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



Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
 - About Ribbon Federal Edge
 - About Ribbon SBC SWe Core
 - About Ribbon SBC Edge
 - About Cisco Unified CM
 - About Avaya IP Office
- Scope/Non-Goals
- Audience
- Prerequisites
- Product and Device Details
- Network Topology and E2E Flow Diagrams
- Document Workflow
- Installing Ribbon Federal Edge
- Ribbon SBC SWe Core
 - Static Route for media IP addresses of External Peer
 - SBC Configuration for External DNS Server
 - SBC Configuration for TLS / SRTP Profile
 - SRTP Profile
 - TLS Profile
 - SBC Configuration for Transparency Profile
 - SBC Configuration for Media Profile
 - SBC Configuration for External Network
 - SIP TG Towards External Network
 - SBC Configuration Towards SBC Edge
 - SBC Configuration for Call Routing
 - ACL Rules for NTP and Web Proxy Feature on SBC SWe Core
 - FIPS Configuration
 - Configuration for DISA LSC SIP trunks
 - Troubleshooting SBC SWe Core
 - Debug Log
 - Accounting Log
 - CDR Viewer
 - Call Trace
- Ribbon SBC Edge Configuration
 - FXS Configuration
 - CAS Supplementary Service Profile
 - Call Transformation Table
 - Signaling Groups
 - Call Routing
- Avaya IP Office Configuration
 - ISDN PRI Trunk
 - POTS Line
 - Outgoing Call Routing
 - Incoming Call Routing
- Cisco Unified Communications Manager Configuration
 - Security Profile
 - SIP Profile
 - SIP Trunk
 - Route Pattern
 - Phone Security Profile
 - End User Configuration
 - Phone Configuration
- Supplementary Services & Features Coverage
- Caveats
- Support
- References
- Conclusion

Interoperable Vendors



Copyright

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

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

Document Overview

This document 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

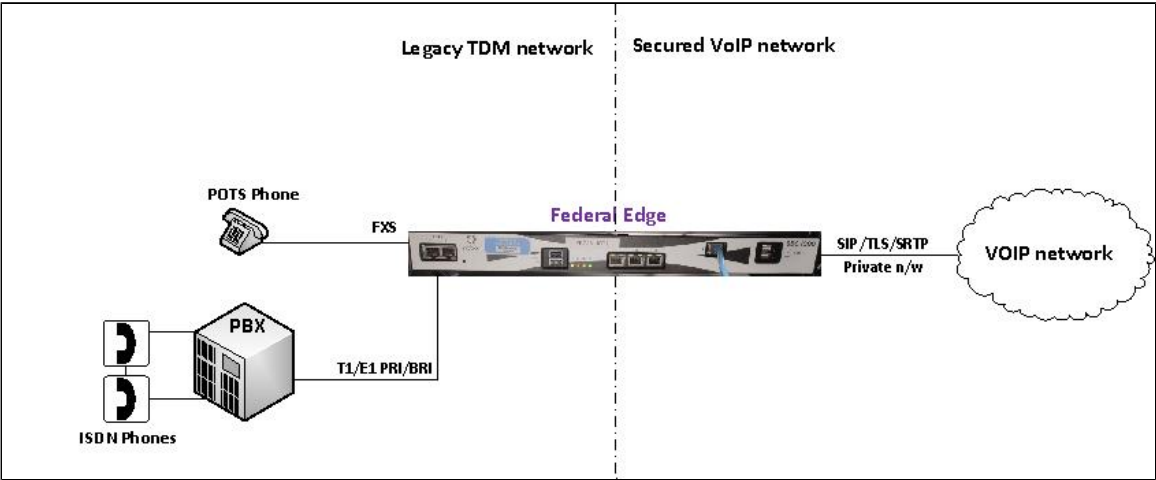
The configuration uses the following equipment and software:

	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

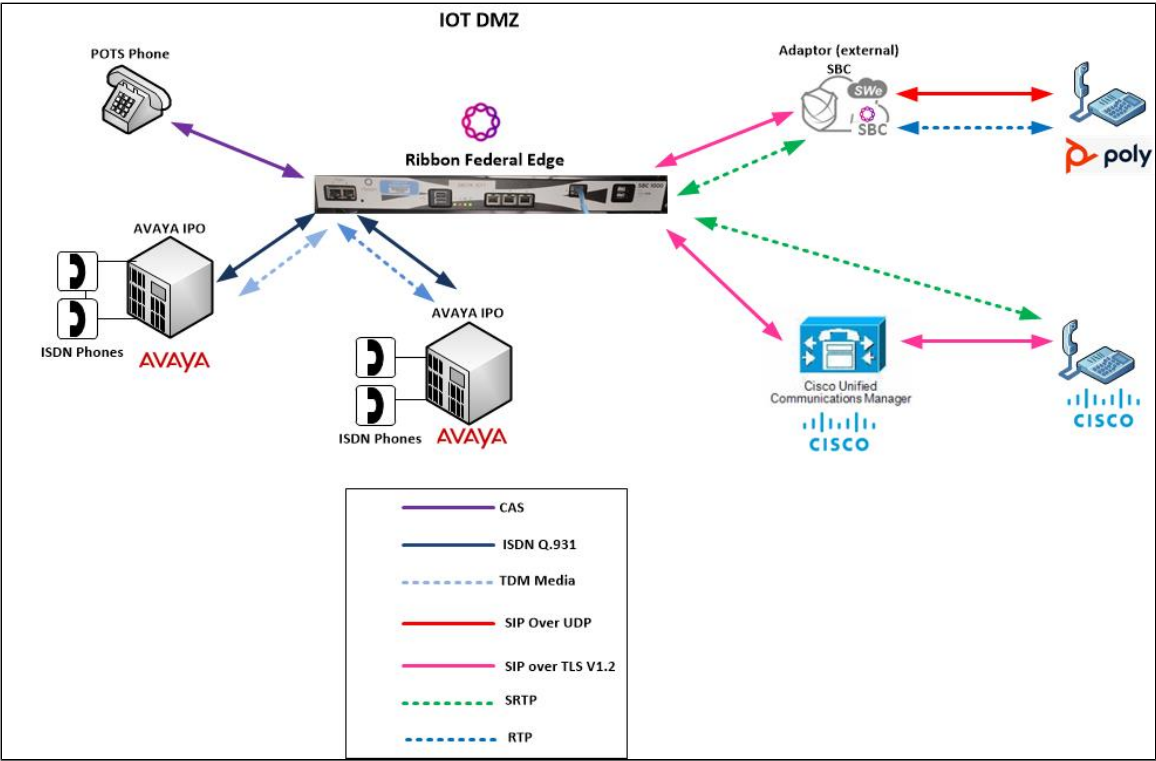
Beetel	Analog Phone	-
Administration and Debugging Tools	Wireshark	V3.0.1

Network Topology and E2E Flow Diagrams

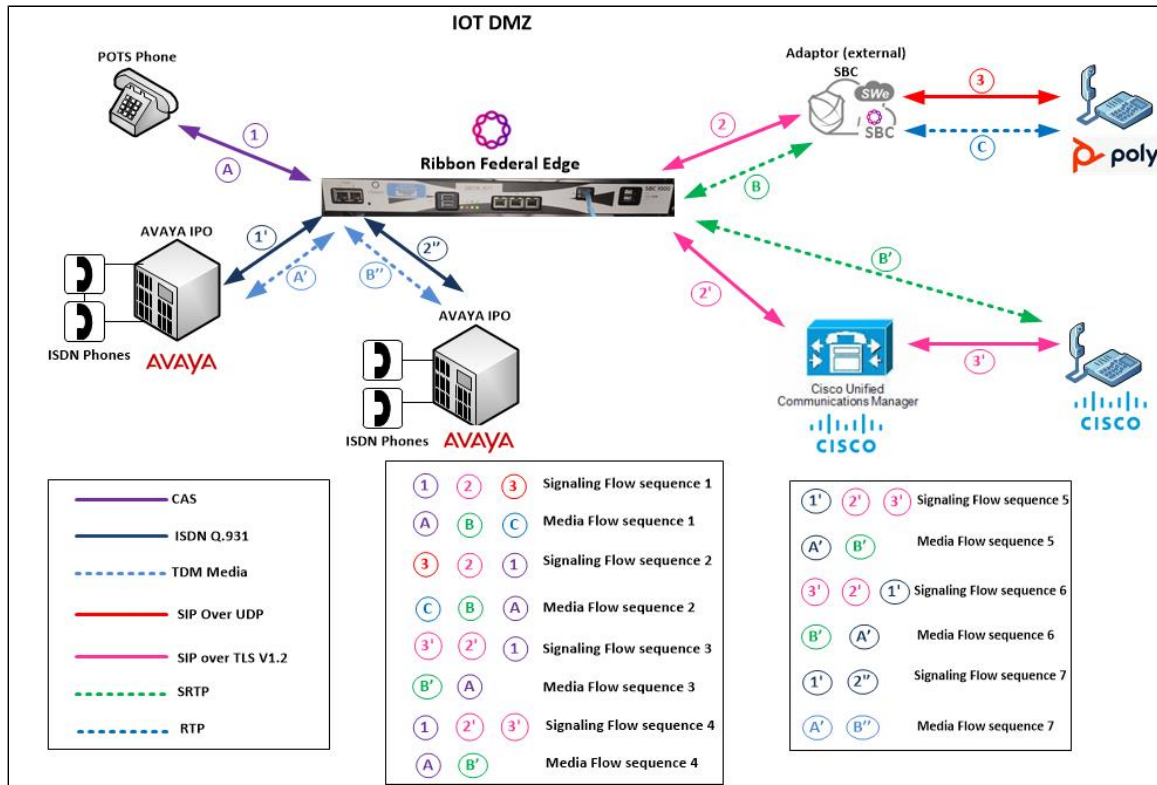
Deployment Topology



Interoperability Test Lab Topology



Call Flow Diagram

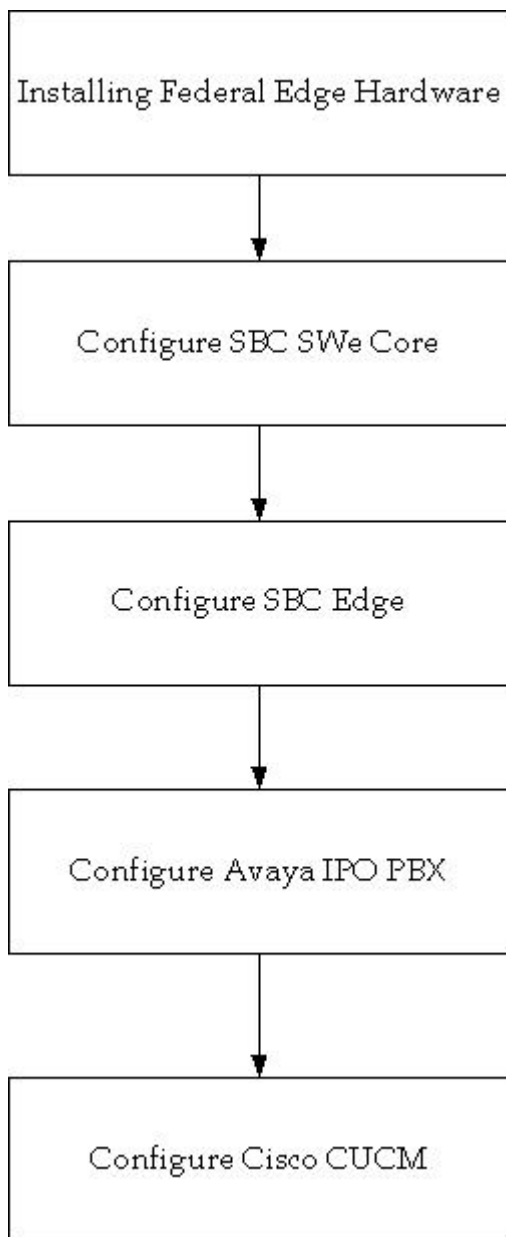


Document Workflow

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 be 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/sftproof/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 aallPayloadSize 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 routeUsingRecvFqdn 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 Sbcl2kNtpAccess precedence 1 protocol udp ipInterfaceGroup
INTERNAL ipInterface PKT0 destinationPort 123 fillRate 2000 bucketSize 50 state enabled
set addressContext default ipAccessControlList rule Sbcl2kEmaAccess 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.



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"

The screenshot shows the EMA web interface. The top navigation bar includes "Home", "Monitoring", "Administration" (selected), "Configuration", "Troubleshooting", "All", and "Custom". Below this is a sub-navigation bar with "Users and Application Management", "System Administration", "Accounting and Logs" (selected), and "Traps and SNMP". The main content area is titled "Type Admin" and displays a table of system logs.

Type	State	File Count	File Size	Message Queue Size	Save To	Filter Level	Rollover Start Time	Rollover Interval	Rollover Type	Rollover Action	File Write Mode	Syslog State	Rename Open Files	Disk Throttle Limit	Ev Lc Va
<input type="radio"/> System	Enabled	32	2048	10	Disk	Major		0	Nonrepetitive	Stop	Default	Disabled	Disabled	10000	Di
<input type="radio"/> Debug	Enabled	32	2048	10	Disk	Info		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di
<input type="radio"/> Trace	Enabled	32	2048	10	Disk	Major		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di
<input type="radio"/> Acct	Enabled	2048	65535	10	Disk	Major		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di
<input type="radio"/> Security	Enabled	32	2048	10	Disk	Major		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di
<input type="radio"/> Audit	Enabled	32	2048	10	Disk	Info		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di
<input type="radio"/> Packet	Enabled	32	2048	10	Disk	Major		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di
<input type="radio"/> Memusage	Enabled	32	2048	10	Disk	Major		0	Nonrepetitive	Stop	Default	Disabled	Disabled		Di

Records 1 through 8 of 8 total

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.

EMA Workspace: Classic Active Calls: 0 Licensed Sessions: 160000 admin

Home Monitoring Administration Configuration Troubleshooting All Custom

Users and Application Management System Administration Accounting and Logs Traps and SNMP

Expand All

Admin

CDR Server

Event Log

Data Agent Admin

Data Agent Status

Filter Admin

Filter Status

Sub System Admin

Type Admin

Type Status

Radius Authentication

Edit Selected Type Admin

Show only required fields

Type debug

State Enabled

File Count 32 (1 - 2048)

File Size 2048 (256 - 65535)

Message Queue Size 10 (2 - 100)

Save To

None

Disk

Filter Level Info

Rollover Start Time

Rollover Interval 0 (0 - 31536000)

Rollover Type

Repetitive

Nonrepetitive

Rollover Action

Start

Stop

Clear Save

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

EMA Workspace: Classic Active Calls: 0 Licensed Sessions: 160000 admin

Home Monitoring Administration Configuration Troubleshooting All Custom

Troubleshooting Tools Call Trace/Logs/Monitors

Expand All

Log Management

Log Management

Filters

Event Logs

Message Logs

System Dump

Apache

Netconf

User Activity

Install Logs

20 entries

Name	Date	Time	Download	Delete
100000C.DBG	09/16/2022	01:45:10	Download	Delete
1000005.SYS	09/16/2022	01:44:03	Download	Delete
100000B.DBG	09/16/2022	01:44:02	Download	Delete
1000019.AUD	09/16/2022	01:43:34	Download	Delete
1000019.MEM	09/16/2022	01:40:19	Download	Delete
1000005.SEC	09/16/2022	01:37:12	Download	Delete
100000A.DBG	09/16/2022	01:13:02	Download	Delete
1000009.DBG	09/16/2022	00:38:47	Download	Delete
1000008.DBG	09/16/2022	00:04:40	Download	Delete

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.

Home

Monitoring

Administration

Configuration

Troubleshooting

All

Custom

Last Visited

Troubleshooting Tools

Call Trace/Logs/Monitors

Expand All

CDR Viewer

Alarms

Call Diagnostics

CDR Viewer

Coredump

HA Pair Differences

Policy Analysis - SSREQ

Search Audit Logs

Statistics Status and Usage

System Dump

TShark

User Activity Log Purge

Troubleshooting

Enabled

Disable

Sip Ladder

Enable

Disabled

CDR Call List

Filters

ALL

Show 10 entries

	Record Type	Start Date	Start Time	End Date	End Time	Duration	Calling Number	Called Number	GCID	Call Disconnect Reason
<input type="radio"/>	ATTEMPT	08/26/2022	14:49:49	08/26/2022	14:49:54	5	9993332001	9993332004	0x0000B44	41
<input type="radio"/>	ATTEMPT	08/26/2022	14:49:49	08/26/2022	14:49:54	5	9993332001	9993332004	0x0000B41	41
<input type="radio"/>	START	08/26/2022	14:49:48	--	--	--	9993332001	9993332007	0x0000B43	--
<input type="radio"/>	START	08/26/2022	14:49:48	--	--	--	9993332001	9993332007	0x00040B3C	--
<input type="radio"/>	START	08/26/2022	14:49:47	--	--	--	9993332001	9993332002	0x000C0B3D	--
<input type="radio"/>	START	08/26/2022	14:49:47	--	--	--	9993332001	9993332002	0x00040B3A	--
<input type="radio"/>	ATTEMPT	08/26/2022	14:49:47	08/26/2022	14:49:52	5	9993332001	9993332003	0x0000B42	102
<input type="radio"/>	ATTEMPT	08/26/2022	14:49:47	08/26/2022	14:49:52	5	9993332001	9993332003	0x00000B3F	102
<input type="radio"/>	ATTEMPT	08/26/2022	14:49:45	08/26/2022	14:49:50	5	9993332001	9993332004	0x0000B40	41
<input type="radio"/>	ATTEMPT	08/26/2022	14:49:45	08/26/2022	14:49:50	5	9993332001	9993332004	0x00000B3D	41

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".

EMA
Workspace: Classic
Active Calls: 0 Licensed Sessions: 160000
admin
Search

Home Monitoring Administration Configuration Troubleshooting All Custom

Expand All

Configure Trace and Media Packet Capture

Call Trace Status and Settings
Save & Start Trace Stop Trace

Call Trace Duration
Run trace until stopped (by clicking the Stop Trace button)
Stop trace after 180 minutes * (1 - 360)

Number of Matches (optional)
Stop trace after the call filters have been matched times (1 - 64)

The call error trace applies only to SIP Call traces
Trace calls with errors of the type Any

Call Trace Status
Call trace stopped.

Sage Tracing
Enable
Disable

Call Trace Filters
Copy Call Filter New Call Filter

Expand All

Call Detail Status
Call Media Status
Call Queuing
Call Remote Media Status
Call Resource Detail Status
Call Routing
Call Summary Status
Call Trace
Signaling Packet Capture
Call Trace Status
Carrier
Country
Deleted Registration Dump
DTLS Sctp Statistics

Create New Call Trace Filter

NameTRACE_TEST(up to 23 characters)
State
☒ Enabled
☐ Disabled
SIPRec Legs Capture
☐ Enabled
☒ Disabled
Capture type
☒ Capture trace information (.trc logs) only
☐ Capture trace information (.trc logs) and media information (.pkt logs)
Detail level to log
Level 2 - Everything but raw hex dumps
Capture calls that match these filters
☒ Called number9123456789(0 - 30 characters)
☐ Calling numberCalling number(0 - 30 characters)
☐ Contractor numberContractor number(0 - 30 characters)
☐ Redirecting numberRedirecting number(0 - 30 characters)
☐ CDDN numberCDDN number(0 - 30 characters)
☐ Transfer capabilityUnrestricted
☐ Trunk GroupTrunk Group(up to 23 characters)
☐ Peer IP addressPeer IP address(nnn.nnn.nnn.nnn)
Stop Match
☐ When a match occurs in this filter, stop trying to match the other filters.
☒ Continue to try to match up to two other filters after a match is found in this filter.

Undo Edits
Save

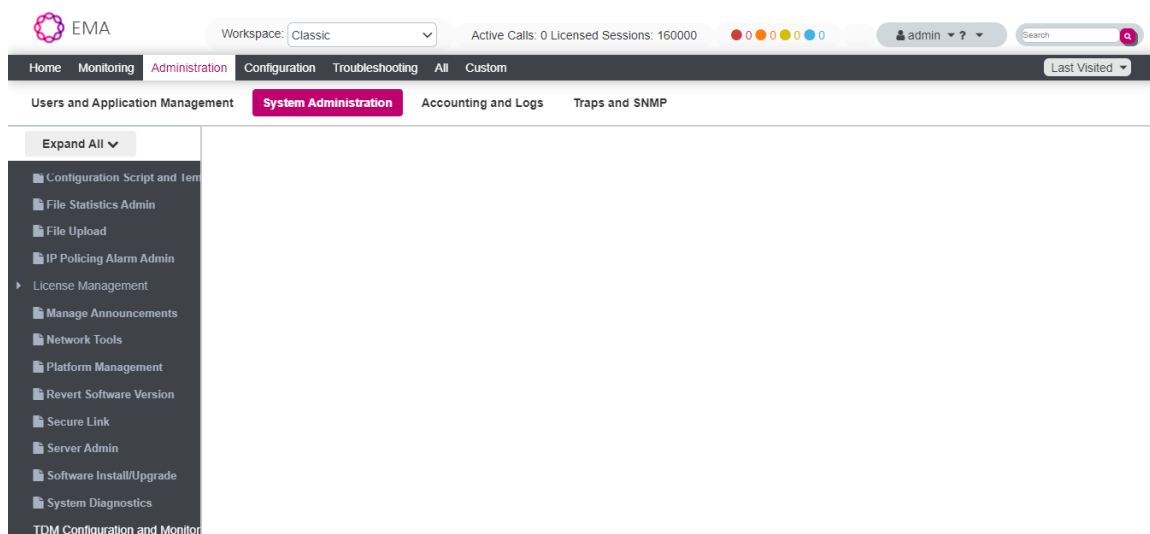
When entering phone numbers, X or x means accept anything in that digit position. For example, 617xx1212 would filter for all numbers 6170001212 through 6179991212. The % symbol acts as a wildcard for all remaining digits. For example, use 978% to trace all calls with a 978 prefix.
Note that when running a level 4 call trace, you are only allowed to filter on Peer IP address. When entering a Peer IP Address, enter 255.255.255.255 to match ALL packets to/from any IP address.

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.

Welcome to Ribbon SBC 2000

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

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

User Name

Password

Login **Cancel**

Copyright © 2010-2022 Ribbon Communications Operating Company, Inc. All Rights Reserved

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

Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help

Device Name: S4007921342017 SBC 2000

Monitor Tasks Settings Diagnostics System

Search...

Expand All | Collapse All | Reload

Call Routing

Signaling Groups

Node Interfaces

System

SIP

CAS

Security

Tone Tables

SNMP/Alarms

Logging Configuration

The Settings tab provides access to the full configuration tree on the SBC 2000. Clicking on the links in the tree will display the relevant content on the right hand panel.

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

Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help

Device Name: S4007921342017 SBC 2000

Monitor Tasks Settings Diagnostics System

Overview Inventory Report Statistics About SBC Edge

System Overview August 15, 2022 11:18:17

System Name	S4007921342017	CPU Usage	5%
Chassis Model	SBC 2000	Memory Usage	32%
Mode	Federal SBC	Total System Memory	491 MB
Node License State	SBC	File Descriptors Opened	1610
Software Bundled	No	CPU Load Average	0.1, 0.15, 0.08
Software Version	11.1.0	Chassis Board Bottom Temp	34 °C
Build Number	637	Chassis Board Top Temp	32 °C
Node Serial Number	S4007921342017	Core Switch Temp	40 °C
Hardware ID	d12099d2b2212b60db55ea	Contact	
Up Time	2 days, 21 hrs, 44 mins, 11 secs	Location	
		Timezone	(GMT) UTC (Zulu)

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

Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help
Device Name: S4007921342017
SBC 2000

Monitor Tasks Settings Diagnostics System

Cards/Modules Status

Total 7 Module Rows

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

Ports Status

Total 32 Port Rows

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 1:15	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

Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help
Device Name: S4007921342017
SBC 2000

Monitor Tasks Settings Diagnostics System

Ports Status

Total 32 Port Rows

Port ID	Port Type	Admin State	Service Status
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.

Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help
Device Name: S4007921342017
SBC 2000

Monitor Tasks Settings Diagnostics System

Search... Expand All Collapse All Reload

- Call Routing
- Signaling Groups
- Node Interfaces
- System
 - Node-Level Settings
 - System Timing
 - Licensing
 - Current Licenses**
 - License Keys
 - Install New License
 - Software Management
- SIP
- CAS
- Security
- Tone Tables
- SNMP/Alarms
- Logging Configuration

Current Licenses

August 15, 2022 11:21:19

Historical Usage

Port Licenses

Total 2 PortLicense Rows

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

Feature Licenses

Total 1 Feature License Row

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.

ribbon Monitor Tasks Settings Diagnostics System Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help Device Name: S4007921342017 SBC 2000

Search... Expand All Collapse All Reload

- Call Routing
- Signaling Groups
- Node Interfaces
- System
- SIP
- CAS
 - CAS Signaling Profiles
 - (FXS) FXS PROFILE
 - Supplementary Service Profiles
- Security
- Tone Tables
- SNMP/Alarms
- Logging Configuration

CAS Signaling Profile Table August 15, 2022 11:23:27

Create CAS Profile + - Total 1 Signaling Profile Row

Description	Type	Primary Key
FXS PROFILE	FXS	1

Description:

Loop Start FXS Properties

Loop Start Type:

Forward Disconnect Duration: * ms (100..3000)

Disconnect Tone Generation:

Flashhook Signal Detection:

Maximum Flashhook Duration: * ms (50..1000)

Minimum Flashhook Duration: * ms (50..1000)

Inter-Digit Timeout: * ms (250..30000)

ribbon Monitor Tasks Settings Diagnostics System Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help Device Name: S4007921342017 SBC 2000

Search... Expand All Collapse All Reload

- Call Routing
- Signaling Groups
- Node Interfaces
- System
- SIP
- CAS
 - CAS Signaling Profiles
 - (FXS) FXS PROFILE
 - Supplementary Service Profiles
- Security
- Tone Tables
- SNMP/Alarms
- Logging Configuration

CAS Signaling Profile Table August 15, 2022 11:23:27

Create CAS Profile + - Total 1 Signaling Profile Row

Description	Type	Primary Key
FXS PROFILE	FXS	1

Maximum Flashhook Duration: * ms (50..1000)

Minimum Flashhook Duration: * ms (50..1000)

Inter-Digit Timeout: * ms (250..30000)

Ringing Cadence

Cadence On: * ms (50..9000)

Cadence Off: * ms (50..9000)

Double Cadence:

Apply

- 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.

ribbon Monitor Tasks Settings Diagnostics System Welcome: s4007921342017 | Last Login: Aug 12, 2022 13:49:56 | Logout | Help Device Name: S4007921342017 SBC 2000

Search... Expand All Collapse All Reload

- Call Routing
- Signaling Groups
- Node Interfaces
- System
- SIP
- CAS
 - CAS Signaling Profiles
 - (FXS) FXS PROFILE
 - Supplementary Service Profiles
 - SUPPLEMENTARY_PROFILE
- Security
- Tone Tables
- SNMP/Alarms
- Logging Configuration

Supplementary Service Profile Table August 15, 2022 11:25:54

Total 1 Supplementary Service Profile Row

Description	Hold	Transfer	Call Waiting	Primary Key
SUPPLEMENTARY_PROFILE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1

Create Supplementary Service Profile - Google Chrome

Not secure <https://10.54.182.154/cgi/phpUI/config.php?cfg=/vie...>

Create Supplementary Service Profile August 15, 2022 11:25:56

Description:

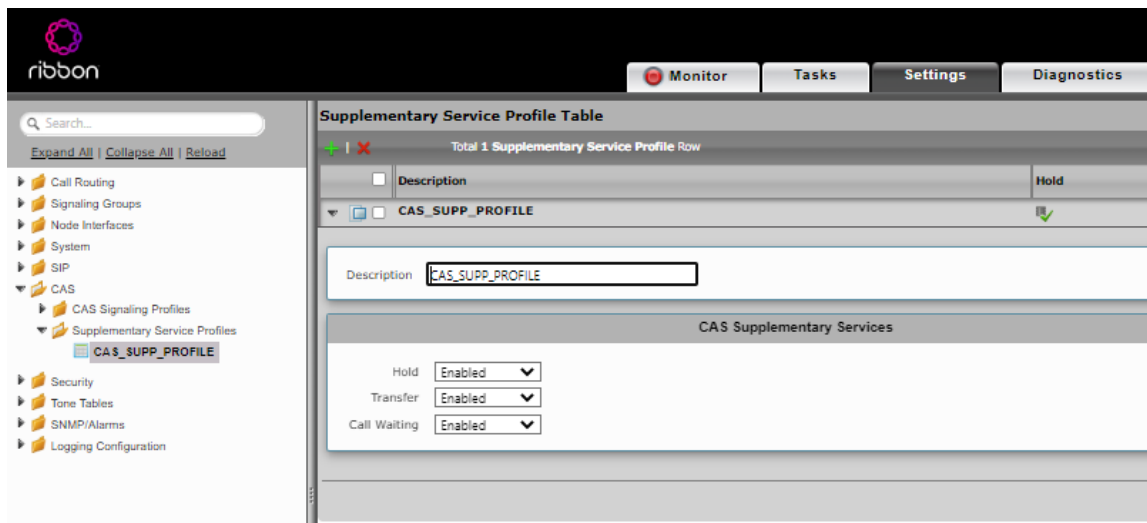
CAS Supplementary Services

Hold:

Transfer:

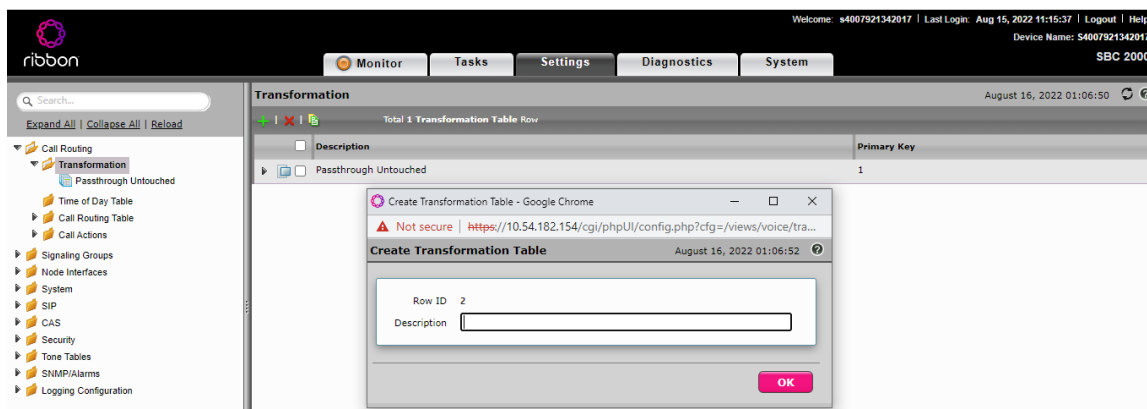
Call Waiting:

OK



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".

ribbon

Welcome: s4007921342017 | Last Login: Aug 15, 2022 11:15:37 | Logout | Help

Device Name: S4007921342017

SBC 2000

Monitor Tasks Settings Diagnostics System

Search...

Expand All | Collapse All | Reload

Call Routing

Signaling Groups

(SIP) Fixed SIP SG

(ISDN) ISDN_SG_1a

(ISDN) ISDN_SG_1b

(ISDN) ISDN_SG_2a

(ISDN) ISDN_SG_2b

(ISDN) ISDN_SG_3a

(ISDN) ISDN_SG_3b

(ISDN) ISDN_SG_4a

(ISDN) ISDN_SG_4b

(CAS) CAS_SG

Node Interfaces

System

SIP

CAS

Signaling Group Table

Create Signaling Group

Total 10 Signaling Group Rows

Type	ISDN Signaling Group	Admin State	Service Status	Display	Primary Key
SIP	CAS Signaling Group	Up	Up	Counters Channels Sessions	1
ISDN	ISDN_SG_1a	Up	Up	Counters Historical Usage	10001
ISDN	ISDN_SG_1b	Up	Up	Counters Historical Usage	10002
ISDN	ISDN_SG_2a	Up	Up	Counters Historical Usage	10003
ISDN	ISDN_SG_2b	Up	Up	Counters Historical Usage	10004
ISDN	ISDN_SG_3a	Up	Up	Counters Historical Usage	10005
ISDN	ISDN_SG_3b	Up	Up	Counters Historical Usage	10006
ISDN	ISDN_SG_4a	Up	Up	Counters Historical Usage	10007
ISDN	ISDN_SG_4b	Up	Up	Counters Historical Usage	10008
CAS	CAS_SG	Up	Up	Counters Historical Usage	20001

ribbon

Welcome: s4007921342017 | Last Login: Sep 27, 2022 06:49:36 | Logout | Help

Device Name: S4007921342017

SBC 2000

Monitor Tasks Settings Diagnostics System

Search...

Expand All | Collapse All | Reload

Call Routing

Signaling Groups

(SIP) Fixed SIP SG

(ISDN) ISDN_SG_1a

(ISDN) ISDN_SG_1b

(ISDN) ISDN_SG_2a

(ISDN) ISDN_SG_2b

(ISDN) ISDN_SG_3a

(ISDN) ISDN_SG_3b

(ISDN) ISDN_SG_4a

(ISDN) ISDN_SG_4b

(CAS) CAS_SG

Node Interfaces

System

SIP

CAS

Security

Tone Tables

SNMP/Alarms

Logging Configuration

ISDN_SG_2b

ISDN_SG_3a

ISDN_SG_3b

ISDN_SG_4a

ISDN_SG_4b

CAS_SG

Description: CAS_SG

Line Type: Analog

Admin State: Enabled

Service Status: Up

Channels and Routing

Direction: Bidirectional

Channel Hunting: Most Idle

Tone Table: Default Tone Table

Action Set Table: None

Call Routing Table: SIP Route Table

CAS Protocol

CAS Signaling Profile: (FXS) FXS_PROFILE

Supplementary Services Profile: SUPPLEMENTARY_SERVICES

Caller ID Type: Disabled

Play Ringback: Auto

Call Forwarding Feature: Enable

No Channel Available Override: 34: No Circuit/Channel Available

Call Setup Response Timer: 255 (180..750) secs

Call Forwarding Activate DTMF: *72

Call Forwarding Deactivate DTMF: *73

Assigned Channels

Total 1 CAS Channel Row

Port Name	Channel Phone Number	Hotline Enabled	Hotline Number	Call Forwarding Activated	Call Forwarding Number
1:1	8885552003	No		No	

Apply

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".

ribbon

Welcome: s4007921342017 | Last Login: Aug 15, 2022 11:15:37 | Logout | Help
Device Name: S4007921342017
SBC 2000

Monitor Tasks Settings Diagnostics System

Search...

Expand All | Collapse All | Reload

Call Routing

Signaling Groups

- (SIP) Fixed SIP SG
- (ISDN) ISDN_SG_1a
- (ISDN) ISDN_SG_1b
- (ISDN) ISDN_SG_2a
- (ISDN) ISDN_SG_2b
- (ISDN) ISDN_SG_3a
- (ISDN) ISDN_SG_3b
- (ISDN) ISDN_SG_4a
- (ISDN) ISDN_SG_4b
- (CAS) CAS_SG

Node Interfaces

System

SIP

CAS

Security

Tone Tables

SNMP/Alarms

Logging Configuration

Signaling Group Table

Total 10 Signaling Group Rows

Type	Description	Admin State	Service Status	Display	Primary Key
SIP	Fixed SIP SG	Up	Up	Counters Channels Sessions	1
ISDN	ISDN_SG_1a	Up	Up	Counters Historical Usage	10001

Description: ISDN_SG_1a

Admin State: Enabled

Service Status: Up

Channels and Routing

Channel Hunting: Most Idle

Direction: Bidirectional

Tone Table: Default Tone Table

Action Set Table: None

Call Routing Table: SIP Route Table

No Channel Available Override: 34: No Circuit/Channel Available

Port and Protocol

Port Name: (T1) Port 2:1

Fractional: No

Switch Variant: NI2

ISDN Side: Network

Play Ringback: Auto on Alert

Service Msg Capability: Enabled

ribbon

Welcome: s4007921342017 | Last Login: Aug 15, 2022 11:15:37 | Logout | Help
Device Name: S4007921342017
SBC 2000

Monitor Tasks Settings Diagnostics System

Search...

Expand All | Collapse All | Reload

Call Routing

Signaling Groups

- (SIP) Fixed SIP SG
- (ISDN) ISDN_SG_1a
- (ISDN) ISDN_SG_1b
- (ISDN) ISDN_SG_2a
- (ISDN) ISDN_SG_2b
- (ISDN) ISDN_SG_3a
- (ISDN) ISDN_SG_3b
- (ISDN) ISDN_SG_4a
- (ISDN) ISDN_SG_4b
- (CAS) CAS_SG

Node Interfaces

System

SIP

CAS

Security

Tone Tables

SNMP/Alarms

Logging Configuration

Signaling Group Table

Total 10 Signaling Group Rows

Type	Description	Admin State	Service Status	Display	Primary Key
SIP	Fixed SIP SG	Up	Up	Counters Channels Sessions	1
ISDN	ISDN_SG_1a	Up	Up	Counters Historical Usage	10001

No Channel Available Override: 34: No Circuit/Channel Available

Play Inband Message Post-Disconnect: No

Call Setup Response Timer: 255 (180..750) secs

Service Msg Capability: Enabled

Stop Far-End T310: Disabled

Indicated Channel: Exclusive

Switch Specific Parameters

Add PI To Setup: None

Early Media for PI: 2(Dest not ISDN): Enabled

Include Channel Interface Identifier: Disabled

Channel Number Bit: Set

Timeout/Timer Settings

T301: 180 (1..600) secs

T302: 15 (1..255) secs

ribbon

Welcome: s4007921342017 | Last Login: Aug 15, 2022 11:15:37 | Logout | Help
Device Name: S4007921342017
SBC 2000

Monitor Tasks Settings Diagnostics System

Search...

Expand All | Collapse All | Reload

Call Routing

Signaling Groups

- (SIP) Fixed SIP SG
- (ISDN) ISDN_SG_1a
- (ISDN) ISDN_SG_1b
- (ISDN) ISDN_SG_2a
- (ISDN) ISDN_SG_2b
- (ISDN) ISDN_SG_3a
- (ISDN) ISDN_SG_3b
- (ISDN) ISDN_SG_4a
- (ISDN) ISDN_SG_4b
- (CAS) CAS_SG

Node Interfaces

System

SIP

CAS

Security

Tone Tables

SNMP/Alarms

Logging Configuration

Signaling Group Table

Total 10 Signaling Group Rows

Type	Description	Admin State	Service Status	Display	Primary Key
SIP	Fixed SIP SG	Up	Up	Counters Channels Sessions	1
ISDN	ISDN_SG_1a	Up	Up	Counters Historical Usage	10001

T301: 180 (1..600) secs

T302: 15 (1..255) secs

T303: 4 (1..255) secs

T305: 30 (1..255) secs

T308: 4 (1..255) secs

T309: 6 (1..255) secs

T310: 10 (1..255) secs

T313: 4 (1..255) secs

T314: 4 (1..255) secs

T316: 120 (1..255) secs

T322: 4 (1..255) secs

T3M1/T323: 120 (1..255) secs

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.

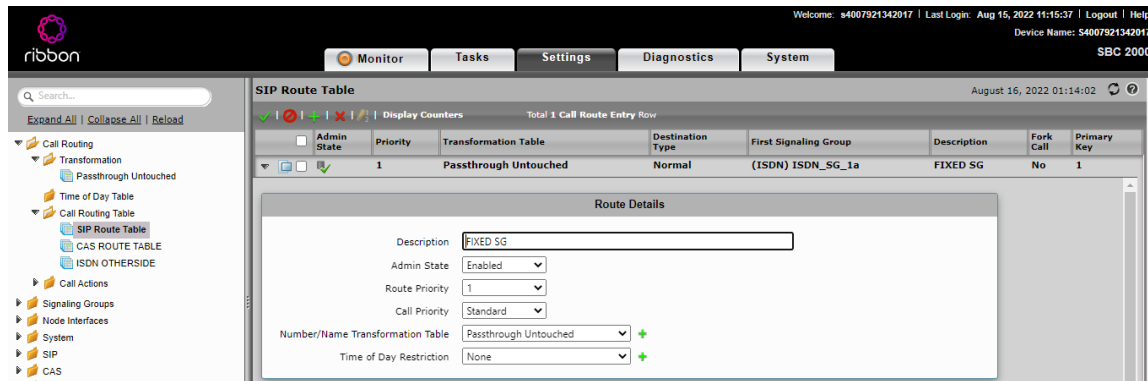
For Routing call from SIP to ISDN or FXS

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

ISDN to SIP

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.

FXS to SIP

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

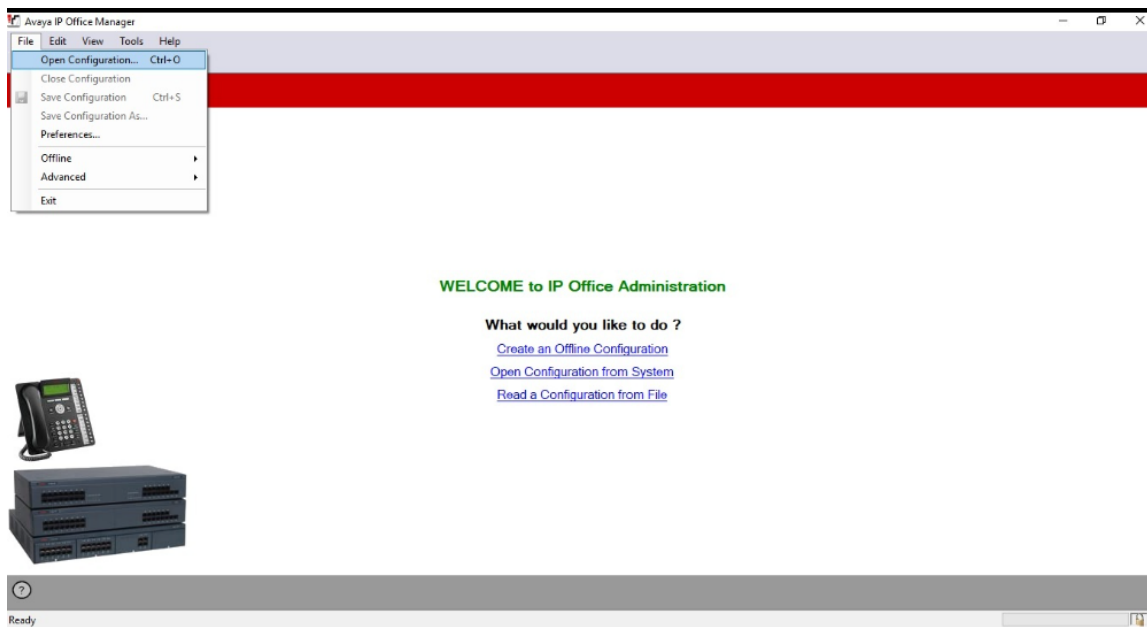
We used Avaya IPO for ISDN PRI Trunk termination.

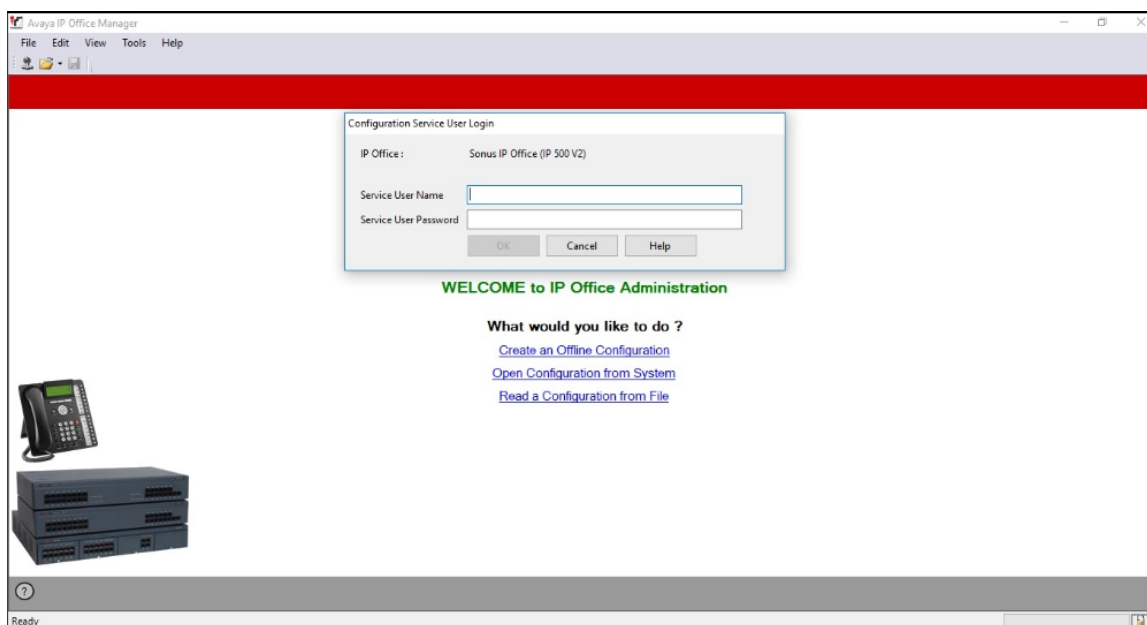
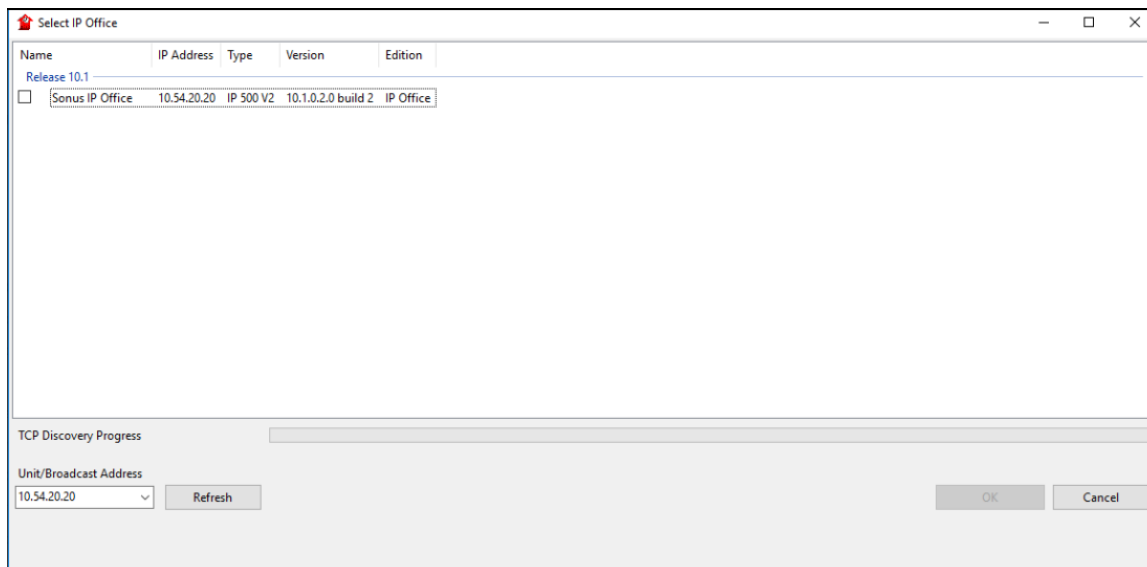
The Avaya IP Office Manager was loaded onto the tester's PC and allowed user login and access to the Avaya IP Office PBX. With Avaya IP Office Manager loaded on your local PC, select **Program Files (x86) > Avaya > IP Office > Manager**. Select the "Manager" application.

AVAYA

Avaya™
IP Office Manager
Version 10.1.0.2.0 build 2

Copyright 2018 Avaya Inc. All rights reserved.





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.

IP Offices

BOOTP (2)

Operator (3)

Sonus IP Office

System (1)

Line (12)

1

2

3

4

17

18

19

20

21

22

23

Control Unit (3)

Extension (29)

User (29)

Group (1)

Short Code (95)

Service (0)

RAS (1)

Incoming Call Route (8)

WAN Port (0)

Directory (0)

Time Profile (0)

Firewall Profile (1)

IP Route (2)

Account Code (0)

License (6)

Tunnel (0)

PRI 24 (Universal) - Line 5

PRI 24 Line Channels

Line Number

05

Line SubType

PRI

Card

2

Port

9

Admin

In Service

Switch Type

NI2

Provider

Local Telco

Send Service Messages

☐

Channel Allocation

23 -> 1

Prefix

Add 'Not end-to-end ISDN' Information Element

Never

Progress Replacement

None

Send Redirecting Number

☐

Test Number

Clock Quality

Network

Framing

ESF

CRC Checking

☒

Zero Suppression

B8ZS

CSU Operation

☐

Line Signaling

CPE

Haul Length

574-688 ft

Incoming Routing Digits

9

☐ Send original calling party for forwarded and twinning calls

Originator number for forwarded and twinning calls

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".

IP Offices

BOOTP (2)

Operator (3)

Sonus IP Office

System (1)

Line (12)

1

2

3

4

5

17

18

19

20

21

22

23

Control Unit (3)

Extension (29)

User (29)

Group (1)

Short Code (95)

Service (0)

RAS (1)

Incoming Call Route (8)

WAN Port (0)

Directory (0)

Time Profile (0)

Firewall Profile (1)

IP Route (2)

Account Code (0)

License (6)

Tunnel (0)

PRI 24 (Universal) - Line 5

PRI 24 Line Channels

Channel	Groups	Line Appearance	Direction	Bearer	S.	Admin
1	0 52	701	Bothway	Any	N.	In Service
2	0 52	702	Bothway	Any	N.	In Service
3	0 52	703	Bothway	Any	N.	In Service
4	0 52	704	Bothway	Any	N.	In Service
5	0 52	705	Bothway	Any	N.	In Service
6	0 0	706	Bothway	Any	N.	Out Of Service
7	0 0	707	Bothway	Any	N.	Out Of Service
8	0 0	708	Bothway	Any	N.	Out Of Service
9	0 0	709	Bothway	Any	N.	Out Of Service
10	0 0	710	Bothway	Any	N.	Out Of Service
11	0 0	711	Bothway	Any	N.	Out Of Service
12	0 0	712	Bothway	Any	N.	Out Of Service
13	0 0	713	Bothway	Any	N.	Out Of Service
14	0 0	714	Bothway	Any	N.	Out Of Service
15	0 0	715	Bothway	Any	N.	Out Of Service
16	0 0	716	Bothway	Any	N.	Out Of Service
17	0 0	717	Bothway	Any	N.	Out Of Service
18	0 0	718	Bothway	Any	N.	Out Of Service
19	0 0	719	Bothway	Any	N.	Out Of Service
20	0 0	720	Bothway	Any	N.	Out Of Service
21	0 0	721	Bothway	Any	N.	Out Of Service
22	0 0	722	Bothway	Any	N.	Out Of Service
23	0 0	723	Bothway	Any	N.	Out Of Service

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.

IP Offices	Analogue Extension: 26 210
<ul style="list-style-type: none"> BOOTP (2) Operator (3) Sonus IP Office System (1) Line (12) Control Unit (3) Extension (29) <ul style="list-style-type: none"> 8009 8007 1 201 2 202 3 203 4 204 5 205 6 206 7 207 8 208 26 210 25 211 8017 212 8018 213 8000 250 8001 500 8002 501 8004 503 8003 504 8005 521 8006 522 8008 523 8011 524 8010 525 8013 528 8014 1234 	<div>Extension Analogue</div> <div> <div>Extension ID</div> <div>26</div> </div> <div> <div>Base Extension</div> <div>210</div> </div> <div> <div>Caller Display Type</div> <div>On</div> </div> <div> <div>Device Type</div> <div>Analogue Handset</div> </div> <div> <div>Location</div> <div>System (None)</div> </div> <div> <div>Module</div> <div>BP2</div> </div> <div> <div>Port</div> <div>2</div> </div> <div> <div>Disable Speakerphone</div> <div><input type="checkbox"/></div> </div>

Click "Standard Telephone" for normal POTS Phone.

IP Offices	Analogue Extension: 26 210
<ul style="list-style-type: none"> BOOTP (2) Operator (3) Sonus IP Office System (1) Line (12) Control Unit (3) Extension (29) <ul style="list-style-type: none"> 8009 8007 1 201 2 202 3 203 4 204 5 205 6 206 7 207 8 208 26 210 25 211 8017 212 8018 213 8000 250 8001 500 8002 501 8004 503 8003 504 8005 521 8006 522 8008 523 8011 524 8010 525 8013 528 8014 1234 	<div>Extension Analogue</div> <div> <div>Equipment Classification</div> <div> <input type="radio"/> Quiet Headset <input type="radio"/> Paging Speaker <input checked="" type="radio"/> Standard Telephone <input type="radio"/> Door Phone 1 <input type="radio"/> Door Phone 2 <input type="radio"/> IVR Port <input type="radio"/> FAX Machine <input type="radio"/> MOH Source </div> </div> <div> <div>Flash Hook Pulse Width</div> <div> <input checked="" type="checkbox"/> Use System Defaults <div>Minimum Width</div> <div>20</div> <div>ms</div> <div>Maximum Width</div> <div>500</div> <div>ms</div> </div> </div> <div> <div>Message Waiting Lamp Indication Type</div> <div>None</div> </div> <div> <div>Hook Persistence</div> <div>100</div> <div>ms</div> </div>

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.

IP Offices	992xxxx: Dial
<ul style="list-style-type: none"> 18668374496 00918067895757 011441582405100 011528183991500 0N 1603xxxxxxx 1610xxxxxxx 1614xxxxxxx 241333xxxx 3xxx 511xxxxxxx 54xxxxxx 5611XXXXXX 6600XXX 8611XXXXXX 8xxx 911 8554 8003337626 919xxxxxxx 962xxxx 9696xx 9722653740 9722653741 9722653743 9722xxxxxx 97255520xx 9727695635 992xxxx 999620428030 Service (0) RAS (1) Incoming Call Route (8) 	<p>Short Code</p> <p>Code: 992xxxx</p> <p>Feature: Dial</p> <p>Telephone Number: 992N</p> <p>Line Group ID: 52</p> <p>Locale:</p> <p>Force Account Code: <input type="checkbox"/></p> <p>Force Authorization Code: <input type="checkbox"/></p>

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).

IP Offices	0 210
<ul style="list-style-type: none"> BOOTP (2) Operator (3) Sonus IP Office <ul style="list-style-type: none"> System (1) Line (12) Control Unit (3) Extension (29) User (29) Group (1) Short Code (95) Service (0) RAS (1) Incoming Call Route (8) <ul style="list-style-type: none"> 20 1 17 18 22 0 210 2 9725552031 1 9725552032 WAN Port (0) Directory (0) Time Profile (0) Firewall Profile (1) IP Route (2) Account Code (0) License (6) Tunnel (0) User Rights (8) ARS (2) <ul style="list-style-type: none"> 50: Main 51: TEST 	<p>Standard Voice Recording Destinations</p> <p>Bearer Capability: Any</p> <p>Line Group ID: 0</p> <p>Incoming Number: 210</p> <p>Incoming Sub Address:</p> <p>Incoming CLI:</p> <p>Locale:</p> <p>Priority: 2 - Medium</p> <p>Tag:</p> <p>Hold Music Source: System Source</p> <p>Ring Tone Override: None</p>

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.

IP Offices

- BOOTP (2)
- Operator (3)
- Sonus IP Office
 - System (1)
 - Line (12)
 - Control Unit (3)
 - Extension (29)
 - User (29)
 - Group (1)
 - Short Code (95)
 - Service (0)
 - RAS (1)
 - Incoming Call Route (8)
 - 20
 - 1
 - 17
 - 18
 - 22
 - 0 210
 - 2 9725552031
 - 1 9725552032
 - WAN Port (0)
 - Directory (0)
 - Time Profile (0)
 - Firewall Profile (1)
 - IP Route (2)
 - Account Code (0)
 - License (6)
 - Tunnel (0)
 - User Rights (8)
 - ARS (2)
 - 50: Main

0 210

Standard

Voice Recording

Destinations

TimeProfile	Destination	Fallback Extension
Default Value	210 Extn210	

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

IP Offices

- Sonus IP Office
 - System (1)
 - Line (12)
 - Control Unit (3)
 - Extension (29)
 - User (29)
 - NoUser
 - RemoteManager
 - 212 212
 - 213 213
 - 250 250
 - 500 500
 - 501 501
 - 503 503
 - 504 504
 - 521 521
 - 522 522
 - 523 523
 - 524 524
 - 525 525
 - 528 528
 - 2022 2022
 - 2022 2022
 - 2030 2030
 - 1234 Akshay_Test
 - 201 Extn201
 - 202 Extn202
 - 203 Extn203
 - 204 Extn204
 - 205 Extn205
 - 206 Extn206
 - 207 Extn207
 - 208 Extn208
 - 210 Extn210

Extn210: 210

User

Voicemail

DND

Short Codes

Source Numbers

Telephony

Forwarding

Dial In

Voice Recording

Button Programming

Menu Programming

Name

Extn210

Password

Confirm Password

Unique Identity

Conference PIN

Confirm Audio Conference PIN

Account Status

Enabled

Full Name

Extension

210

Email Address

Locale

Priority

5

System Phone Rights

None

Profile

Basic User

☐ Resonantist

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

Port 2 is linked to Extension 210.

IP Offices

- Sonus IP Office
- System (1)
- Line (12)
- Control Unit (3)
- Extension (29)
 - 8007
 - 8009
 - 1 201
 - 2 202
 - 3 203
 - 4 204
 - 5 205
 - 6 206
 - 7 207
 - 8 208
 - 26 210
 - 25 211
 - 8017 212
 - 8018 213
 - 8000 250
 - 8001 500
 - 8002 501
 - 8004 503
 - 8003 504
 - 8005 521

Analogue Extension: 26 210

Extension / Analogue

Extension ID

26


Base Extension

210

Caller Display Type

On

Device Type



Analogue Handset

Location

System (None)

Module

BP2

Port

2

Disable Speakerphone

☐

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

System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help

SIP Trunk Security Profile Configuration

Save
Delete
Copy
Reset
Apply Config
Add New

Status
i Status: Ready

SIP Trunk Security Profile Information

Name*
Secure SIP Trunk Profile- aish-fedral

Description
Secure SIP Trunk Profile authenticated by null String

Device Security Mode
Encrypted

Incoming Transport Type*
TLS

Outgoing Transport Type
TLS

☐ Enable Digest Authentication

Nonce Validity Time (mins)*
600

Secure Certificate Subject or Subject Alternate Name
fedcore5.interopdomain.com

Incoming Port*
5061

☐ Enable Application level authorization

☒ Accept presence subscription

☒ Accept out-of-dialog refer**

☒ Accept unsolicited notification

☒ Accept replaces header

☐ Transmit security status

☐ Allow charging header

SIP V.150 Outbound SDP Offer Filtering*
Use Default Filter

Save
Delete
Copy
Reset
Apply Config
Add New

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 -alsh

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

Trunk Configuration

Save

Delete

Reset

Add New

SIP Trunk Status

Service Status: Full Service

Duration: Time In Full Service: 3 days 14 hours 43 minutes

Device Information

Product:

SIP Trunk

Device Protocol:

SIP

Trunk Service Type

None(Default)

Device Name*

FEDRAL_AISH

Description

FEDRAL_AISH

Device Pool*

Default

Common Device Configuration

< None >

Call Classification*

Use System Default

Media Resource Group List

san_media_grplist

Location*

Hub_None

AAR Group

< None >

Tunneled Protocol*

None

QSIG Variant*

No Changes

ASN.1 ROSE OID Encoding*

No Changes

Packet Capture Mode*

None

Packet Capture Duration

0

☐ Media Termination Point Required

☒ Retry Video Call as Audio

☐ Path Replacement Support

☐ Transmit UTF-8 for Calling Party Name

☐ Transmit UTF-8 Names in QSIG APDU

☐ Unattended Port

☒ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure*

When using both sRTP and TLS

Route Class Signaling Enabled*

Default

Use Trusted Relay Point*

Default

Call Routing Information

☒ Remote-Party-Id

☒ Asserted-Identity

Asserted-Type*

Default

SIP Privacy*

Default

Trust Received Identity*

Trust All (Default)

Inbound Calls

Significant Digits*

All

Connected Line ID Presentation*

Default

Connected Name Presentation*

Default

Calling Search Space

< None >

AAR Calling Search Space

< None >

Prefix DN

☐ Redirecting Diversion Header Delivery - Inbound

Incoming Calling Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings

Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default	0	< None >	<input checked="" type="checkbox"/>

Incoming Called Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings

Default Prefix Settings

Incoming Called Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings

Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default	0	< None >	<input checked="" type="checkbox"/>

Connected Party Settings

Connected Party Transformation CSS

< None >

☒ Use Device Pool Connected Party Transformation CSS

Outbound Calls

Called Party Transformation CSS

< None >

☒ Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS

< None >

☒ Use Device Pool Calling Party Transformation CSS

Calling Party Selection*

Originator

Calling Line ID Presentation*

Default

Calling Name Presentation*

Default

Calling and Connected Party Info Format*

Deliver DN only in connected party

☐ Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS

< None >

☒ Use Device Pool Redirecting Party Transformation CSS

Presentation Information

☐ Anonymous Presentation

Presentation Number

Presentation Name

Confidential and Proprietary. Copyright © 2020-2023 Ribbon Communications Operating Company, Inc. © 2020-2023 ECI Telecom Ltd.

Presentation Information

☐ Anonymous Presentation
Presentation Number
Presentation Name

☐ Send Presentation Name and Number only in the FROM header and not in the other identity headers

SIP Information

Destination

☐ Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1 * 172.16.106.205		5061	down	local=2	Time Down: 0 day 0 hour 9 minutes <div></div>

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

Normalization Script

Normalization Script < None >

☐ Enable Trace

Parameter Name	Parameter Value
1	

Recording Information

☒ None
☐ This trunk connects to a recording-enabled gateway
☐ This trunk connects to other clusters with recording-enabled gateways

Geolocation Configuration

Geolocation < None >
Geolocation Filter < None >
☐ Send Geolocation Information

Save Delete Reset Add New

i *- Indicates required item.

i **. Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

Route Pattern

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

Figure 3: Route Pattern

System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help

Route Pattern Configuration

Save

Delete

Copy

Add New

Status

i Status: Ready

Pattern Definition

Route Pattern* \+1444555200X
Route Partition < None >
Description FEDERAL_ISDN_PHONE
Numbering Plan -- Not Selected --
Route Filter < None >
MLPP Precedence* Default
☐ Apply Call Blocking Percentage
Resource Priority Namespace Network Domain < None >
Route Class* Default
Gateway/Route List* FEDERAL_AISH (Edit)
Route Option
☒ Route this pattern
☐ Block this pattern No Error
Call Classification* OffNet
External Call Control Profile < None >
☐ Allow Device Override
☒ Provide Outside Dial Tone
☐ Allow Overlap Sending
☐ Urgent Priority
☐ Require Forced Authorization Code
Authorization Level* 0
☐ Require Client Matter Code

Calling Party Transformations

☐ Use Calling Party's External Phone Number Mask
Calling Party Transform Mask
Prefix Digits (Outgoing Calls)

Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Calling Party Number Type*	Cisco CallManager
Calling Party Numbering Plan*	Cisco CallManager

Connected Party Transformations

Connected Line ID Presentation*	Default
Connected Name Presentation*	Default

Called Party Transformations

Discard Digits	< None >
Called Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Called Party Number Type*	Cisco CallManager
Called Party Numbering Plan*	Cisco CallManager

ISDN Network-Specific Facilities Information Element

Network Service Protocol	-- Not Selected --				
Carrier Identification Code					
Network Service	-- Not Selected --	Service Parameter Name	< Not Exist >	Service Parameter Value	

*- indicates required item.

Phone Security Profile

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

Figure 4: Phone Security Profile

Phone Security Profile Configuration

Status

Status: Ready

Phone Security Profile Information

Product Type:	Cisco 8865
Device Protocol:	SIP
Name*	Secure Cisco 8865
Description	Secure Cisco 8865
Nonce Validity Time*	600
Device Security Mode	Encrypted
Transport Type*	TLS
<input type="checkbox"/> Enable Digest Authentication <input checked="" type="checkbox"/> TFTP Encrypted Config	

Phone Security Profile CAPF Information

Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*	5061
-----------------	------

*- indicates required item.

System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help

Phone Configuration

Save
Delete
Copy
Reset
Apply Config
Add New

Related Links: Back To Find/List

Status

Status: Ready

Modify Button Items

Line [1] - +19993332064 (no partition)

Line [2] - Add a new DN

Add a new SD

Add a new SD

Add a new SD

Add On Module(s) -----

Add a new SD

Add a new SD

Add a new SD

Add a new SD

Add a new SD

Unassigned Associated Items -----

Add a new SD

Alerting Calls

All Calls

Answer Oldest

Add a new BLF Directed Call Park

Call Park

Call Pickup

CallBack

Phone Type

Product Type: Cisco 8865
Device Protocol: SIP

Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager 10.54.22.250
IPv4 Address: 172.16.108.249
Active Load ID: sip8845_65.12-5-1SR3-74
Inactive Load ID: sip8845_65.11-0-1SR1-2
Download Status: None

Device Information

☒ Device is Active
☒ Device is trusted

MAC Address* 08CCA7858938 (SEP08CCA7858938)
Description SEP08CCA7858938

Current On-Premise Onboarding Method is set to Autoregistration. Activation Code will only apply to onboarding via MRA.
☐ Require Activation Code for Onboarding

☐ Allow Activation Code via MRA

Activation Code MRA Service Domain -- Not Selected -- View Details
Device Pool* Default View Details
Common Device Configuration < None > View Details
Phone Button Template* Standard 8865 SIP
Softkey Template < None >
Common Phone Profile* Standard Common Phone Profile View Details
Calling Search Space < None >
AAR Calling Search Space < None >

End User Configuration

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

Figure 5: End User Configuration

System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help

End User Configuration

Save
Delete
Add New

Status

Status: Ready

User Information

User Status Enabled Local User
User ID* +19993332054
Password
Confirm Password
Self-Service User ID
PIN
Confirm PIN
Last name* cisco phone
Middle name
First name
Display name
Title
Directory URI
Telephone Number
Home Number
Mobile Number
Pager Number
Mail ID
Manager User ID
Department
User Locale < None >
Associated PC/Site Code

Edit Credential
Edit Credential

MLPP User Identification Number

MLPP Password

Confirm MLPP Password

MLPP Precedence Authorization Level

Default

CAPF Information

Associated CAPF Profiles

View Details

Permissions Information

Groups

Admin-3rd Party API

Application Client Users

Standard Audit Users

Standard CAR Admin Users

Standard CCM Admin Users

Add to Access Control Group

Remove from Access Control Group

View Details

Roles

Standard AXL API Access

Standard Admin Rep Tool Admin

Standard Audit Log Administration

Standard CCM Admin Users

Standard CCM End Users

View Details

Conference Now Information

☐ Enable End User to Host Conference Now

Meeting Number

Attendees Access Code

Save

Delete

Add New

i

*- indicates required item.

Phone Configuration

Select **Device > Phone** Phone configuration.

Figure 6: Phone Configuration

System

Call Routing

Media Resources

Advanced Features

Device

Application

User Management

Bulk Administration

Help

Phone Configuration

Related Links: Back To Find/List

Save

Delete

Copy

Reset

Apply Config

Add New

Status

Status: Ready

Association

Modify Button Items

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

Phone Type

Product Type: Cisco 8865

Device Protocol: SIP

Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager 10.54.22.250

IP Address: 172.16.108.248

Active Load ID: slp8845_65.12-5-1SR3-74

Inactive Load ID: slp8845_65.11-0-1SR1-2

Download Status: None

Device Information

Device Is Active

Device Is Trusted

MAC Address: 08CCA785A8F4 (SEP08CCA785A8F4)

Description: SEP08CCA785A8F4

Current On-Premise Onboarding Method is set to Autoregistration. Activation Code will only apply to onboarding via MRA.

Require Activation Code for Onboarding

Allow Activation Code via MRA

Activation Code MRA Service Domain

Device Pool

Common Device Configuration

Phone Button Template

Softkey Template

Common Phone Profile

Calling Search Space

18	CallBack	AAR Calling Search Space	< None >
19	Do Not Disturb	Media Resource Group List	san_media_grplist
20	Group Call Pickup	User Hold MOH Audio Source	< None >
21	Hunt Group Logout	Network Hold MOH Audio Source	< None >
22	Intercom [1] - Add a new Intercom	Location*	Hub_None
23	Malicious Call Identification	AAR Group	< None >
24	Meet Me Conference	User Locale	< None >
25	Mobility	Network Locale	< None >
26	Other Pickup	Built In Bridge*	Default
27	Quality Reporting Tool	Privacy*	Default
28	Queue Status	Device Mobility Mode*	Default View Current Device Mobility Settings
29	Redial	Wireless LAN Profile Group	< None > View Details
30	Add a new SURF	Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)
31	Services	Owner User ID*	+19993332054
32	Add a new BLF SD	Mobility User ID	< None >
33	Privacy	Phone Personalization*	Default
34	None	Services Provisioning*	Default

Phone Load Name	
Use Trusted Relay Point*	Default
BLF Audible Alert Setting (Phone Idle)*	Default
BLF Audible Alert Setting (Phone Busy)*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Geolocation	< None >
<input type="checkbox"/> Ignore Presentation Indicators (Internal calls only)	
<input checked="" type="checkbox"/> Allow Control of Device from CTI	
<input checked="" type="checkbox"/> Logged Into Hunt Group	
<input type="checkbox"/> Remote Device	

<input type="checkbox"/> Protected Device***** <input type="checkbox"/> Hot line Device***** <input type="checkbox"/> Require off-premise location
--

Number Presentation Transformation Caller ID For Calls From This Phone Calling Party Transformation CSS < None > <input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)
Remote Number Calling Party Transformation CSS < None > <input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)

Protocol Specific Information Packet Capture Mode* None Packet Capture Duration 0 BLF Presence Group* Standard Presence group SIP Dial Rules < None > MTP Preferred Originating Codec* 711ulaw Device Security Profile* Secure Cisco 8865 Rerouting Calling Search Space < None > SUBSCRIBE Calling Search Space < None > SIP Profile* Standard SIP Profile -aish View Details Digest User < None > <input type="checkbox"/> Media Termination Point Required <input type="checkbox"/> Unattended Port <input type="checkbox"/> Require DTMF Reception
--

Certification Authority Proxy Function (CAPF) Information Certificate Operation* No Pending Operation Authentication Mode* By Null String Authentication String <input type="button" value="Generate String"/> Key Order* RSA Only RSA Key Size (Bits)* 2048 EC Key Size (Bits) Operation Completes By 2022 12 25 12 (YYYY-MM-DD:HH) Certificate Operation Status: None Note: Security Profile Contains Addition CAPF Settings.
Expansion Module Information Module 1 < None > Module 1 Load Name Module 2 < None > Module 2 Load Name Module 3 < None > Module 3 Load Name
External Data Locations Information (Leave blank to use default) Information Directory Messages Services

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.

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved.