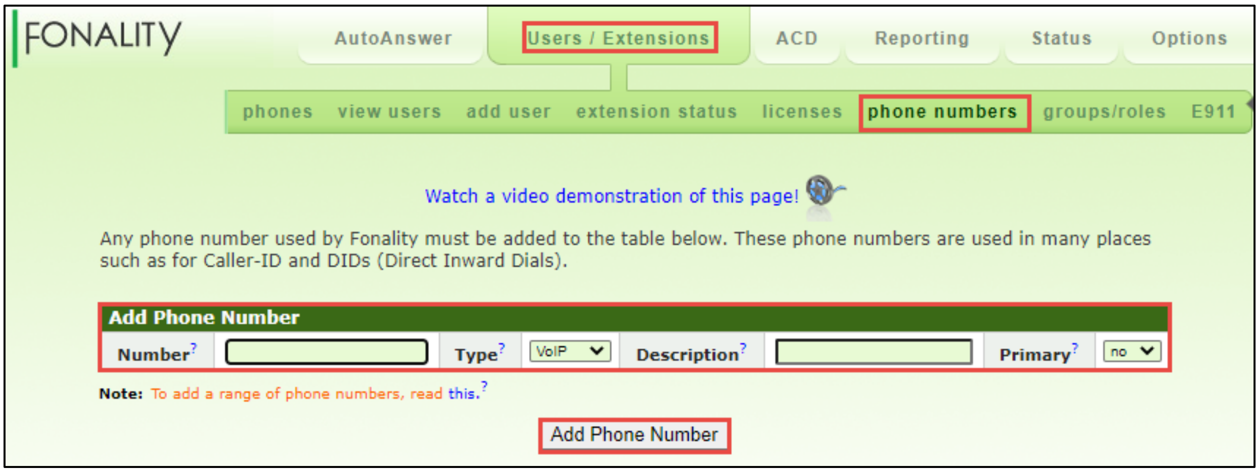

Figure 5: Add Phone Number

4.2.3 Add User

1. Click on **Users / Extensions** and choose **add user**
2. Choose the option "**I want to add a new user and a new extension**"
3. Enter the **First Name, Last Name, Description, Web Username** and **Web Password** in the **Personal Information** Section
4. Choose **Voicemail Enabled** as **YES**, Set the **Voicemail Password**, and leave the rest to default values in **Voicemail settings** section

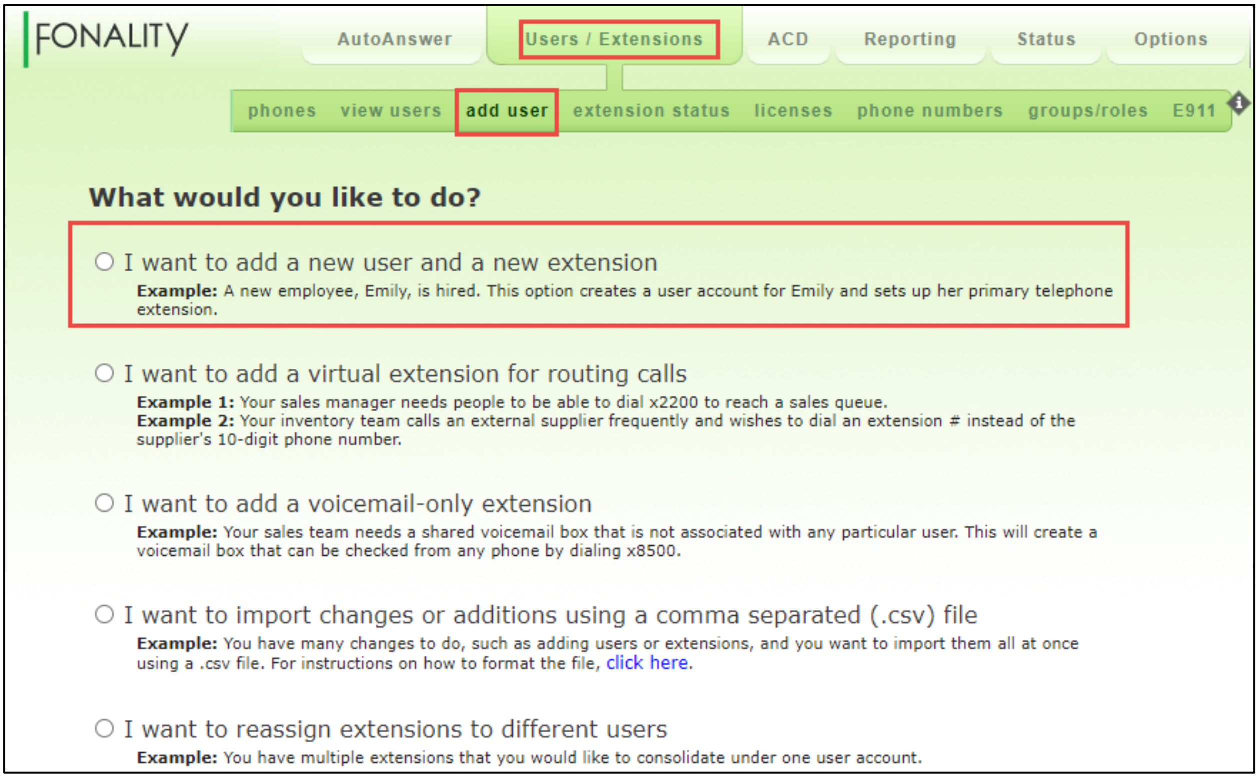

Figure 6: Add User

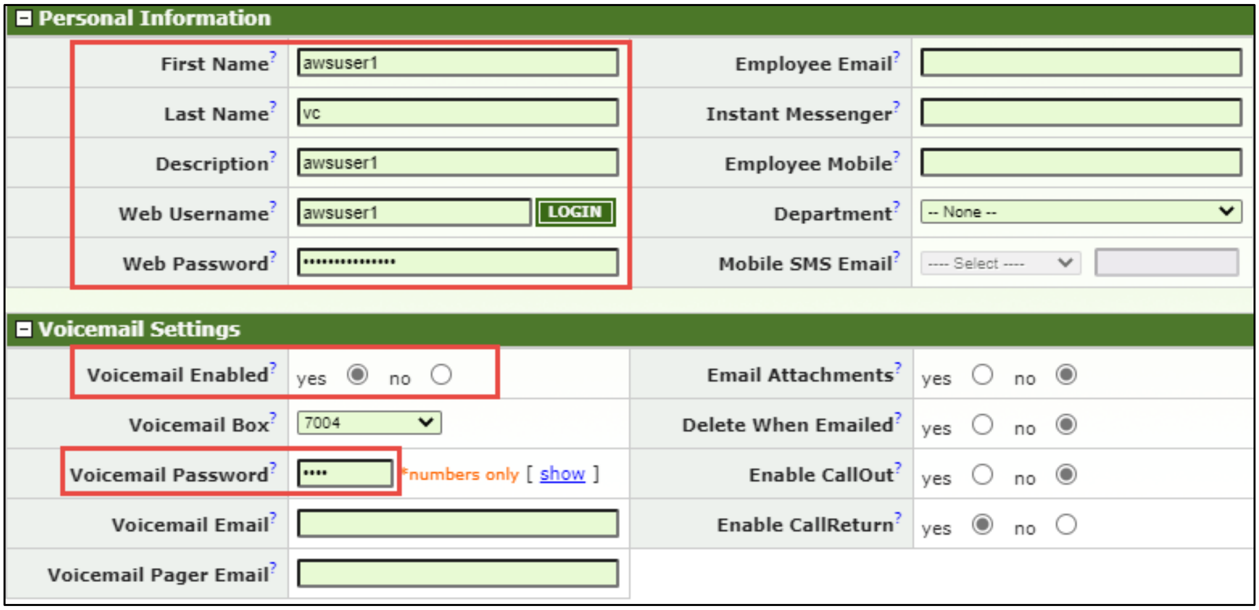

Figure 7: Add User Contd.,

5. Choose **Advanced User** under **User License** and leave the rest to default values in **License settings** section
6. Choose the **Inbound Phone No** and the **Outbound Caller-ID** and leave the rest to default values in **Routing and Appearance** Settings

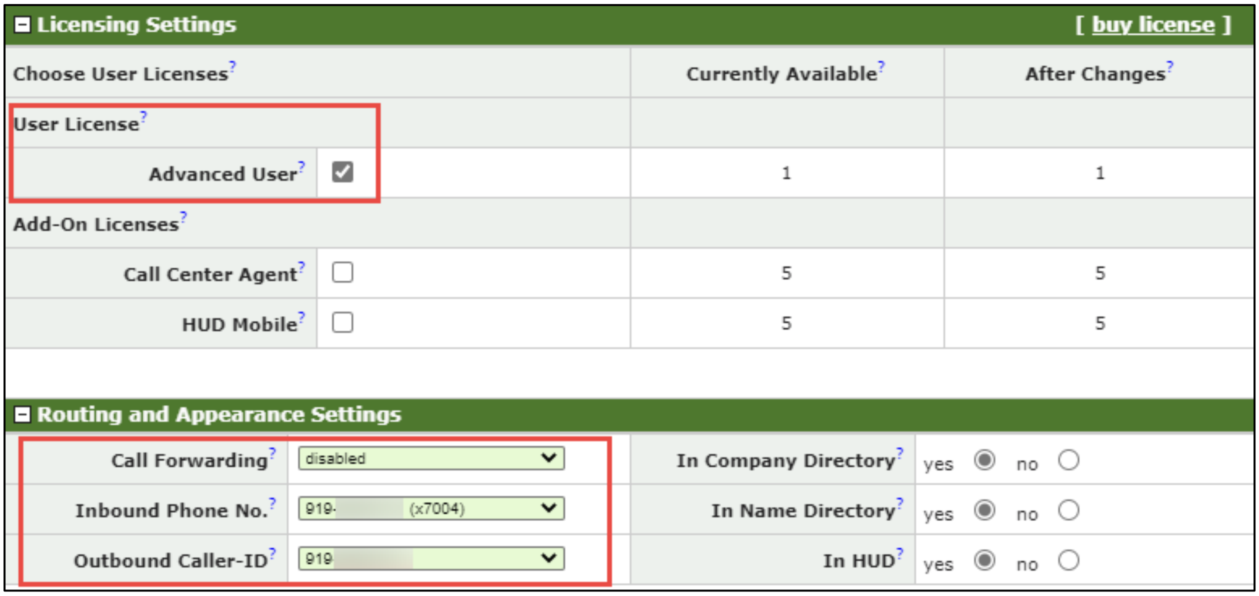

Figure 8: Add User-Contd.,

4.2.4 SIP Trunk

1. Click on **Options** and choose "**voip" submenu**
2. In the **Add VoIP Account** section enter **Route Name, Username, Password, Provider** set to **Other**, Select the option **SIP** from drop down menu, **Register** set to **No** and **Server** address set to the Ribbon SWe LAN IP address
3. Click on **Add VoIP Account**

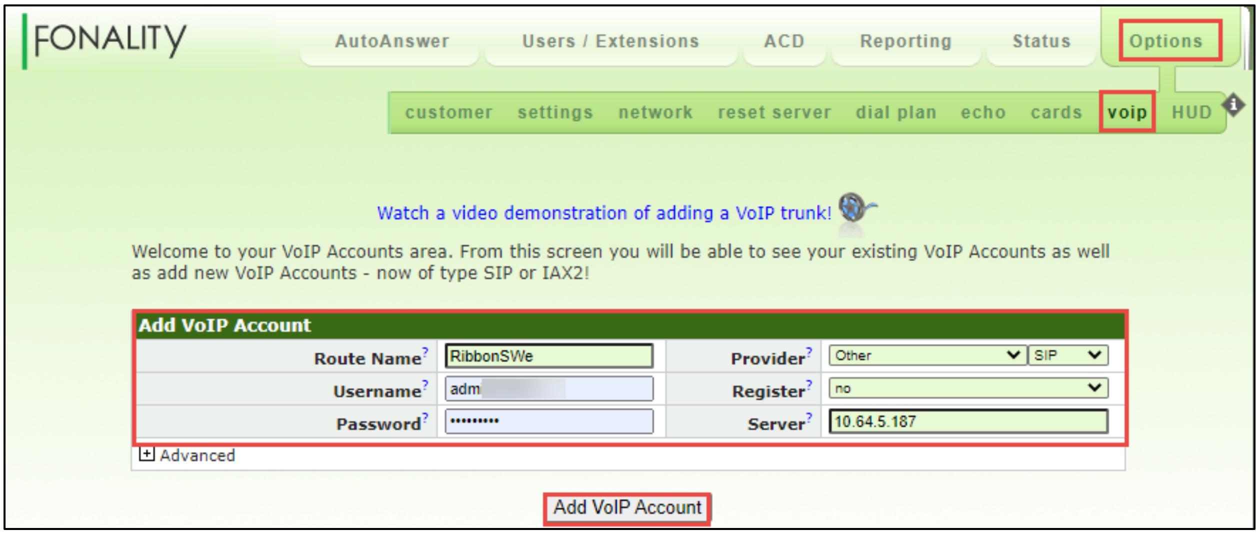

Figure 9: SIP Trunk

4. Click on **Advanced** and enter the **From Domain**, Choose the **Codec 1** as ulaw and **DTMF Mode** as rfc2833 and leave the rest to default values. Click on **Update VoIP Account**

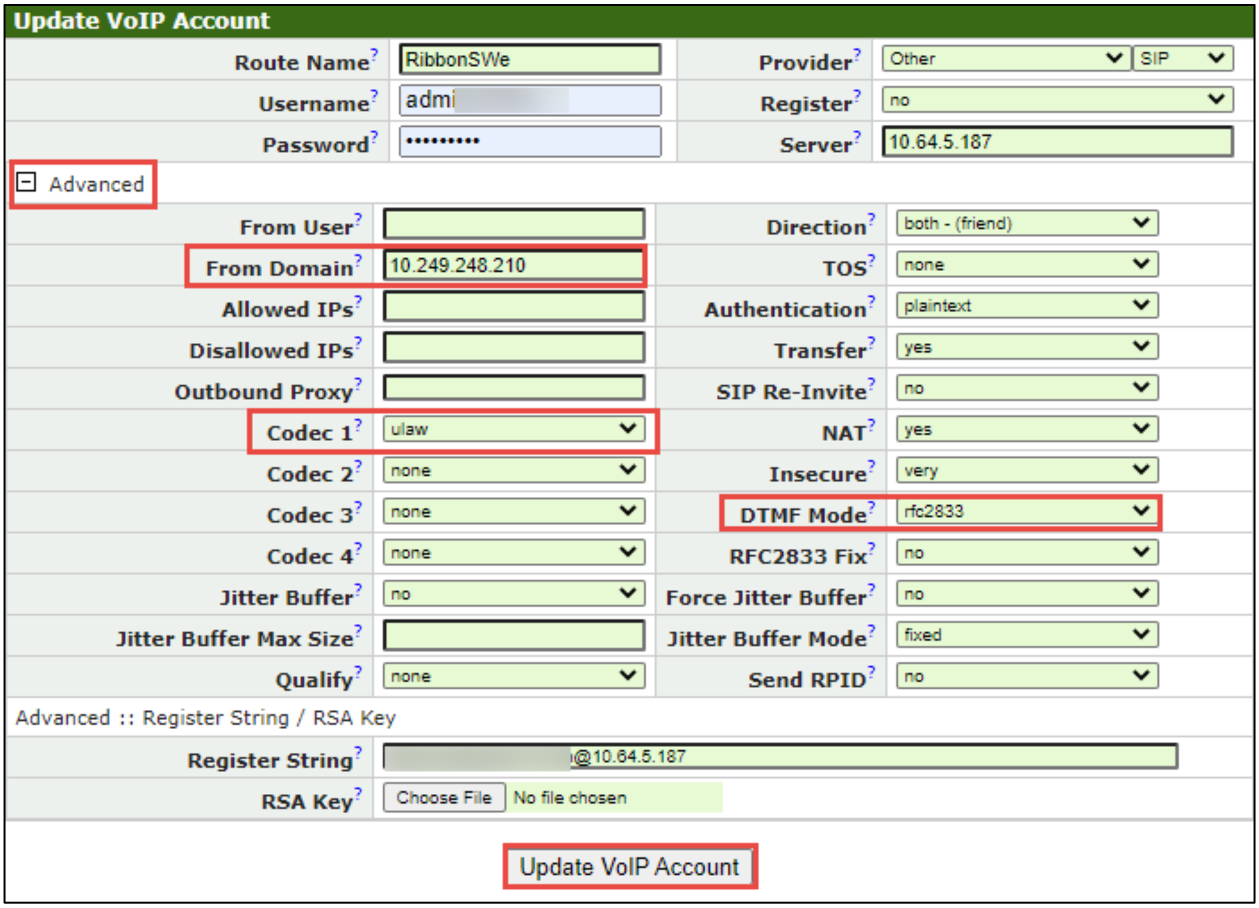

Figure 10: SIP Trunk Contd.,

4.2.5 Dial Plan

1. Click on **Options** and choose **dial plan**
2. In the **Add Dial Plan Entry** section, Enter the first few digits of the DID to be dialed for outbound calling in **Dial String**, **Type** set to Long Distance, **Route** set to Route name as created earlier in Section 4.2.4 and **Strip Digits** set to 1 to remove the Prefix
3. In the **Toll Restriction(advanced)** section, move **Advanced User Role** and **Basic User Role** to **Current Roles** and click on **Add Dial Plan**

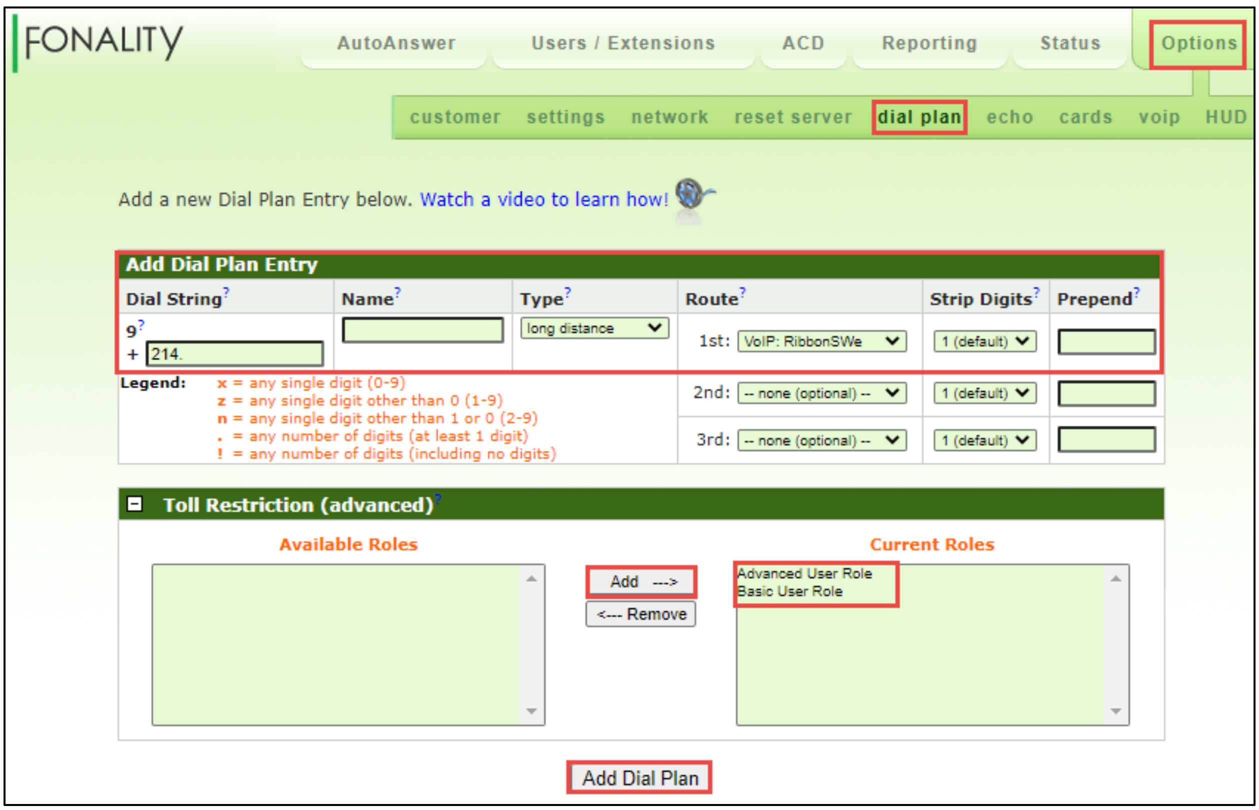

Figure 11: Dial Plan

4.3 Ribbon SWe Configuration

This section sets out the configuration steps for Ribbon SWe configuration.

4.3.1 IP Interface Group

- set addressContext default ipInterfaceGroup Internal_IPIG ipInterface pkt0 ipAddress 10.64.5.187 prefix 24 mode inService state enabled
- set addressContext default ipInterfaceGroup External_IPIG ipInterface pkt1 ipAddress 192.XX.XX.XX prefix 24 mode inService state enabled
- commit

4.3.2 DNS Group

- set addressContext default dnsGroup EXT_DNS interface External_IPIG server DNS1 ipAddress 8.8.8.8 state enabled
- commit

4.3.3 Zone

FONALITY

- set addressContext default zone FONALITY_ZONE id 210

Amazon Chime Voice Connector

- set addressContext default zone AMAZONCVC_ZONE id 310
- set addressContext default zone AMAZONCVC_ZONE dnsGroup EXT_DNS

4.3.4 SIP Signaling Port

FONALITY

- set addressContext default zone FONALITY_ZONE sipSigPort 210 ipInterfaceGroupName Internal_IPIG
- set addressContext default zone FONALITY_ZONE sipSigPort 210 ipAddressV4 10.64.5.187
- set addressContext default zone FONALITY_ZONE sipSigPort 210 portNumber 5060
- set addressContext default zone FONALITY_ZONE sipSigPort 210 mode inService

- set addressContext default zone FONALITY_ZONE sipSigPort 210 state enabled
- set addressContext default zone FONALITY_ZONE sipSigPort 210 transportProtocolsAllowed sip-udp
- commit

Amazon Chime Voice Connector

- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 ipInterfaceGroupName External_IPIG
- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 ipAddressV4 192.XX.XX.XX
- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 portNumber 5060
- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 mode inService
- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 state enabled
- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 transportProtocolsAllowed sip-udp
- commit

4.3.5 Media Codec Entry

- set profiles media codecEntry G711-DEFAULT codec g711
- set profiles media codecEntry G711-DEFAULT dtmf relay rfc2833
- set profiles media codecEntry G711-DEFAULT packetSize 20
- commit

4.3.6 Packet Service Profile

FONALITY

- set profiles media packetServiceProfile DEFAULT_PBX_PSP preferredRtpPayloadTypeForDtmfRelay 101
- set profiles media packetServiceProfile DEFAULT_PBX_PSP silenceInsertionDescriptor g711SidRtpPayloadType 13
- set profiles media packetServiceProfile DEFAULT_PBX_PSP codec codecEntry1 G711-DEFAULT
- commit

Amazon Chime Voice Connector

- set profiles media packetServiceProfile DEFAULT_SERVPROV_PSP preferredRtpPayloadTypeForDtmfRelay 101
- set profiles media packetServiceProfile DEFAULT_SERVPROV_PSP silenceInsertionDescriptor g711SidRtpPayloadType 13
- set profiles media packetServiceProfile DEFAULT_SERVPROV_PSP codec codecEntry1 G711-DEFAULT
- commit

4.3.7 Ip Signaling Profile

FONALITY

- set profiles signaling ipSignalingProfile DEFAULT_PBX_IPSP commonIpAttributes transparencyFlags reasonHeader enable
- set profiles signaling ipSignalingProfile DEFAULT_PBX_IPSP commonIpAttributes flags sendPtimeInSdp enable
- set profiles signaling ipSignalingProfile DEFAULT_PBX_IPSP egressIpAttributes transport type1 udp
- set profiles signaling ipSignalingProfile DEFAULT_PBX_IPSP egressIpAttributes privacy privacyInformation pAssertedId
- commit

Amazon Chime Voice Connector

- set profiles signaling ipSignalingProfile DEFAULT_SERVPROV_IPSP commonIpAttributes transparencyFlags reasonHeader enable
- set profiles signaling ipSignalingProfile DEFAULT_SERVPROV_IPSP commonIpAttributes flags sendPtimeInSdp enable
- set profiles signaling ipSignalingProfile DEFAULT_SERVPROV_IPSP egressIpAttributes transport type1 udp
- set profiles signaling ipSignalingProfile DEFAULT_SERVPROV_IPSP egressIpAttributes privacy privacyInformation pAssertedId
- commit

4.3.8 SIP Trunk

FONALITY

- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG media mediaIpInterfaceGroupName Internal_IPIG
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG policy digitParameterHandling numberingPlan NANP_ACCESS
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG policy callRouting elementRoutingPriority DEFAULT_IP
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG policy media packetServiceProfile DEFAULT_PBX_PSP
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG policy signaling ipSignalingProfile DEFAULT_PBX_IPSP
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG ingressIpPrefix 0.0.0.0 0
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG state enabled
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG mode inService
- commit

Amazon Chime Voice Connector

- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG media mediaIpInterfaceGroupName External_IPIG
- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG policy digitParameterHandling numberingPlan NANP_ACCESS
- set addressContext default zone FONALITY_ZONE sipTrunkGroup FONALITY_TG policy callRouting elementRoutingPriority DEFAULT_IP
- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG policy media packetServiceProfile DEFAULT_SERVPROV_PSP
- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG policy signaling ipSignalingProfile DEFAULT_SERVPROV_IPSP
- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG ingressIpPrefix 0.0.0.0 0
- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG mode inService
- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG state enabled

- commit

4.3.9 Path Check Profile

- set profiles services pathCheckProfile AMAZONCVC_OPTIONS protocol sipOptions
- set profiles services pathCheckProfile AMAZONCVC_OPTIONS sendInterval 60
- set profiles services pathCheckProfile AMAZONCVC_OPTIONS replyTimeoutCount 1
- set profiles services pathCheckProfile AMAZONCVC_OPTIONS recoveryCount 1
- set profiles services pathCheckProfile AMAZONCVC_OPTIONS transportPreference preference1 udp
- commit

4.3.10 IP Peer

FONALITY

- set addressContext default zone FONALITY_ZONE ipPeer FONALITY_PEER ipAddress 10.249.248.210
- set addressContext default zone FONALITY_ZONE ipPeer FONALITY_PEER ipPort 5060
- set addressContext default zone FONALITY_ZONE ipPeer FONALITY_PEER policy description "FONALITY"

Amazon Chime Voice Connector

- set addressContext default zone AMAZONCVC_ZONE ipPeer AMAZONCVC_PEER policy sip fqdn gdnbxxxxxxx.voiceconnector.chime.aws fqdnPort 5060
- set addressContext default zone AMAZONCVC_ZONE ipPeer AMAZONCVC_PEER pathCheck profile AMAZONCVC_OPTIONS
- set addressContext default zone AMAZONCVC_ZONE ipPeer AMAZONCVC_PEER pathCheck hostName gdnbxxxxxxx.voiceconnector.chime.aws
- set addressContext default zone AMAZONCVC_ZONE ipPeer AMAZONCVC_PEER pathCheck hostPort 5060 state enabled
- commit

4.3.11 Static Route

- set addressContext default staticRoute 0.0.0.0 0 192.xx.xx.xx External_IPIG pkt1
- set addressContext default staticRoute 0.0.0.0 0 10.64.1.1 Internal_IPIG pkt0
- commit

4.3.12 Routing Label

FONALITY

- set global callRouting routingLabel FONALITY_RL routingLabelRoute 1 trunkGroup FONALITY_TG inService inService
- set global callRouting routingLabel FONALITY_RL routingLabelRoute 1 ipPeer FONALITY_PEER inService inService
- commit

Amazon Chime Voice Connector

- set global callRouting routingLabel AMAZONCVC_RL routingLabelRoute 1 trunkGroup AMAZONCVC_TG inService inService
- set global callRouting routingLabel AMAZONCVC_RL routingLabelRoute 1 ipPeer AMAZONCVC_PEER inService inService
- commit

4.3.13 Route

FONALITY

- set global callRouting route none Sonus_NULL Sonus_NULL standard 919 1 all all ALL none Sonus_NULL routingLabel FONALITY_RL
- commit

Amazon Chime Voice Connector

- set global callRouting route trunkGroup FONALITY_TG RIBSBCSWE standard Sonus_NULL 1 all all ALL none Sonus_NULL routingLabel AMAZONCVC_RL
- commit

4.3.14 TLS Configuration

4.3.14.1 Import Amazon Chime Voice Connector Certificate

Amazon Chime Voice Connector Root Certificate can be downloaded from Amazon Chime Voice Connector account

- set system security pki certificate ACVC_CERT type remote fileName Amazoncert.der state enabled
- commit

4.3.14.2 Create Crypto Suite Profile

- set profiles security cryptoSuiteProfile CRYPTO_PROF entry 1 cryptoSuite AES-CM-128-HMAC-SHA1-32
- set profiles security cryptoSuiteProfile CRYPTO_PROF entry 2 cryptoSuite AES-CM-128-HMAC-SHA1-80
- commit

4.3.14.3 Create TLS Profile

- set profiles security tlsProfile TLS_PROF clientCertName ACVC_CERT serverCertName defaultSBCCert cipherSuite1 rsa-with-aes-128-cbc-sha authClient false allowedRoles clientandserver acceptableCertValidationErrors invalidPurpose v1_2 enabled
- commit

4.3.14.4 SIP Manipulation

Ribbon SWe process the inbound calls when the incoming INVITE from Amazon Chime Voice Connector contains only the Crypto attributes AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32. When the Incoming INVITE from Amazon Chime Voice Connector contains the following Crypto attributes in addition to AES_CM_128 then Ribbon SWe rejects the call with “501 Not Implemented” due to Crypto errors. If you remove the following crypto attributes then the Inbound call from Amazon Chime Voice Connector to Ribbon SWe worked as expected

- AES_192_CM_HMAC_SHA1_80
- AES_192_CM_HMAC_SHA1_32
- AES_256_CM_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_32

The following SIP Manipulation are added to remove AES_256 and AES_192 Cryptos in the Incoming INVITE

Rule to remove contents after AES_256

- set profiles signaling sipAdaptorProfile Delete-crypto state enabled
- set profiles signaling sipAdaptorProfile Delete-crypto advancedSMM enabled
- set profiles signaling sipAdaptorProfile Delete-crypto profileType messageManipulation
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 applyMatchHeader one
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 criterion 1 type message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 criterion 1 message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 criterion 1 message messageTypes all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 criterion 2 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 criterion 2 messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 criterion 2 messageBody condition exist
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 operation regpostdel
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 to
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 to type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 to messageBodyValue all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 regexp
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 regexp string AES_256
- set profiles signaling sipAdaptorProfile Delete-crypto rule 1 action 1 regexp matchInstance all
- commit

Rule to remove matching string "a=crypto:5 AES_256"

- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 applyMatchHeader one
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 criterion 1 type message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 criterion 1 message

- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 criterion 1 message messageTypes all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 criterion 2 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 criterion 2 messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 criterion 2 messageBody condition exist
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 operation regdel
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 to
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 to type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 to messageBodyValue all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 regexp
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 regexp string "a=crypto:5 AES_256"
- set profiles signaling sipAdaptorProfile Delete-crypto rule 2 action 1 regexp matchInstance all
- commit

Rule to remove contents after AES_192

- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 applyMatchHeader one
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 criterion 1 type message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 criterion 1 message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 criterion 1 message messageTypes all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 criterion 2 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 criterion 2 messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 criterion 2 messageBody condition exist
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 operation regpostdel
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 to

- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 to type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 to messageBodyValue all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 regexp
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 regexp string AES_192
- set profiles signaling sipAdaptorProfile Delete-crypto rule 3 action 1 regexp matchInstance all
- commit

Rule to remove matching string "a=crypto:5 AES_192"

- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 applyMatchHeader one
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 criterion 1 type message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 criterion 1 message
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 criterion 1 message messageTypes all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 criterion 2 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 criterion 2 messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 criterion 2 messageBody condition exist
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 operation regdel
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 to
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 to type messageBody
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 to messageBodyValue all
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 regexp
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 regexp string "a=crypto:3 AES_192"
- set profiles signaling sipAdaptorProfile Delete-crypto rule 4 action 1 regexp matchInstance all
- commit

4.3.14.5 Packet Service Profile with Crypto Suite

- set profiles media packetServiceProfile DEFAULT_SERVPROV_PSP secureRtpRtcp cryptoSuiteProfile CRYPTO_PROF
- set profiles media packetServiceProfile DEFAULT_SERVPROV_PSP secureRtpRtcp flags enableSrtp enable
- set profiles media packetServiceProfile DEFAULT_SERVPROV_PSP secureRtpRtcp flags allowFallback disable
- commit

4.3.14.6 IP Signaling Profile

- set profiles signaling ipSignalingProfile DEFAULT_SERVPROV_IPSP egressIpAttributes transport type1 tlsOverTcp
- commit

4.3.14.7 SIP Signaling Port

- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 tlsProfileName TLS_PROF
- set addressContext default zone AMAZONCVC_ZONE sipSigPort 310 transportProtocolsAllowed sip-tls-tcp
- commit

4.3.14.8 SIP Trunk

- set addressContext default zone AMAZONCVC_ZONE sipTrunkGroup AMAZONCVC_TG signaling messageManipulation inputAdapterProfile Delete-crypto
- commit