Ribbon Federal Edge R22.01 Interop with Cisco Unified CM & Avaya IPO : Interoperability Guide

Table of Contents

Interoperable Vendors

Copyright

Document Overview

This document outlines the configuration best practices for Ribbon Federal Edge solution when deployed with Cisco Unified CM and Avaya IPO.

About Ribbon Federal Edge

The Ribbon Federal Edge Solution is an on-premises voice services appliance that offers government agencies UC security, interoperability, and survivability at lower costs than other alternatives in the market. It is a multi-functional platform providing connectivity between legacy network & Voice over IP (SIP) network. The Federal Edge Solution aggregates the following Ribbon individual products into a single, cohesive unit:

1. SBC 1000 or SBC 2000, as gateway interface to Federal Edge appliance
2. SBC SWe Core on multicore ASM (Application Solution Module), as voice interface within Federal Edge solution

About Ribbon SBC SWe Core

The SBC SWe Core addresses the next-generation needs of SIP communications by delivering embedded media transcoding, robust security and advanced call routing in a high-performance, small form-factor device enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP Trunking, secure Unified Communications and Voice over IP (VoIP).

The SBC SWe Core provides a reliable, scalable platform for IP interconnect to deliver security, session control, bandwidth management, advanced media services and integrated billing/reporting tools in an SBC appliance. This versatile series of SBCs can be deployed as peering SBCs, access SBCs or enterprise SBCs (eSBCs). The SBC product family is tested for interoperability and performance against a variety of third-party products and call flow configurations in the customer networks.

The SBC SWe Core is installed in VMware ESXi platform on multi-core ASM. The Application Solution Module (ASM) module is a separate, fully-functional server installed inside the SBC Edge Portfolio (SBC 1000/2000) chassis. The ASM can host a variety of applications that support the SBC Edge Portfolio. If purchased with the SBC Edge Portfolio, the ASM module is factory installed. For more details, please refer Application Solution Module.

About Ribbon SBC Edge

The Ribbon Session Border Controller Edge (SBC Edge) provides best-in class communications security. The SBC Edge simplifies the deployment of robust communications security services for SIP Trunking and TDM connectivity via FXS, PRI etc.

About Cisco Unified CM

Cisco Unified Communications Manager (CUCM) is the core call control application of Cisco's collaboration portfolio. It provides reliable, highly secure, scalable, and efficient enterprise call and session management.

About Avaya IP Office

Avaya IP Office (IPO) is a single, stackable, scalable small business communications system that offers technical flexibility using digital (ISDN), analog (FXS), IP (SIP) or any combination of these - and resiliency. The Avaya IP Office Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device.

Scope/Non-Goals

This document provides configuration best practices for deploying Ribbon's Federal Edge consisting of installing & configuring SBC SWe Core and SBC Edge in SBC 2000/SBC 1000 hardware. 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, and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Ribbon SBC SWe Core & Ribbon SBC Edge (1000/2000 hardware).

To perform this interop, you need to:

- use the graphical user interface (GUI) or command line interface (CLI) of the Ribbon product
- have understanding of the basic concepts of TLS, IP Routing, TDM (FXS/T1-E1/PRI)
- have understanding of SIP/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 2000 or 1000 Hardware
- VMware ESXi 6.7.0
- Ribbon SBC SWe Core
- Ribbon SBC SWe Core license & Ribbon SBC Edge (1000 or 2000 hardware) License
    - A valid license from Ribbon is required to enable functionality on Ribbon SBCs. Each SBC license provides a base set of capabilities to allow enabling and adding of additional features and capacity, as required.
    - Contact Ribbon Sales / Support for License
- TLS certificates for SBC SWe Core
    - Please refer to Managing Certificates
- SIP Peer details
- NTP Server Details
- DHCP Server / DNS Server details

Product and Device Details

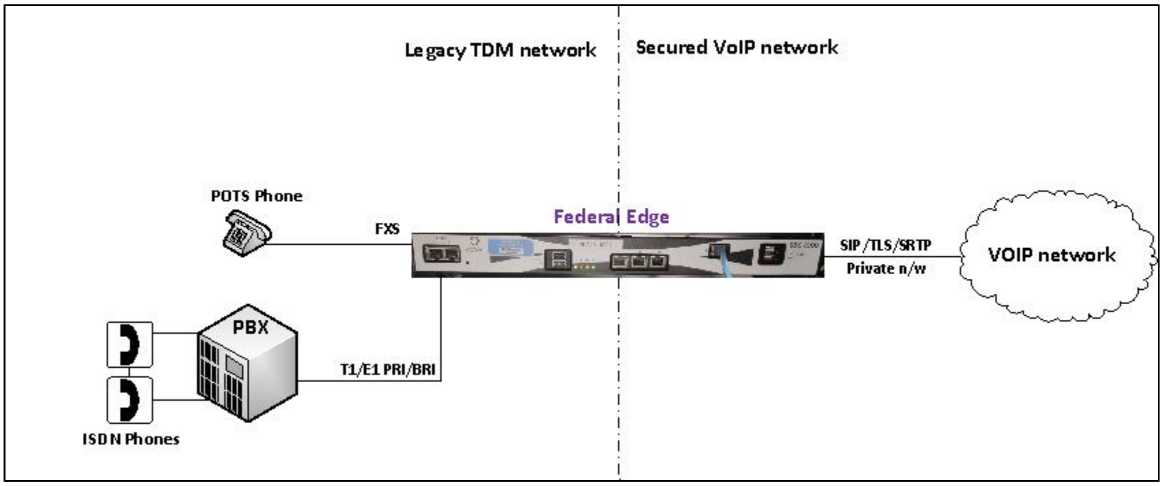
The configuration uses the following equipment and software:

	Equipment/Service	Software Version
Ribbon Communications	SBC SWe Core	V10.01.00-S000
	SBC Edge (1000 / 2000 hardware)	V11.1.0
VMware	VMware ESXi	V6.7.0 Update 3 with USB -LAN driver package
Cisco	Cisco Unified CM	12.5.1.11900-146
Avaya	IP Office	V10.1.0.2.0 Build2
Poly (Former Polycom)	Model: VVX 411 VOIP phone	5.5.2.12475
Cisco	Model: CP-8865 VOIP phone	sip8845_65.12-5-1SR3-74

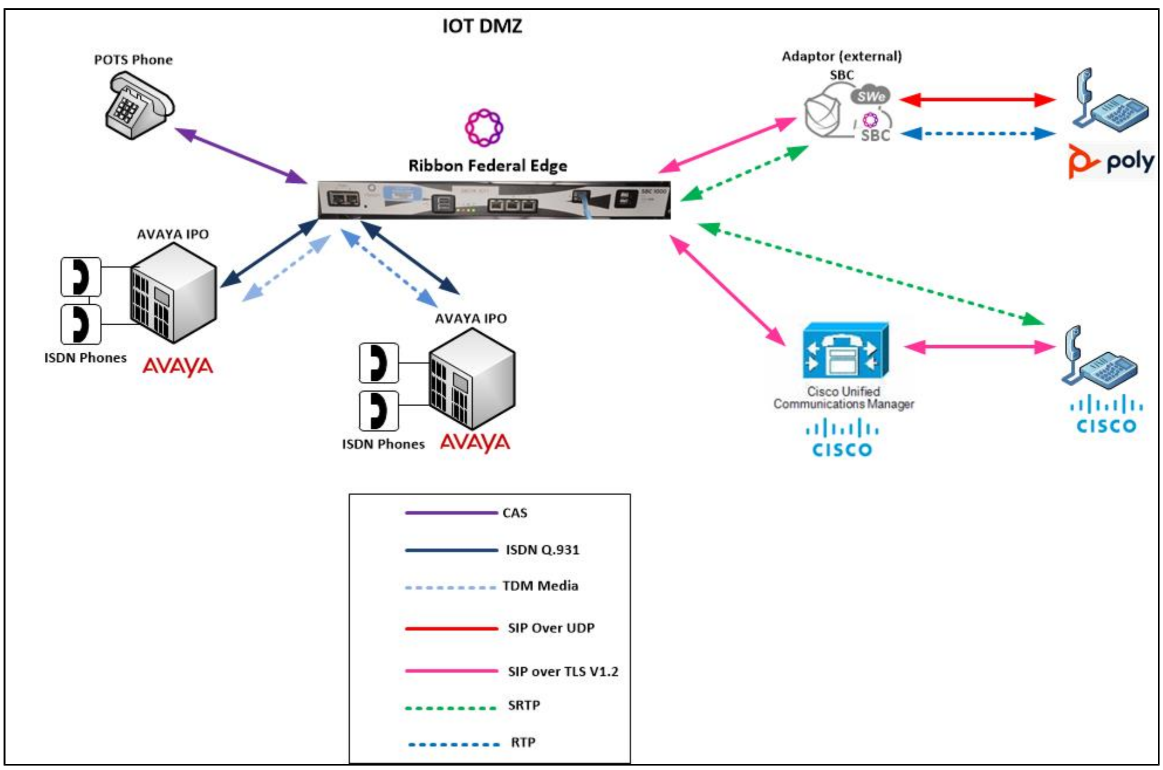
Beetel	Analog Phone	-
Administration and Debugging Tools	Wireshark	V3.0.1

Network Topology and E2E Flow Diagrams

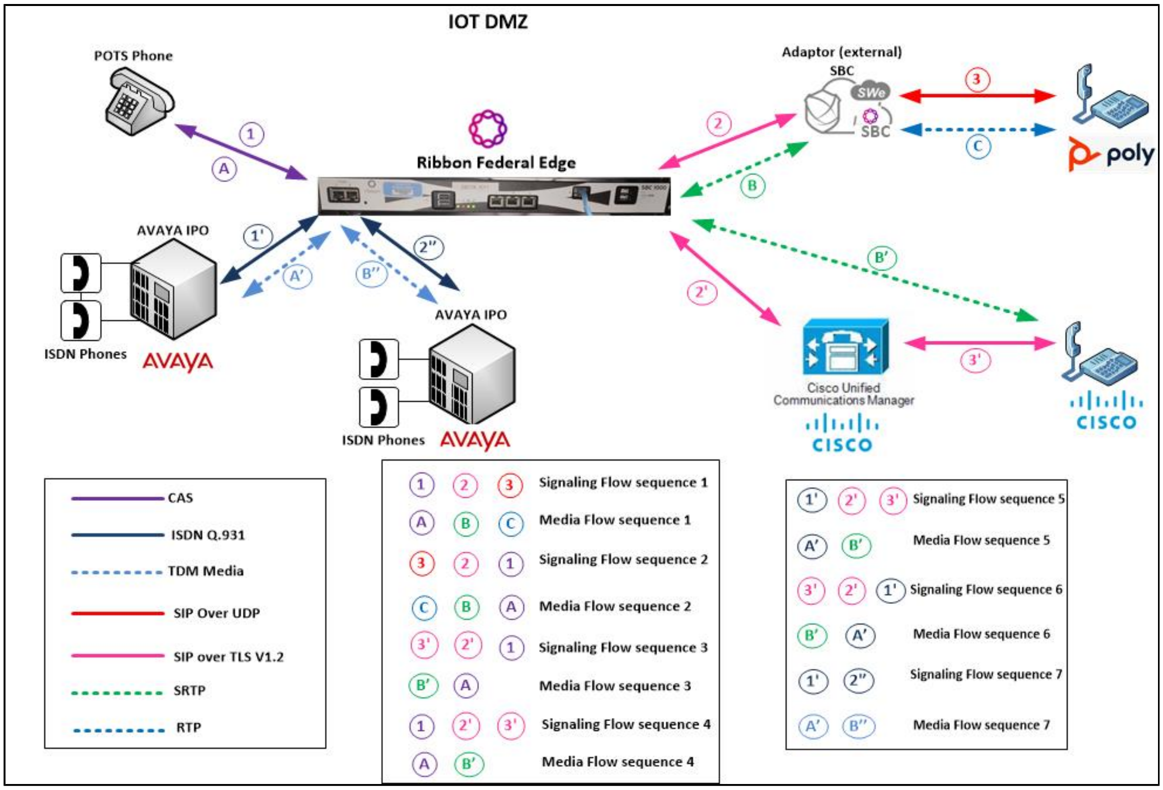
Deployment Topology



Interoperability Test Lab Topology



Call Flow Diagram

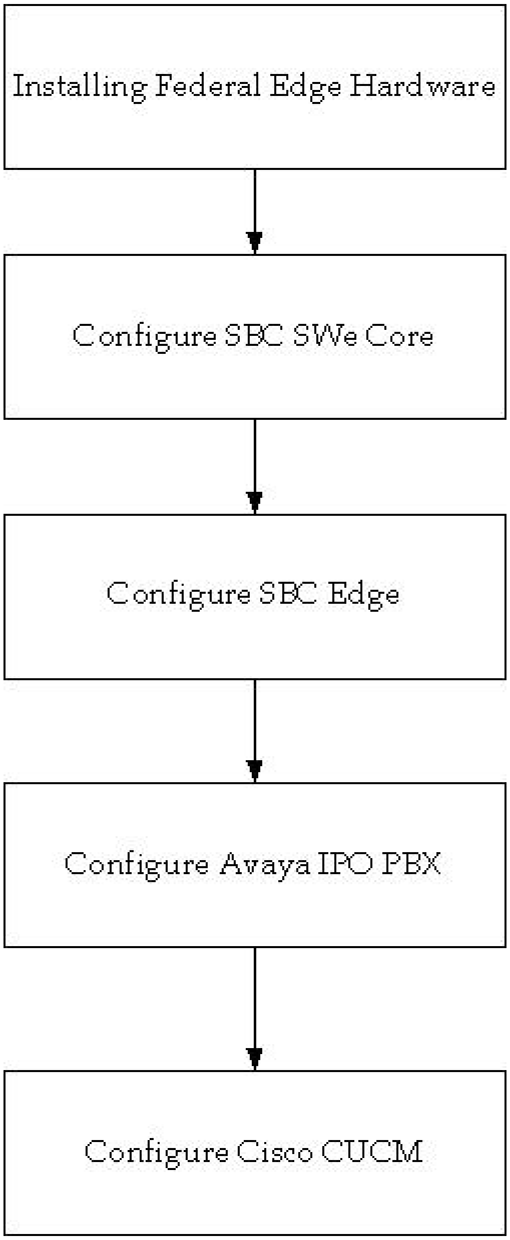


Document Workflow

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

1. Install Ribbon Federal Edge Hardware
2. Configure SBC SWe Core for VOIP connectivity with External Peer
3. Configure SBC Edge for FXS connectivity with Analog Phones and ISDN connectivity with PBX
4. Configure Avaya IPO for ISDN connectivity with Federal Edge
5. Configure Cisco CUCM for VOIP connectivity with Federal Edge

Figure 4:



Installing Ribbon Federal Edge

To deploy Federal Edge, refer to the following mentioned links:

- Install the Federal Edge Hardware
- Configure the Federal Edge Solution

Ribbon SBC SWe Core

Note 1:

All the configuration for SBC Core in upcoming section is automatically generated and applied during initial boot up at customer premise with a boot up script which asks for the following mentioned values:

- SBC System name in all **UPPERCASE** (unique name within the network which will be used to identify this SBC but it should not be matching with hostname, example: **FED2SBC1**),
- CE name (it is linux operating system's hostname and it can be a subset of System name but it has to different from System name, example: **fed2sbc1ce**)
- Management IPV4 address, Management IPV4 Prefix ((example format: 8 if netmask is 255.0.0.0 or 16 if netmask is 255.255.0.0 or 24 if netmask is 255.255.255.0)) and IPV4 Gateway
- "NTP server IPV4 address" for NTP syncing with external NTP server
- "Sig Media interface IPV4 address", "Sig Media interface IPV4 Prefix" (example format: 8 if netmask is 255.0.0.0 or 16 if netmask is 255.255.0.0 or 24 if netmask is 255.255.255.0) and "Sig Media interface IPV4 Gateway"
- DNS server IPV4 address
- Primary IP Peer address and Port (ie: External Primary SBC IP address and Port)
- Secondary IP Peer address and Port (ie: External Secondary SBC IP address and Port, if not available, enter dummy IP and port in this step)

Note 2:

The following mentioned additional configuration may need to be done manually based on customer requirement:

- TLSProfile
- StaticRouteformediaIPaddressesofExternalPeer
- ConfigurationforDISALSCSIPtrunks

Configure IP Interface Group

An IP Interface Group is a named object containing one or more IP interfaces (IP addresses). The IP Interface Group is Address Context-specific (e.g. permanently bound to a particular Address Context), and is the primary tool to manage disjointed networks (separate networks that are not designed to communicate directly). An IP Interface Group is the local manifestation of a segregated network domain. The service section of an IP trunk group and a Signaling Port typically reference an IP Interface Group in order to restrict signaling and/or media activity to that IP Interface Group.

```
set addressContext default ipInterfaceGroup INTERNAL ipInterface PKT0 ceName <CE_NAME> portName pkt0 ipAddress
169.254.10.2 prefix 24 mode outOfService state disabled
commit
set addressContext default ipInterfaceGroup INTERNAL ipInterface PKT0 mode inService state enabled
commit

set addressContext default ipInterfaceGroup EXTERNAL ipInterface PKT1 ceName <CE_NAME> portName pkt1 ipAddress
<IPaddress> prefix <prefix> mode outOfService state disabled
commit
set addressContext default ipInterfaceGroup EXTERNAL ipInterface PKT1 mode inService state enabled
commit
```

Configure Static Route

IP Static Route object specifies the gateway to which you wish to direct traffic from your Packet, Management, or Link Interface. In effect, this object allows you to add, change, and delete gateways (next Hops) to these interfaces. Interface and static routes combine to form the IP routing table for your network.

An IP Static Route provides a route to each potential call destination IP address. The static route is used to add static IP routes for the IP interfaces. A static route indicates the next Hop gateway and IP interface to use for a particular peer network IP prefix.

```
set addressContext default staticRoute <External DNS IP address> 32 <next hop IP> EXTERNAL PKT1 preference 100
commit


set addressContext default staticRoute <External Primary SBC Peer's IP Address> 32 <next hop IP> EXTERNAL PKT1
preference 100
commit

set addressContext default staticRoute <External Secondary SBC Peer's IP Address> 32 <next hop IP> EXTERNAL PKT1
preference 100
commit

set addressContext default staticRoute <External Cisco CUCM's IP address> 32 <next hop IP> EXTERNAL PKT1
preference 100
commit
```

Static Route for media IP addresses of External Peer

The following mentioned case is not part of automatic configuration. It needs to be taken care of manually.

In case the Peer's media IP address is different from Peer's SIP Signaling IP address, then they can use the following command to allow that specific media IP address or media IP address range

```
set addressContext default staticRoute <Peer's media IP address or range> <prefix> <next hop IP> EXTERNAL PKT1
preference 100
commit
```

SBC Configuration for External DNS Server

This configuration is required to configure external DNS server to which SBC need to send its DNS queries and receive the DNS response from.

```
set addressContext default dnsGroup EXT_DNS
set addressContext default dnsGroup EXT_DNS type ip interface EXTERNAL server DNS1 ipAddress <DNS IP address>
state enabled
commit
```

SBC Configuration for TLS / SRTP Profile

The Public Key Infrastructure (PKI) provides a common set of infrastructure features supporting public key and certificate-based authentication based on the RSA public/private key pairs and X.509 digital certificates. Import all the required certificated to SBC under /opt/sonus/external/.

TLS Profile creates and configures a profile for implementing the Transport Layer Security (TLS) protocol to use with SIP over TLS. TLS is an IETF protocol for securing communications across an untrusted network. Normally, SIP packets travel in plain text over TCP or UDP connections. Secure SIP is a security measure that uses TLS, the successor to the Secure Sockets Layer (SSL) protocol.

To add a TLS protection-level policy, create a TLS PROFILE and configure each of the parameters.

The TLS profile is specified on the SIP Signaling Port and controls behavior of all TLS connections established on that signaling port.

SRTP Profile

SRTP Profile is to specify the crypto algorithms required for handling SRTP media.

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

TLS Profile

TLS Profile is required for handling the TLS handshake as per customer requirement.

> The following mentioned case is not part of automatic configuration. It need to be taken care manually.

Its recommended to upload customer's own ".p12" and ".der" files in /home/sftproot/external/ as root user in linux prompt or by login to EMA and Go to "Administration" System Admin File upload.

The file names in the following command need to be changed to customer's own files. This need to be done by customer manually.

```
### client certificate .p12 file - CHANGE THIS TO ACTUAL CUSTOMER FILE AT CUSTOMER PREMISE
set system security pki certificate SBC_CERT fileName sonuscert.p12 passPhrase gsx9000 type local state enabled
commit

### NOTE: the default sonuscert.p12 file need to be replaced with customer's ".p12" file manually

### root CA .der files - CHANGE THIS TO ACTUAL CUSTOMER FILE AT CUSTOMER PREMISE
set system security pki certificate CA_CERT fileName defaultCaCert.der type remote state enabled passPhrase gsx9000
commit

### NOTE: the default defaultCaCert.der file need to be replaced with customer's ".der" file manually

set profiles security tlsProfile TLS_PROF clientCertName SBC_CERT
set profiles security tlsProfile TLS_PROF serverCertName SBC_CERT
set profiles security tlsProfile TLS_PROF acceptableCertValidationErrors invalidPurpose
set profiles security tlsProfile TLS_PROF cipherSuite1 tls_ecdhe_rsa_with_aes_256_cbc_sha384
set profiles security tlsProfile TLS_PROF cipherSuite2 tls_ecdhe_rsa_with_aes_128_cbc_sha
set profiles security tlsProfile TLS_PROF cipherSuite3 rsa-with-aes-128-cbc-sha
set profiles security tlsProfile TLS_PROF v1_1 disabled v1_0 disabled v1_2 enabled
commit

set profiles security EmaTlsProfile defaultEmaTlsProfile ClientCaCert CA_CERT
set profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName SBC_CERT
commit
set oam ema clientAuthMethod usernamePasswordOrPkiCert
commit
```

SBC Configuration for Transparency Profile

This configuration is to enable SBC to transparently pass the sip headers in received SIP messages.

```
set profiles services transparencyProfile TP_EXT_SSL state enabled
set profiles services transparencyProfile TP_EXT_SSL sipHeader to ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader via ignoreTransparency no
set profiles services transparencyProfile TP_EXT_SSL sipHeader from ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader path ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader min-se ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader contact ignoreTransparency no
set profiles services transparencyProfile TP_EXT_SSL sipHeader expires ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader require ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader request-uri ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader Service-route ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader proxy-Require ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader session-expires ignoreTransparency yes
set profiles services transparencyProfile TP_EXT_SSL sipHeader Content-Encoding excludedMethods invite,notify,info,
refer,options,update,bye,prack,cancel
set profiles services transparencyProfile TP_EXT_SSL sipHeader Resource-Priority
set profiles services transparencyProfile TP_EXT_SSL sipHeader P-Asserted-Identity ignoreTransparency no
set profiles services transparencyProfile TP_EXT_SSL sipHeader Resource-Priority
set profiles services transparencyProfile TP_EXT_SSL sipHeader P-Asserted-Identity ignoreTransparency no
set profiles services transparencyProfile TP_EXT_SSL sipMessageBody application/pidf+xml excludedMethods invite,
info,message,refer,options,update,bye,prack,cancel
set profiles services transparencyProfile TP_EXT_SSL sipMessageBody application/simple-message-summary
excludedMethods invite,info,message,refer,options,update,bye,prack,cancel
commit
```

SBC Configuration for Media Profile

This configuration is required to specify the supported codecs in SBC and transcoding setting required for this network.

```
set profiles media codecEntry G711U_SS_FED codec g711ss packetSize 20 law ULAW dtmf relay rfc2833
set profiles media codecEntry G711U_SS_FED fax toneTreatment fallbackToG711
commit
set profiles media codecEntry G711A_SS_FED codec g711ss packetSize 20 law ALAW dtmf relay rfc2833
set profiles media codecEntry G711A_SS_FED fax toneTreatment fallbackToG711
commit
set profiles media codecEntry G729AB_FED codec g729ab packetSize 20 dtmf relay rfc2833
set profiles media codecEntry G729AB_FED fax toneTreatment fallbackToG711
commit
set profiles media codecEntry G729A_FED codec g729a packetSize 20 dtmf relay rfc2833
set profiles media codecEntry G729A_FED fax toneTreatment fallbackToG711
commit



set profiles media codecEntry G711U_SS_INT codec g711ss packetSize 20 law ULAW dtmf relay rfc2833
set profiles media codecEntry G711U_SS_INT fax toneTreatment fallbackToG711
commit
set profiles media codecEntry G711A_SS_INT codec g711ss packetSize 20 law ALAW dtmf relay rfc2833
set profiles media codecEntry G711A_SS_INT fax toneTreatment fallbackToG711
commit


### MEDIA PROFILE ON INTERNAL SIDE


set profiles media packetServiceProfile INTERNAL_PSP codec codecEntry1 G711U_SS_INT
set profiles media packetServiceProfile INTERNAL_PSP codec codecEntry2 G711A_SS_INT
set profiles media packetServiceProfile INTERNAL_PSP rtcpOptions rtcp disable
set profiles media packetServiceProfile INTERNAL_PSP peerAbsenceAction none
set profiles media packetServiceProfile INTERNAL_PSP silenceInsertionDescriptor g711SidRtpPayloadType 13
set profiles media packetServiceProfile INTERNAL_PSP silenceInsertionDescriptor heartbeat enable
set profiles media packetServiceProfile INTERNAL_PSP aal1PayloadSize 47
set profiles media packetServiceProfile INTERNAL_PSP packetToPacketControl transcode conditional
set profiles media packetServiceProfile INTERNAL_PSP packetToPacketControl codecsAllowedForTranscoding thisLeg ""
set profiles media packetServiceProfile INTERNAL_PSP packetToPacketControl codecsAllowedForTranscoding otherLeg ""
set profiles media packetServiceProfile INTERNAL_PSP flags digitDetectSendEnabled disable
set profiles media packetServiceProfile INTERNAL_PSP flags useDirectMedia disable
set profiles media packetServiceProfile INTERNAL_PSP secureRtpRtcp flags allowFallback disable
set profiles media packetServiceProfile INTERNAL_PSP secureRtpRtcp flags enableSrtp disable
set profiles media packetServiceProfile INTERNAL_PSP secureRtpRtcp flags resetROCOnKeyChange disable
set profiles media packetServiceProfile INTERNAL_PSP secureRtpRtcp flags resetEncDecROCOnDecKeyChange disable
set profiles media packetServiceProfile INTERNAL_PSP secureRtpRtcp flags updateCryptoKeysOnModify disable
set profiles media packetServiceProfile INTERNAL_PSP secureRtpRtcp flags allowPassthru disable
set profiles media packetServiceProfile INTERNAL_PSP preferredRtpPayloadTypeForDtmfRelay 101
set profiles media packetServiceProfile INTERNAL_PSP honorRemotePrecedence disable
set profiles media packetServiceProfile INTERNAL_PSP sendRoutePSPPrecedence disable
commit



### MEDIA PROFILE ON EXTERNAL SIDE

set profiles media packetServiceProfile EXTERNAL_PSP codec codecEntry1 G711U_SS_FED
set profiles media packetServiceProfile EXTERNAL_PSP codec codecEntry2 G711A_SS_FED
set profiles media packetServiceProfile EXTERNAL_PSP codec codecEntry3 G729AB_FED
set profiles media packetServiceProfile EXTERNAL_PSP codec codecEntry4 G729A_FED
set profiles media packetServiceProfile EXTERNAL_PSP packetToPacketControl transcode conditional
set profiles media packetServiceProfile EXTERNAL_PSP packetToPacketControl codecsAllowedForTranscoding thisLeg g729
set profiles media packetServiceProfile EXTERNAL_PSP packetToPacketControl codecsAllowedForTranscoding otherLeg
g711u

set profiles media packetServiceProfile EXTERNAL_PSP rtcpOptions rtcp enable terminationForPassthrough enable
set profiles media packetServiceProfile EXTERNAL_PSP preferredRtpPayloadTypeForDtmfRelay 101
set profiles media packetServiceProfile EXTERNAL_PSP silenceInsertionDescriptor g711SidRtpPayloadType 13 heartbeat
enable
set profiles media packetServiceProfile EXTERNAL_PSP secureRtpRtcp flags enableSrtp enable
set profiles media packetServiceProfile EXTERNAL_PSP secureRtpRtcp flags allowFallback enable
set profiles media packetServiceProfile EXTERNAL_PSP secureRtpRtcp cryptoSuiteProfile CRYPT_PROF
commit
```

SBC Configuration for External Network

Create External Zone and configure sipSigPort for connecting to external network.

A Zone is used to group a set of objects unique to a particular customer environment.

A SIP Signaling Port is a logical address permanently bound to a specific zone, and is used to send and receive SIP call signaling packets. A SIP Signaling Port is capable of multiple transports such as UDP, TCP, and TLS/TCP. Here, we use TLS for Federal Edge.

```
set addressContext default zone EXTERNAL_ZONE id 3
commit

### EXTERNAL SIP SIGNALING IP
set addressContext default zone EXTERNAL_ZONE id 3 sipSigPort 1 ipInterfaceGroupName EXTERNAL ipAddressV4 <SIP
signaling IP> portNumber 5060 transportProtocolsAllowed sip-tls-tcp
set addressContext default zone EXTERNAL_ZONE id 3 sipSigPort 1 state enabled mode inService
commit


### DNS linked to EXTERNAL TG
set addressContext default zone EXTERNAL_ZONE dnsGroup EXT_DNS
commit

### ASSIGN TLS PROFILE TO SIP SIGNALING PORT

set addressContext default zone EXTERNAL_ZONE sipSigPort 1 state disabled mode outOfService
commit

set addressContext default zone EXTERNAL_ZONE sipSigPort 1 tlsProfileName TLS_PROF
set addressContext default zone EXTERNAL_ZONE sipSigPort 1 state enabled mode inService
commit
```

SIP TG Towards External Network

SIP Trunk Groups are used to apply a wide-ranging set of call management functions to a group of peer devices (endpoints) within the network. SIP Trunk Groups are created within a specific address context and zone.

All SBC signaling and routing (both Trunking and Access) are based upon Trunk Group configurations defined within zones. A zone can contain multiple Trunk Groups.

```
### EXTERNAL TG SIP SIGNALING SETTINGS

set profiles signaling ipSignalingProfile EXTERNAL_IPSP ipProtocolType sipOnly
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags includeReasonHeader enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags
includeTransportTypeInContactHeader enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags routeUsingRecvdFqdn enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags sendPtimeInSdp enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags sendRtcpPortInSdp enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags storePChargingVector enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags publishIPInHoldSDP enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes relayFlags statusCode4xx6xx enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags
minimizeRelayingOfMediaChangesFromOtherCallLegAll enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags
relayDataPathModeChangeFromOtherCallLeg enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes flags disableMediaLockDown enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP commonIpAttributes optionTagInRequireHeader
suppressReplaceTag enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes numberGlobalizationProfile DEFAULT_IP
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes flags disable2806Compliance enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes domainName
useIpSignalingPeerDomainInRequestUri enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes domainName useSipDomainInPAIHeader
enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes domainName useSipDomainNameInFromField
enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes domainName
useZoneLevelDomainNameInContact enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes privacy transparency disable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes privacy privacyInformation pPreferredId
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes privacy flags includePrivacy enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes privacy flags privacyRequiredByProxy
disable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes privacy flags msLyncPrivacySupport
enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes redirect flags
forceRequeryForRedirection enable
set profiles signaling ipSignalingProfile EXTERNAL_IPSP egressIpAttributes transport type1 tlsOverTcp
set profiles signaling ipSignalingProfile EXTERNAL_IPSP ingressIpAttributes flags sendSdpIn200OkIf18xReliable
enable
commit

### EXTERNAL TG TOWARDS NON-TEAMS USERS

set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG media mediaIpInterfaceGroupName EXTERNAL
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG policy media packetServiceProfile
EXTERNAL_PSP
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG policy signaling ipSignalingProfile
EXTERNAL_IPSP
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG signaling rel100Support enabled
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG services dnsSupportType a-only
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG services natTraversal iceSupport none
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG ingressIpPrefix <External Primary SBC
Peer's IP Address> 32
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG ingressIpPrefix <External Secondary SBC
Peer's IP Address> 32
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG signaling honorMaddrParam enabled
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG signaling relayNonInviteRequest enabled
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG media sdpAttributesSelectiveRelay enabled
set addressContext default zone EXTERNAL_ZONE sipTrunkGroup EXTERNAL_TG mode inService state enabled
commit
```

SBC Configuration Towards SBC Edge

Create a new INTERNAL zone and sip signaling port to communicate with SBC Edge. It's UDP as it's internal between SBC SWe Core and SBC Edge.

```
### INTERNAL ZONE FOR SBC1K/2K COMMUNICATION

set addressContext default zone INTERNAL_ZONE id 2
commit

### INTERNAL SIP SIGNALING IP
set addressContext default zone INTERNAL_ZONE id 2 sipSigPort 2 ipInterfaceGroupName INTERNAL ipAddressV4
169.254.10.2 portNumber 5060 transportProtocolsAllowed sip-udp
commit
set addressContext default zone INTERNAL_ZONE id 2 sipSigPort 2 mode inService state enabled
commit
```

SIP TG for Internal zone

Create a new Trunk group and attach it to a zone.

```
### INTERNAL TG SIGNALING SETTINGS
set profiles signaling ipSignalingProfile INTERNAL_IPSP ipProtocolType sipOnly
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags includeReasonHeader enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags
includeTransportTypeInContactHeader enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags
minimizeRelayingOfMediaChangesFromOtherCallLegAll enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags
relayDataPathModeChangeFromOtherCallLeg enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags disableMediaLockDown enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags sendPtimeInSdp enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP commonIpAttributes flags lockDownPreferredCodec enable
set profiles signaling ipSignalingProfile INTERNAL_IPSP egressIpAttributes flags disable2806Compliance enable
commit

### INTERNAL TG

set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG media mediaIpInterfaceGroupName INTERNAL
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG signaling rel100Support enabled
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG services dnsSupportType a-only
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG services natTraversal iceSupport none
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG ingressIpPrefix 169.254.10.1 32
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG signaling honorMaddrParam enabled
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG signaling relayNonInviteRequest enabled
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG media sdpAttributesSelectiveRelay enabled
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG media lateMediaSupport passthru
set addressContext default zone INTERNAL_ZONE sipTrunkGroup INTERNAL_TG mode inService state enabled
commit
```

SBC Configuration for Call Routing

This section is to create and configure call routing.

```
### CALL ROUTING PRIORITY
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry _private 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry nationalOperator 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry localOperator 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry nationalType 1 entityType trunkGroup
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry nationalType 2 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry internationalType 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry internationalOperator 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry longDistanceOperator 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry ipVpnService 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry test 1 entityType none
```

```
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry transit 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry otherCarrierChosen 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry carrierCutThrough 1 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry userName 1 entityType trunkGroup
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry userName 2 entityType none
set profiles callRouting elementRoutingPriority ROUTING_PRIORITY entry mobile 1 entityType none
commit

### PEERS

### INTERNAL SBC1K/2K PEER

set addressContext default zone INTERNAL_ZONE ipPeer INTERNAL_PEER ipAddress 169.254.10.1 ipPort 5060
commit


### TO EXTERNAL SBC5400

set addressContext default zone EXTERNAL_ZONE ipPeer EXTERNAL_PEER1 ipAddress <External Primary SBC Peer's IP
Address> ipPort 5060
commit

set addressContext default zone EXTERNAL_ZONE ipPeer EXTERNAL_PEER2 ipAddress <External Primary SBC Peer's IP
Address> ipPort 5060
commit

### INTERNAL ROUTE TOWARDS SBC1K2K
set global callRouting routingLabel INTERNAL_RL routingLabelRoute 1 trunkGroup INTERNAL_TG ipPeer INTERNAL_PEER
inService inService
commit


### EXTERNAL ROUTE TOWARDS SBC 5400

set global callRouting routingLabel EXTERNAL_RL overflowNumber ""
set global callRouting routingLabel EXTERNAL_RL overflowNOA none
set global callRouting routingLabel EXTERNAL_RL overflowNPI none
set global callRouting routingLabel EXTERNAL_RL routePrioritizationType sequence
set global callRouting routingLabel EXTERNAL_RL action routes
set global callRouting routingLabel EXTERNAL_RL numRoutesPerCall 10
commit


set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 routeType trunkGroup
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 trunkGroup EXTERNAL_TG
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 ipPeer EXTERNAL_PEER1
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 proportion 0
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 cost 1000000
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 inService inService
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 1 testing normal
commit

set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 routeType trunkGroup
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 trunkGroup EXTERNAL_TG
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 ipPeer EXTERNAL_PEER2
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 proportion 0
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 cost 1000000
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 inService inService
set global callRouting routingLabel EXTERNAL_RL routingLabelRoute 2 testing normal
commit

### TG BASED ROUTING TOWARDS INTERNAL PSTN
set global callRouting route trunkGroup EXTERNAL_TG FED1KCORE standard Sonus_NULL Sonus_NULL all all ALL none
Sonus_NULL routingLabel INTERNAL_RL
commit
set global callRouting route trunkGroup EXTERNAL_TG FED1KCORE username Sonus_NULL Sonus_NULL all all ALL none
Sonus_NULL routingLabel INTERNAL_RL
commit

### TG BASED ROUTING TOWARDS EXTERNAL SBC 5400
set global callRouting route trunkGroup INTERNAL_TG FED1KCORE standard Sonus_NULL Sonus_NULL all all ALL none
Sonus_NULL routingLabel EXTERNAL_RL
```

```
commit
set global callRouting route trunkGroup INTERNAL_TG FED1KCORE username Sonus_NULL Sonus_NULL all all ALL none
Sonus_NULL routingLabel EXTERNAL_RL
commit
```

ACL Rules for NTP and Web Proxy Feature on SBC SWe Core

This section configures ACL rules required for NTP sync between SBC Edge and SBC Core and for accessing the SBC Edge UI via SBC Core EMA.

```
### ACLs for NTP and Web Proxy
set addressContext default ipAccessControlList rule Sbc1k2kNtpAccess precedence 1 protocol udp ipInterfaceGroup
INTERNAL ipInterface PKT0 destinationPort 123 fillRate 2000 bucketSize 50 state enabled
set addressContext default ipAccessControlList rule Sbc1k2kEmaAccess precedence 2 protocol any ipInterfaceGroup
INTERNAL ipInterface PKT0 sourcePort 32443 fillRate 2000 bucketSize 50 state enabled
```

FIPS Configuration

This configuration enables FIPS-140-2 security on SBC.

```
##FIPS Configuration.. Always keep this at last##
set profiles security tlsProfile defaultTlsProfile v1_0 disabled v1_1 disabled v1_2 enabled
set profiles security EmaTlsProfile defaultEmaTlsProfile v1_0 disabled v1_1 disabled v1_2 enabled
set oam snmp version v3only
set system admin FED1KCORE fips-140-2 mode enabled
commit
```

Configuration for DISA LSC SIP trunks

The following case mentioned is not part of automatic configuration. It need to be taken care manually.

Ports and protocols for SIP trunk:

- Signaling (SIP/TLS) - TCP 5061 bi-directional
- Media (SRTP) - UDP 16384-32764 bi-directional

Connection/Certs Notes:

- Any IP address must be allowed to get to your SBC address for media purposes.
- On your SBC, you must have root CA-3 from a CSR and intermediate CA-53/54/60 certs.
- In-band DTMF (RFC 2833) i.e. 101 telephone-events are supported
- Ping-method, Option pings every 30 seconds, keep-alive *(Refer the attached SMM rule to create and apply in the Ribbon SBC DISA sipTrkGrp)*
- TCP keep-alive enabled
- The CCA-ID for your site must be sent on the contact line of the INVITE message for the WANSS to process the call *(Refer the attached SMM rule to create and apply in the Ribbon SBC DISA sipTrkGrp) Note: CCA-ID unique for each site*

Device Note:

Only SRTP is sent. If phones are not secure, then there has to be an SRTP to RTP conversion done at your SBC.

SMM_Rule_CCA_ID...Disa_SipTrk.txt

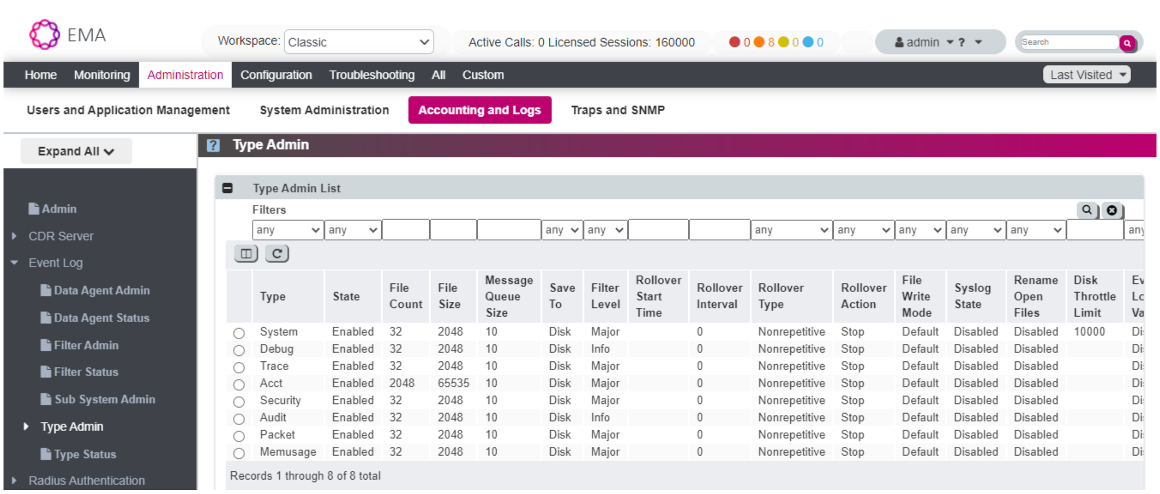
SMM_Rule_for_Di...Trk_OPTIONS.txt

Troubleshooting SBC SWe Core

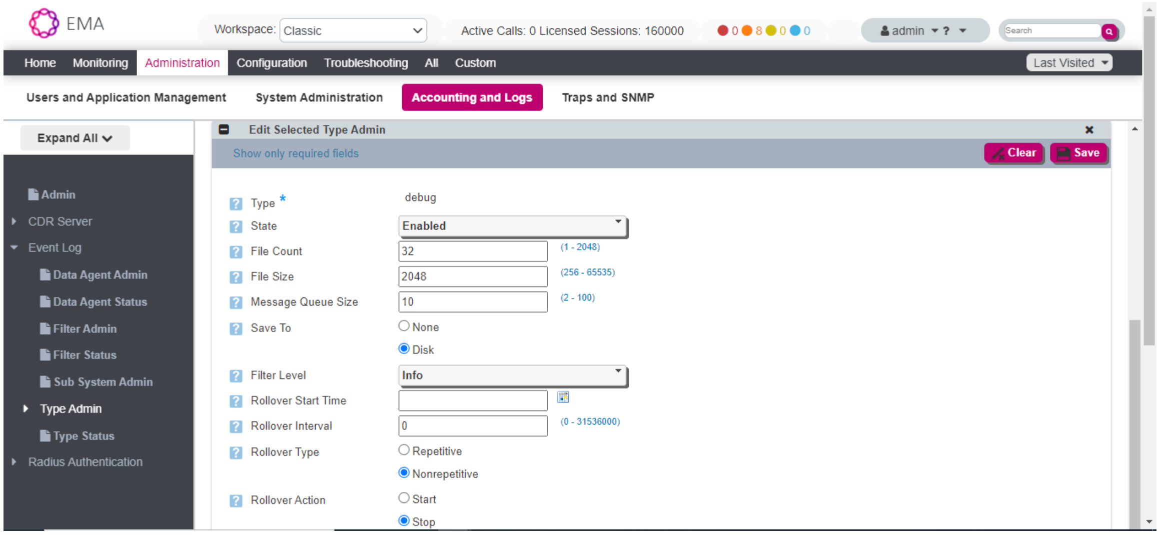
For troubleshooting single call issue, one can use "Debug log" during no load scenario (or) one can use "Call Trace" option during load scenario.

Debug Log

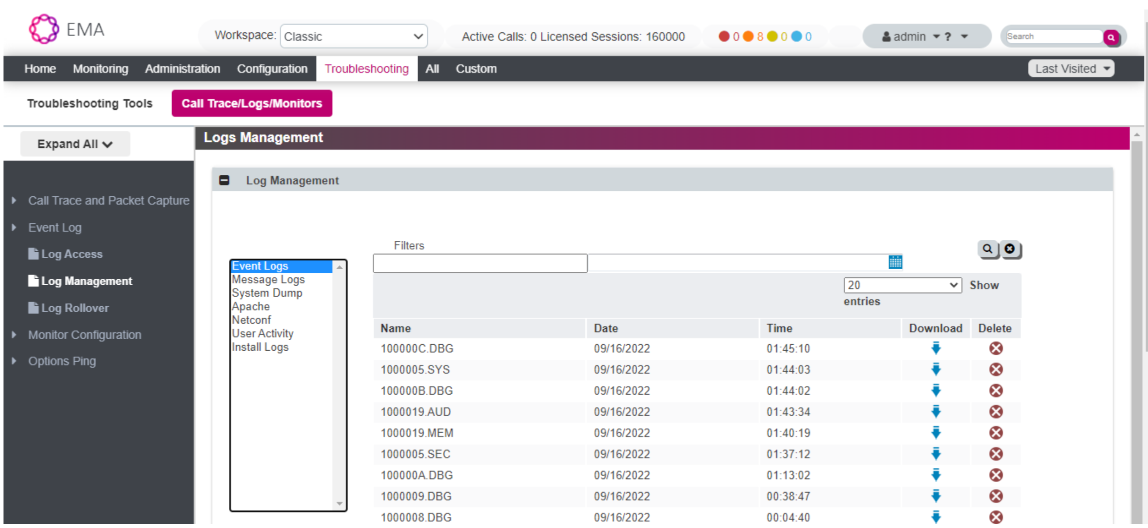
Login to SBC SWe Core's EMA in web browser using the mgmt IPV4 address and then click "Administration" "Accounting and Logs" "Event Log" "Type Admin"



Select Type as "Debug" and set the "Filter Level" to "Info" & click "Save" for debugging during no load scenario and then revert back to "Major" & Click "Save" once the debugging is done or once traffic usage starts.



Go to "Troubleshooting" "Call Trace/Logs/Monitors" "Event Log" "Log Management" and Select "Event Logs" and click Download icon against the **". DBG" File** log for troubleshooting



Accounting Log

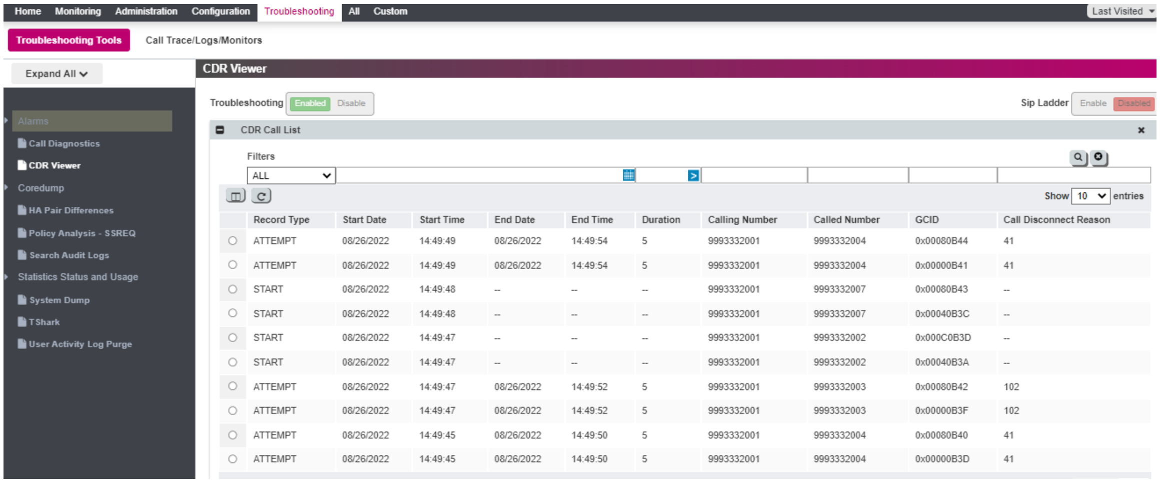
Accounting logs are the CDR files which capture successful and failed calls. Start, Stop, Intermediate records for every calls can be captured and Attempt records can be captured for Failed call.

Go to "Troubleshooting" "Call Trace/Logs/Monitors" "Event Log" "Log Management" and Select "Event Logs" and click Download icon against the **". ACT" File** log for processing CDR files.

CDR Viewer

This is another option to view CDR files. Go to ""Troubleshooting" "Troubleshooting Tools" CDR Viewer.

Click "Enable" on the right pane. Make some calls and you can see each CDRs getting listed with few basic information including call disconnect reason.



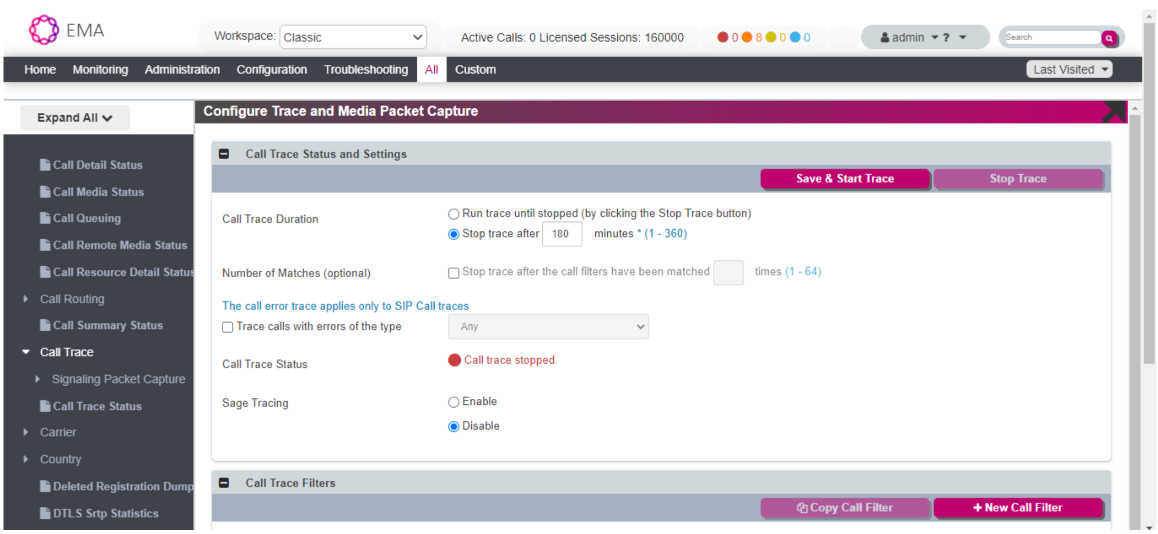
If you want to troubleshoot some specific failed calls, you can use the following mentioned "Call Trace" option.

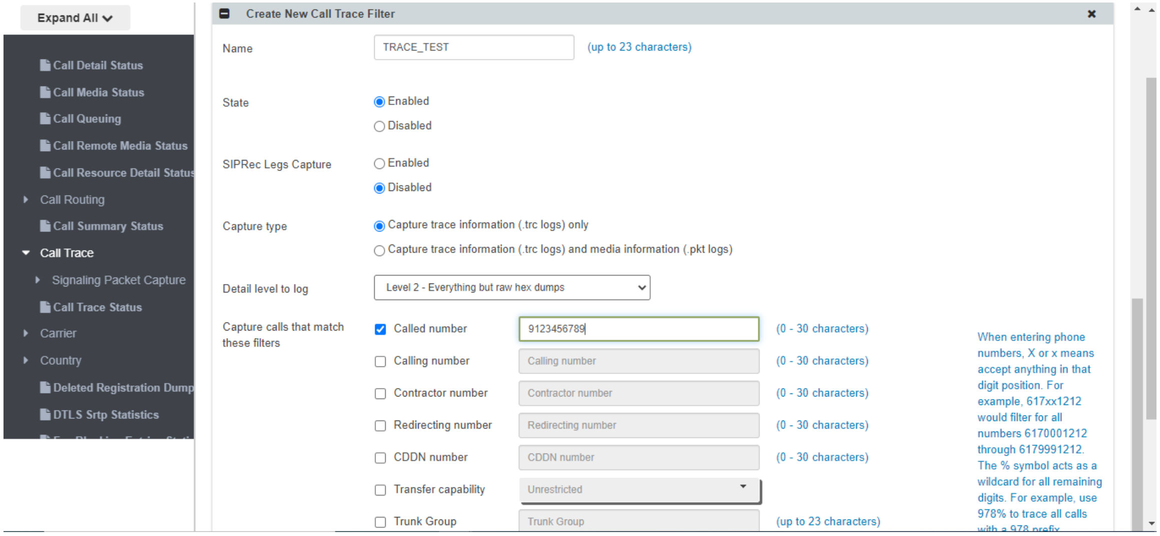
Call Trace

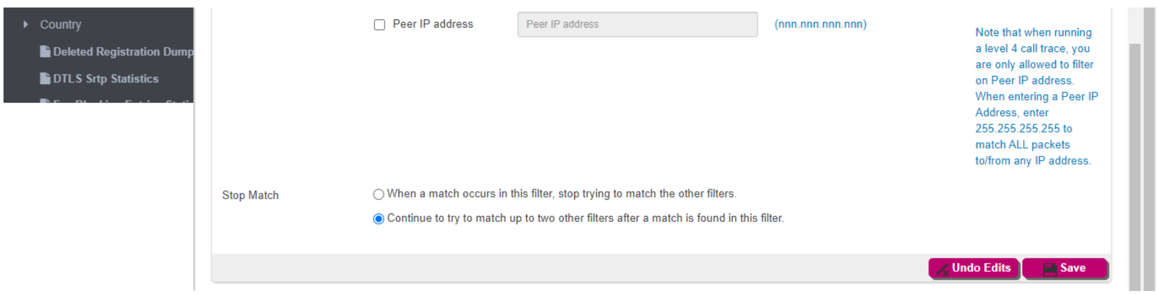
For debugging particular call using called number or calling number etc in production, one can use the following mentioned option.

Go to "Troubleshooting" "Call Trace and Packet Capture" "Call Trace" "+New Call Filter".

Enter "Name" of the Call Filter and set "state" to enabled and set "Capture calls that match these filters" to either "Called number" or calling number or any other filters or any combination of these filters and then click "save".





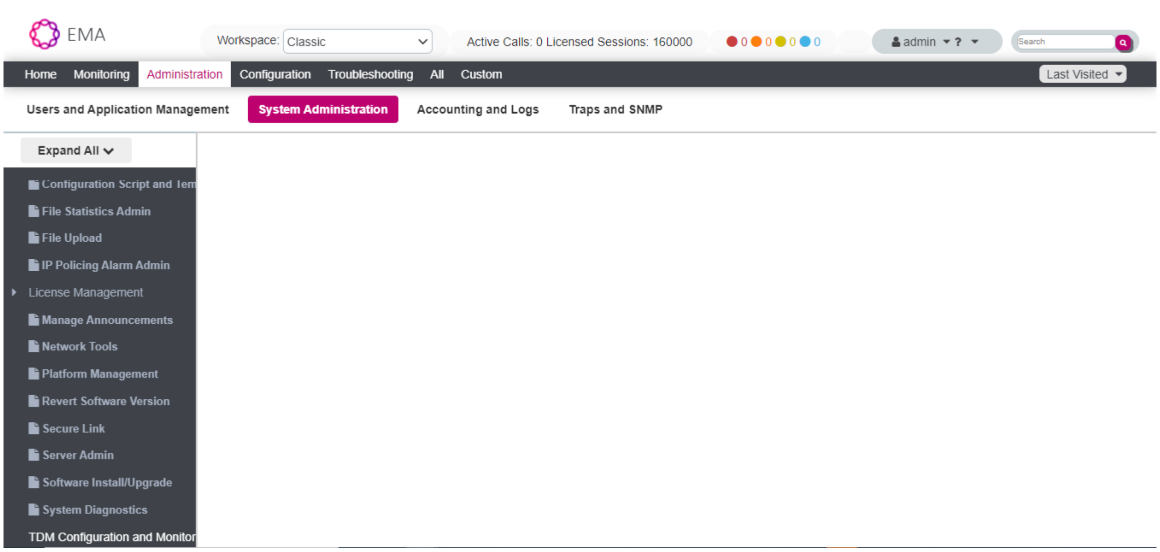


Make a call matching the set filters and check the .TRC File for debugging using the following mentioned step.

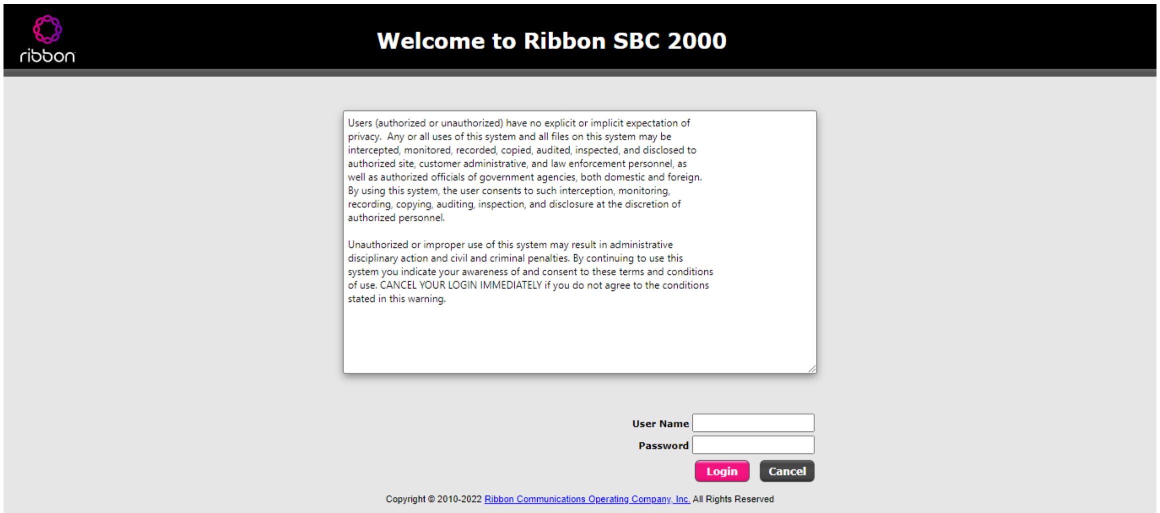
Go to "Troubleshooting" "Call Trace/Logs/Monitors" "Event Log" "Log Management" and Select "Event Logs" and click Download icon against the **". TRC" File** for troubleshooting.

Ribbon SBC Edge Configuration

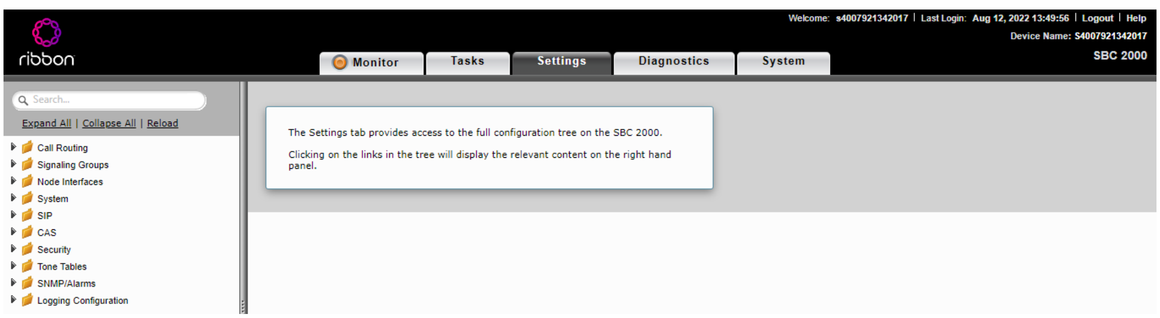
- Login to SBC Edge (2000 or 1000) via EMA GUI login using web browser by typing EMA IP address.
- Once the EMA page is opened, Go to "Administration System Administration TDM Configuration & Monitoring".



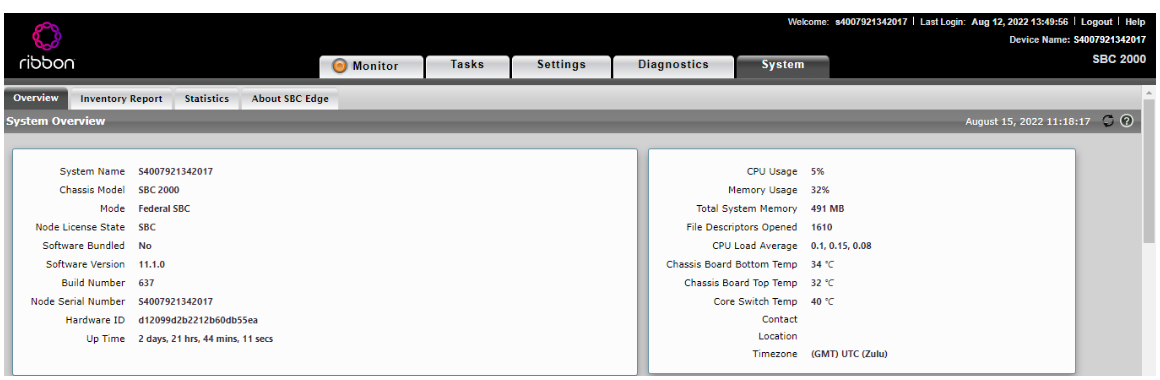
- Upon clicking "TDM Configuration and Monitoring", the SBC Edge Login page will appear in a new Tab.



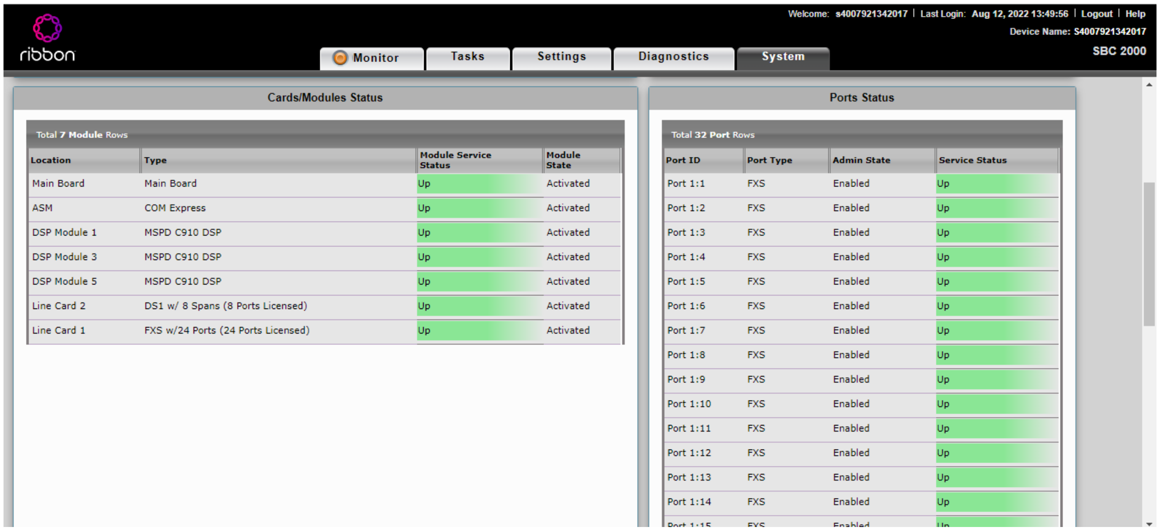
1. Enter the login credentials, and it will take you to the following page.



- Go to System Tab and check the current build name to ensure the required build is in place.

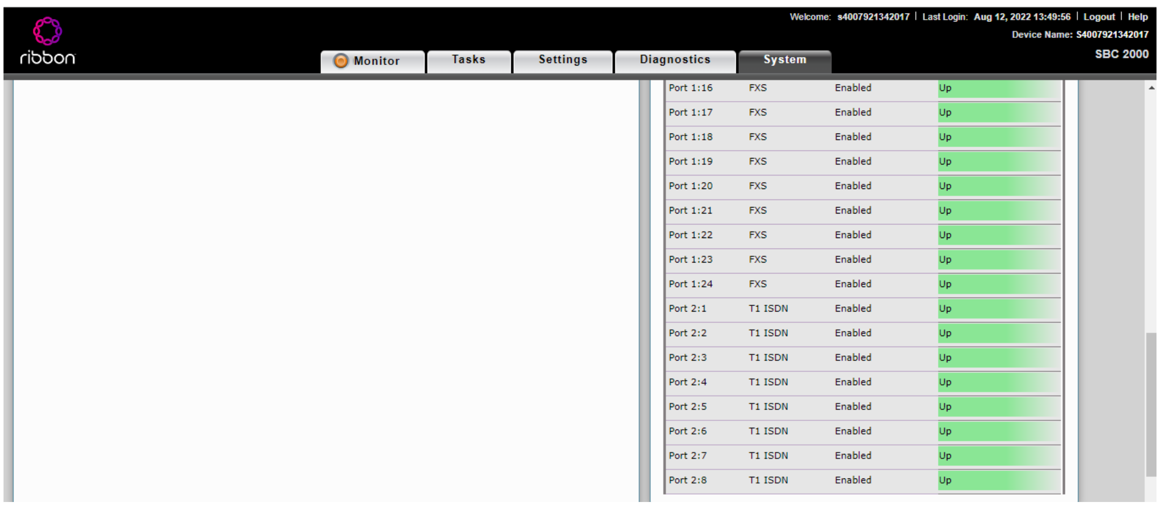


- Check the required TDM Ports (FXS/ISDN) are displayed as ordered by customer.



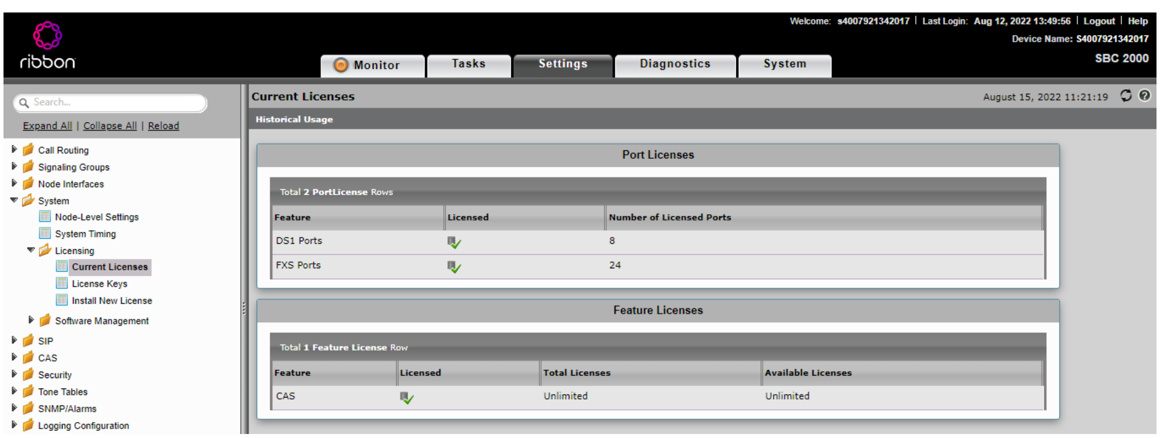
Location	Type	Module Service Status	Module State
Main Board	Main Board	Up	Activated
ASM	COM Express	Up	Activated
DSP Module 1	MSPD C910 DSP	Up	Activated
DSP Module 3	MSPD C910 DSP	Up	Activated
DSP Module 5	MSPD C910 DSP	Up	Activated
Line Card 2	DS1 w/ 8 Spans (8 Ports Licensed)	Up	Activated
Line Card 1	FXS w/24 Ports (24 Ports Licensed)	Up	Activated

Port ID	Port Type	Admin State	Service Status
Port 1:1	FXS	Enabled	Up
Port 1:2	FXS	Enabled	Up
Port 1:3	FXS	Enabled	Up
Port 1:4	FXS	Enabled	Up
Port 1:5	FXS	Enabled	Up
Port 1:6	FXS	Enabled	Up
Port 1:7	FXS	Enabled	Up
Port 1:8	FXS	Enabled	Up
Port 1:9	FXS	Enabled	Up
Port 1:10	FXS	Enabled	Up
Port 1:11	FXS	Enabled	Up
Port 1:12	FXS	Enabled	Up
Port 1:13	FXS	Enabled	Up
Port 1:14	FXS	Enabled	Up



Port 1:16	FXS	Enabled	Up
Port 1:17	FXS	Enabled	Up
Port 1:18	FXS	Enabled	Up
Port 1:19	FXS	Enabled	Up
Port 1:20	FXS	Enabled	Up
Port 1:21	FXS	Enabled	Up
Port 1:22	FXS	Enabled	Up
Port 1:23	FXS	Enabled	Up
Port 1:24	FXS	Enabled	Up
Port 2:1	T1 ISDN	Enabled	Up
Port 2:2	T1 ISDN	Enabled	Up
Port 2:3	T1 ISDN	Enabled	Up
Port 2:4	T1 ISDN	Enabled	Up
Port 2:5	T1 ISDN	Enabled	Up
Port 2:6	T1 ISDN	Enabled	Up
Port 2:7	T1 ISDN	Enabled	Up
Port 2:8	T1 ISDN	Enabled	Up

- Check the current licenses by going to "Settings" Tab System Licensing Current Licenses.

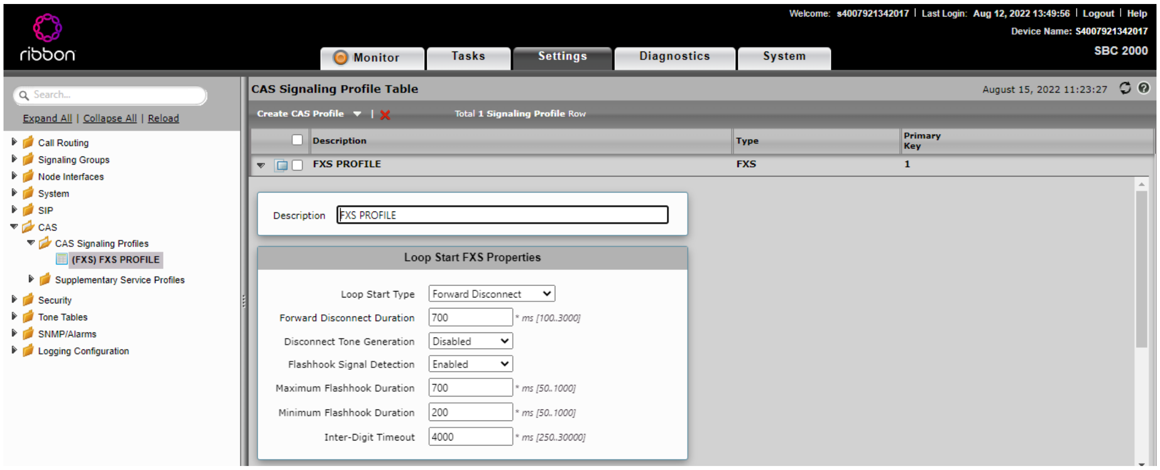


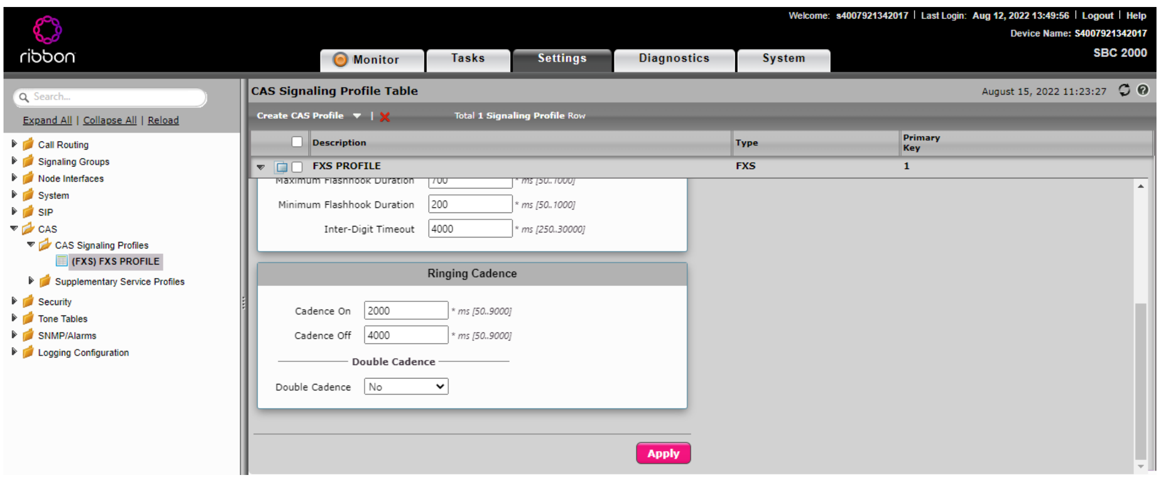
Feature	Licensed	Number of Licensed Ports
DS1 Ports	✓	8
FXS Ports	✓	24

Feature	Licensed	Total Licenses	Available Licenses
CAS	✓	Unlimited	Unlimited

FXS Configuration

Configure CAS Profile by going to "Settings" tab CAS CAS Signaling Profiles Create CAS Profile.

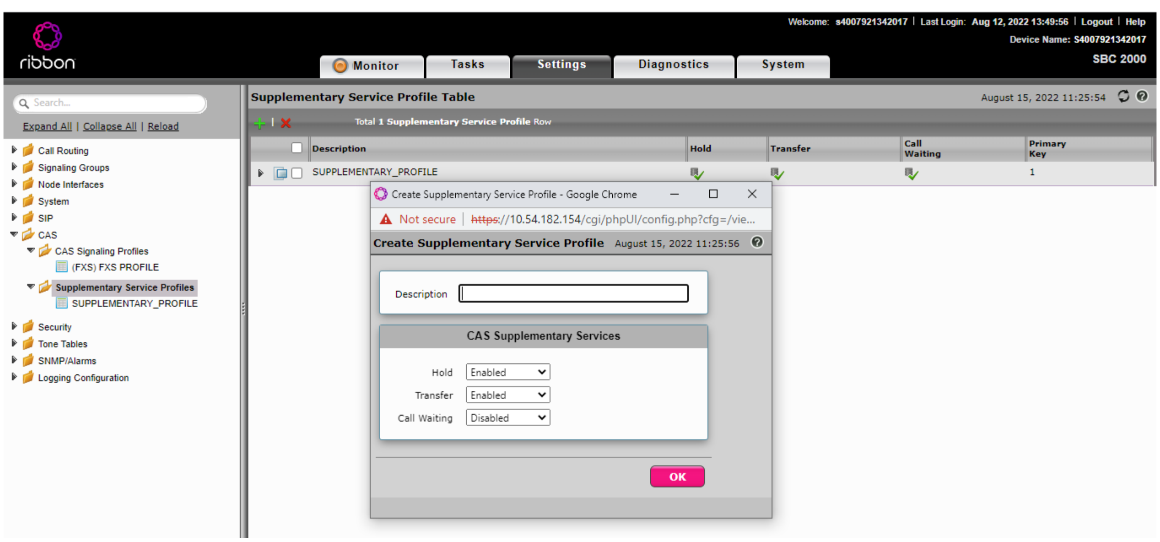


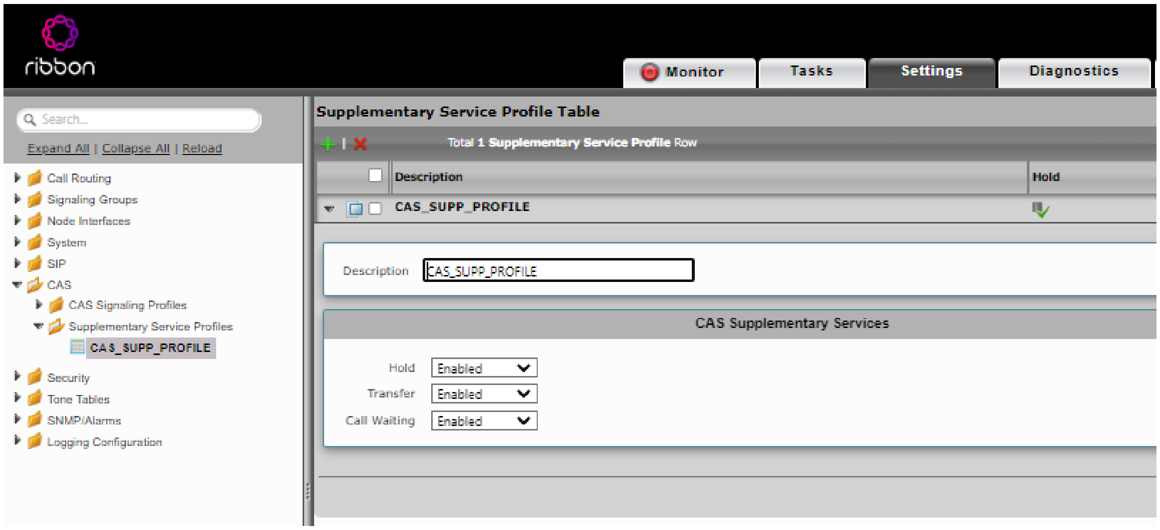


- Click Apply once all settings are chosen as required.

CAS Supplementary Service Profile

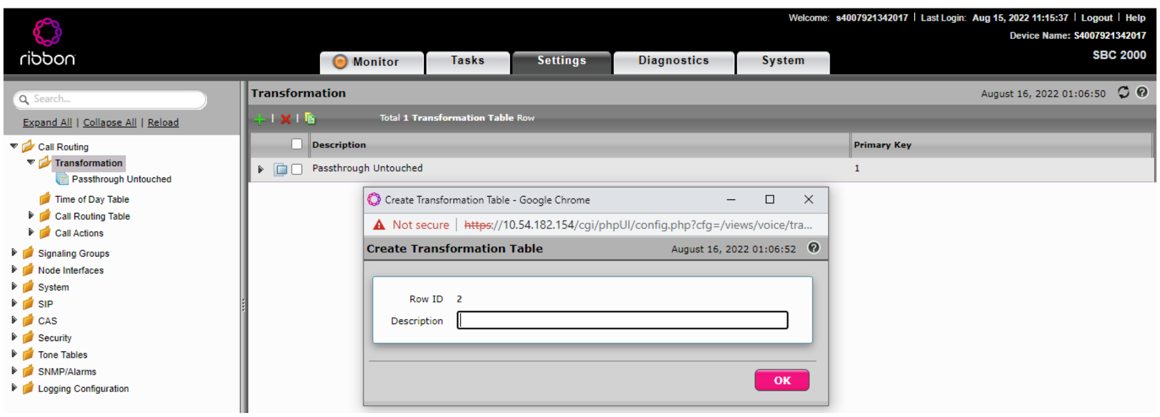
- Create CAS Supplementary service Profile by going to "Settings" tab CAS Supplementary service Profiles Create CAS Profile.
- Enable Call Hold, Call Transfer, Call waiting services.





Call Transformation Table

- Go to Settings Call routing Transformation Click + symbol to create new transformation table.
- This is required to match the incoming called number and any alteration required for that number in order to select a particular Destination signaling group (SIP signaling group or ISDN signaling group or FXS signaling group). One needs to create separate Transformation Table for calls destined to FXS and calls destined to ISDN.



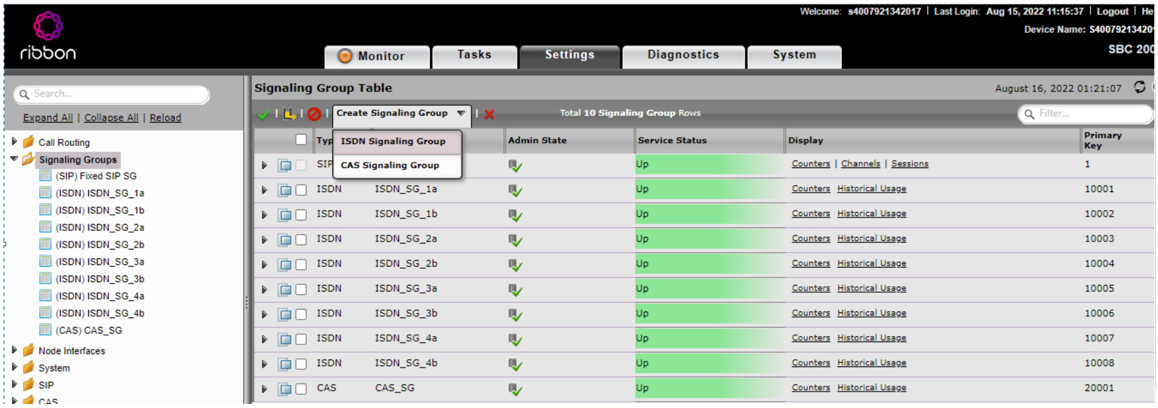
Signaling Groups

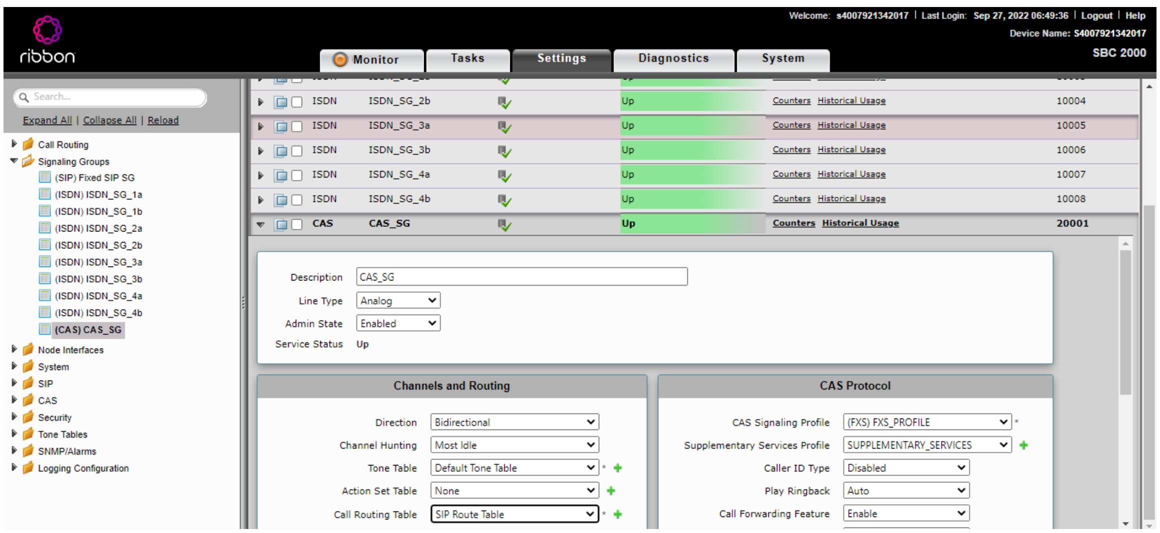
There will be default SIP signaling group called "**Fixed SIP SG**" which one cannot modify.

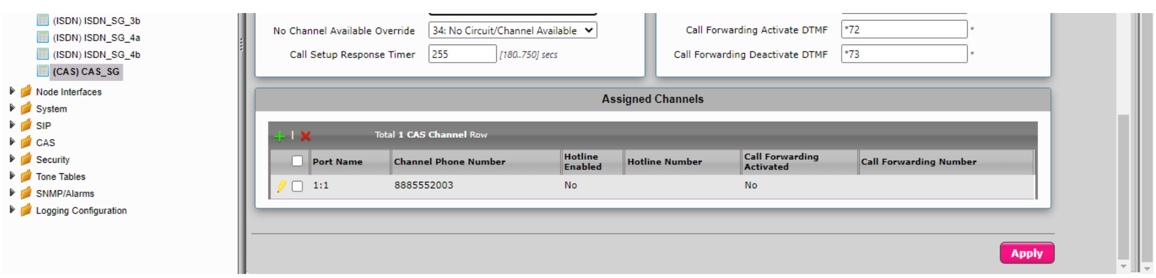
Hence, one need to create and configure ISDN (PRI) / FXS (CAS) signaling groups.

CAS Signaling Group

- Go to Settings Signaling groups Click + to create CAS signaling group (say, **CAS_SG**).
- Link the required Call routing table, CAS Signaling profile, Supplementary service profile and the required FXS Port & corresponding phone number.
- Leave the rest to default values including default Call Routing table "SIP Route Table".

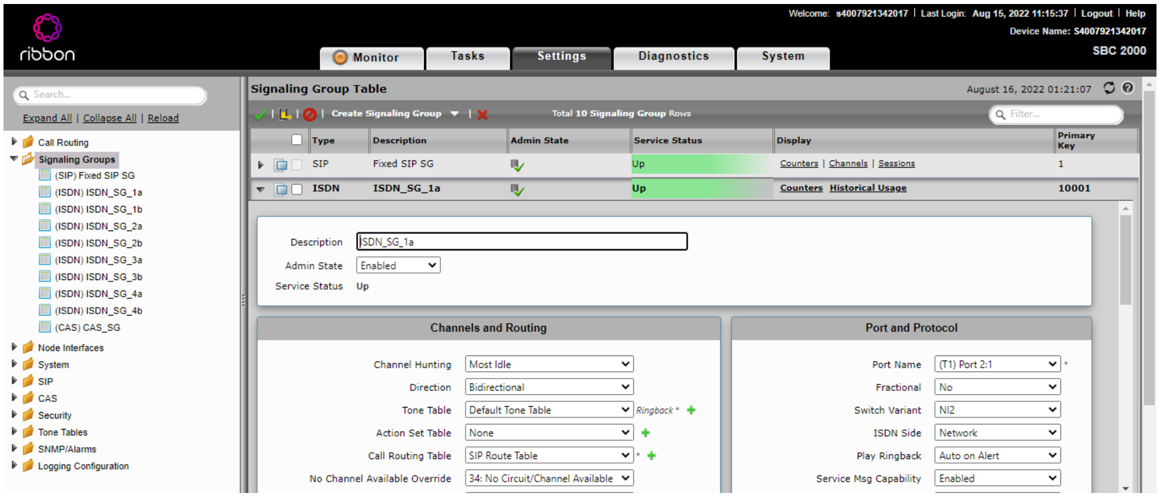


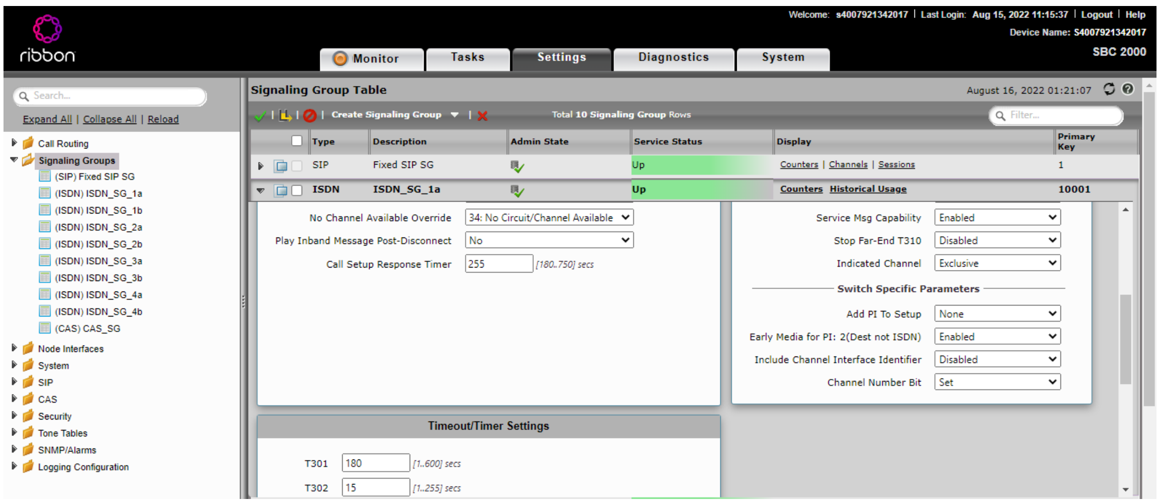


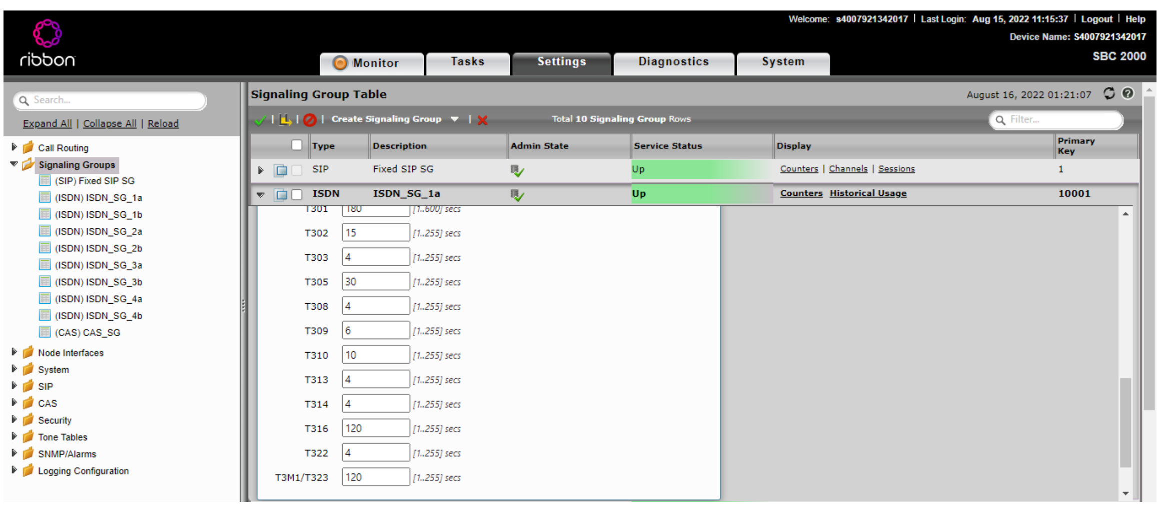


ISDN signaling group

- Go to Settings Signaling groups Click + to create ISDN signaling group (say, **ISDN_SG_1a**).
- Configure switch variant to NI2 and link required Port number from the drop down and leave the rest to default values including default Call Routing table "SIP Route Table".







Call Routing

Call Routing helps to link transformation table and the destination signaling group to be chosen.

Call routing is linked to each call origination signaling group, so, SBC refers to call routing section for routing the call to correct destination.

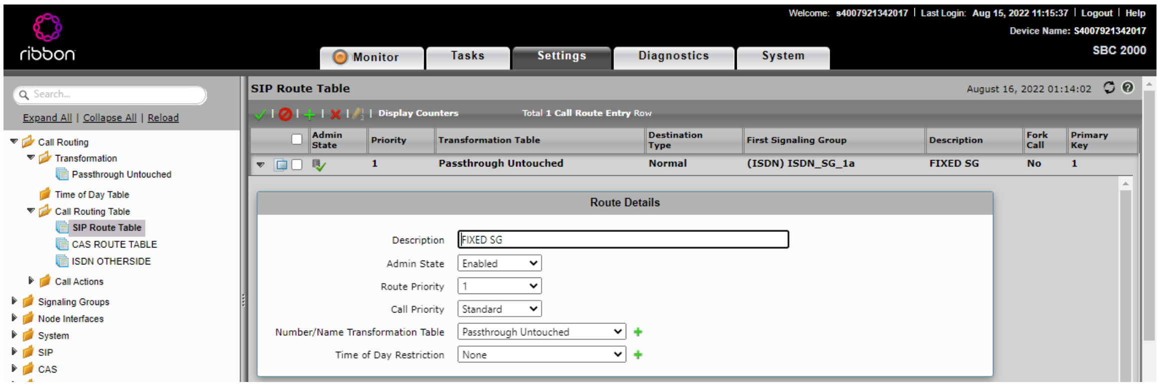
For Routing call from SIP to ISDN or FXS

There is a default **FIXED SIP SG** which is meant for internal communication between SBC SWe Core & SBC Edge and it has default **SIP Route Table** linked.

One need to configure the SIP Route table with a transformation table for either ISDN or for FXS or both and link them to either ISDN signaling group or CAS Signaling group or both based on the need.

If the criteria in transformation table matches, then destination signaling group (ISDN or CAS) can be chosen to route the call via that particular signaling group.

- Go to Settings Call routing Call Routing Table Click default "SIP Route Table" which is present by default expand it to change configuration.
- Change the "name / number transformation table" linked to SIP Route table as required to required ISDN or FXS Transformation table name.
- Add the required destination signaling group as ISDN or FXS.



For Routing call from ISDN or FXS to SIP

<u>ISDN to SIP</u>

1. Create a Call Routing table to route call coming from ISDN.
2. Create and assign the Transformation table for handling calls destined towards SIP side.
3. Assign **FIXED SIP SG** as the destination signaling group.

<u>FXS to SIP</u>

1. Create a Call Routing table to route call coming from FXS.
2. Create and assign the Transformation table for handling calls destined towards SIP side.
3. Assign **FIXED SIP SG** as the destination signaling group.

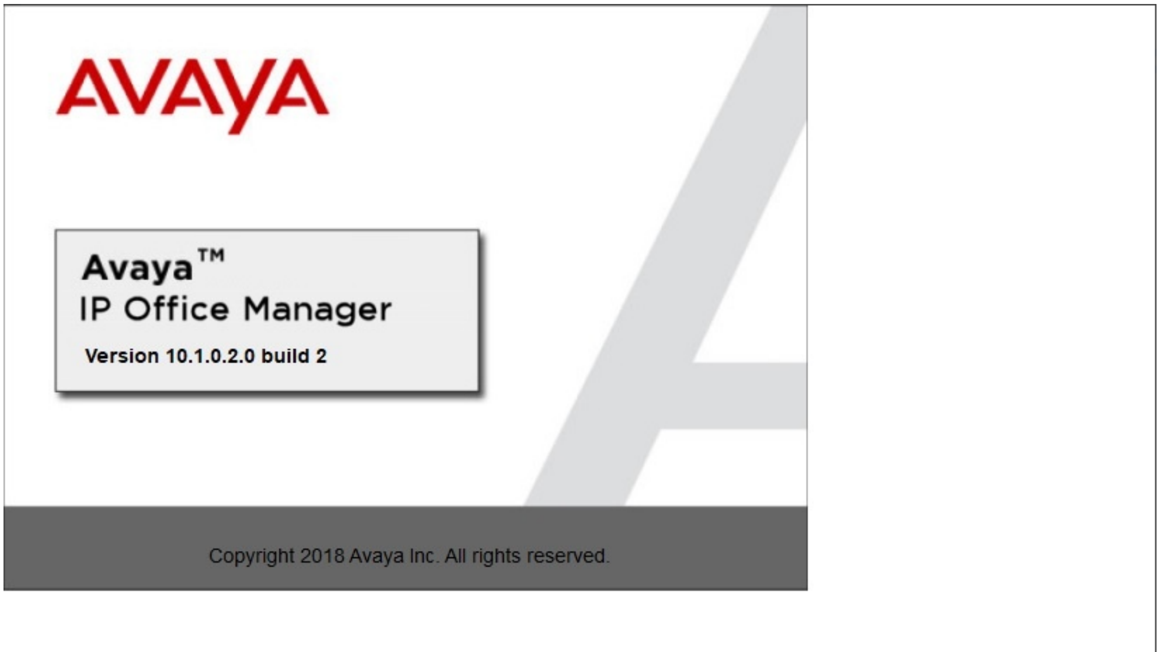
For Routing call from ISDN to ISDN

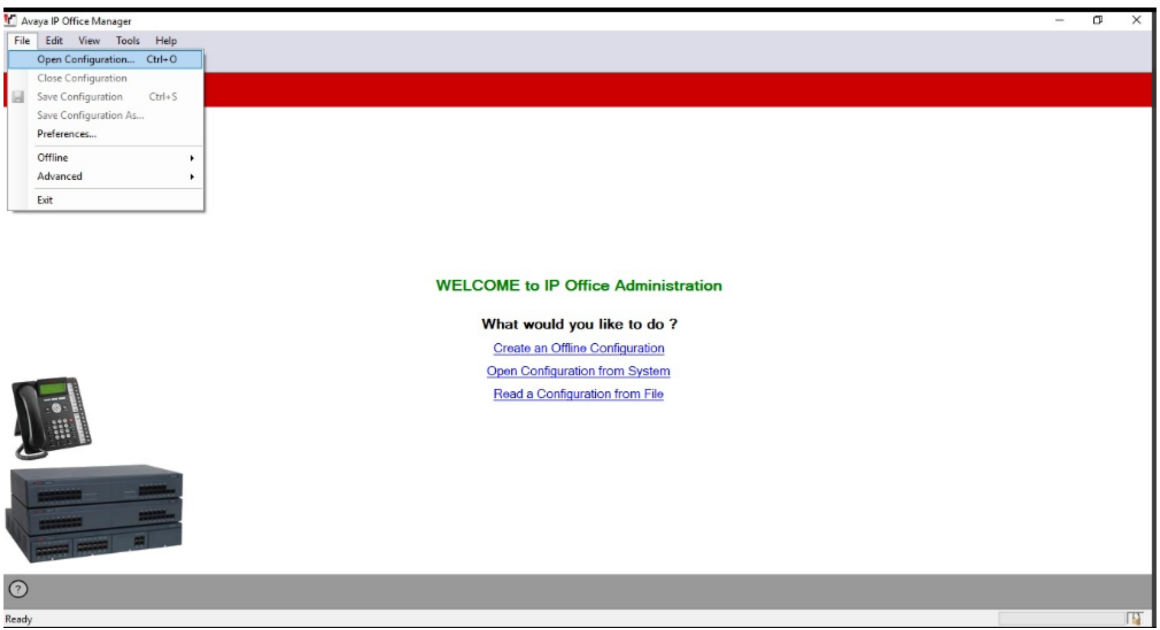
1. Create a Call Routing table to route call coming from ISDN and destined to another ISDN.
2. Create and assign the Transformation table for handling calls destined towards another ISDN.
3. Assign another ISDN signaling group as the destination signaling group.

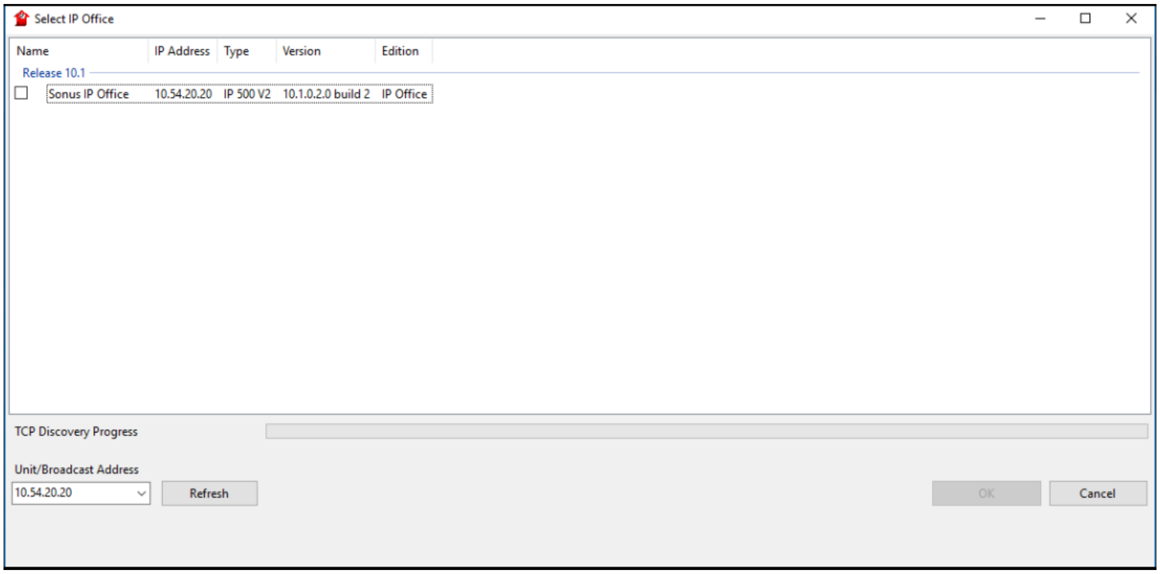
Avaya IP Office Configuration

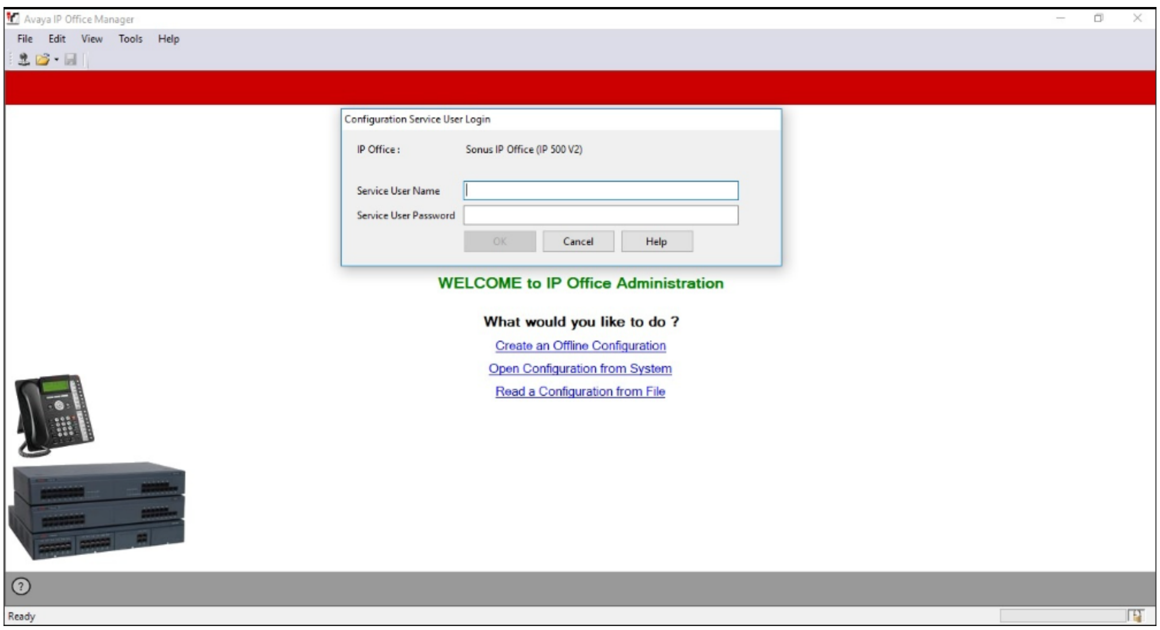
We used Avaya IPO for ISDN PRI Trunk termination.

The Avaya IP Office Manager was loaded onto the tester's PC and allowed user login and access to the Avaya IP Office PBX. With Avaya IP Office Manager loaded on your local PC, select **Program Files (x86) > Avaya > IP Office > Manager**. Select the "Manager" application.


AVAYA
Avaya™
IP Office Manager
Version 10.1.0.2.0 build 2
Copyright 2018 Avaya Inc. All rights reserved.


Avaya IP Office Manager
File
Edit
View
Tools
Help
Open Configuration... Ctrl+O
Close Configuration
Save Configuration Ctrl+S
Save Configuration As...
Preferences...
Offline
Advanced
Exit
WELCOME to IP Office Administration
What would you like to do ?
Create an Offline Configuration
Open Configuration from System
Read a Configuration from File
Ready





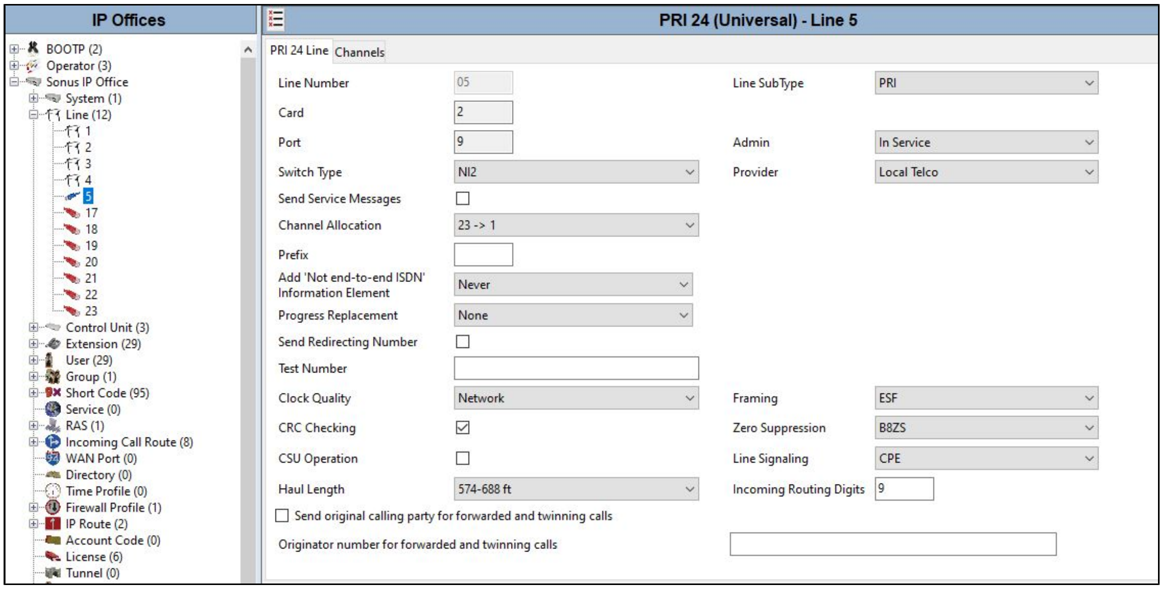
ISDN PRI Trunk

To access the System settings, click the name of the IP Office system. Select **Sonus IP Office Line .5 (configured as PRI Trunk) PRI 24 Line**.

To Configure PRI Trunk, Open Avaya Manager. Go to "Line" section, create a Line and specify the ISDN Physical Port number (which has T1 connected) .

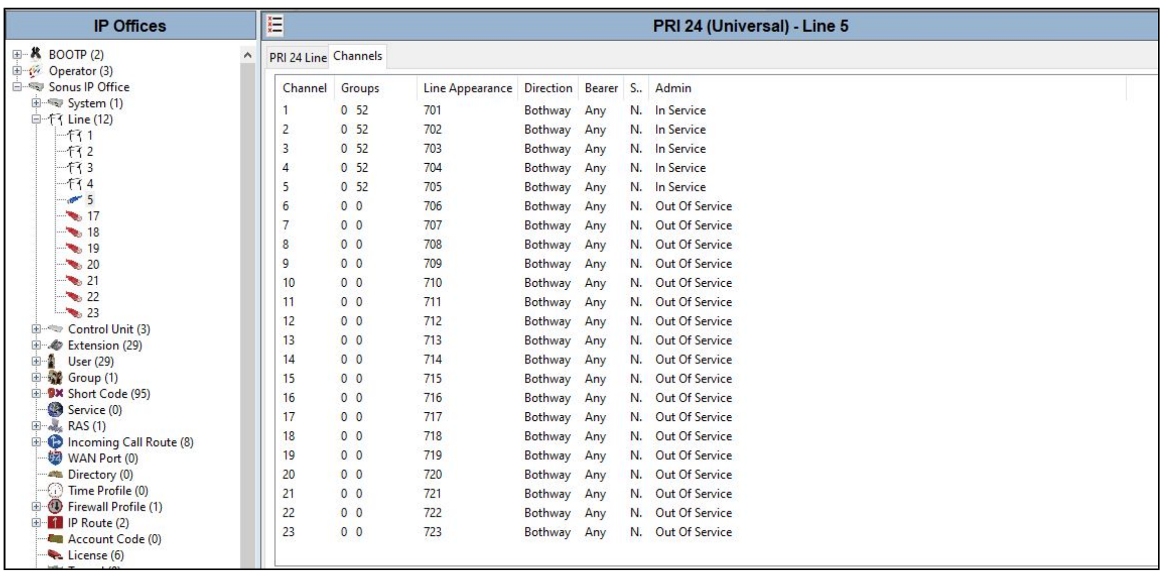
In the following sample config, Port number 9 (though Line number is 05) is configured as PRI as that port number is ISDN in equipment.

Switch Type & **Clock Quality** can be changed according to customer requirement.



PRI Channels can be configured individually as "Inservice" or "Out Of Service" and direction can be incoming, outgoing or Bothway.

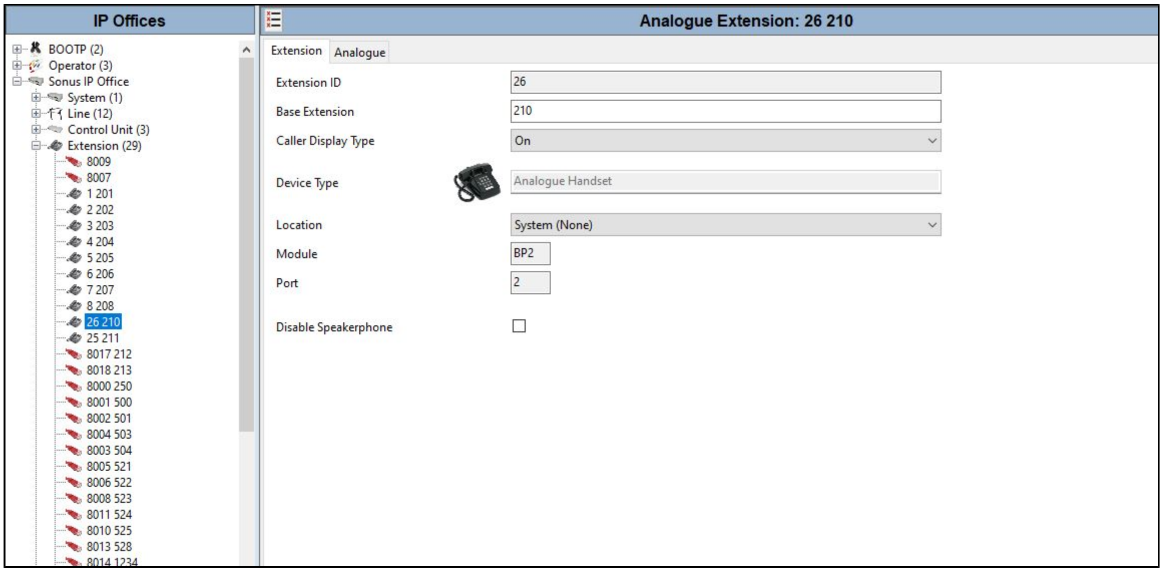
Each Channel can be configured with Line Group ID. In the following sample config, its configured as "52".



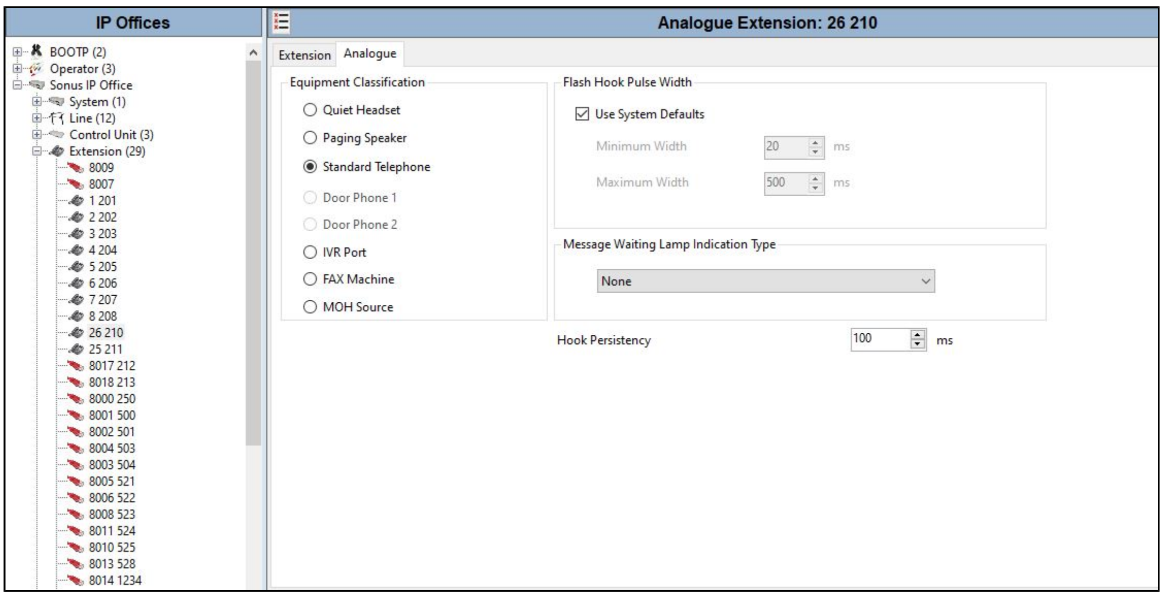
POTS Line

Connect one POTS Phone in one of the FXS Port in Avaya IPO. Go to "Extension" section and create new extension ID and extension number & specify correct Physical Port.

In the following sample config, POTS phone is connected to Port 2.



Click "Standard Telephone" for normal POTS Phone.

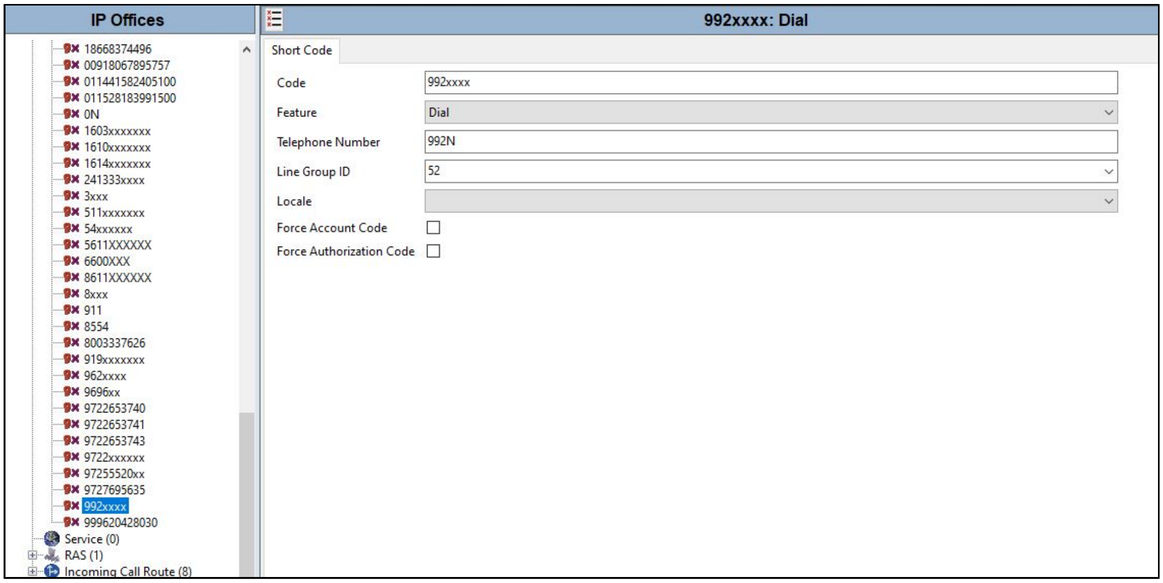


Outgoing Call Routing

Go to "Short Code" section, create new short code and feature "Dial" and Line Group ID.

Line Group ID is very important configuration. Line Group ID should match with outgoing Trunk's Line Group ID.

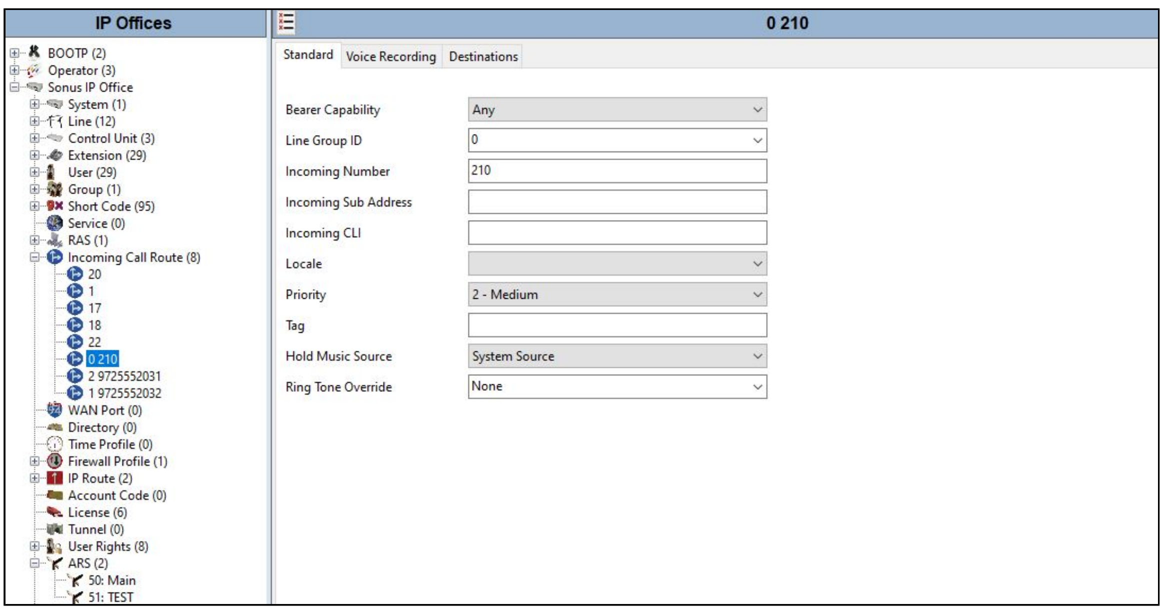
In the following sample config, 992xxxx means after 992, four more digits need to be dialed and it can be any 4 digit after 992.



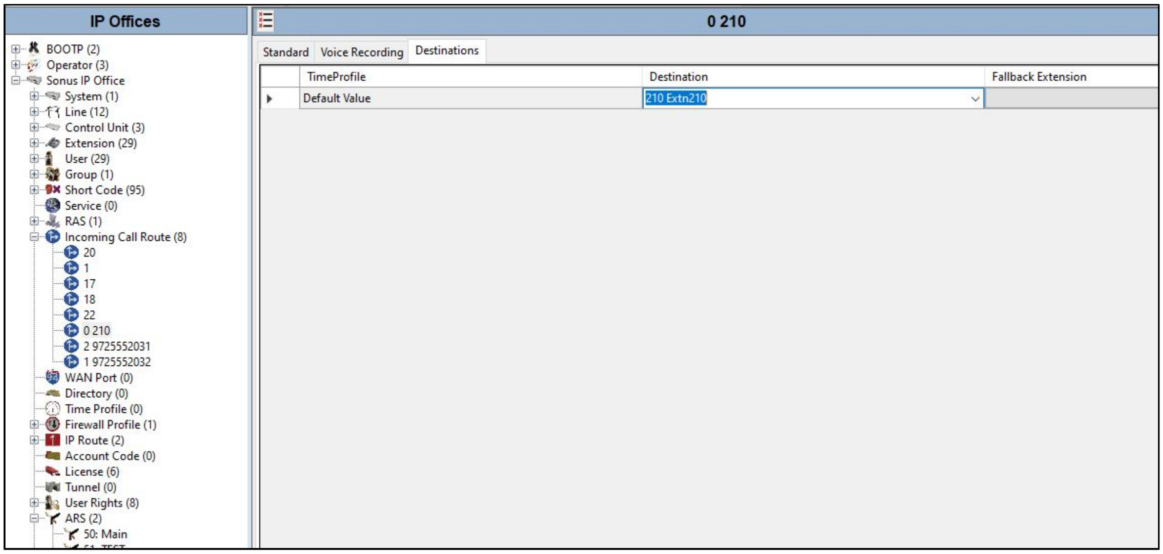
Incoming Call Routing

Go to Incoming call Route section. Line Group ID "0" means, call can come from any "Line Group ID". Incoming number can be specified.

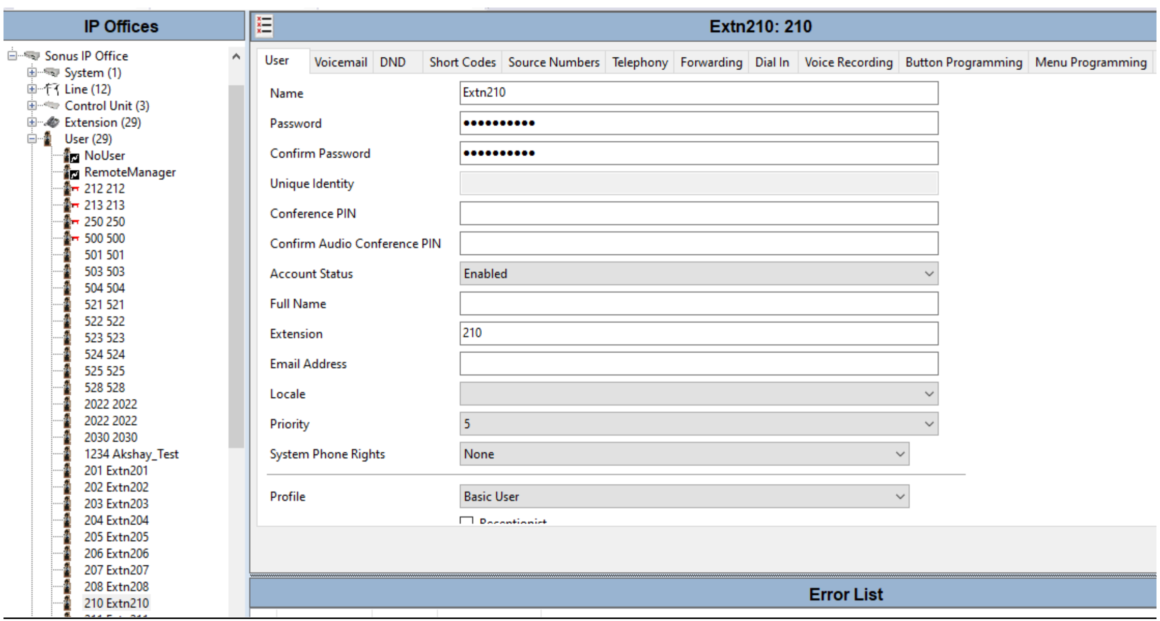
When the incoming number is matched, call will be routed to "Destination" configured on Destination Tab. In this case, Destination is one of the FXS Port (here, Port 2).



Go To Destination Tab and select "User" (example: 210 Extn210) configured under "User" section with extension "210" configured under "Extension" section with Port number "2" in the following example.

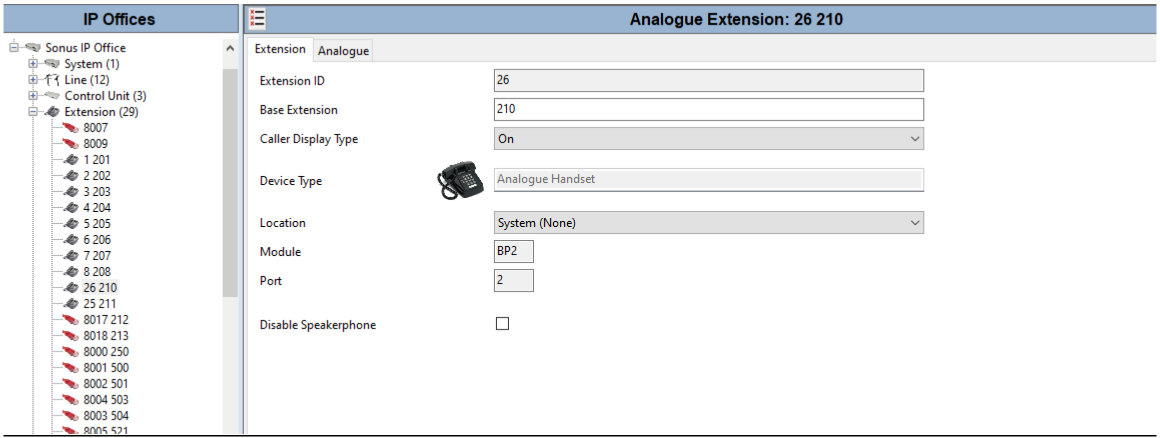


"User" section is shown in the following screen capture.



"Extension" section is shown in the following screen capture.

Port 2 is linked to Extension 210.



Cisco Unified Communications Manager Configuration

We used CUCM for originating / terminating TLS / SRTP calls.

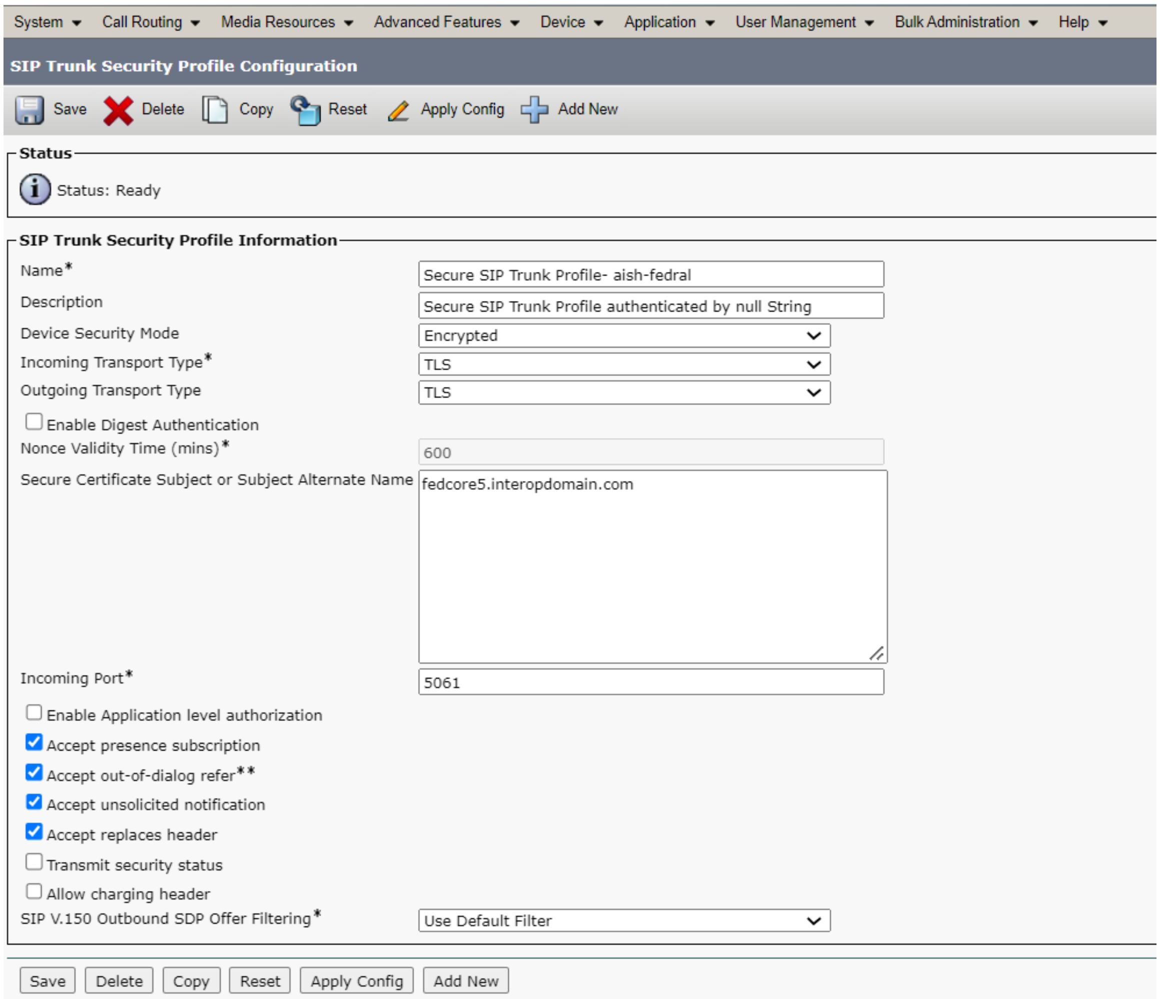
The following configurations are included in this section:

- Security Profile
- SIP Profile
- SIP Trunk
- Route Group
- Route List
- Route Pattern

Security Profile

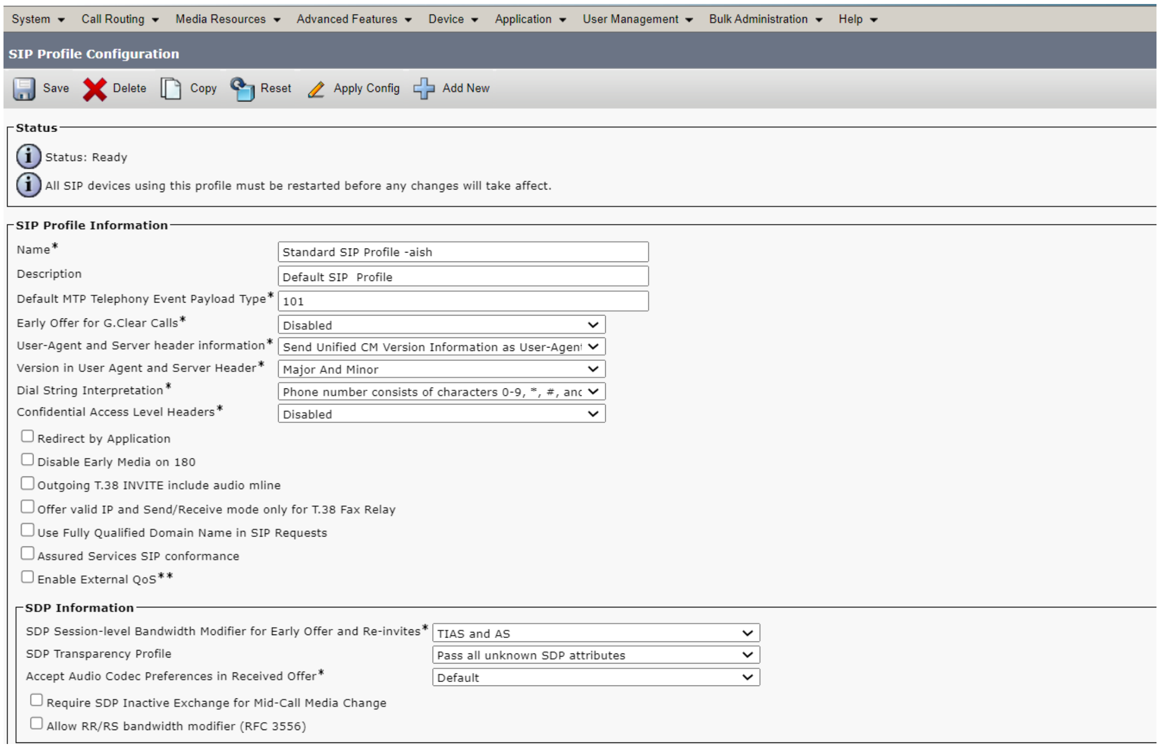
Select **System > Security > SIP Trunk Security Profile**.

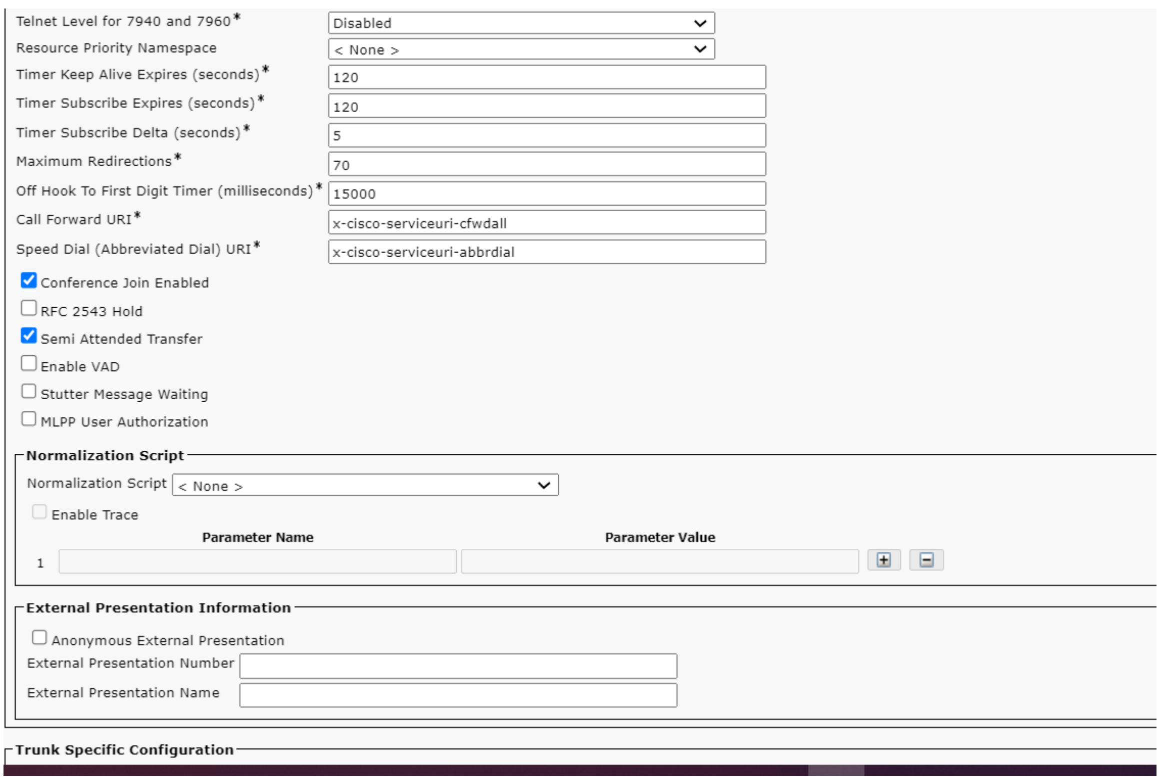
Figure 1: Security Profile First Trunk

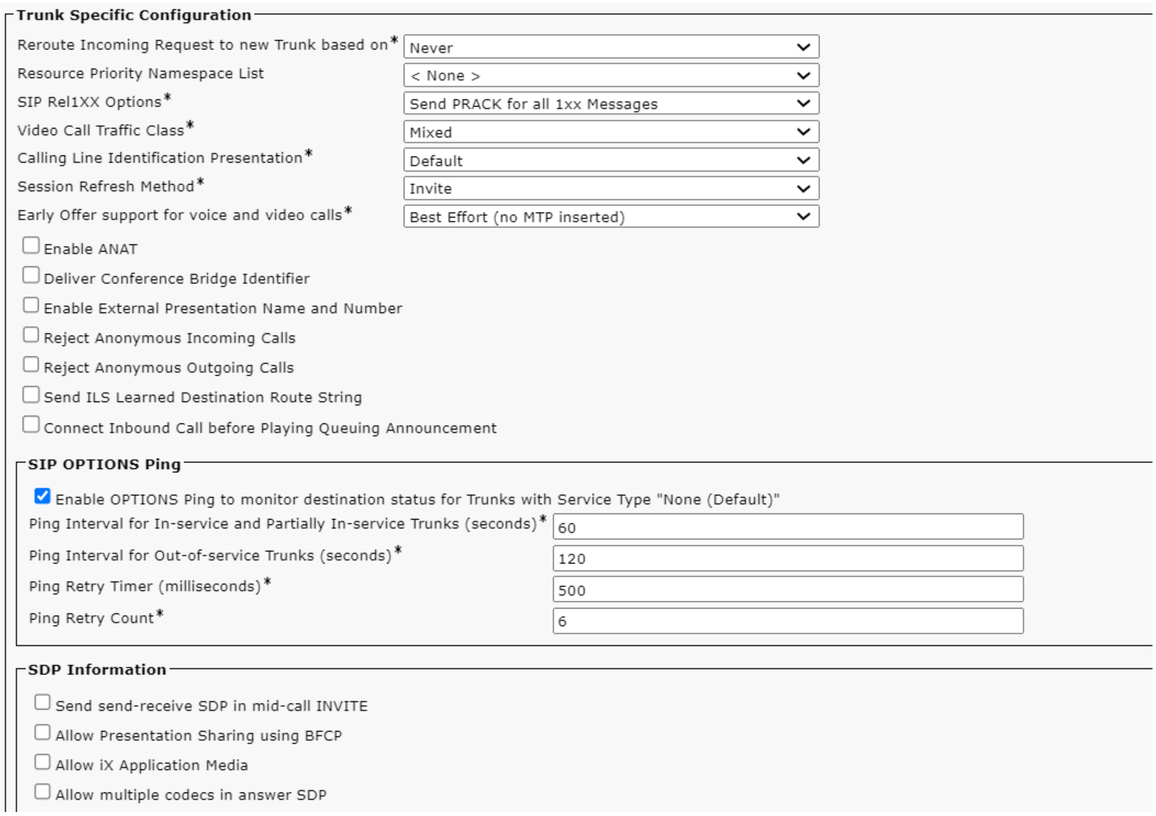


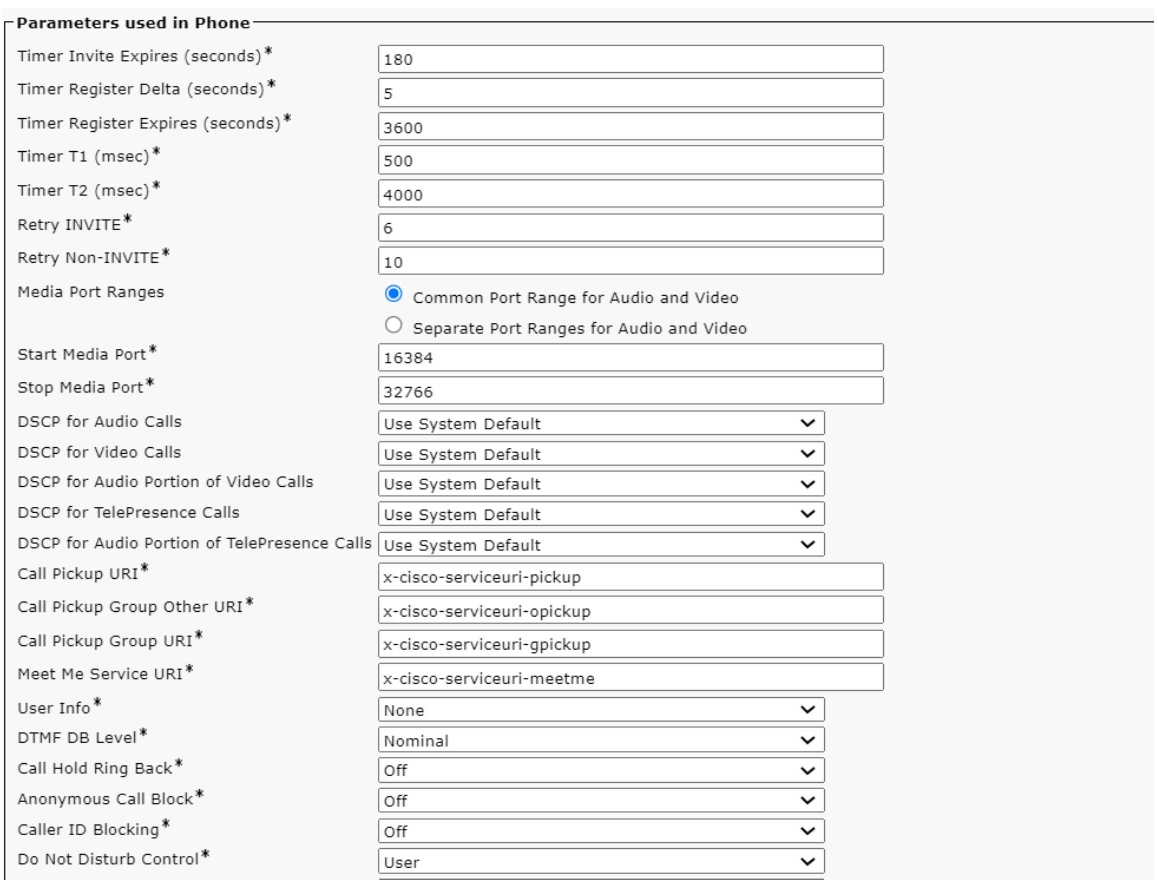
SIP Profile

Select **Device > Device Settings > SIP Profile**.


System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
SIP Profile Configuration
Save Delete Copy Reset Apply Config Add New
Status
Status: Ready
All SIP devices using this profile must be restarted before any changes will take affect.
SIP Profile Information
Name* Standard SIP Profile -aish
Description Default SIP Profile
Default MTP Telephony Event Payload Type* 101
Early Offer for G.Clear Calls* Disabled
User-Agent and Server header information* Send Unified CM Version Information as User-Agent
Version in User Agent and Server Header* Major And Minor
Dial String Interpretation* Phone number consists of characters 0-9, *, #, and
Confidential Access Level Headers* Disabled
Redirect by Application
Disable Early Media on 180
Outgoing T.38 INVITE include audio mline
Offer valid IP and Send/Receive mode only for T.38 Fax Relay
Use Fully Qualified Domain Name in SIP Requests
Assured Services SIP conformance
Enable External QoS**
SDP Information
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites* TIAS and AS
SDP Transparency Profile Pass all unknown SDP attributes
Accept Audio Codec Preferences in Received Offer* Default
Require SDP Inactive Exchange for Mid-Call Media Change
Allow RR/RS bandwidth modifier (RFC 3556)


Telnet Level for 7940 and 7960* Disabled
Resource Priority Namespace < None >
Timer Keep Alive Expires (seconds)* 120
Timer Subscribe Expires (seconds)* 120
Timer Subscribe Delta (seconds)* 5
Maximum Redirections* 70
Off Hook To First Digit Timer (milliseconds)* 15000
Call Forward URI* x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI* x-cisco-serviceuri-abbrdial
Conference Join Enabled
RFC 2543 Hold
Semi Attended Transfer
Enable VAD
Stutter Message Waiting
MLPP User Authorization
Normalization Script
Normalization Script < None >
Enable Trace
Parameter Name
Parameter Value
1
External Presentation Information
Anonymous External Presentation
External Presentation Number
External Presentation Name
Trunk Specific Configuration

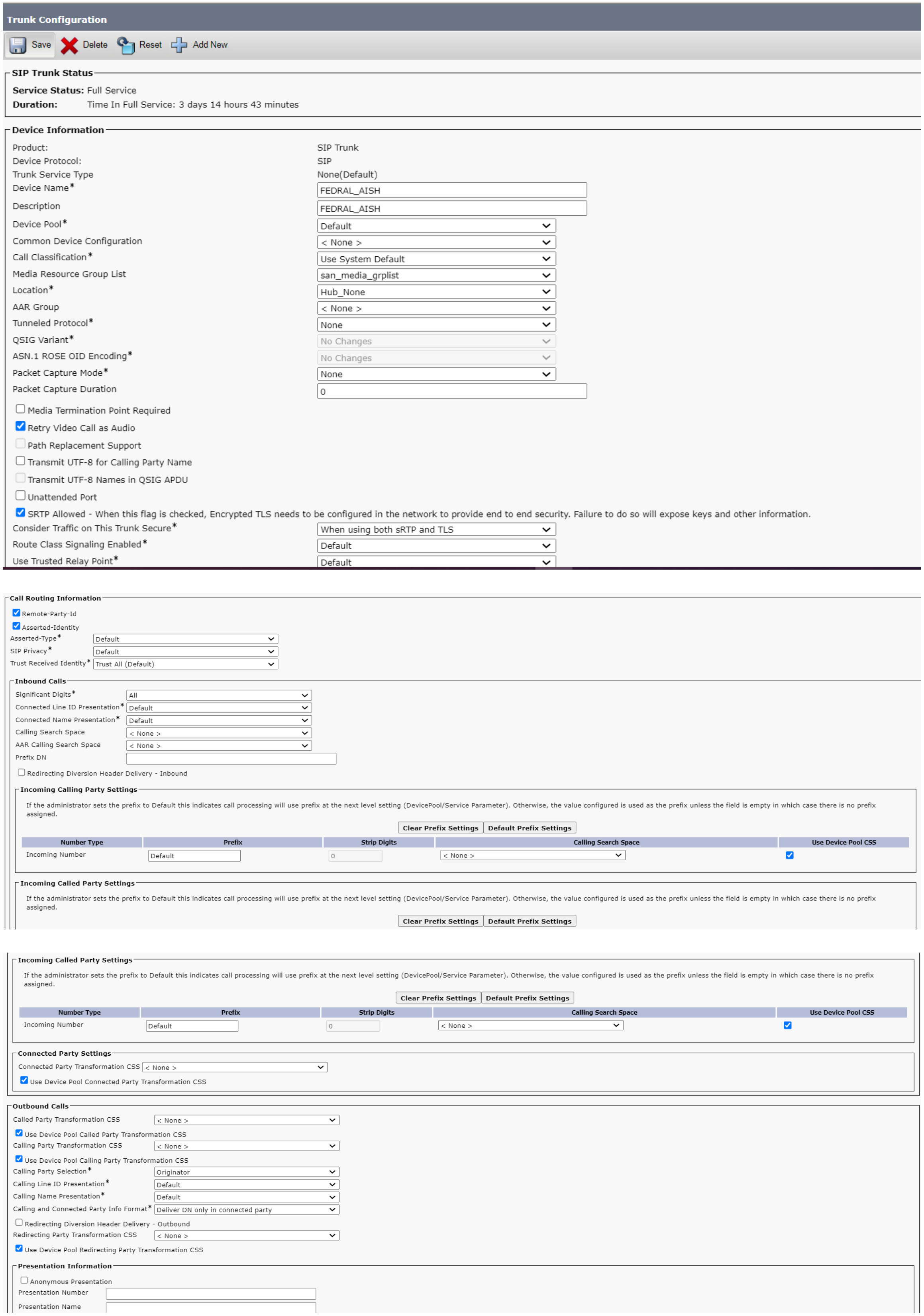

Trunk Specific Configuration
Reroute Incoming Request to new Trunk based on*
Never
Resource Priority Namespace List
< None >
SIP Rel1XX Options*
Send PRACK for all 1xx Messages
Video Call Traffic Class*
Mixed
Calling Line Identification Presentation*
Default
Session Refresh Method*
Invite
Early Offer support for voice and video calls*
Best Effort (no MTP inserted)
Enable ANAT
Deliver Conference Bridge Identifier
Enable External Presentation Name and Number
Reject Anonymous Incoming Calls
Reject Anonymous Outgoing Calls
Send ILS Learned Destination Route String
Connect Inbound Call before Playing Queuing Announcement
SIP OPTIONS Ping
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"
Ping Interval for In-service and Partially In-service Trunks (seconds)*
60
Ping Interval for Out-of-service Trunks (seconds)*
120
Ping Retry Timer (milliseconds)*
500
Ping Retry Count*
6
SDP Information
Send send-receive SDP in mid-call INVITE
Allow Presentation Sharing using BFCP
Allow iX Application Media
Allow multiple codecs in answer SDP

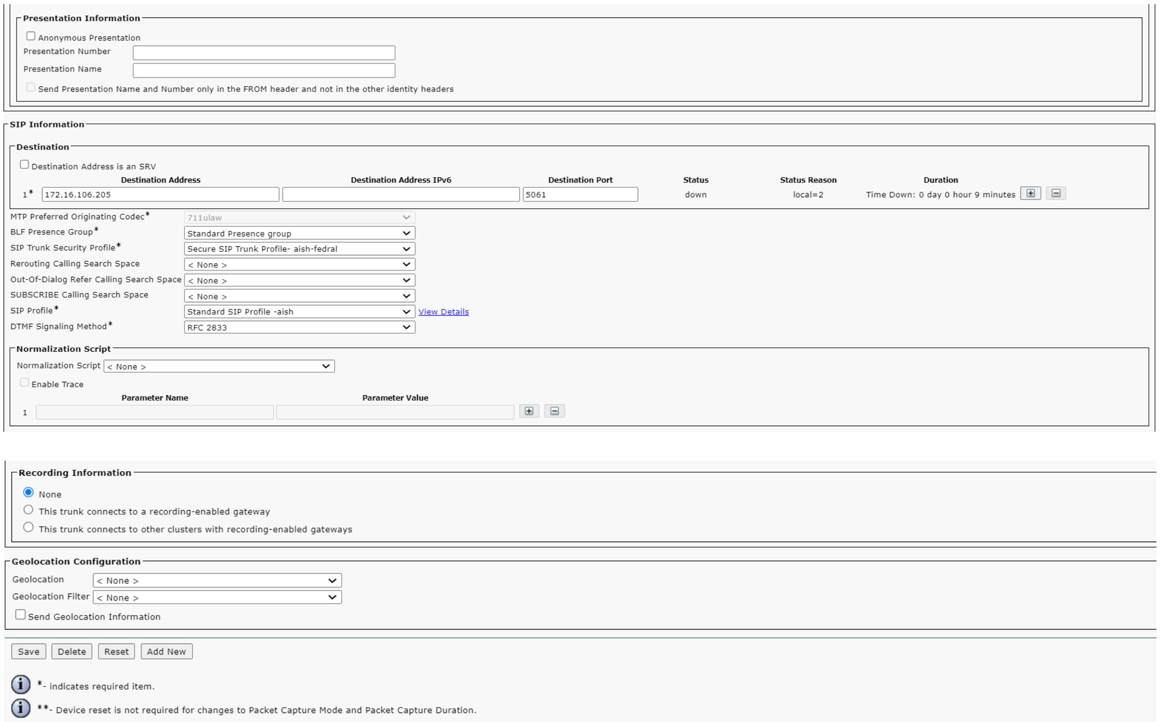

Parameters used in Phone
Timer Invite Expires (seconds)*
180
Timer Register Delta (seconds)*
5
Timer Register Expires (seconds)*
3600
Timer T1 (msec)*
500
Timer T2 (msec)*
4000
Retry INVITE*
6
Retry Non-INVITE*
10
Media Port Ranges
Common Port Range for Audio and Video
Separate Port Ranges for Audio and Video
Start Media Port*
16384
Stop Media Port*
32766
DSCP for Audio Calls
Use System Default
DSCP for Video Calls
Use System Default
DSCP for Audio Portion of Video Calls
Use System Default
DSCP for TelePresence Calls
Use System Default
DSCP for Audio Portion of TelePresence Calls
Use System Default
Call Pickup URI*
x-cisco-serviceuri-pickup
Call Pickup Group Other URI*
x-cisco-serviceuri-opickup
Call Pickup Group URI*
x-cisco-serviceuri-gpickup
Meet Me Service URI*
x-cisco-serviceuri-meetme
User Info*
None
DTMF DB Level*
Nominal
Call Hold Ring Back*
Off
Anonymous Call Block*
Off
Caller ID Blocking*
Off
Do Not Disturb Control*
User

SIP Trunk

Select **Device > Trunk > Add New**.

Figure 2: First SIP Trunk

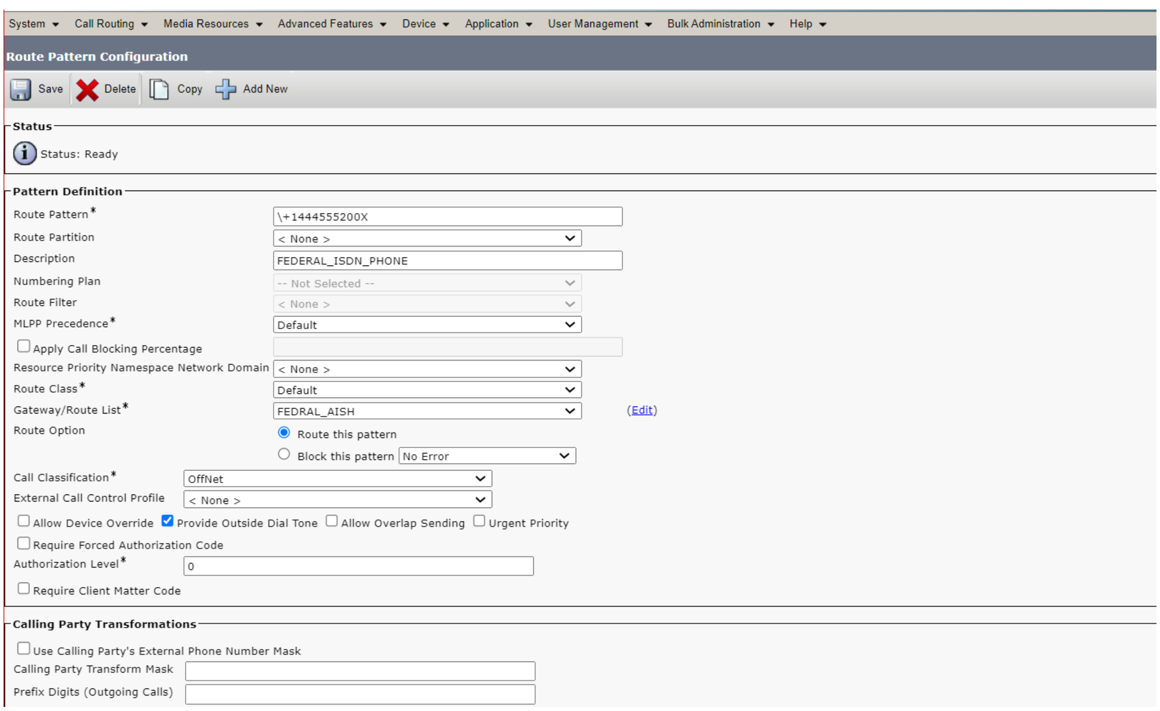


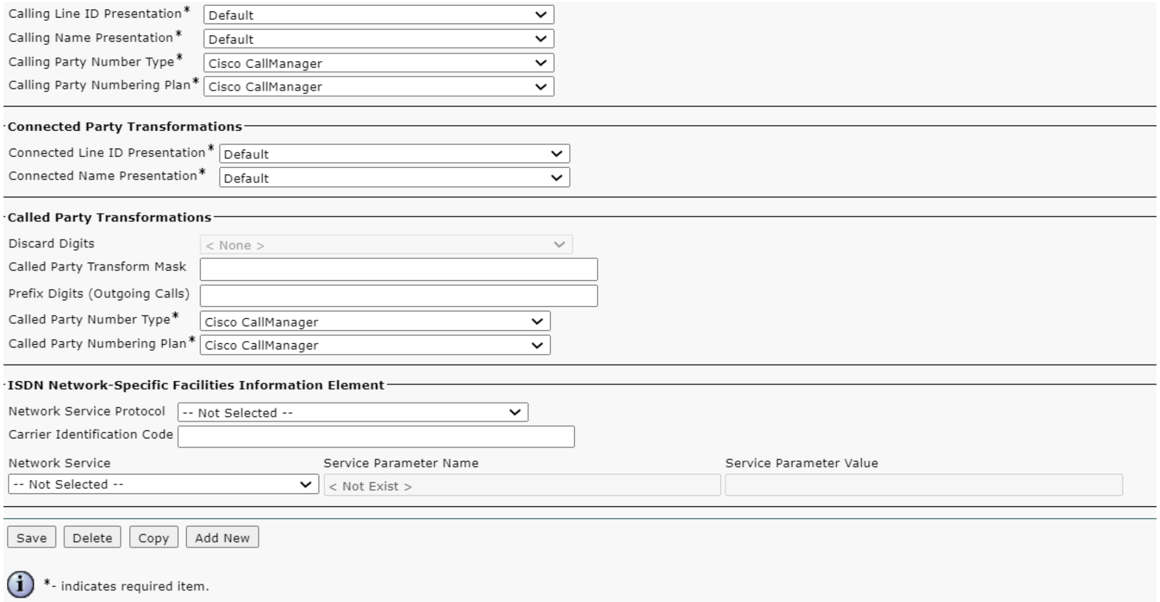


Route Pattern

Select **Call Routing > Route/Hunt > Route Pattern > Add New**.

Figure 3: Route Pattern

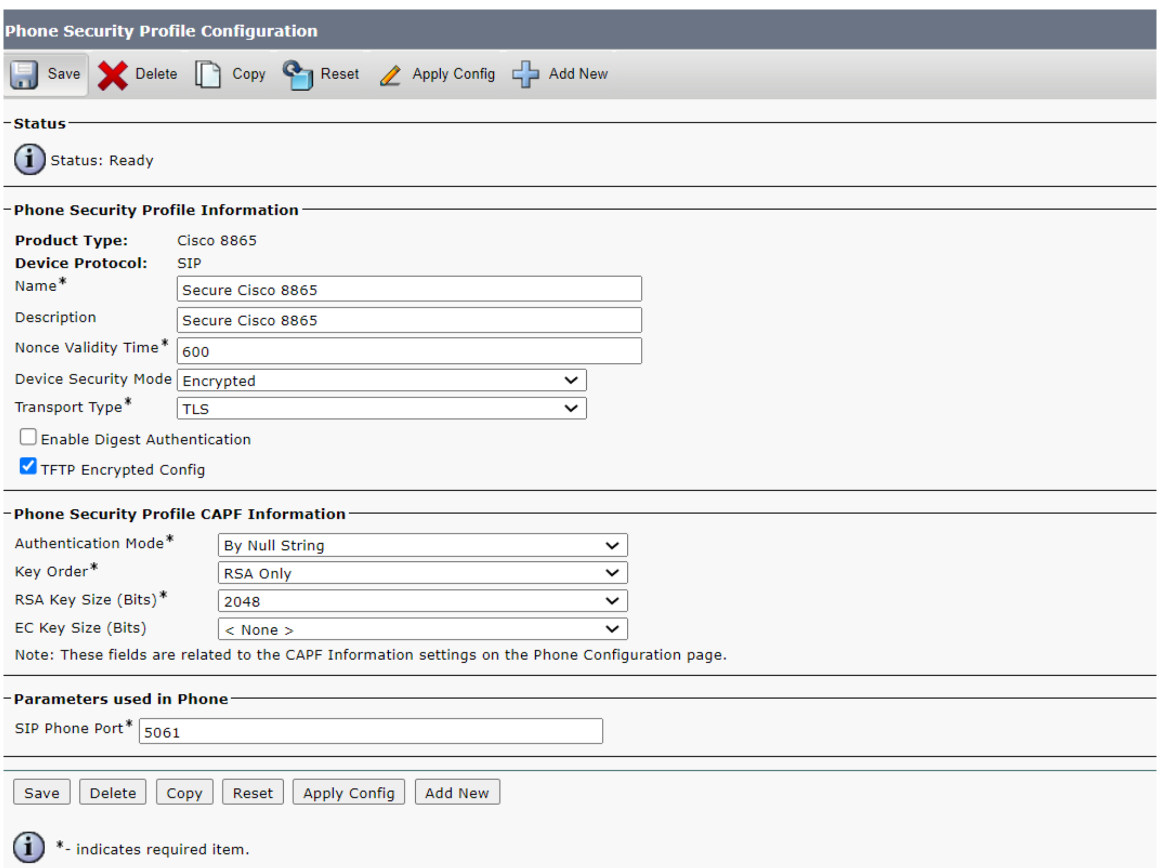


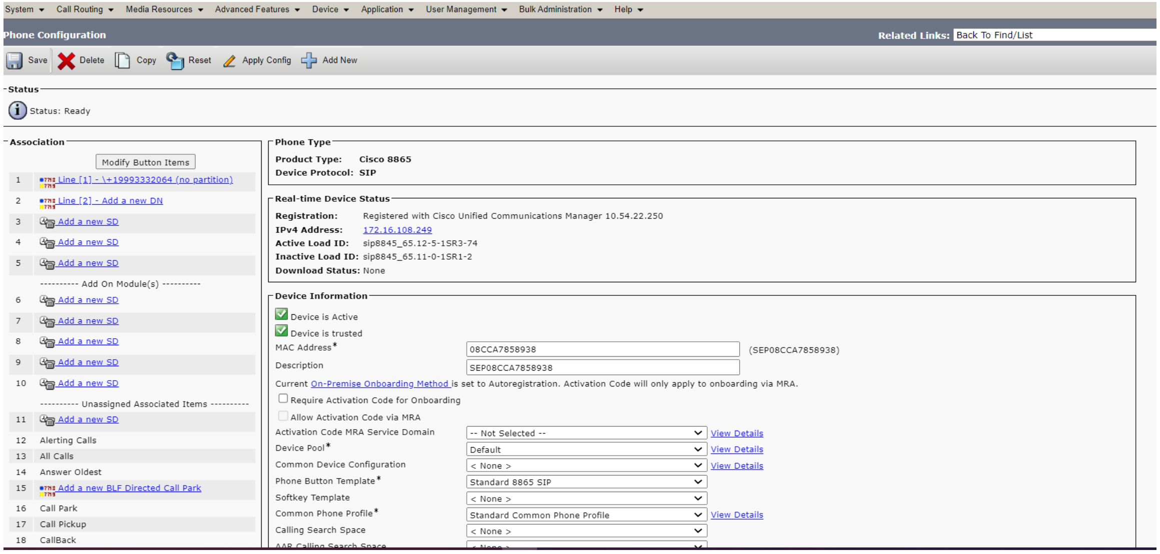


Phone Security Profile

Select **System > Security > Phone Secuirty Profile**

Figure 4: Phone Secuirty Profile

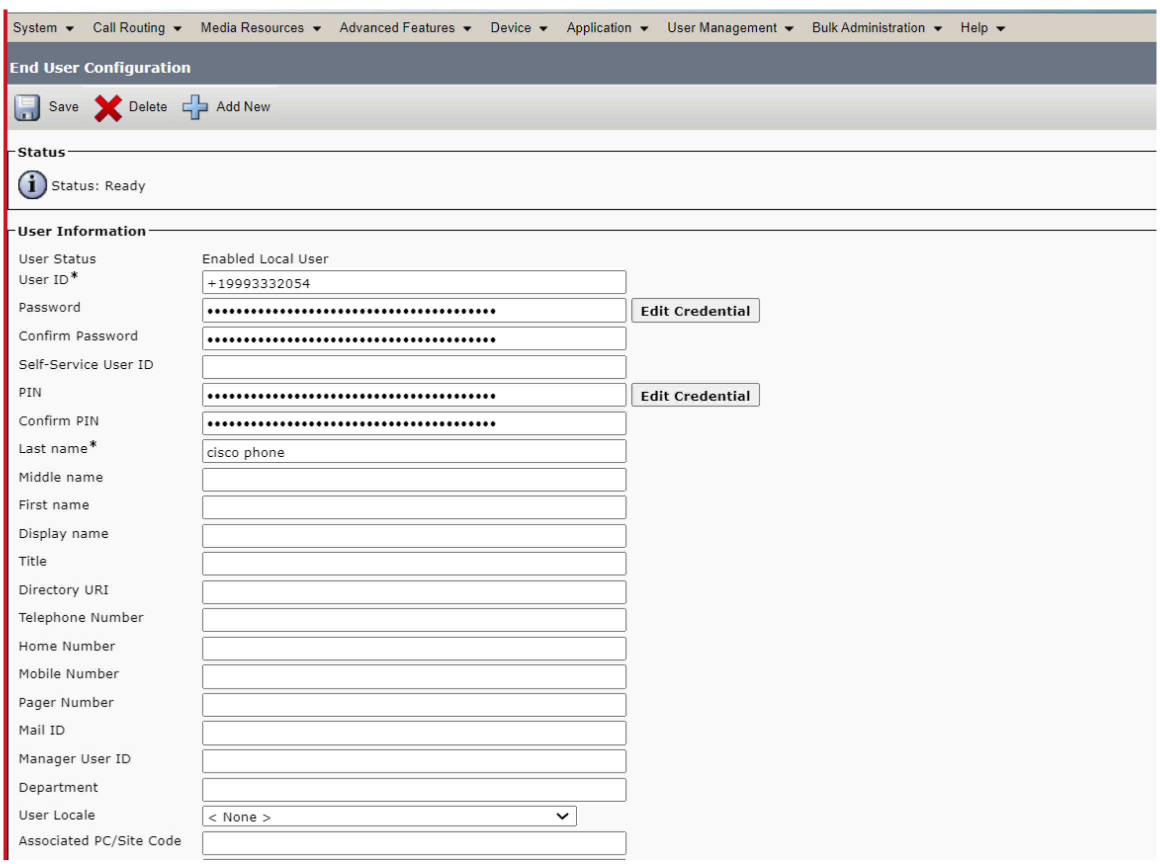


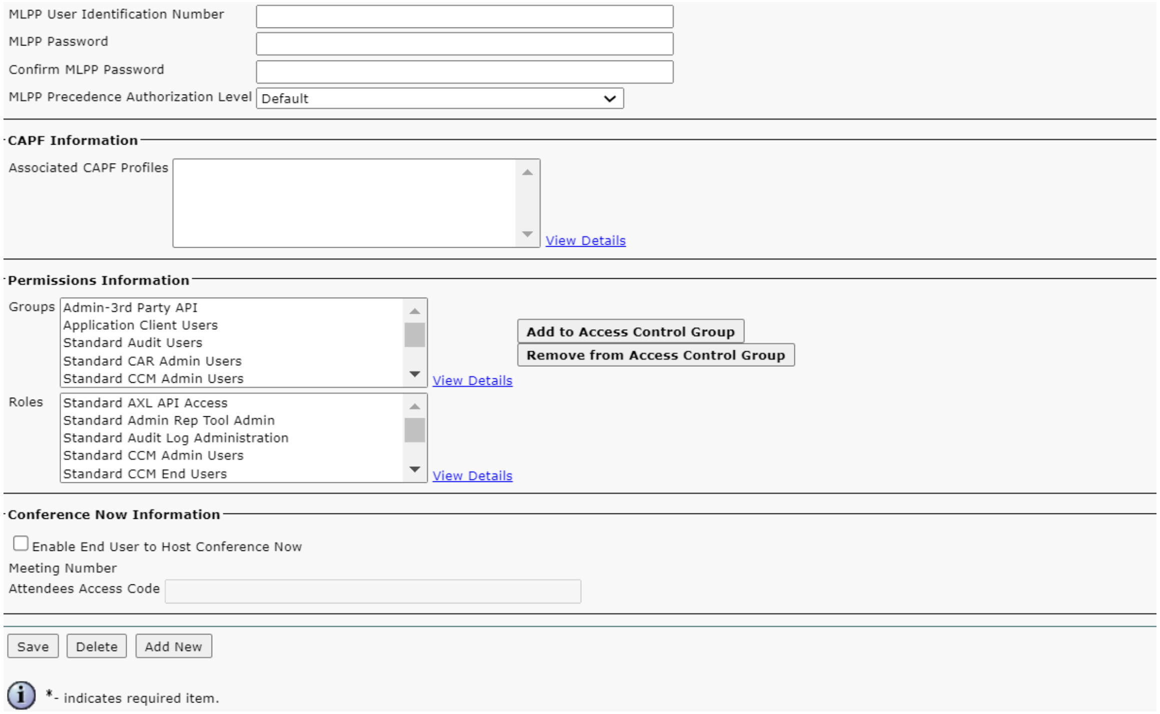


End User Configuration

Select **User management > End user configuration**.

Figure 5: End User Configuration

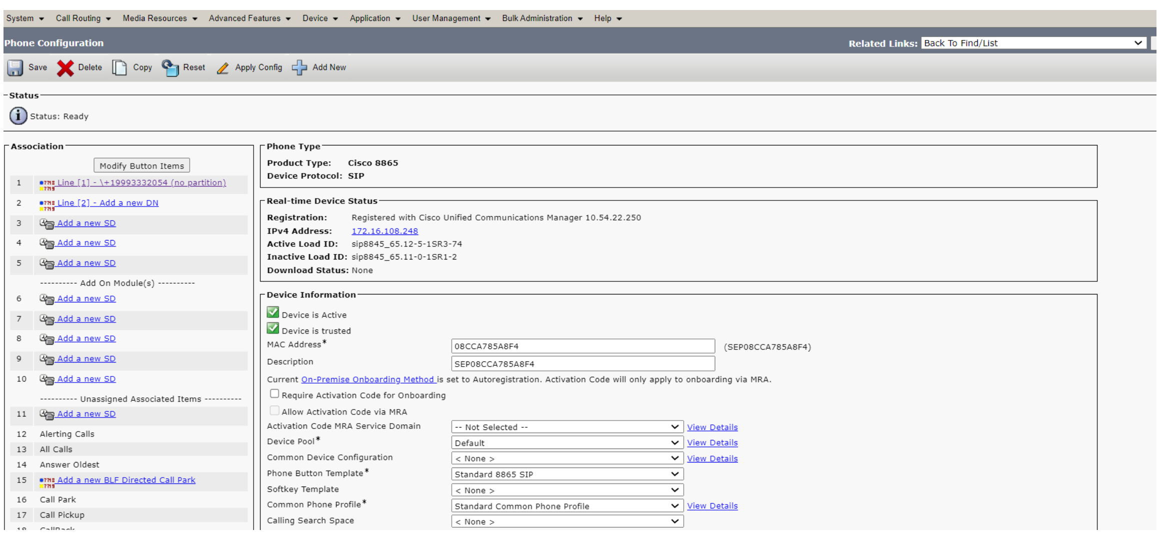


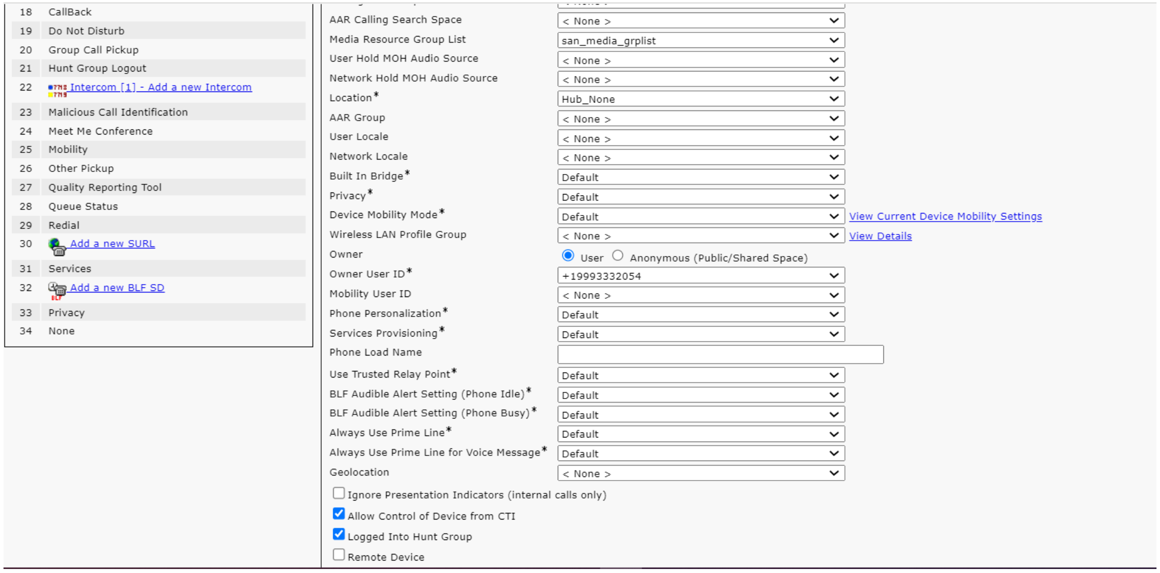


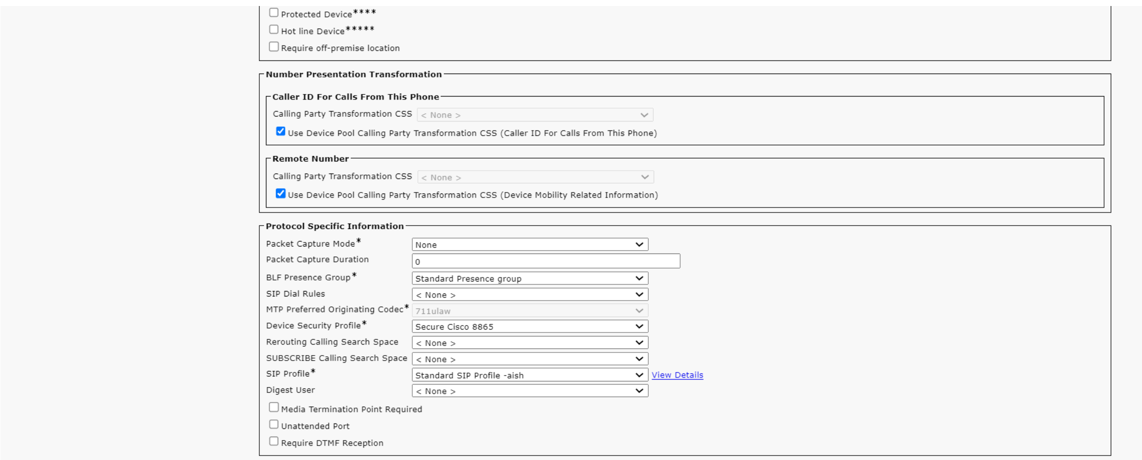
Phone Configuration

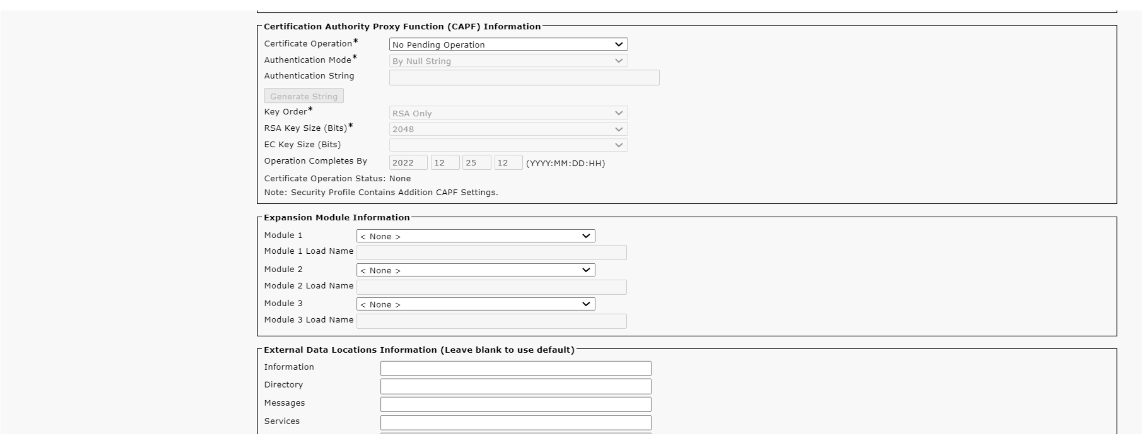
Select **Device > Phone Phone configuration**.

Figure 6: Phone Configuration









Supplementary Services & Features Coverage

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

Sr. No	Supplementary Services/ Features	Coverage
1	Basic Call Setup & Termination	✔

2	DTMF - Inband (FXS / ISDN)	✔
3	DTMF - RFC2833	✔
4	Ringback tone (FXS / ISDN)	✔
5	Call Hold/ Resume (FXS)	✔
6	Call Transfer (FXS)	✔
7	Call Transfer (Blind/ Unattended)	✔
8	Call Transfer (Consultative/ Attended)	✔
9	Transcoding (Voice)	✔
10	Music On Hold	✘
11	TLS with SRTP	✔
12	FAX VOIP (G711 Passthru with TLS/SRTP)	✔
13	FAX (FXS)	✔
14	FAX (ISDN)	✔
15	Ringback from FXS	✔
16	Ringback from ISDN	✔
17	Call Waiting (FXS)	✔
18	Delayed Offer	✔
19	SRTP to RTP & vice-versa	✔
20	TLS to UDP & vice-versa	✔

Legend

Supported	✔
Not Supported	✘

Caveats

There are a few caveats and observations for both Federal Edge 1K and Federal Edge 2K:

- 2nd NTP server in SBC Core can't be added in first try. It needs to be deleted and recreated 2nd time.
- FXS Blind transfer service support is work in progress.
- MOH won't work as wav file can't be uploaded.
- Video call is not supported on Federal Edge.
- G711A law + G729 without CN offer from ingress Peer would cause extra Re-invite or update from SBC Core towards Ingress Peer.
- Fax T.38 with SRTP is not recommended on Federal Edge.
- With LRBT enabled, SBC Core sends G711A law with wrong payload type in SDP.

Federal Edge 2000

The following observation is for Federal Edge 2K only:

- Rebooting SBC Edge in SBC 2000 UI will do power cycle of ASM. This is not observed in Federal Edge 1K.

Federal Edge 1000

The following observation is for Federal Edge 1K only:

- FXS Call Hold / Resume doesn't work on SBC 1000 and fix is being worked out.
- After factory reset, SBC 1000 UI won't be accessible for 7 hours.
- After factory reset, some times (not always) ntp.conf file will be missing in SBC 1000.

Support

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

- 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 & solutions, please visit: https://ribboncommunications.com/products.

Conclusion

This Interoperability Guide describes successful configuration of Federal Edge (Ribbon SBC SWe Core & Ribbon SBC Edge 2000/1000) with CUCM & Avaya IPO.

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.