

---

# Ribbon SBC Core SWe R10.1 Interop with NICE Engage 6.15 : Interoperability Guide

---



---

## Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
- Scope/Non-Goals
- Audience
- Prerequisites
- Product and Device Details
- Network Topology and E2E Flow Diagrams
  - Deployment Topology
  - Interoperability Test Lab Topology
  - Call Flow Diagram
- Document Workflow
- Installing Ribbon SBC SWe Core
  - Ribbon SBC Standalone
  - Ribbon SBC High Availability
- CLI Configurations for Ribbon SBC SWe Core
  - Global Configuration
  - SBC Configuration for Endpoints
  - SBC Configurations for SIPRec
  - TLS Certificates
  - TLS Profile
- PSX Configurations for Ribbon SBC SWe Core
  - Configuring Class of Service
  - Configuring Gateway
  - Configuring Globalization Profile
  - Configuring IP Signaling Profile
  - Configuring Codec Entry Profile
  - Configuring Packet Service Profile
    - Packet Service Profile IN
    - Packet Service Profile OUT
  - Configuring IP Signaling Peer Group
  - Configuring Carrier
  - Configuring Element Routing Priority Profile
  - Configuring Signaling Profile
  - Configuring Feature Control Profile
  - Configuring Trunk Groups
    - Trunk Group IN
    - Trunk Group OUT
  - Configuring Routes
    - Routing Label
    - Routes
  - Configuring SIPRec
    - NICE Trunk Group
    - SRS Cluster
    - SRS Group Profile
    - Call Recording Criteria
    - Call Forking to two Active recorders
    - Redundancy with Active-Standby SRSs
    - Quad Recording
  - Media Encryption
    - Towards Endpoint
    - Towards NICE SIP Recorder
- Ribbon SBC SWe Core High Availability
- NICE Configuration
  - Application Server
  - Metadata Support
  - VRSP NoFailback mode
  - Transport Configurations
  - Sequential Forking
  - Parallel Forking
  - NICE Business Analyzer
- 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 the Ribbon SBC SWe Core & PSX when deployed with NICE Recording Server.

### **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.

### **About Ribbon PSX :**

The Ribbon PSX provides centralized policy and call routing engine for both Ribbon distributed Call Processing Node (CPN) such as GSX/SBC and also third-party call processing nodes. When deployed in Service Provider network or Enterprises network, it interfaces with these call processing nodes while processing either TDM (SS7, PRA) or SIP calls.

### **About NICE SIP Recorder :**

The NICE Engage Platform provides comprehensive Omnichannel interaction recording to help organizations provide customers a coherent experience by providing a single place to define and implement compliance and quality practices across all channels.

## Scope/Non-Goals

---

This document provides configuration best practices for deploying Ribbon's SBC SWe Core for NICE SIP recording Interop. Note that these are configuration best practices and each customer may have unique needs and networks. Ribbon recommends that customers work with network design and deployment engineers to establish the network design which best meets their requirements.

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

To perform this interop, you need to:

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

**Note**

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

## Prerequisites

---

The following aspects are required before proceeding with the interop:

- Ribbon SBC SWe Core
- Ribbon SBC SWe Core 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.
- TLS certificates for SBC SWe Core
  - Please refer to [Managing Certificates](#)
- Ribbon PSX
- NICE Engage setup



NICE VRSP server functions as a SIP Proxy to set up SIP sessions between the SBC and the NICE.VRSP internally communicates to NICE AIR server which acts as a recording server. In active standby mode we have two VRSP servers with one as Active and one as Standby. Throughout this document from SBC perspective, we will be mentioning VRSP server as SRS[Session Recording Server].

## Product and Device Details

---

The configuration uses the following equipment and software:

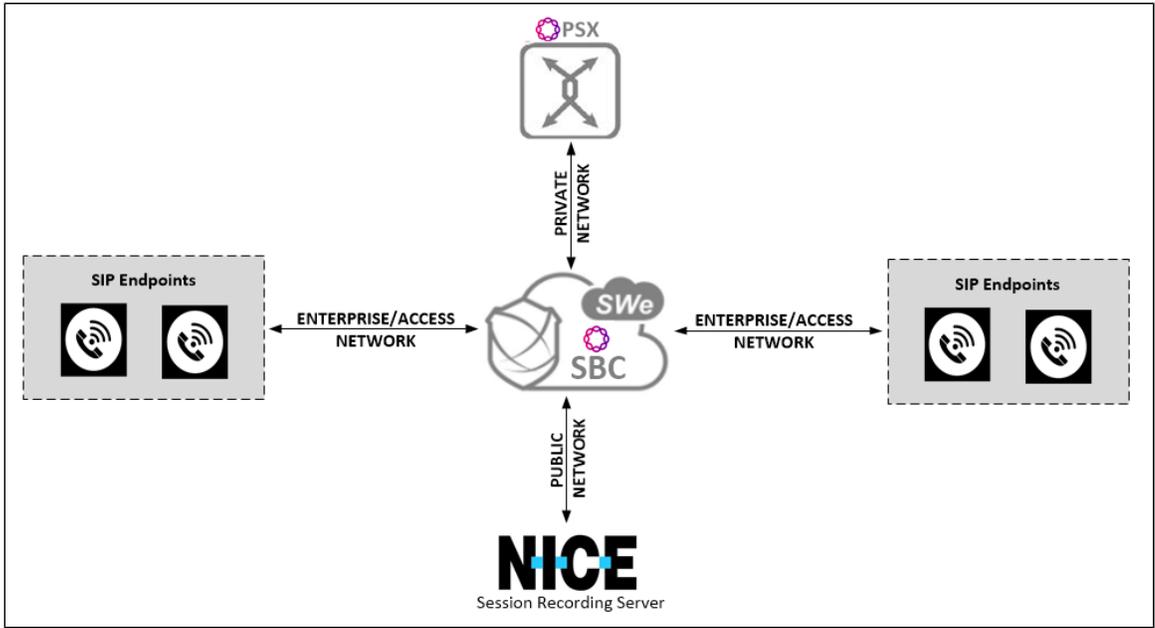
Product	Equipment/Service	Software Version
<b>Ribbon Communications</b>	SBC SWe Core	V10.01.00-R000
	PSX	V14.1
<b>Third-Party Equipment</b>	NICE Recording Server	V6.15
<b>Endpoints</b>	PhonerLite	V2.96
	Zoiper5	V5.5.8
<b>Administration and Debugging Tools</b>	Wireshark	V3.0.1

## Network Topology and E2E Flow Diagrams

---

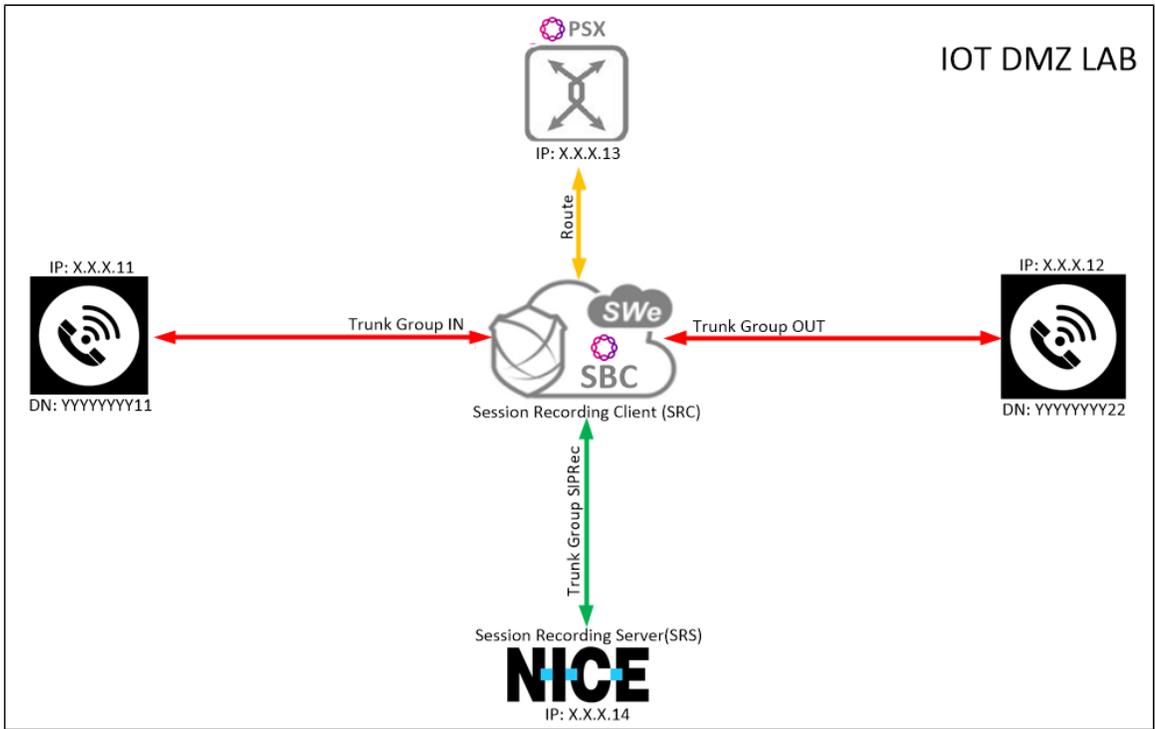
### Deployment Topology

Figure 1:



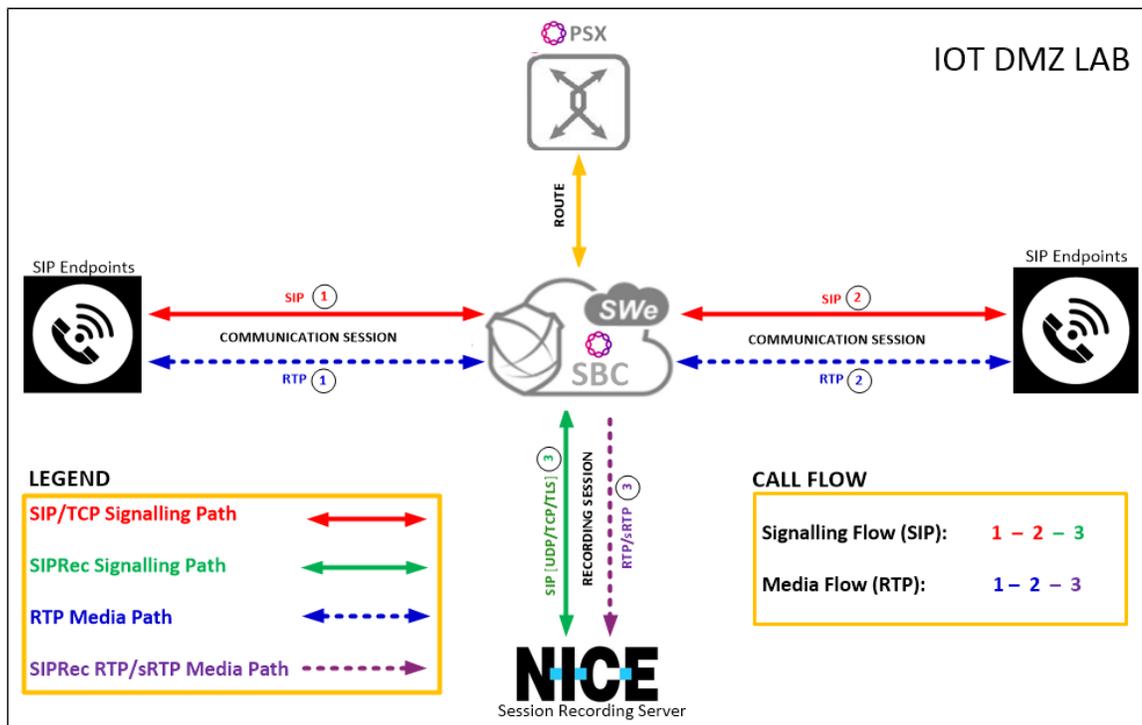
## Interoperability Test Lab Topology

Figure 2:



## Call Flow Diagram

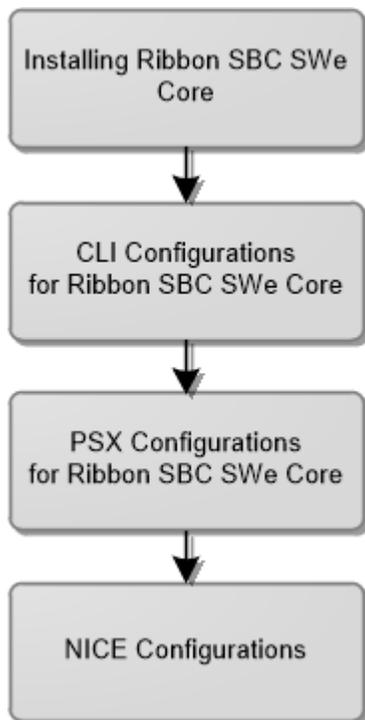
Figure 3:



## Document Workflow

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

Figure 4:



## Installing Ribbon SBC SWe Core

### Ribbon SBC Standalone

To deploy Ribbon SBC SWe Core StandAlone instance, refer to [SBC Core 10.1.x Documentation](#)

## Ribbon SBC High Availability

To deploy Ribbon SBC SWe Core in HA mode on different platforms, refer to [SBC Core Software Installation and Upgrade Guide](#)



During this interop, SBC SWe Core HA was installed on VMware platform by following the procedure described in [Installing SBC Application in High Availability Mode](#).



- After successful installation, ensure the time on both Active and Standby SBCs is in sync.
- NTP Sync verification:
  - Run the command 'timedatectl' to check if NTP is synchronized.
  - File /etc/ntp.conf should contain the IP of the NTP server that you have configured during installation

## CLI Configurations for Ribbon SBC SWe Core

### Global Configuration

#### 1. 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 IG1 ipInterface IP1 ceName SBCSIPREC
set addressContext default ipInterfaceGroup IG1 ipInterface IP1 portName pkt0
set addressContext default ipInterfaceGroup IG1 ipInterface IP1 ipAddress <The primary IP address of the interface>
set addressContext default ipInterfaceGroup IG1 ipInterface IP1 prefix <The IP subnet prefix of this Interface>
set addressContext default ipInterfaceGroup IG1 ipInterface IP1 mode inService
set addressContext default ipInterfaceGroup IG1 ipInterface IP1 state enabled
set addressContext default ipInterfaceGroup IG2 ipInterface IP2 ceName SBCSIPREC
set addressContext default ipInterfaceGroup IG2 ipInterface IP2 portName pkt1
set addressContext default ipInterfaceGroup IG2 ipInterface IP2 ipAddress <The primary IP address of the interface>
set addressContext default ipInterfaceGroup IG2 ipInterface IP2 prefix <The IP subnet prefix of this Interface>
set addressContext default ipInterfaceGroup IG2 ipInterface IP2 mode inService
set addressContext default ipInterfaceGroup IG2 ipInterface IP2 state enabled
commit
```

#### 2. 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 <destinationIpAddress> 0 <nextHopIpAddress> IG1 IP1 preference 100
set addressContext default staticRoute <destinationIpAddress> 0 <nextHopIpAddress> IG2 IP2 preference 100
commit
```

## SBC Configuration for Endpoints

#### 1. Create new Zone and configure sipSigPort

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.

```

set addressContext default zone zone1 id 111
set addressContext default zone zone1 sipSigPort 1 ipInterfaceGroupName IG1
set addressContext default zone zone1 sipSigPort 1 ipAddressV4 <IPv4 address>
set addressContext default zone zone1 sipSigPort 1 portNumber <1-65535>
set addressContext default zone zone1 sipSigPort 1 mode inService
set addressContext default zone zone1 sipSigPort 1 state enabled
set addressContext default zone zone1 sipSigPort 1 transportProtocolsAllowed sip-udp,sip-tcp,sip-tls-tcp
set addressContext default zone zone2 id 222
set addressContext default zone zone2 sipSigPort 2 ipInterfaceGroupName IG2
set addressContext default zone zone2 sipSigPort 2 ipAddressV4 <IPv4 address>
set addressContext default zone zone2 sipSigPort 2 portNumber <1-65535>
set addressContext default zone zone2 sipSigPort 2 mode inService
set addressContext default zone zone2 sipSigPort 2 state enabled
set addressContext default zone zone2 sipSigPort 2 transportProtocolsAllowed sip-udp,sip-tcp,sip-tls-tcp
commit

```

## 2. Create basic Trunk Group Configurations

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.



Please ensure to configure similar transport preferences in CLI and PSX Trunk Group configurations

```

set addressContext default zone zone1 sipTrunkGroup SIPREC_TG1 signaling transportPreference preferencel tcp
set addressContext default zone zone1 sipTrunkGroup SIPREC_TG1 media mediaIpInterfaceGroupName IG1
set addressContext default zone zone1 sipTrunkGroup SIPREC_TG1 ingressIpPrefix <IP address> <prefix>
set addressContext default zone zone1 sipTrunkGroup SIPREC_TG1 state enabled
set addressContext default zone zone1 sipTrunkGroup SIPREC_TG1 mode inService
set addressContext default zone zone2 sipTrunkGroup SIPREC_TG2 signaling transportPreference preferencel tcp
set addressContext default zone zone2 sipTrunkGroup SIPREC_TG2 media mediaIpInterfaceGroupName IG2
set addressContext default zone zone2 sipTrunkGroup SIPREC_TG2 ingressIpPrefix <IP address> <prefix>
set addressContext default zone zone2 sipTrunkGroup SIPREC_TG2 state enabled
set addressContext default zone zone2 sipTrunkGroup SIPREC_TG2 mode inService
commit

```

## SBC Configurations for SIPRec

We must make a separate TG with separate zone and sipSigport and attach that to egress IP interface group. This sip trunk is toward NICE recorder.

### 1. Create new Zone and Configure Sip Sigport for SIPRec Zone.

```

set addressContext default zone zone4 id 444
set addressContext default zone zone4 sipSigPort 4 ipInterfaceGroupName IG2
set addressContext default zone zone4 sipSigPort 4 ipAddressV4 <IPv4 address>
set addressContext default zone zone4 sipSigPort 4 portNumber <1-65535>
set addressContext default zone zone4 sipSigPort 4 transportProtocolsAllowed sip-udp,sip-tcp,sip-tls-tcp
set addressContext default zone zone4 sipSigPort 4 siprec enabled
set addressContext default zone zone4 sipSigPort 4 mode inService
set addressContext default zone zone4 sipSigPort 4 state enabled
commit

```

### 2. Configure Trunk group for SIPRec zone.



Please ensure to configure similar transport preferences in CLI and PSX Trunk Group configurations

Also, Transport preference mentioned in SRS Group profile should match transport preferences in Trunk Group towards SIPRec zone.

```

set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 media mediaIpInterfaceGroupName IG2
set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 ingressIpPrefix <IP address> <prefix>
set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 signaling transportPreference preferencel tls-tcp
set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 state enabled
set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 mode inService
commit

```

3. The Path Check Profile specifies the conditions that constitute a connectivity failure, and in the event of such a failure, the conditions that constitute a connectivity recovery. This profile specifies the configuration for OPTIONS PING.

```

set profiles services pathCheckProfile sip_recording1 protocol sipOptions
set profiles services pathCheckProfile sip_recording1 sendInterval 10
set profiles services pathCheckProfile sip_recording1 replyTimeoutCount 3
set profiles services pathCheckProfile sip_recording1 recoveryCount 1
set profiles services pathCheckProfile sip_recording1 failureResponseCodes [ all5xx ]
set profiles services pathCheckProfile sip_recording1 transportPreference preferencel tls-tcp

```

4. Configure the SRS IP as an ipPeer in the SIPREC zone (the zone containing the Trunk Group configured for the SRS) and attach the pathcheck profile to it.

```

set addressContext default zone zone4 ipPeer SIPREC_VRSP1 ipAddress <The IPv4 or IPv6 address of the Peer>
set addressContext default zone zone4 ipPeer SIPREC_VRSP1 ipPort <0-65535>
set addressContext default zone zone4 ipPeer SIPREC_VRSP1 pathCheck profile sip_recording1
set addressContext default zone zone4 ipPeer SIPREC_VRSP1 pathCheck state enabled
set addressContext default zone zone4 ipPeer SIPREC_VRSP2 ipAddress <The IPv4 or IPv6 address of the Peer>
set addressContext default zone zone4 ipPeer SIPREC_VRSP2 ipPort <0-65535>
set addressContext default zone zone4 ipPeer SIPREC_VRSP2 pathCheck profile sip_recording1
set addressContext default zone zone4 ipPeer SIPREC_VRSP2 pathCheck state enabled
commit

```

5. NICE does not support SIP INFO method towards SIPRec . So, disable SIP INFO method towards SIPRec Trunk Group.

```

set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 signaling methods info reject
commit

```

5. Create sipRecMetadataProfile with version 1 as per RFC 7865 and associate the profile to SIPRec Trunk Group.



When sipRecMetadataProfile is not configured, by default SBC supports backward compatibility and pre-defined metadata for passing proprietary call specific information from the SRC to the SRS.

Refer to [MetadataSupport](#) for additional NICE configurations.

```

set profiles services sipRecMetadataProfile t1 state enabled
set profiles services sipRecMetadataProfile t1 version 1
comm
set addressContext default zone zone4 sipTrunkGroup SIPREC_TG4 services sipRecMetadataProfile t1
comm

```

## TLS Certificates

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 and execute the following commands.

```

#### SRS1 Application Server Certificate Import ####
set system security pki certificate NICE_REMOTE1 state enabled
set system security pki certificate NICE_REMOTE1 fileName <SRS1 Certificate filename imported in SBC>
set system security pki certificate NICE_REMOTE1 type remote
comm

#### SRS2 Interaction Server Certificate Import ####
set system security pki certificate NICE_REMOTE2 state enabled
set system security pki certificate NICE_REMOTE2 fileName <SRS2 Certificate filename imported in SBC>
set system security pki certificate NICE_REMOTE2 type remote
comm

#### SBC Certificate Import ####
set system security pki certificate SBC_LOCAL state enabled
set system security pki certificate SBC_LOCAL fileName <SBC local Certificate filename imported in SBC>
set system security pki certificate SBC_LOCAL passphrase xxxx
set system security pki certificate SBC_LOCAL type local
comm

```

## TLS Profile

This object 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.

```

#### TLS Profile for SIP Endpoint ####
set profiles security tlsProfile TLS_SIPREC1 appAuthTimer 5
set profiles security tlsProfile TLS_SIPREC1 handshakeTimer 5
set profiles security tlsProfile TLS_SIPREC1 sessionResumpTimer 3600
set profiles security tlsProfile TLS_SIPREC1 cipherSuite1 rsa-with-aes-128-cbc-sha
set profiles security tlsProfile TLS_SIPREC1 cipherSuite2 rsa-with-aes-256-cbc-sha
set profiles security tlsProfile TLS_SIPREC1 cipherSuite3 tls_rsa_with_aes_256_gcm_sha384
set profiles security tlsProfile TLS_SIPREC1 allowedRoles clientandserver
set profiles security tlsProfile TLS_SIPREC1 authClient true
set profiles security tlsProfile TLS_SIPREC1 clientCertName SBC_LOCAL
set profiles security tlsProfile TLS_SIPREC1 serverCertName SBC_LOCAL
set profiles security tlsProfile TLS_SIPREC1 acceptableCertValidationErrors none
set profiles security tlsProfile TLS_SIPREC1 v1_0 enabled
set profiles security tlsProfile TLS_SIPREC1 v1_1 enabled
set profiles security tlsProfile TLS_SIPREC1 v1_2 enabled
set profiles security tlsProfile TLS_SIPREC1 suppressEmptyFragments disabled
set profiles security tlsProfile TLS_SIPREC1 peerNameVerify disabled
commit

#### TLS Profile for NICE SIP Recording Trunk ####
set profiles security tlsProfile testsiprectlsroot appAuthTimer 5
set profiles security tlsProfile testsiprectlsroot handshakeTimer 5
set profiles security tlsProfile testsiprectlsroot sessionResumpTimer 3600
set profiles security tlsProfile testsiprectlsroot cipherSuite1 rsa-with-aes-128-cbc-sha
set profiles security tlsProfile testsiprectlsroot cipherSuite2 rsa-with-aes-256-cbc-sha
set profiles security tlsProfile testsiprectlsroot cipherSuite3 tls_rsa_with_aes_256_gcm_sha384
set profiles security tlsProfile testsiprectlsroot allowedRoles clientandserver
set profiles security tlsProfile testsiprectlsroot authClient true
set profiles security tlsProfile testsiprectlsroot clientCertName SBC_LOCAL
set profiles security tlsProfile testsiprectlsroot serverCertName SBC_LOCAL
set profiles security tlsProfile testsiprectlsroot acceptableCertValidationErrors none
set profiles security tlsProfile testsiprectlsroot v1_0 enabled
set profiles security tlsProfile testsiprectlsroot v1_1 enabled
set profiles security tlsProfile testsiprectlsroot v1_2 enabled
set profiles security tlsProfile testsiprectlsroot suppressEmptyFragments disabled
set profiles security tlsProfile testsiprectlsroot peerNameVerify disabled
commit

```

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

```
##### Attach TLS profile to SIPrec zone #####
set addressContext default zone zone4 sipSigPort 4 tlsProfileName testsiprectlsroot
comm

##### Attach TLS profile to SIPrec zone (If TLS transport is enabled)#####
set addressContext default zone zone1 sipSigPort 1 tlsProfileName TLS_SIPREC1
set addressContext default zone zone2 sipSigPort 2 tlsProfileName TLS_SIPREC1
comm
```

## SBC Configuration to enable PSX

We need to disable local PolicyServer and configure remote PSX details in SBC SWe Core.

```
set system policyServer localServer PSX_LOCAL_SERVER state disabled
set system policyServer localServer PSX_LOCAL_SERVER mode outOfService
set system policyServer remoteServer IOTPSX ipAddress 172.16.100.216
set system policyServer remoteServer IOTPSX state enabled
set system policyServer remoteServer IOTPSX mode active
set system policyServer remoteServer IOTPSX action force
commit
```

## PSX Configurations forRibbonSBC SWe Core

### Configuring Class of Service

Please note that we have used default Class Of Service 'DEFAULT\_IP' for our testing.

Figure 5:

Class Of Service:

Description:

<p>Service Flags</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Authcode</li> <li><input type="checkbox"/> Blocking</li> <li><input type="checkbox"/> Business Group Blocking</li> <li><input type="checkbox"/> Business Group Origination Blocking</li> <li><input type="checkbox"/> Calling Forced Routing</li> <li><input type="checkbox"/> Destination Forced Routing</li> <li><input type="checkbox"/> DTMF</li> <li><input type="checkbox"/> Hifraud Countries</li> <li><input type="checkbox"/> Infodigit Screening</li> <li><input type="checkbox"/> Ingress CPC Screening</li> <li><input type="checkbox"/> Message Waiting Indicator</li> <li><input type="checkbox"/> Message Waiting Indicator Update</li> <li><input type="checkbox"/> SAC/Non-SAC Routing</li> <li><input type="checkbox"/> Services Standard Routing</li> <li><input type="checkbox"/> Short Key Translation</li> </ul>	<p>Non-Subscriber Call Routing</p> <ul style="list-style-type: none"> <li>0+</li> <li>0+ IDDD</li> <li>0-</li> <li>00</li> <li>1+</li> <li>Carrier Cut Through</li> <li>IDDD</li> <li>Private</li> <li>Switch ID Trunk Group ID</li> <li>User Name</li> </ul>	<p>Casual Calling Routing</p> <ul style="list-style-type: none"> <li>0+</li> <li>0+ IDDD</li> <li>0-</li> <li>00</li> <li>1+</li> <li>Carrier Cut Through</li> <li>IDDD</li> </ul>
---	---	--

Figure6:

Services

Authcode Script: <None> [Runtime Variables](#)

International Number Blocking: <None> [Runtime Variables](#)

Screening: <None> [Runtime Variables](#)

DTMF Profile: <None>

Short Key Profile: <None>

Message Waiting Indicator

Script: <None>

Service Number:

Blocking Profile	Script	Sequence	Time Range

Service Exception Profile: <None>

New Open Delete [Runtime Variables](#)

## Configuring Gateway

1. Configure a gateway with the SBC name and the management IP address.

Figure 7:

PSX Manager V14.01.00R000  
User: - North America

Menu

<Configure>

<Admin>

Gateway

**Gateway**

SQL Search Criteria (8 entries)

Gateway: \*

Search More...

Gateway

DEFAULT

IOTCHANDANCE

NATSWE

SBCPOOJA

**SBCSYAM1**

STISBC

TESTGW

ZOOM

2. From the Gateway configuration UI, enter the name of gateway that is configured in the SBC.

**i** Gateway name should be same as systemname in SBC conf file and should be capitalized.

Figure8:

GATEWAY: SBCSYAM1 LRNS

Switch: SOFTSWITCH

Gateway Group: DEFAULT

Cluster Profile: <None>

Default Trunk Group: SIP

Charge Band Profile: <None>

Traffic Control Escape Profile: <None>

Mobile Switch ID: 1  None

Signaling Gateway Group: <None>

Enum Authority Profile: <None>

Address Reachability Service Profile: <None>

SMM Profile Group: <None>

Peer Throttling Profile: <None>

P-Origination-ID:   Autogenerate

Context Info

Flags

CAMEL Services Supported  Route CAMEL Subscription Calls

CDP Gateway  Traffic Management

MTRR Supported  Logical SBC

Display

Allow Mixed Characters in Gateway Name

H.323 Control

Prune Routes

Configure SBC management IP in IPv4 Address and default port number 2569.

Figure 9:

IPv4 Address: 8 . 8 . 8 . 8 Port Number: 2569

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Prefer IPv4  Prefer IPv6

H.323 IP4 Address: 0 . 0 . 0 . 0 H.323 Port Number: 1720

H323 IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Set As Default H.323 Gateway For This IP Address

Prefer IPv4  Prefer IPv6

SIP IP4 Address: 0 . 0 . 0 . 0 SIP Port Number: 5060

SIP IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Set As Default SIP Gateway For This IP Address

Prefer IPv4  Prefer IPv6

Server FQDN  FQDN Port Number: 0

Prefer IPv4  Prefer IPv6

Perform DNS query for SIP Server Selection

Local Routes Filtering/Prioritization

Apply At Ingress Gateway  Apply At Ingress Cluster

Services

Not Screened  Screened - Normal  Screened - Fraud

Class Of Service: DEFAULT\_IP

Service Exception Profile: <None>

## Configuring Globalization Profile

This object is used to define numbers that are to be globalized for egress SIP message headers. Specify a profile entry for each number type that needs to be globalized. The profile includes a digit type, a source for the country code, and a flag to enable the globalization. Assign Globalize Profiles to egress trunk groups by selecting them on the IP Signaling Profile for each trunk group.

Figure10:

Globalize Profile: SIPREC\_Profile

Description: Doing globalization plus populating country code

Globalize Profile Data

Number Type: Calling Number

Use Digit Type For URI

Digit Type

- <All>
- 900 Premium Toll
- 950 Carrier Access
- Carrier Access
- Directory Assistance
- Easily Identifiable Number
- Emergency
- Government Emergency

Country Code Source: Origination

Country Code Fallback: <None>

Globalize Flag

Add/Modify

Number Type	Country Code	Globalize Flag	Country Code Fallback
Calling Number	Origination	Enabled	<None>
Called Number	Origination	Enabled	<None>
LNP Routing Number	Destination	Enabled	<None>
Redirection	Destination	Enabled	<None>
Original Called Number	Origination	Enabled	<None>
Location	Origination	Enabled	<None>
Redirecting	Origination	Enabled	<None>
Billing Number	Origination	Enabled	<None>
GN: Dialed Digits	Destination	Enabled	<None>
GN: Destination	Destination	Enabled	<None>

Delete

Figure11:

Number Type	Country Code	Globalize Flag	Country Code Fallback
GN: User Calling, Not Screened	Origination	Enabled	<None>
GN: Redirecting Terminating	Destination	Enabled	<None>
GN: Ported Dialed	Destination	Enabled	<None>
GN: Called CES Id	Destination	Enabled	<None>
GN: Additional Called	Destination	Enabled	<None>
GN: Additional Connected	Destination	Enabled	<None>
GN: Additional Calling	Origination	Enabled	<None>
GN: Additional Original Called	Destination	Enabled	<None>
GN: Additional Redirecting	Origination	Enabled	<None>
GN: Additional Redirection	Destination	Enabled	<None>
Contractor Number	Origination	Enabled	<None>

Figure12:

Number Type	Country Code	Globalize Flag	Country Code Fallback
GN: Additional Calling	Origination	Enabled	<None>
GN: Additional Original Called	Destination	Enabled	<None>
GN: Additional Redirecting	Origination	Enabled	<None>
GN: Additional Redirection	Destination	Enabled	<None>
Contractor Number	Origination	Enabled	<None>
GN: Network Provided Number	Destination	Enabled	<None>
Dialed Number	Origination	Enabled	<None>
GN: Third Party Number	Destination	Enabled	<None>
GN: Collect Call Number	Destination	Enabled	<None>
GN: Local ANI	Origination	Enabled	<None>
To URI User	Origination	Enabled	<None>

## Configuring IP Signaling Profile

This object specifies parameters associated with H.323, SIP, SIP-I communication that are sent as part of the outgoing signaling message after standard protocol rules have been applied.

You can associate IP signaling profiles with IP trunk groups and virtual trunk groups.

Figure13:

IP SIGNALING PROFILE: SIPREC\_IPSP\_TCP

Common IP Attributes - Communicating With The Peer Regardless Of Call Direction

<input type="checkbox"/> Accept Alert Info	<input type="checkbox"/> No Content Disposition
<input type="checkbox"/> Add P-Charging Function Addr	<input type="checkbox"/> No Port Number 5060
<input type="checkbox"/> Add Path/Service Route Per TG	<input type="checkbox"/> No Userinfo In Contact Header
<input type="checkbox"/> Audio Codec Change through Empty TCS	<input type="checkbox"/> Only Selected Codec In Session Refresh
<input type="checkbox"/> Call Hold Interworking	<input type="checkbox"/> Override Relay For Non SIP Egress Leg
<input type="checkbox"/> Calling Party Type Number If Present	<input type="checkbox"/> P-Called-Party-Id-Support
<input type="checkbox"/> Clearmode For Data Calls	<input type="checkbox"/> P-ChgMsg-Info
<input type="checkbox"/> Create P-Charging-Vector	<input type="checkbox"/> Relay Data Path Mode Changes To The Other Leg
<input type="checkbox"/> Create P-Visited-Network Id	<input type="checkbox"/> Reject REFER
<input type="checkbox"/> Create Path Header	<input type="checkbox"/> Replace Host On Via Header
<input type="checkbox"/> Create Service-Route Header	<input type="checkbox"/> Reject REFER With IP
<input type="checkbox"/> Customized Session Timer Behavior	<input type="checkbox"/> Reject REFER With TN
<input type="checkbox"/> Disable Also Header	<input type="checkbox"/> ReQuery PSX on REGISTER Refresh
<input type="checkbox"/> Disable Constrained Capacities	<input type="checkbox"/> Restrict History Info Header
<input type="checkbox"/> Disable Host Translation	<input type="checkbox"/> Route Using Received FQDN
<input type="checkbox"/> Disable Media Lock Down	<input type="checkbox"/> SDP O-line Only Compares
<input type="checkbox"/> Disable Refer-To URI Parameters	<input type="checkbox"/> Send All Allowed Codecs For Late Media Invite Or Re-Invite
<input type="checkbox"/> Discard Received Reason Header	<input type="checkbox"/> Send Direct Media Info In SDP Attribute
<input type="checkbox"/> Do Not Include SS Attribute In Re-INVITE	<input type="checkbox"/> Send Empty TCS

Figure14:

<input type="checkbox"/> Don't Send REFER With IP	<input type="checkbox"/> Send Only Preferred Codec
<input type="checkbox"/> Don't Send REFER With TN	<input type="checkbox"/> Send PTIME In SDP
<input type="checkbox"/> End To End BYE	<input type="checkbox"/> Send RTCP Port In SDP
<input type="checkbox"/> End To End RE-INVITE	<input type="checkbox"/> Session Timer Refresh Update
<input type="checkbox"/> End To End UPDATE	<input type="checkbox"/> Set Accept Header To Application SDP Only
<input type="checkbox"/> Suppress End To End Session Refresh	<input type="checkbox"/> Set Oline Dash
<input type="checkbox"/> End To End PRACK	<input type="checkbox"/> Set Session Version Zero
<input type="checkbox"/> Enable Default PUI Procedures	<input type="checkbox"/> Set Sline Dash
<input type="checkbox"/> Enable Dial String Handling	<input type="checkbox"/> Store P-Charging Function Addr
<input type="checkbox"/> Include G729 with G729A when offer PSP has G729A	<input checked="" type="checkbox"/> Store P-Charging Vector
<input type="checkbox"/> Include IP Ports In FROM And TO Headers	<input type="checkbox"/> Store Path Header
<input type="checkbox"/> Include Reason Header (Q.850)	<input type="checkbox"/> Store Service-Route Header
<input type="checkbox"/> Include SS Attribute In Initial Invite	<input type="checkbox"/> Suppress Min-SE if not received
<input checked="" type="checkbox"/> Include Transport Type In Contact Header	<input type="checkbox"/> Terminal Portability Interworking
<input type="checkbox"/> Insert Peer Address As Top Route Header	<input type="checkbox"/> Send RTCP BandWidth Info
<input type="checkbox"/> Lockdown Preferred Codec	<input type="checkbox"/> Validate Access Nw Info Header
<input type="checkbox"/> Map Cause Location	<input type="checkbox"/> Use Psx Route for Registered Invite
<input type="checkbox"/> Map SGD In P-Sig-Info Header	<input type="checkbox"/> From Header Anonymisation
<input type="checkbox"/> Map Suspend/Resume Event In P-Svc-Info Header	<input type="checkbox"/> Create ISUP Message Body

Figure15:

<input type="checkbox"/> Map UUI In P-Sig-Info Header	<input type="checkbox"/> Disable Transparently Passing ISUP Message Body
<input type="checkbox"/> MIME Cause Precede Reason Header Cause	<input type="checkbox"/> aiToPemInterworking
<input type="checkbox"/> Minimize Relaying Of Media Changes From Other Call Leg	<input type="checkbox"/> Send SBC Supported Codecs For Late Media Re-Invite
<input type="checkbox"/> No Service Route Hdr For Emergency Registration	<input type="checkbox"/> Select Core Stream For Multi Stream Audio Or Image Call
<input type="checkbox"/> Publish IP In Hold SDP	<input type="checkbox"/> Disable Non Core Audio And Image Streams
<input type="checkbox"/> Insert PAccess Network Info	<input type="checkbox"/> Map DPM to Send and Receive for Initial Dialog
<input type="checkbox"/> Contact Transparency For Isfocus Media Tag	<input type="checkbox"/> Suppress Refer Relay From Other Leg
<input type="checkbox"/> Support S-CSCF Restoration Procedures	<input type="checkbox"/> Support Call Info With SIP Cause 608 RFC 8688
<input type="checkbox"/> Insert UE Flow Info	
<input type="checkbox"/> Include SIP Reason Header	
<b>Call Preservation Flags</b>	
<input type="checkbox"/> Call Preservation	
Call Preservation Time Out: <input type="text" value="5"/>	
<b>Call Transfer Flags</b>	
Handle IP Addresses Not Present In Network Selector Table (NST): <input type="text" value="Route Via Transferring IPTG"/>	
<input type="checkbox"/> Force Re-Route Via PSX Query	
<input type="checkbox"/> Skip Re-Route Via PSX Query	
<b>Local Media Control Flags</b>	
<input type="checkbox"/> Enable HOLD on REFER	

**Figure16:**

<b>Option Tag In Require Header</b>	
<input type="checkbox"/> Suppress Replace Tag	
<b>Option Tag In Supported Header</b>	
<input type="checkbox"/> Suppress Replace Tag	
<b>PreConditions Profile</b>	
<input type="checkbox"/> State	
<input type="checkbox"/> Support If Egress IPTG	<input type="checkbox"/> Strength Optional Policy
<input type="checkbox"/> Strength Mandatory Policy	<input type="checkbox"/> UPDATE Preconditions Policy
Strength Mandatory Priority:	<input type="text" value="1"/>
Strength Optional Priority:	<input type="text" value="1"/>
UPDATE Preconditions Priority:	<input type="text" value="1"/>
<b>Relay Flags</b>	
<input type="checkbox"/> Conference Event Package	<input type="checkbox"/> PUBLISH
<input type="checkbox"/> Dialog Event Package	<input type="checkbox"/> REFER
<input type="checkbox"/> DTMF Body	<input type="checkbox"/> Reg Event Package
<input type="checkbox"/> Force 503 To 500 Relay	<input type="checkbox"/> Ribbon Media Body
<input type="checkbox"/> Info	<input type="checkbox"/> Status Code 3XX
<input type="checkbox"/> Message	<input type="checkbox"/> Status Code 4XX-6XX
<input type="checkbox"/> Notify	<input type="checkbox"/> Third Party Bodies
<input type="checkbox"/> Options	<input type="checkbox"/> Update without SDP

**Figure17:**

Reason Phrase 4XX 6XX

Refer To Header Relay

Reject the REFER request if no match is found     relay the REFER request if no match is found     relay the REFER request without matching

Transparency Flags

<input type="checkbox"/> Accept-Contact Header	<input type="checkbox"/> Reason Header
<input type="checkbox"/> Accept-Language Header	<input type="checkbox"/> Referred-By Header
<input type="checkbox"/> Accept Header	<input type="checkbox"/> Resource Priority Option Tag
<input type="checkbox"/> Alert Information Header	<input type="checkbox"/> Request-URI
<input type="checkbox"/> Allow Header	<input type="checkbox"/> Resource-Lists Body
<input type="checkbox"/> Authcode Headers	<input type="checkbox"/> RLMI Body
<input type="checkbox"/> Call-Info Header	<input type="checkbox"/> Route Header
<input type="checkbox"/> Contact Header*	<input type="checkbox"/> Server Header
<input type="checkbox"/> Error Info	<input type="checkbox"/> Service-Route Header
<input type="checkbox"/> Event Header	<input type="checkbox"/> Simple-Filter Body
<input type="checkbox"/> External Body	<input type="checkbox"/> SIP Body
<input type="checkbox"/> From Header	<input type="checkbox"/> SIPFRAG Body
<input type="checkbox"/> Geo Location Error	<input type="checkbox"/> Target-Dialog Header
<input type="checkbox"/> Geo Location Header	<input type="checkbox"/> To Header
<input type="checkbox"/> Geo Location Route	<input type="checkbox"/> Tone Body
<input type="checkbox"/> History Info	<input type="checkbox"/> Unknown Body

**Figure18:**

<input type="checkbox"/> Image Body	<input type="checkbox"/> Unknown Header
<input type="checkbox"/> Max_forwards Header	<input type="checkbox"/> User-Agent Header
<input type="checkbox"/> MWI Body	<input type="checkbox"/> User-To-User Header
<input type="checkbox"/> Pass Complete Contact Header	<input type="checkbox"/> Via Header
<input type="checkbox"/> P-Access-Network-Info Header	<input type="checkbox"/> Warning Header
<input type="checkbox"/> P-Called-Party-Id	<input type="checkbox"/> Watcherinfo Body
<input type="checkbox"/> P-Charging-Vector Header	<input type="checkbox"/> X-ATP
<input type="checkbox"/> P-Early-Media	
<input type="checkbox"/> P-Visited-Network-ID Header	
<input type="checkbox"/> Path Header	
<input type="checkbox"/> Pidf Body	
<input type="checkbox"/> Pidf-Diff Body	
<input type="checkbox"/> QSIG Body	

Transparency Profile

SBC Transparency Profile:

Flags

Apply Setting to SBC TG     Apply Setting to "Use SIP In Core" Egress TG if Applicable

PDCS-Billing Info Header

Transparency

From the drop down, select Globalization Profile created above.

**Figure19:**

Include Privacy

Sip In Core  Use SIP In Core

Header Encryption Flags  Path Header  Service Route Header

Subscription Package Support  Support Reg Event  Use PSX Route For SBC Initiated Subscribe

Registrar Recovery  Register to Alternate on Primary Down  Override Internal Expires Timer  
 Revert to Primary On Recovery  Deregister Alternate on Primary Recovery

Egress IP Attributes - Sending A Call In The Forward Direction To The Peer

IP Protocol Type:  SIP Only  SIP-I  H.323  Wireless

IP Signaling MIME Content Type: ISUP

IP Signaling Treatment: Interwork

MIME Content Type Version: 0

Globalize Number Profile: SIPREC\_Profile

Localize Profile: <None>

Phone-Context Parameter Length: 0

Media Qos Kpi Profile: <None>

Signaling Qos Kpi Profile: <None>

Figure20:

Flags

<input type="checkbox"/> Accept 3XX With RN	<input type="checkbox"/> Qos Based Routing
<input type="checkbox"/> BGCF Target Scheme Transparency	<input type="checkbox"/> Prefix RN to Dialed Digits
<input type="checkbox"/> Convert Inactive To Sendrcv	<input type="checkbox"/> Reject 3XX With IP
<input type="checkbox"/> Delay Cut Through	<input type="checkbox"/> Reject 3XX With TN
<input type="checkbox"/> Disable 2806 Compliance	<input type="checkbox"/> Same CallId For Required Authorization
<input type="checkbox"/> Disable Optional Register Parameters	<input type="checkbox"/> Transit PAI From Unregistered Peer
<input checked="" type="checkbox"/> Disposition Handling Required	<input type="checkbox"/> Suppress UNREGISTER
<input type="checkbox"/> Don't Send Fast Start Proposal	<input type="checkbox"/> TTC-ISUP Mapping
<input type="checkbox"/> Enable 3261 Cancel Handling	<input type="checkbox"/> Use Called Party In Request URI
<input type="checkbox"/> Include ENUM Parameters	<input type="checkbox"/> Use Colon In SDP Media Type Parameter
<input type="checkbox"/> Insert In Band Indication	<input type="checkbox"/> Use JIP from 3XX Response in PDCS-Billing-Info-Header
<input type="checkbox"/> Add Loop Back Route Header	<input type="checkbox"/> Validate ISUB Address
<input type="checkbox"/> Map 181 Or 182 Message To 183	<input type="checkbox"/> Wait Till Connect Before Abandon FastStart
<input type="checkbox"/> Map 3xx Contact URL To Route Header	<input type="checkbox"/> Restrict User Equal To Phone
<input type="checkbox"/> Map Contractor Number In P-Sig-Info Header	<input type="checkbox"/> Ignore SDP After Offer Answer Completed
<input type="checkbox"/> Use Network Provided Screening Indicator For Calling Number	<input type="checkbox"/> Map Diversion Header To Charge Number
<input type="checkbox"/> MonitorRtpOnEgressUpdate	<input type="checkbox"/> Map RN, OCN, RDI To Diversion Header
<input type="checkbox"/> Honor Subsequent SDP Answer	<input type="checkbox"/> Enable Globalization of Numbers starting with Alphabet

Figure21:

<input type="checkbox"/> Ignore Unmodified Called Userpart If Truncated	<input type="checkbox"/> Ignore Unmodified Calling Userpart If Truncated
BCI	
<input type="checkbox"/> BCI Interwork Encountered	<input type="checkbox"/> BCI ISDN Access
Carrier Information	
<input type="checkbox"/> Disconnect If Neither Terminating CA Nor CIC Received	<input type="checkbox"/> Use Terminating CIC From SIP
<input type="checkbox"/> Use Terminating CA From SIP	
Domain Name	
<input type="checkbox"/> Preserve Ingress FROM Domain Name	<input type="checkbox"/> Use Lower Case Domain Names
<input type="checkbox"/> Preserve Ingress R-URI Domain Name	<input type="checkbox"/> Use SIP Domain Name In FROM Field
<input checked="" type="checkbox"/> Use IP Signaling Peer Domain In R-URI	<input type="checkbox"/> Use Zone Level Domain Name In Contact
<input type="checkbox"/> Use DMPPM Manipulated Host Name In R-URI	<input type="checkbox"/> Use SIP Domain Name In Request URI
<input type="checkbox"/> Use Zone Level Domain Name in Path Header	<input type="checkbox"/> Use Called URI As R-URI
<input type="checkbox"/> Use SIP Domain Name In PAI Header	<input type="checkbox"/> Use PSX Modified To URI Host Part
<input type="checkbox"/> Do not use PSX Unmodified From URI Host Part	<input type="checkbox"/> Do not use PSX Unmodified PAI URI Host Part
ISUB	
<input type="checkbox"/> Allow NSAP ISUB	<input type="checkbox"/> Include Called Party ISUB
<input type="checkbox"/> Allow User Specified ISUB	<input type="checkbox"/> Include Calling Party ISUB
Number Portability Attributes	
NPD1 Options: <input checked="" type="radio"/> Include npdi <input type="radio"/> Include npdi=yes <input type="radio"/> Do Not Include npdi	

Figure22:

Flags
<input type="checkbox"/> Disable m
Privacy
<input type="checkbox"/> Transparency
<input type="checkbox"/> AnonymizeHostIpAddress
Privacy Information: <input checked="" type="radio"/> P-Preferred-ID <input type="radio"/> P-Asserted-ID <input type="radio"/> Remote-Party-ID
Flags
<input checked="" type="checkbox"/> Include Privacy <input type="checkbox"/> Privacy Required by Proxy
<input type="checkbox"/> MS Lync Privacy Support <input type="checkbox"/> Include Embedded PAI Header in Redirected INVITE
<input type="checkbox"/> Do Not Include Tel URI In PAI Header
Redirect
Mode: <input type="text" value="Accept Redirection"/>
Contact Handling: <input checked="" type="radio"/> Merge Received Contacts with Existing Contacts <input type="radio"/> Purge Existing Contacts
Flags
<input type="checkbox"/> Skip Crankback Profile And Always Crankback <input type="checkbox"/> Honor Embedded Headers in 3xx
<input type="checkbox"/> Force Re-query for Redirection <input type="checkbox"/> Enhanced Local Redirection
<input type="checkbox"/> Skip DTG Lookup For 3XX Contact
SIP Cause Mapping
Internal To SIP Cause Mapping: <input type="text" value="1 - DEFAULT"/>
SIP To Internal Cause Mapping: <input type="text" value="1 - DEFAULT"/>

Figure23:

Internal to SIP Cause Mapping Profile Name

SIP to Internal Cause Mapping Profile Name

**SIP Headers And Parameters**

Include Charge Information:  Include None  Include P-Charge-Info

Session-Expires Refresher:  Not Send  UAC  UAS

None  Original Called Number (OCN)

SIP TO Header Mapping:  Called Number  GAP Dialed Number

Fallback to called number if OCN is not present  Fallback to called number if GAP Dialed number is not present

PI Allowed Send CPC In:  DEFAULT  FROM  PAI  BOTH

Destination Trunk Group Options:

Originating Trunk Group Options:

Generate Call-ID Using:

**Flags**

Include CIC  Include PSTN Parameters

Include CPC Information  Include Qvalue

Include NPI  Skip CSeq Check In Early Dialog

Include OLIP  Transparency For Destination Trunk Group Parameter

Include P-K-Adn  End To End Ack

No CDR Change In End To End Ack

**Figure24:**

**Call Forwarding**

Diversion-History Info Interworking (RFC 6044 compliance)

**Redirection Information**

Diversion  Diversion With Transparency

PK Header

**History Information**

Include History-Info  Cause Parameter In RFC 4458  Reason With Cause Value As Per RFC 4244

**CPC Mapping Flags**

Map CPC when Presentation Indicator is Restricted

Any CPC  CPC=Priority

**Send CPC Param In**

Default  PAI  From  Both (PAI and From)

**P Charge Info**

Transparency

P-Charge-Info Information:  URI Parameter  User Parameter  Header Parameter

**Flags**

Include NPI  Include NOA

**SIP Jurisdiction Support**

Jurisdiction Support:  Enable  Disable

SBC JIP Profile:

Use Transport Type object to configure the preferred transport.

**Figure 25:**

Flags

Apply Settings to SBC TG  Apply Settings to "Use SIP In Core" Egress TG if Applicable

---

SIP RPH ETS

Action For ETS 400 Response With 417 Reason Code:

ETS Default Priority Value:

Flags

Add/Modify ETS Resource Priority Header  Use Incoming ETS Resource Value

Do Not Include Require RPH

---

SIP Variant Type

SIP Variant Type:

Flags

Apply Setting to SBC TG  Apply Setting to "Use SIP In Core" Egress TG if Applicable

---

Transport Type

Transport Type 1:

Transport Type 2:

Transport Type 3:

Transport Type 4:

Use configured transport for egress leg

**Figure26:**

Ingress IP Attributes - Signaling Back A Message To The Peer That We Receive A Call From

Flags

<input type="checkbox"/> 181 Supported	<input type="checkbox"/> Registration Support 3xx
<input type="checkbox"/> 182 Supported	<input type="checkbox"/> Send 183 On Initiating Disconnect Treatment
<input type="checkbox"/> Convert Progress To Alert	<input type="checkbox"/> Send Fast Start Response In CP
<input type="checkbox"/> Don't Send Facility Message	<input type="checkbox"/> Send SDP In 200 OK If 18x Reliable
<input type="checkbox"/> Don't Send 3XX With IP	<input type="checkbox"/> Send Updated SDP In 200 OK
<input type="checkbox"/> Don't Send 3XX With TN	<input type="checkbox"/> Send SDP In Subsequent 18x
<input type="checkbox"/> Map Called Party Category In P-Sig-Info Header	<input type="checkbox"/> Send TLS Connection Failure Response
<input type="checkbox"/> No SDP In 180 Supported	<input type="checkbox"/> Suppress 183 For 3xx Redirect Response
<input type="checkbox"/> Refuse Fast Start Proposal	<input type="checkbox"/> Suppress 183 Without SDP
<input type="checkbox"/> Registration Expires in Expires Header	<input type="checkbox"/> Override 3xx Relay
<input type="checkbox"/> Map Subsequent 180 to 183	<input type="checkbox"/> Send BIT-H Of BCI In Outgoing Invite
<input type="checkbox"/> Early Media Authorization	<input type="checkbox"/> Convert Alert To Progress
<input type="checkbox"/> Report Early Media Auth	<input type="checkbox"/> Process Qtype and Attach DPC/SSN info in 3xx

**Figure27:**

Carrier Information

Generate Terminating CA  Generate Terminating CIC

---

History Information

Include History-Info  Cause Parameter In RFC 4458  Reason With Cause Value As Per RFC 4244

Access Transfer Profile:

---

Trf Parameters

Preferred Trf Uri:

Preferred Mrb Uri:

---

Enum Parameters

TTL:

## Configuring Codec Entry Profile

Codecs define the audio encoding methods and their associated attributes. You can add custom codec entries which are then available to include when configuring codecs in a Packet Service Profile. When you add a codec entry, the parameters available change, depending on the base codec you select. You can also configure options for a selected Codec Entry that specify how to handle DTMF digits in the media stream.

Define the codec entry priorities and codec names.

### DTMF Types Configuration

Use the DTMF relay window under Codec Entry configured in Packet Service Profiles to specify how to handle DTMF digits in the media stream.

Figure28:

Codec Entry:	G711-DEFAULT
Audio Encoding:	G.711
Coding Rate (kbits/s):	6.3
Fax Tone Treatment:	<None>
Packet Size (ms):	10
Preferred RTP Payload Type:	128
Max Interleave Depth:	0
Fax Treatment Failure Handling <input type="radio"/> Disconnect <input checked="" type="radio"/> Continue	
G.711 Law <input type="radio"/> Law From Other Leg <input type="radio"/> A Law <input checked="" type="radio"/> U Law <input type="checkbox"/> G.711 Send SID	
Modem Tone Treatment <input checked="" type="radio"/> None <input type="radio"/> Notify Peer <input type="radio"/> Disconnect <input type="radio"/> Fallback To G.711 <input type="radio"/> Apply Fax Treatment	
Modem Treatment Failure Handling <input type="radio"/> Disconnect <input checked="" type="radio"/> Continue	
Honor Tone Detection <input type="checkbox"/> Fax <input type="checkbox"/> Modem	
DTMF Relay <input checked="" type="radio"/> None <input type="radio"/> Out-Of-Band <input type="radio"/> RFC 2833 <input type="radio"/> Either OOB Or 2833 <input type="radio"/> Both OOB And 2833 <input checked="" type="checkbox"/> DTMF Remove Digits <input type="checkbox"/> enable DTMF Duration DTMF Duration(ms): 300	

Figure29:

AMR & AMR-WB Options <input type="checkbox"/> AMRWB lu-UP Mode <input type="checkbox"/> Mode Change Neighbor <input type="checkbox"/> RTCP APP CMR <input type="checkbox"/> Initial Codec Mode as per 3GPP 26.114	
FEC Redundancy <input checked="" type="radio"/> 0 <input type="radio"/> 1 <input type="radio"/> 2	
AMR-WB Mode Set (Kbps) <input type="checkbox"/> 6.6 <input type="checkbox"/> 14.25 <input type="checkbox"/> 19.85 <input type="checkbox"/> 8.85 <input type="checkbox"/> 15.85 <input type="checkbox"/> 23.05 <input type="checkbox"/> 12.65 <input type="checkbox"/> 18.25 <input type="checkbox"/> 23.85	
Silence Suppression <input type="checkbox"/> Silence Suppression <input type="radio"/> vad1 <input checked="" type="radio"/> vad2	
OPUS Options <input type="checkbox"/> UseCBR <input type="checkbox"/> UseFEC <input type="checkbox"/> UseDTX Max Average Bit Rate (bits/sec): 20000	

Figure30:

EVS Options <input type="checkbox"/> UseCompatHeader <input type="checkbox"/> Support EVS-AMR-WB-IO Mode <input type="checkbox"/> Support Asymmetric Bit Rate		
Partial Redundancy <input checked="" type="radio"/> -1 <input type="radio"/> 0 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 5 <input type="radio"/> 7		
Max Channels <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 6 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5		
BR Set Min Bit Rate: <input type="text"/> Max Bit Rate: <input type="text"/>		
SILK Options <input type="checkbox"/> UseSilkDTX Max Average Bit Rate (bits/sec): 0		

### Video Call Configuration

Configure Maximum Video Bandwidth and Video Bandwidth Reduction Factor in packet service profile to enable video calls.

**Figure 44:**

Video Calls

Maximum Video Bandwidth (kbps): 2000

Video Bandwidth Reduction Factor (%): 1

Audio Only If Video Is Prevented

IPv4 TOS: 0

IPv6 Traffic Class: 0

IEEE 802.1Q VLAN COS: 0

Codec List Profile: <None>

## Configuring Packet Service Profile

Each Packet Service Profile is configured for a pair of gateways, and includes entries for up to four audio/video encoding methods. The pair of gateways can be originating for destination gateways in the same gateway group, or can be originating for destination gateways in an inter-gateway group.

### Packet Service Profile IN

From the Drop Down, select the codec Entry profiles created during initial steps,

**Figure 31:**

Packet Service Profile: SIPREC\_PSP\_INGRESS

Silence Factor: 40

Voice Initial Playout Buffer Delay (ms): 10

Type Of Service: 0

AAL1 Payload Size: 47

Preferred RTP Payload Type For DTMF Relay: <None>

Media Packet COS: 0

Monitoring Profile: <None>

Media Peer Inactivity Timeout (s): 0

Codec Entry

Codec Entry: G729A-DEFAULT

Add Update

Codec Entry	Value
1	G711-DEFAULT

**Figure32:**

T.38	
Number of Redundant Packets	<input checked="" type="radio"/> 0 <input type="radio"/> 1
Low Speed Number of Redundant Packets	<input checked="" type="radio"/> 0 <input type="radio"/> 1
T.38v0 Maximum Bit Rate	<input checked="" type="radio"/> 2.4 kbits/s <input type="radio"/> 4.8 kbits/s <input type="radio"/> 9.6 kbits/s
Data Rate Management Type	<input checked="" type="radio"/> Type 1 - Local Generation of TCF <input type="radio"/> Type 2 - Transfer of
Use Max Bit Rate Only	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
ECM	<input type="checkbox"/> ECM Preferred
T38FaxMaxDatagram Size without Redundancy	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
T.38FaxProtocolVersion:	T.38(v0)
Honor Remote Precedence	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Send Route PSP Precedence	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Packet-To-Packet Control	Transcode
	<input type="radio"/> Only <input checked="" type="radio"/> Conditional <input type="radio"/> Determined By PSP For Other Leg <input type="radio"/> Trans

### Transcoding:

Use the Codexes Allowed For Transcoding window to specify, for a Packet Service profile (PSP), between which codexes you want the SBC to allow transcoding. Checking options on this window specifies that the codexes selected in the "This Leg" row can be transcoded to those selected in the "Other Leg" row, and vice versa.

PSPs are assigned to both legs of a call. Therefore the Codexes Allowed For Transcoding values applied to a particular call reflect the contributions of both profiles, with the ingress and egress call legs being viewed as "This Leg" by one profile and as the "Other Leg" by the other profile.

This control specifies the transcoding method used for the associated packet flow.

The SBC performs transcoding for media streams carried between two IP devices by translating the streams from the ingress audio encoding format to the egress audio encoding format when the devices do not share a common codex. In some environments, transcoding may be preferred over negotiating the attributes of a common codex.

- **Conditional**The SBC performs transcoding when any of the conditions specified in the Conditions In Addition To "No Common Codex" section are met.
- **Determined By PSP For Other Leg**The SBC performs transcoding based on the transcoding options specified in the packet service profile assigned to the other leg of the call. When selected, PSX Manager disables the check boxes in the Codexes Allowed for Transcoding section.
- **Only**The SBC performs transcoding for the codexes selected in the Codex Allowed For Transcoding section (see definition below). None of the conditions specified in the Conditions In Addition To "No Common Codex" section are used in determining when to perform transcoding.
- **Transcoder Free Transparency**When selected, the SBC transparently passes the PSP from the ingress call-leg to the egress call-leg, bypassing transcoding.

**Figure33:**

Packet-To-Packet Control

Transcode

Only       Conditional       Determined By PSP For Other Leg       Transcode

Conditions In Addition To "No Common Codec"

Apply Fax Tone Treatment       Different Silence Suppression

Different DTMF Relay       Honor Answer Preference

Different Packet Size       Honor Offer Preference

Different 2833 Payload Type

Codecs Allowed For Transcoding

This Leg:  G.711 A     G.711 U     G.722     G.722.2     G.723.1     G.726     G.729     OPUS     EVS     SILK     T.38     iLBC     AMR

Other Leg:  G.711 A     G.711 U     G.722     G.722.2     G.723.1     G.726     G.729     OPUS     EVS     SILK     T.38     iLBC     AMR

RTCP

RTCP      Packet Loss Threshold (Packets Lost/100,000 Packets): 0

RR Bandwidth: 250

RS Bandwidth: 250

Packet Loss Action

None       Trap       Trap And Disconnect

Enable RTCP Only For HELD Calls       Termination For Pass-Through Calls

RTCP-MUX       Generate RTCP for T140 if not received from other leg

RTCP-XR

Relay       Relay Or Terminate

**RTCP configuration:**

Use this object to specify Real Time Control Protocol (RTCP) options for the call. RTCP is used to report network traffic congestion data.

When set to **Enable**, Use RTCP for the call leg.

**Figure34:**

Packet Service Profile

SQL Search Criteria (19 entries)

Packet Service Profile: \*

Search    More...    -

Packet Service Profile

- ATOS\_IN
- ATOS\_OUT
- DEFAULT
- ENT\_ACM\_DEFAULT\_PSP
- ENT\_AVAYASM\_DEFAULT\_PSP
- ENT\_CUCM\_DEFAULT\_PSP
- ENT\_LYNCS\_PSP\_TCP
- ENT\_LYNCS\_PSP\_TLS
- PSTN\_PSP
- SIPREC\_PSP
- SIPREC\_PSP\_EGRESS
- SIPREC\_PSP\_EGRESS1
- SIPREC\_PSP\_EGRESS2
- SIPREC\_PSP\_EGRESS\_pob
- SIPREC\_PSP\_INGRESS
- SIPREC\_PSP\_INGRESS\_G729
- SRTP\_SIPREC\_PSP\_EGRESS

Different Packet Size       Honor Offer Preference

Different 2833 Payload Type

Codecs Allowed For Transcoding

This Leg:  G.711 A     G.711 U     G.722     G.722.2     G.723.1     G.726     G.729     OPUS     EVS     SILK     T.38     iLBC     AMR

Other Leg:  G.711 A     G.711 U     G.722     G.722.2     G.723.1     G.726     G.729     OPUS     EVS     SILK     T.38     iLBC     AMR

RTCP

RTCP      Packet Loss Threshold (Packets Lost/100,000 Packets): 0

RR Bandwidth: 250

RS Bandwidth: 250

Packet Loss Action

None       Trap       Trap And Disconnect

Enable RTCP Only For HELD Calls       Termination For Pass-Through Calls

RTCP-MUX       Generate RTCP for T140 if not received from other leg

RTCP-XR

Relay       Relay Or Terminate

**Figure35:**

Peer Absence Action

None  Trap  Trap And C

---

Silence Insertion Descriptor

G.711 Silence Insertion Descriptor RTP Payload Type: 13

Silence Insertion Descriptor Heartbeat

---

Data Calls

Initial Playout Buffer Delay (ms): 50

Packet Size: 20

Preferred RTP Payload Type: 56

---

Video Calls

Maximum Video Bandwidth (kbps): 0

Video Bandwidth Reduction Factor (%): 0

Audio Only If Video Is Prevented

IPv4 TOS: 0

IPv6 Traffic Class: 0

IEEE 802.1Q VLAN COS: 0

Codec List Profile: <None>

---

Qos Values

MSRP DSCP: 0

DTLS SCTP DSCP: 0

T140 DSCP: 0

Application Dscp: 0

Secure RTP/RTCP > Crypto Suite Profile is used for srtp configurations. Please refer [Media Encryption](#) for more details

**Figure36:**

Non RTP Stream

Max Non Rtp Bandwidth(kbps): 0

Non RTP TLS Profile Name: defaultTlsProfile

---

Audio Transparency

Unknown Codec Packet Size(ms) 10

Unknown Codec Bit Rate(kbps) 124

---

Secure RTP/RTCP

Crypto Suite Profile: <None>

Flags

Allow Fallback  Enable SRTP

Reset ROC On Session Key Change  Reset Enc/Dec/ROC on Decryption Key Change

Update Crypto On Modify  Allow Pass Through

---

DTLS/SRTP

Crypto Suite Profile: <None>

Flags

Allow Fallback  Enable DTLS

Relay DTLS SRTP  Relay DTLS SCTP

**Figure37:**

Flags

DSCP Passthrough  Interwork DTMF OOB-2833 Without Transcoding

Digit Detect Send Enabled  Use Direct Media

Disallow Data Calls  Validate Peer Support for DTMF Events

SSRC Randomize  HD Codec Preferred

Reserve BW for Preferred Audio Common Codec  Prefer NB PassThru Over HDTranscode

Police on Heaviest Audio Codec  Match Offered Codec Group If Nb Only

t140 Call  Force Route PSP Order

Allow Audio Transcode For MultiStream Call  SSRC Randomize For Srtp

Generate and Signal SSRC and CName  Vtp Support

Allow Mid Call SSRC Modification  Always Send Timestamp

## Packet Service Profile OUT

Figure38:

Packet Service Profile:	SIPREC_PSP_EGRESS
Silence Factor:	40
Voice Initial Playout Buffer Delay (ms):	10
Type Of Service:	0
AAL1 Payload Size:	47
Preferred RTP Payload Type For DTMF Relay:	<None>
Media Packet COS:	0
Monitoring Profile:	<None>
Media Peer Inactivity Timeout (s):	0
Codec Entry	
Codec Entry:	G729A-DEFAULT
<input type="button" value="Add"/> <input type="button" value="Update"/>	
Codec Entry	Value
1	G711-DEFAULT
<input type="button" value="Delete"/>	

Figure39:

T.38	
Number of Redundant Packets	<input checked="" type="radio"/> 0 <input type="radio"/> 1
Low Speed Number of Redundant Packets	<input checked="" type="radio"/> 0 <input type="radio"/> 1
T.38v0 Maximum Bit Rate	<input checked="" type="radio"/> 2.4 kbits/s <input type="radio"/> 4.8 kbits/s <input type="radio"/> 9.6 kbits/s
Data Rate Management Type	<input checked="" type="radio"/> Type 1 - Local Generation of TCF <input type="radio"/> Type 2 - Transfer of
Use Max Bit Rate Only	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
ECM	<input type="checkbox"/> ECM Preferred
T38FaxMaxDatagram Size without Redundancy	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
T.38FaxProtocolVersion:	T.38(v0)
Honor Remote Precedence	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Send Route PSP Precedence	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Packet-To-Packet Control	
Transcode	<input type="radio"/> Only <input checked="" type="radio"/> Conditional <input type="radio"/> Determined By PSP For Other Leg <input type="radio"/> Trans

Figure40:

Packet-To-Packet Control

Transcode

Only  Conditional  Determined By PSP For Other Leg  Transcode

Conditions In Addition To "No Common Codec"

Apply Fax Tone Treatment  Different Silence Suppression

Different DTMF Relay  Honor Answer Preference

Different Packet Size  Honor Offer Preference

Different 2833 Payload Type

Codecs Allowed For Transcoding

This Leg:  G.711 A  G.711 U  G.722  G.722.2  G.723.1  G.726  G.729  OPUS  EVS  SILK  T.38  iLBC  AMR

Other Leg:  G.711 A  G.711 U  G.722  G.722.2  G.723.1  G.726  G.729  OPUS  EVS  SILK  T.38  iLBC  AMR

RTCP

RTCP Packet Loss Threshold (Packets Lost/100,000 Packets): 0

RR Bandwidth: 250

RS Bandwidth: 250

Packet Loss Action

None  Trap  Trap And Disconnect

Enable RTCP Only For HELD Calls  Termination For Pass-Through Calls

RTCP-MUX  Generate RTCP for T140 if not received from other leg

RTCP-XR

Relay  Relay Or Terminate

Figure41:

Peer Absence Action

None  Trap  Trap And Disconnect

Silence Insertion Descriptor

G.711 Silence Insertion Descriptor RTP Payload Type: 13

Silence Insertion Descriptor Heartbeat

Data Calls

Initial Playout Buffer Delay (ms): 50

Packet Size: 20

Preferred RTP Payload Type: 56

Video Calls

Maximum Video Bandwidth (kbps): 0

Video Bandwidth Reduction Factor (%): 0

Audio Only If Video Is Prevented

IPv4 TOS: 0

IPv6 Traffic Class: 0

IEEE 802.1Q VLAN COS: 0

Codec List Profile: <None>

Qos Values

MSRP DSCP: 0

DTLS SCTP DSCP: 0

T140 DSCP: 0

Application DSCP: 0

Figure 42:

Non RTP Stream

Max Non Rtp Bandwidth(kbps): 0

Non RTP TLS Profile Name: defaultTlsProfile

---

Audio Transparency

Unknown Codec Packet Size(ms) 10

Unknown Codec Bit Rate(kbps) 124

---

Secure RTP/RTCP

Crypto Suite Profile: <None>

Flags

Allow Fallback  Enable SRTP

Reset ROC On Session Key Change  Reset Enc/Dec/ROC on Decryption Key Change

Update Crypto On Modify  Allow Pass Through

---

DTLS/SRTP

Crypto Suite Profile: <None>

Flags

Allow Fallback  Enable DTLS

Relay DTLS SRTP  Relay DTLS SCTP

Figure 43:

Flags

DSCP Passthrough  Interwork DTMF OOB-2833 Without Transcoding

Digit Detect Send Enabled  Use Direct Media

Disallow Data Calls  Validate Peer Support for DTMF Events

SSRC Randomize  HD Codec Preferred

Reserve BW for Preferred Audio Common Codec  Prefer NB PassThru Over HDTranscode

Police on Heaviest Audio Codec  Match Offered Codec Group If Nb Only

t140 Call  Force Route PSP Order

Allow Audio Transcode For MultiStream Call  SSRC Randomize For Sntp

Generate and Signal SSRC and CName  Vtp Support

Allow Mid Call SSRC Modification  Always Send Timestamp

## Configuring IP Signaling Peer Group

IP Peer is an entity of the Session Border Controller, which is configured inside the Zone. It acts as a destination endpoint for the call to be routed towards. An IP Peer constitutes an IPv4/IPv6 address or a Fully Qualified Domain Name (FQDN) with a port number.

Figure 45:

IP Signaling Peer Group: SIPREC\_PEER1

Description:

Policy Profile Group: <None>

Flags

Send All Peer IP Addresses/FQDNs

Number of Routes to Try: 1  All

Route Prioritization:  Sequence  Round Robin  All Proportion

Peer Group Data

Sequence Number: 0

IPv4 Address: 8 . 8 . 8 . 8 Port Number: 8

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port Number: 0

Server FQDN: Port Number: 0

Proportion: 0

In Service

[Add/Update](#)

Sequence Number	IP Address	Port Number	Server FQDN	Port Number	Send	Service Status	Proportion
0	8.8.8.8	8		0	IP Address	In Service	0

Figure 46:

IP Signaling Peer Group: SIPREC\_PEER2

Description:

Policy Profile Group: <None>

Flags

Send All Peer IP Addresses/FQDNs

Number of Routes to Try: 1  All

Route Prioritization:  Sequence  Round Robin  All Proportion

Peer Group Data

Sequence Number: 0

IPv4 Address: 8 . 8 . 8 . 8 Port Number: 8

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port Number: 0

Server FQDN: Port Number: 0

Proportion: 0

In Service

[Add/Update](#)

Sequence Number	IP Address	Port Number	Server FQDN	Port Number	Send	Service Status	Proportion
0	8.8.8.8	8		0	IP Address	In Service	0

## Configuring Carrier

Please note that we have used default Carrier '0000' for our testing.

Figure 47:

Carrier: 0000

Partition: DEFAULT

Preferred Packet Service Profile ID Group: <None>

Signaling Profile: <None>

SIP Domain: <None>

Service Provider Id (Hex): 0

Context Info

Ingress CVT Rule: <None>

Egress CVT Rule: <None>

Flags

Escaped

Ignore Tandem Script On Redirection

Scripts

Casual Routing: <None> [Runtime Variables](#)

Nonsubscriber: <None> [Runtime Variables](#)

Tandem: <None> [Runtime Variables](#)

Services

Not Screened  Screened - Normal  Screened - Fraud

Class Of Service: <None>

Service Exception Profile: <None>

## Configuring Element Routing Priority Profile

Please note that we have cloned and used default Element Routing Priority for our testing.

Figure 48:

Element Routing Priority: SIPREC

Call Property

Call Type: Private

Priority: 1

Network: All

Toll Indication: <All>

Entity Type: <None>

Priority: 1

Add Update

Call Type	Call Priority	Network	Toll Indication	Entity Type	Priority
Private	1	All	<All>	<None>	1
0+	1	All	<All>	<None>	1
0-	1	All	<All>	<None>	1
1+	1	All	<All>	Trunk Group	1
1+	2	All	<All>	<None>	2
IDDD	1	All	<All>	<None>	1
0+ IDDD	1	All	<All>	<None>	1
00	1	All	<All>	<None>	1
IP VPN Service	1	All	<All>	<None>	1
Test	1	All	<All>	<None>	1
Transit	1	All	<All>	<None>	1
Other Carrier Chosen	1	All	<All>	<None>	1
Carrier Cut Through	1	All	<All>	<None>	1
User Name	1	All	<All>	<None>	1
Mobile	1	All	<All>	<None>	1

## Configuring SignalingProfile

Please note that we have used default Signaling Profile 'DEFAULT\_IP\_PROFILE' for our testing.

Figure 49:

SIGNALING PROFILE: DEFAULT\_IP\_PROFILE

Transit Carrier Indicator Profile: <None>

Generic Digit Type: <Unknown>

Ingress

CFT

Send CFT Information

CFT Information For Early Backward Message:  Off Net  On Net

Ingress Flags

Disallow Missing Calling Number

Disallow Without Billing Number

Disallow Without OLIP

Don't Generate Exit Message

Don't Send Restricted Connected Line Identity

Don't Send Connected Number

Don't Send Unrequested Connected Line Identity

Enable Redirection Capability

Enable Transfer Connect

FE Parameter In Short Form

Generate Charge Message

Generate CPG for Call Forward Notify

Inbound TNS Allowed

Normalize Carrier Code

Propagate Egress Channel Information

Propagate FE Parameter

Treat CIC 0000 As No CIC

Use ISUP Immediate REL On SUS Timer

Validate GAP Type Ported Number

Figure 50:

Egress			
TNS Flags			
Inter LATA Local:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Intra LATA Local:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Inter LATA Toll:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Intra LATA Toll:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
0:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
0+ Inter LATA:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
0+ Intra LATA:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
00:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
IDDD:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
0+IDDD:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Calling Name:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Calling Number:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Charge Number:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
CIP:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
CSP:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
JIP:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
OLIP:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Original Called Number:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send
Redirecting Number:	<input checked="" type="radio"/> No Input	<input type="radio"/> Send	<input type="radio"/> Don't Send

Figure 51:

Redirect Capability:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Redirect Count:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Redirect Information:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Calling Party/Billing Number:	<input type="text" value="&lt;None&gt;"/>	
Egress Flags		
<input type="checkbox"/> Add Prefix 011 For International Calls	<input type="checkbox"/> Propagate Charge Message	
<input type="checkbox"/> Add Prefix 1 For Inter LATA Calls	<input type="checkbox"/> Propagate GD Parameter	
<input type="checkbox"/> Add Prefix 1 For Intra LATA Calls	<input type="checkbox"/> Propagate Ingress Channel Information	
<input type="checkbox"/> Annex E Support	<input type="checkbox"/> Reorder Trunk as Low Priority Based On ISUP Preference	
<input type="checkbox"/> Apply Switch Type CPC Profile	<input type="checkbox"/> Reroute On Signaling Congestion	
<input type="checkbox"/> Called Number 7 Digits	<input checked="" type="checkbox"/> Reset OLIP For Toll Free Calls	
<input type="checkbox"/> Calling Number 7 Digits	<input type="checkbox"/> Restore Calling Number If Derived From Billing Number	
<input type="checkbox"/> Change Bearer Cap From 3.1KHz To Speech	<input type="checkbox"/> Restore Calling Number If Derived From OCN	
<input type="checkbox"/> Convert Numbers To E164 Format	<input type="checkbox"/> Restore Calling Number If Derived From Redirecting Number	
<input type="checkbox"/> CPC Mapping	<input type="checkbox"/> Restore Calling Number If Derived From Trunk Group	
<input type="checkbox"/> Dialed Number As Called Number	<input type="checkbox"/> Restore FCI International Bit	
<input type="checkbox"/> Discard GAP Additional Calling If Same As Calling Number And Ingress SIP	<input type="checkbox"/> Send Billing Number As Calling Number	
<input type="checkbox"/> Don't Strip Calling Number For Restricted Presentation	<input type="checkbox"/> Send Billing Number As Calling Number If Calling Number Not Present	
<input type="checkbox"/> Forced Override OLIP Value	<input type="checkbox"/> Send Contract Number If Allowed By Ingress SIP	
<input type="checkbox"/> Generate FE Parameter	<input type="checkbox"/> Send DM/PM Manipulated Billing Number	
<input type="checkbox"/> OLI Mapping	<input type="checkbox"/> Send Toll Free Number In GAP Parameter	

Figure 52:

<input type="checkbox"/> Prefix RN to Dialed Digits	<input checked="" type="checkbox"/> Send Toll Free Number In OCN Parameter
	<input type="checkbox"/> Suppress ONI
	<input type="checkbox"/> Undo LNP
	<input type="checkbox"/> Use Output ANI For CDNIS
CFT	
Egress CFT Information:	<input checked="" type="radio"/> Off Net <input type="radio"/> On Net
Generate PartitionID + NetID In NetworkData In IAM	
<input type="checkbox"/> Generate PartitionId + NetId In NetworkData In IAM	
<input type="checkbox"/> Propagate PartitionId + NetId In NetworkData In IAM	
<input type="checkbox"/> Override PartitionId + NetId In NetworkData In IAM	
IP Double Dip Control Flags	
<input type="checkbox"/> Called Number From Alternate Called Number	<input type="checkbox"/> Restore Translated Numbers
<input type="checkbox"/> Restore Ingress Numbers Except Translated Numbers	<input type="checkbox"/> Skip Egress Trunk Group Processing
Mobile Call Delivery	
Original Called Number:	<input checked="" type="radio"/> No Input <input type="radio"/> Send <input type="radio"/> Don't Send
Redirection Information:	<input checked="" type="radio"/> No Input <input type="radio"/> Send <input type="radio"/> Don't Send

**Figure 53:**

Redirection Capability Flags	
<input type="checkbox"/> Enable Redirection Capability	
Number Control Profile:	<None>
Redirect Information Profile:	<None>
Flags	
<input type="checkbox"/> Check Ingress Trunk Group Redirection Capability	<input type="checkbox"/> Check Redirection Capability Of Number Used For Routing In Number Control Profile
<input type="checkbox"/> Check Number Control Profile For Received Called Number	<input type="checkbox"/> Check SIP Indirect DIP And Username Translation Source Number
<input type="checkbox"/> Check Received Redirection Parameters	
Common	
Common Flags	
<input checked="" type="checkbox"/> Trusted For COL	<input type="checkbox"/> COLP/COLR IGW Support
Access Transport	
<input checked="" type="radio"/> Yes <input type="radio"/> No	
International Gateway Support	
<input type="checkbox"/> Don't Convert Called Number	<input type="checkbox"/> Don't Convert Calling Number

## Configuring Feature Control Profile

Please note that we have used default Feature Control Profile 'DEFAULT\_IP' for our testing.

**Figure 54:**

Feature Control Profile: DEFAULT\_IP

Features (Set 1)

- Always Apply Default Calling Party Number From Trunk Group
- Always Apply Default Presentation Indicator From Trunk Group
- Apply Business Group Services
- Apply Calling Party Services
- Apply Default If Calling Party Number Not Present
- Apply Default If Calling Party Number Not Subscriber
- Apply Destination Services
- Apply Dial Plan
- Apply Digit Length Enforcement
- Apply OLIP Services
- Determine JIP
- Determine LATA, Region and MTA
- Determine MTA For LRN in Ported Calls
- Determine LATA, Region and MTA for LRN in Ported Calls
- Exclude LATA Sub-Zone Id For Determining Toll Indication
- Filter Routes Before Prioritization
- Normalize Digits
- Process Called Number
- Process Calling Number
- Process Generic Digits

Figure 55:

- Process Presentation Setting
- Process Screening Setting
- Use Billing Number For Normalization
- Use Billing Number For Subscriber
- Use Trunk Group Country
- Use Trunk Group Country For Blocking Profile

Features (Set 2)

- Always Use Billing Number For Calling Party Number
- Always Use Ingress CSP
- Always Use Redirecting Number For Calling Number
- Always Use Trunk Group JIP
- Apply All Countries Routing
- Apply CPC Services
- Determine Charge Band
- Do Not Replace Calling Number For Emergency Calls
- Error On Misrouted LRN
- No Local Calls
- Process Called Party NOA
- Process Called Party NPI
- Process Calling Party NOA
- Process Calling Party NPI

Figure 56:

<input type="checkbox"/> Skip Called Party Services For Misrouted LRN <input type="checkbox"/> Skip LRN Validation And Unporting From LNP <input type="checkbox"/> Skip LNP For Toll Calls <input type="checkbox"/> Treat Not Presubscribed Input Carrier Input As Not A Casual Call <input type="checkbox"/> Treat Presubscribed Input Carrier Input As Not A Casual Call <input type="checkbox"/> Trigger LNP For 0+ Dialed Calls <input type="checkbox"/> Use Billing Number For Calling Party Number If Calling Party Number Not Present <input type="checkbox"/> Use OCN For Calling Party Number If Redirecting Number Not Present <input type="checkbox"/> Use Redirecting Number For Subscriber
<b>Features (Set 3)</b> <input type="checkbox"/> Add Number of Prefix Digits Stripped To Overlap Dialing Parameters <input type="checkbox"/> All Provisioned Calling and Called Digits Matched for Local Calling Area Determination <input type="checkbox"/> Allow CMT Call <input type="checkbox"/> Apply Network Traffic Management On Indirect Dip <input type="checkbox"/> Always Process Called Number If NOA Unknown <input type="checkbox"/> Always Process Calling Number If NOA Unknown <input type="checkbox"/> Dont Apply Called Party Services During LNP Transition <input type="checkbox"/> Fetch Subscriber With Country Code Prefixed <input type="checkbox"/> Generate ECI <input checked="" type="checkbox"/> Process Redirection Number <input type="checkbox"/> SSG Calling Party Use Signal-In Number

**Figure 57:**

<input type="checkbox"/> Translated Emergency Number <input type="checkbox"/> Try Alternate Address For SIPE <input type="checkbox"/> Use Redirecting BG <input type="checkbox"/> Use Redirecting Number For Called Number Normalization <input type="checkbox"/> Use Redirecting Number Instead Of CLI For DDI Screening <input type="checkbox"/> Apply LATA from Trunk Group If Calling Number Not Present <input checked="" type="checkbox"/> Perform Route Header Based Routing <input type="checkbox"/> Use Destination IP address in Standard Routing <input type="checkbox"/> Disable Fallback To 7 Digits Hosted LNP Lookup <input type="checkbox"/> Determine Charge Band Profile from TG <input type="checkbox"/> Dont Send \1 In Enum Response	
<b>Features (Set 4)</b> <input type="checkbox"/> Accept Calls With RPH If Dialed Number Is Non ETS <input type="checkbox"/> Enable RPH ETS <table border="1"> <tr> <td> <b>Process Destination Trunk Group And Trunk-Context</b>  <input checked="" type="checkbox"/> Process TGRP  <input type="checkbox"/> Process Trunk-context </td> </tr> </table> <input type="checkbox"/> Process Enumdi Parameter <input checked="" type="checkbox"/> Process Originating Trunk Group And Trunk-Context Over OTG <input type="checkbox"/> SIP Cause Code Mapping	<b>Process Destination Trunk Group And Trunk-Context</b> <input checked="" type="checkbox"/> Process TGRP <input type="checkbox"/> Process Trunk-context
<b>Process Destination Trunk Group And Trunk-Context</b> <input checked="" type="checkbox"/> Process TGRP <input type="checkbox"/> Process Trunk-context	

**Figure 58:**

- Skip Number Translations For Valid Service Routes
- Include Retry After For 503 Responses
- Process Swid And Tgid From Sip Invite
- Don't Restart Timer C on 1xx
- Override Trunkgroup With Subscriber End Point Profile
- Fetch State For ENUM SIP AoR
- Enable Per Route Routing Label
- Do Not Validate GAP
- Process ISUP MIME From SIP Message Body
- Use Flex Variable for Origination Jurisdiction Determination
- Use Flex Variable for Destination Jurisdiction Determination
- Process Screening For Call Origination

**Figure 59:**

**URI Processing**

- Process TO URI User
- Process FROM URI User
- Process PAI URI User
- Process Diversion URI User
- Process Called URI User
- Process Calling URI User
- Process History-Info URI User
- Start Using Processed URI User Data

**IP Protocol Flags**

- Use IP Protocol Flags

**Flags**

- Default Called User As A User Name
- Default Calling User As A User Name
- Disable Egress Check And Don't Send Contract Number
- Prefer BICC instead of ISUP routes for FCI preferred value
- Proxy/Redirector Force Route Calls With Non-Local IP Address
- Reject Calls To Non-Local Domains
- Reject Calls To Non-Local IP Addresses
- Support Domain Name In 300 Contact
- Support PAI Header in CONTACT
- Honor Phone-Context Parameter
- Enable Stir Shaken

**PSX Processing Mode**

Proxy
  Redirector

## Configuring Trunk Groups

Create two Trunk Groups for Ingress and Egress and associate the Trunk Groups to the gateway created in Step-1.



**Warning**

Mandatory! You must capitalize SIP Trunk Group names.

### Trunk Group IN

Follow the instructions below for Ingress Trunk Group.

**Figure 60:**

Trunk Group:	SIPREC_TG1	<input type="checkbox"/> Unrestricted
Gateway:	SBCSYAM1	
Description:		
Auto Recall Profile:	<None>	
Call Processing Localization Variant:	North America	
Calling Area:	<None>	
Carrier:	0000	
Carrier Selection Priority:	<None>	
Country:	1 - USA, Canada and Caribbean	
DDI Range Profile:	<None>	
Destination Switch Type:	Access	
Direction:	Two Way	
Element Routing Priority Profile:	SIPREC	
Feature Control Profile:	DEFAULT_IP	
IP Signaling Profile:	SIPREC_IPSP_TCP	
LATA:	<None>	
Local Recursion Profile:	<None>	
Maximum Satellite Hops:	Three or More Satellite Hops	
Network Data Partition:	0	
Network Data Net:	0	
Next Hop Domain:	<None>	
Number Analysis Profile:	<None>	
Number Length Enforcement:	<None>	

Figure 61:

Originating Carrier:	<None>	
PPR Profile:	<None>	
Pseudo Carrier:	<None>	
Remote Sip Peer Type:	None	
Region:	<None>	
Routing Criteria Profile:	<None>	
SCP Business Service Group:	0	
Signaling Profile:	DEFAULT_IP_PROFILE	
Signaling Flag:	GR394 ISUP	
SIP Domain:	<None>	
SIP Response Code Profile:	<None>	
TDM Type:	Other	
Tone And Announcement Profile:	<None>	
Trunk Group COS:		
Trunk Group COS Profile:	<None>	
Trunk Group Domain:	<None>	
Trunk Number:		
Zone Index Profile:	<None>	
ZZ Profile:	<None>	
Charge Band Profile:	<None>	

Figure 62:

Enum Domain Profile:	<None>
Flexible Variable Rule:	<None>
STI Profile:	<None>
P-Origination-ID:	<input type="text"/> <input type="checkbox"/> Autogenerate <input type="button" value="Clear"/>
RPH Signaling Profile:	<None>
Beep Tone Profile:	<None>
STI Generic Profile:	<None>
IPSP Generic Profiles:	<None>
Context Info	<input type="text"/>

Ingress

Charge Indicator:	None
Default CPC:	<None>
Default OLIP:	<None>
Dial Plan Profile:	<None>
Forced OLIP Value:	<None>
In DM/PM Rule:	<None>
Info Transfer Capability Profile:	<None>
IP Version Preference:	IPv4 Only
ONI:	<input type="text"/>
JIP:	<input type="text"/>

Figure 63:

NPA:	<input type="text"/>
Numbering Plan:	NANP_ACCESS
In Policy Profile Group:	<None>
CVT Rule:	<None>
Service Detect Policy Profile Group:	<None>

Flags

<input type="checkbox"/> Allow Hex Digits In Cdpn	<input type="checkbox"/> Non-Zero Video Bandwidth Based Routing for H.323
<input type="checkbox"/> Discard NPDI	<input type="checkbox"/> Non-Zero Video Bandwidth Based Routing for SIP
<input type="checkbox"/> Discard RN	<input type="checkbox"/> Overlap Dialing
<input type="checkbox"/> HD Preferred Routing	<input type="checkbox"/> TNS Circuit Code Based Routing
<input type="checkbox"/> HD Supported Routing	<input type="checkbox"/> Use IPTG Routing (Hop By Hop Routing) For Ingress

Egress

Charge Indicator:	None
Out DM/PM Rule:	<None>
Out Policy Profile Group:	<None>
CVT Rule:	<None>
Trunk Context:	<input type="text"/>
R-URI Host:	<input type="text"/>
R-URI Host Port:	0

Figure 64:

**Flags**

Disable Crankback

Enable JIP Interwork

Use Preferred Identity

Send STI Verified Display Name

---

**Billing**

Billing Plan: <None>

Billing Information: <None>

Default Billing Number:

Nature Of Address: <None>

Numbering Plan Indicator: <None>

---

**Calling Party Number**

Calling Party:

Nature Of Address: <None>

Numbering Plan Indicator: <None>

Presentation: <None>

Screening: <None>

Default Presentation: <None>

**Figure 65:**

**Flags**

Do Not Use For Fallback Bearer Capability

Escaped

Out Of Service

Satellite Trunk

Use Sac NonSac Call Types For ZZ Profile

---

**PTG**

IP Signaling Peer Group: SIPREC\_PEER1

IP Peer Supported

Packet Service Profile ID Group: SIPREC\_INGRESS

Egress IP Signaling Profile: SIPREC\_IPSP\_TCP

---

**Packet Service Profile**

Preferred Packet Service Profile ID Group: <None>

Destination Override

---

**Traffic Management Options**

Trunk Group Reservation Level 1: 10

Trunk Group Reservation Level 2: 5

---

**VPN Information**

Business Group: <None>

Business Location: <None>

Business Group From CLI

**Figure 66:**

**Services**

Not Screened       Screened - Normal       Screened - Fraud

Class Of Service: <None>

Service Exception Profile: <None>

---

**Use SIP in Core**

Inter Gateway IP Signaling Profile: <None>

Egress IP Signaling Profile: <None>

---

**SIP Used in Core**

Inter Gateway IP Signaling Profile: <None>

Egress IP Signaling Profile: <None>

## Trunk Group OUT

Follow the instructions below for Egress Trunk Group.

**Figure 67:**

Trunk Group:	SIPREC_TG2	<input type="checkbox"/> Unrestricted
Gateway:	SBCCSYAM1	
Description:		
Auto Recall Profile:	<None>	
Call Processing Localization Variant:	North America	
Calling Area:	<None>	
Carrier:	0000	
Carrier Selection Priority:	<None>	
Country:	1 - USA, Canada and Caribbean	
DDI Range Profile:	<None>	
Destination Switch Type:	Access	
Direction:	Two Way	
Element Routing Priority Profile:	SIPREC	
Feature Control Profile:	DEFAULT_IP	
IP Signaling Profile:	SIPREC_IPSP_TCP	
LATA:	<None>	
Local Recursion Profile:	<None>	
Maximum Satellite Hops:	Three or More Satellite Hops	
Network Data Partition:	0	
Network Data Net:	0	
Next Hop Domain:	<None>	
Number Analysis Profile:	<None>	
Number Length Enforcement:	<None>	

Figure 68:

Originating Carrier:	<None>	
PPR Profile:	<None>	
Pseudo Carrier:	<None>	
Remote Sip Peer Type:	None	
Region:	<None>	
Routing Criteria Profile:	<None>	
SCP Business Service Group:	0	
Signaling Profile:	DEFAULT_IP_PROFILE	
Signaling Flag:	GR394 ISUP	
SIP Domain:	<None>	
SIP Response Code Profile:	<None>	
TDM Type:	Other	
Tone And Announcement Profile:	<None>	
Trunk Group COS:		
Trunk Group COS Profile:	<None>	
Trunk Group Domain:	<None>	
Trunk Number:		
Zone Index Profile:	<None>	
ZZ Profile:	<None>	
Charge Band Profile:	<None>	

Figure 69:

Enum Domain Profile:	<None>
Flexible Variable Rule:	<None>
STI Profile:	<None>
P-Origination-ID:	<input type="text"/> <input type="checkbox"/> Autogenerate <input type="button" value="Clear"/>
RPH Signaling Profile:	<None>
Beep Tone Profile:	<None>
STI Generic Profile:	<None>
IPSP Generic Profiles:	<None>
Context Info	<input type="text"/>

Ingress

Charge Indicator:	None
Default CPC:	<None>
Default OLIP:	<None>
Dial Plan Profile:	<None>
Forced OLIP Value:	<None>
In DM/PM Rule:	<None>
Info Transfer Capability Profile:	<None>
IP Version Preference:	IPv4 Only
ONI:	<input type="text"/>
JIP:	<input type="text"/>

Figure 70:

NPA:	<input type="text"/>
Numbering Plan:	NANP_ACCESS
In Policy Profile Group:	<None>
CVT Rule:	<None>
Service Detect Policy Profile Group:	<None>

Flags

<input type="checkbox"/> Allow Hex Digits In Cdpn	<input type="checkbox"/> Non-Zero Video Bandwidth Based Routing for H.323
<input type="checkbox"/> Discard NPDI	<input type="checkbox"/> Non-Zero Video Bandwidth Based Routing for SIP
<input type="checkbox"/> Discard RN	<input type="checkbox"/> Overlap Dialing
<input type="checkbox"/> HD Preferred Routing	<input type="checkbox"/> TNS Circuit Code Based Routing
<input type="checkbox"/> HD Supported Routing	<input type="checkbox"/> Use IPTG Routing (Hop By Hop Routing) For Ingress

Egress

Charge Indicator:	None
Out DM/PM Rule:	<None>
Out Policy Profile Group:	<None>
CVT Rule:	<None>
Trunk Context:	<input type="text"/>
R-URI Host:	<input type="text"/>
R-URI Host Port:	0

Figure 71:

Flags

- Disable Crankback
- Enable JIP Interwork
- Use Preferred Identity
- Send STI Verified Display Name

Billing

Billing Plan: <None>

Billing Information: <None>

Default Billing Number:

Nature Of Address: <None>

Numbering Plan Indicator: <None>

Calling Party Number

Calling Party:

Nature Of Address: <None>

Numbering Plan Indicator: <None>

Presentation: <None>

Screening: <None>

Default Presentation: <None>

Figure 72:

Flags

- Do Not Use For Fallback Bearer Capability
- Escaped
- Out Of Service
- Satellite Trunk
- Use Sac NonSac Call Types For ZZ Profile

IPTG

IP Signaling Peer Group: SIPREC\_PEER2

IP Peer Supported

Packet Service Profile ID Group: SIPREC\_EGRESS

Egress IP Signaling Profile: SIPREC\_IPSP\_TCP

Packet Service Profile

Preferred Packet Service Profile ID Group: <None>

Destination Override

Traffic Management Options

Trunk Group Reservation Level 1: 10

Trunk Group Reservation Level 2: 5

VPN Information

Business Group: <None>

Business Location: <None>

Business Group From CLI

Figure 73:

Services

Not Screened       Screened - Normal       Screened - Fraud

Class Of Service: <None>

Service Exception Profile: <None>

Use SIP in Core

Inter Gateway IP Signaling Profile: <None>

Egress IP Signaling Profile: <None>

SIP Used in Core

Inter Gateway IP Signaling Profile: <None>

Egress IP Signaling Profile: <None>

## Configuring Routes

Routing allows you to send calls to the correct destination. You can use routing options based on your requirements. Configure the standard and specific routes (with usernames) to ensure that no matter how the called party is addressed (a number or username), the SBC routes the message to the Core. Create Route entries for standard Trunk Group routing with Matching Criteria and a Routing Label destination.

## Routing Label

A routing label is associated with a route. Each route includes a gateway/trunk group pair. Routing labels provide the link between an entry in the Standard Route table and the set of routes associated with that Standard Route table entry.

### Routing Label 1

Figure 74:

Routing Label: SIPREC\_RL1

Action

Routes  Script  Route Hopping  LCR

Number Of Routes Requested: 10  All

Number Of Routes Per Call: 1

Script: <None> [Runtime Variables](#)

Partition: <None>

DMPM Rule: <None>  Apply Later

CPC Screening: <None>

Overflow Number:

Overflow Nature Of Address: <None>

Overflow Numbering Plan Indicator: <None>

Call Parameter Filter Group: <None>

Call Parameter Filter Profile Script: <None>

Call Parameter Filter Criteria Cluster: <None>

Routing Criteria

Use Entity Type <None>

Partition

Ignore  Do not Use  Use

Destination

Ignore  Do not Use  Use

Route Prioritization Type

Sequence  Proportion  Round Robin  All Proportion  Least Cost Routing

Figure 75:

Use TAR Routes

TAR Route Prioritization Type

Sequence  Proportion  Round Robin  All Proportion  Least Cost Routing

Route Prioritization Type For Equal Cost Routes: Sequence

Local Routes

Pass Only Local Routes  Prioritize Local Routes  Do Nothing

Filter Criteria Routes

Pass Only Filter Criteria Routes  Prioritize Filter Criteria Routes  Do Not Change Route Order

Flags

Continue Number Translation  Continue CNAM Translation  No Connect Signal To Be Sent  Use Configured NAPTR Order and Preference Value

Routes

Type	Endpoint 1	Endpoint 2	IP Peer	Sequence	Proport...	Status	TAR Ac...	TAR Lo...	DM/P...	Apply ...	Testing	Cost	Skip LR	STI T...	N...	N...
GSX Gateway	SIPREC_TG1	SBCSYAM1		1	0	In Service	Normal	0		Do Not...	Normal	1000000	Disab...	0	65...	65...

Figure 76:

**Route** [X]

Type: GSX Gateway

Gateway: SBCSYAM1

Trunk Group: SIPREC\_TG1

IP Peer: <None>

Sequence: 1

Proportion: 0

Cost: 1000000

TAR Action: Normal

TAR Location: 0

NAPTR Order: 65536

NAPTR Preference: 65536

DMPM Rule: <None>  Apply Later

Testing:  Normal  Test  Non-Test

In Service  Skip Local Recursion

Signing  Local Tagging  Verification

OK Cancel

## Routing Label 2

Figure 77:

Routing Label: SIPREC\_RL2

Action

Routes  Script  Route Hopping  LCR

Number Of Routes Requested: 10  All

Number Of Routes Per Call: 1

Script: <None> [Runtime Variables](#)

Partition: <None>

DMPM Rule: <None>  Apply Later

CPC Screening: <None>

Overflow Number:

Overflow Nature Of Address: <None>

Overflow Numbering Plan Indicator: <None>

Call Parameter Filter Group: <None>

Call Parameter Filter Profile Script: <None>

Call Parameter Filter Criteria Cluster: <None>

Routing Criteria

Use Entity Type <None>

Partition

Ignore  Do not Use  Use

Destination

Ignore  Do not Use  Use

Route Prioritization Type

Sequence  Proportion  Round Robin  All Proportion  Least Cost Routing

Figure 78:

Route Prioritization Type For Equal Cost Routes: Sequence

Use TAR Routes

TAR Route Prioritization Type

Sequence     Proportion     Round Robin     All Proportion     Least Cost Routing

Route Prioritization Type For Equal Cost Routes: Sequence

Local Routes

Pass Only Local Routes     Prioritize Local Routes     Do Nothing

Filter Criteria Routes

Pass Only Filter Criteria Routes     Prioritize Filter Criteria Routes     Do Not Change Route Order

Flags

Continue Number Translation     Continue CNAM Translation     No Connect Signal To Be Sent     Use Configured NAPTR Order and Preference Value

Routes

Type	Endpoint 1	Endpoint 2	IP Peer	Sequence	Proport...	Status	TAR Ac...	TAR Lo...	DM/P...	Apply ...	Testing	Cost	Skip LR	STI T...	N...	N...
GSX Gateway	SIPREC_TG2	SBCSYAM1		0	0	In Service	Normal	0		Do Not...	Normal	1000000	Disab...	0	65...	65...

Figure 79:

**Route**

Type: GSX Gateway

Gateway: SBCSYAM1

Trunk Group: SIPREC\_TG2

IP Peer: <None>

Sequence: 0

Proportion: 0

Cost: 1000000

TAR Action: Normal

TAR Location: 0

NAPTR Order: 65536

NAPTR Preference: 65536

DMPM Rule: <None>  Apply Later

Testing:  Normal     Test     Non-Test

In Service     Skip Local Recursion

Signing     Local Tagging     Verification

OK Cancel

## Routes

Routing allows you to send calls to the correct destination. You can use routing options based on your requirements. Configure the standard and specific routes (with usernames) to ensure that no matter how the called party is addressed (a number or username), the SBC routes the message to the Core. Create Route entries for standard Trunk Group routing with Matching Criteria and a Routing Label destination.

### Route 1

Figure 80:

Host: 172.16.100.216 @ 4330  
Master (SWE) - V14.01.00R000

View: Standard Route    Close All    Perspective: Full View

Entity Type: <None>

Not Applicable

Not Applicable

Not Applicable

Call Parameter Filter Profile: <None>

Call Parameter Filter Profile Group: <None>

Destination National: 5555511111

Destination Country: 1 - USA, Canada and Caribbean

Domain Name: <None>

IP Address: . . .

Partition: DEFAULT

Routing Label: SIPREC\_RL1

Call Type

Transmission Medium

- Speech
- 3.1 KHz Audio
- 7.0 KHz Audio
- 56 kbps
- 64 kbps
- Packet
- Multirate
- 384 kbps
- 1536 kbps

All Call Type Bits

Time Range: ALL

## Route 2

Figure 81:

Entity Type: <None>

Not Applicable

Not Applicable

Not Applicable

Call Parameter Filter Profile: <None>

Call Parameter Filter Profile Group: <None>

Destination National: 2222222222

Destination Country: 1 - USA, Canada and Caribbean

Domain Name: <None>

IP Address: . . .

Partition: DEFAULT

Routing Label: SIPREC\_RL2

Call Type

Transmission Medium

- Speech
- 3.1 KHz Audio
- 7.0 KHz Audio
- 56 kbps
- 64 kbps
- Packet
- Multirate
- 384 kbps
- 1536 kbps

All Call Type Bits

Time Range: ALL

## Configuring SIPRec

The PSX uses the following configurable objects when determining whether a call needs to be recorded or not:

- Recording Criteria contain the rules to match for invoking call recording (this is the same for SIPREC and MCT).
- SRS Groups contains multiple Recording profiles for SRS redundancy (up to 8).
  - Transport

- IP V4/V6 address port
- Encryption data (for SRTP)
- IP TG to be used by the SBC for RS session
- Contains data of multiple SRS servers
- Recording Cluster profile contains multiple SRS Groups for simultaneous recording (up to 4).

## NICE Trunk Group

Create Trunk Group in PSX for SIPRec with the same name created above using SBC CLI. Duplicate default IP Signaling Profile and Packet Service Profile and map it to NICE TG.

Figure 82:

Trunk Group:	SIPREC_TG4	<input type="checkbox"/> Unrestricted
Gateway:	SBCPOOJA	
Description:		
Auto Recall Profile:	<None>	
Call Processing Localization Variant:	North America	
Calling Area:	<None>	
Carrier:	0000	
Carrier Selection Priority:	<None>	
Country:	1 - USA, Canada and Caribbean	
DDI Range Profile:	<None>	
Destination Switch Type:	Access	
Direction:	Two Way	
Element Routing Priority Profile:	SIPREC	
Feature Control Profile:	DEFAULT_IP	
IP Signaling Profile:	SIPREC_IPSP	
LATA:	<None>	
Local Recursion Profile:	<None>	
Maximum Satellite Hops:	Three or More Satellite Hops	
Network Data Partition:	0	
Network Data Net:	0	
Next Hop Domain:	<None>	
Number Analysis Profile:	<None>	
Number Length Enforcement:	<None>	
Originating Carrier:	<None>	

Figure 83:

PPR Profile:	<None>
Pseudo Carrier:	<None>
Remote Sip Peer Type:	None
Region:	<None>
Routing Criteria Profile:	<None>
SCP Business Service Group:	0
Signaling Profile:	DEFAULT_IP_PROFILE
Signaling Flag:	GR394 ISUP
SIP Domain:	<None>
SIP Response Code Profile:	<None>
TDM Type:	Other
Tone And Announcement Profile:	<None>
Trunk Group COS:	
Trunk Group COS Profile:	<None>
Trunk Group Domain:	<None>
Trunk Number:	
Zone Index Profile:	<None>
ZZ Profile:	<None>
Charge Band Profile:	<None>
Enum Domain Profile:	<None>
Flexible Variable Rule:	<None>

Figure 84:

STI Profile: <None>

P-Origination-ID:   Autogenerate

RPH Signaling Profile: <None>

Beep Tone Profile: <None>

STI Generic Profile: <None>

IPSP Generic Profiles: <None>

Context Info

Ingress

Charge Indicator: None

Default CPC: <None>

Default OLIP: <None>

Dial Plan Profile: <None>

Forced OLIP Value: <None>

In DM/PM Rule: <None>

Info Transfer Capability Profile: <None>

IP Version Preference: IPv4 Only

ONI:

JIP:

NPA:

Numbering Plan: NANP\_ACCESS

In Policy Profile Group: <None>

Figure 85:

CVT Rule: <None>

Service Detect Policy Profile Group: <None>

Flags

Allow Hex Digits In Cdpn  Non-Zero Video Bandwidth Based Routing for H.323

Discard NPDI  Non-Zero Video Bandwidth Based Routing for SIP

Discard RN  Overlap Dialing

HD Preferred Routing  TNS Circuit Code Based Routing

HD Supported Routing  Use IPTG Routing (Hop By Hop Routing) For Ingress

Egress

Charge Indicator: None

Out DM/PM Rule: <None>

Out Policy Profile Group: <None>

CVT Rule: <None>

Trunk Context:

R-URI Host:  R-URI Host Port: 0

Flags

Disable Crankback

Enable JIP Interwork

Use Preferred Identity

Send STI Verified Display Name

Figure 86:

<b>Billing</b>	
Billing Plan:	<None>
Billing Information:	<None>
Default Billing Number:	
Nature Of Address:	<None>
Numbering Plan Indicator:	<None>
<b>Calling Party Number</b>	
Calling Party:	
Nature Of Address:	<None>
Numbering Plan Indicator:	<None>
Presentation:	<None>
Screening:	<None>
Default Presentation:	<None>
<b>Flags</b>	
<input checked="" type="checkbox"/> Do Not Use For Fallback Bearer Capability	<input type="checkbox"/> Out Of Service
<input type="checkbox"/> Escaped	<input type="checkbox"/> Satellite Trunk
	<input type="checkbox"/> Use Sac NonSac Call Types For ZZ Profile
<b>IP TG</b>	
IP Signaling Peer Group:	SIPREC_PEER2
	<input checked="" type="checkbox"/> IP Peer Supported
Packet Service Profile ID Group:	SIPREC_EGRESS1

**Figure 87:**

<input checked="" type="checkbox"/> Egress IP Signaling Profile:	SIPREC_IPSP
<b>Packet Service Profile</b>	
Preferred Packet Service Profile ID Group:	<None>
	<input type="checkbox"/> Destination Override
<b>Traffic Management Options</b>	
Trunk Group Reservation Level 1:	10
Trunk Group Reservation Level 2:	5
<b>VPN Information</b>	
Business Group:	<None>
Business Location:	<None>
	<input type="checkbox"/> Business Group From CLI
<b>Services</b>	
<input checked="" type="radio"/> Not Screened	<input type="radio"/> Screened - Normal
	<input type="radio"/> Screened - Fraud
Class Of Service:	<None>
Service Exception Profile:	<None>
<b>Use SIP in Core</b>	
Inter Gateway IP Signaling Profile:	<None>
Egress IP Signaling Profile:	<None>
<b>SIP Used in Core</b>	
Inter Gateway IP Signaling Profile:	<None>
Egress IP Signaling Profile:	<None>

## SRS Cluster

An SRS is the target to which the SBC sends session recordings. The SBC supports configuring multiple SRS' on the PSX using SRS Group Profiles. SRS Cluster contains multiple SRS Groups for simultaneous recording (up to 4).

**Figure 88:**

SRS Group Cluster Id: SRSCLUSTER\_1

Description:

Sequence Number: 0

SRS Group Id: SRSPROFILE\_1

Add/Update

Sequence Number	SRS Group Id
0	SRSPROFILE_1

## SRS Group Profile

Provide NICE recorder, primary and secondary IPv4 or IPv6 address and port (5060). Also, mention the NICE TG name. The name of the NICE TG created in the SBC and the PSX should be the same, otherwise recording would not be initiated toward NICE. Transport type can be set to UDP/TCP/TLS. We have to configure appropriate transport at NICE for successful recordings. Please refer to [NICE transport configurations](#) for NICE specific configurations

To enable SRTP, we can choose CryptoSuite from the dropdown. For more details refer [Media Encryption](#)



1. NICE SRS IP and port details should be configured as per customer deployment.
2. Transport preference mentioned in SRS Group profile should match transport preferences in Trunk Group towards SIPRec zone.

Figure 89:

SRS Group Profile ID: SRSPROFILE\_1

Description:

SRS Group Properties

Number Of Simultaneous Stream: 1

Load Distribution:  Sequence  RoundRobin

SRS Server Properties

Sequence Number: 3

Trunkgroup ID: SIPREC\_TG4

Crypto Suite Profile: SIPREC\_CRYPTO

IPv4 Address: 3 . 3 . 3 . 3 Port V4 Number: 5060

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port V6 Number: 0

Server FQDN:  Port Number: 0

SRS Server Transport:  UDP  TCP  TLS

Enable SRTP

Add/Update

Sequence Number	SRS IP/FQDN Address	Port	Transport	Trunkgroup ID	Crypto Suite ID
0	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPTO
1	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPTO
2	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPTO
3	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPTO

## Call Recording Criteria

Provide call criteria for recording which you wish to record, like calling number, called number, ingress and egress TG, SBC name, the leg you want to record, and either ingress or egress. Recorder type should be SIPRec. Enable the criteria. When a call is made, it shall be recorded if it falls under this criteria.

Figure 90:

Call Recording Criteria: CRC\_SIPREC1

SRS Group Cluster: SRSCLUSTER\_1

Ingress Trunk Group Id: <None>

Egress Trunk Group Id: <None>

Calling Party Id:

Called Party Id:

Next Hop IPv4 Signaling Address: 0 . 0 . 0 . 0

Next Hop IPv6 Signaling Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Previous Hop IPv4 Signaling Address: 0 . 0 . 0 . 0

Previous Hop IPv6 Signaling Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

GSX Name: SBCSYAM1

Recording Type: Ingress Leg

Recording Stop Criteria: 0  Manual  Number Of Calls

Recording Duration: 0

Recorder Type: SIPRec

Beep Tone Profile: <None>

Criteria Enabled

## Call Forking to two Active recorders

Configure Number of Simultaneous Stream to "2", for SBC to stream media simultaneously to two **Active** SRSs.

 Use this configuration only when you have two independent NICE recorder setups with both configured SRSs running in Active mode.

Figure 91:

SRS Group Profile ID: SRSPROFILE\_1

Description:

SRS Group Properties

Number Of Simultaneous Stream: 1

Load Distribution:  Sequence  RoundRobin

SRS Server Properties

Sequence Number: 3

Trunkgroup ID: SIPREC\_TG4

Crypto Suite Profile: SIPREC\_CRYPT0

IPv4 Address: 3 . 3 . 3 . 3 Port V4 Number: 5060

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port V6 Number: 0

Server FQDN: Port Number: 0

SRS Server Transport:  UDP  TCP  TLS

Enable SRTP

Add/Update

Sequence Number	SRS IP/FQDN Address	Port	Transport	Trunkgroup ID	Crypto Suite ID
0	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
1	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0

## Redundancy with Active-Standby SRSs

With the SRS redundancy solution, the integration includes two SRS, where one is active (primary-SRS1) and the standby is inactive (secondary-SRS2). If the primary SRS fails, then the secondary SRS becomes active.



Ribbon recommends NICE to be configured with Failback disabled. Refer to [NICE configuration for NoFailback mode](#) for additional NICE configuration changes.

With Failback disabled, If the primary SRS fails, the secondary SRS becomes active. When the primary SRS comes back up, the secondary SRS remains active and the primary server becomes inactive.

### Sequential Forking

When the number of simultaneous streams is set to 1, the SBC shall start streaming to active SRS with lowest sequence number[SRS1]. If the SRS1 goes down, the SBC blacklists the SRS1 and the SBC automatically uses the next active SRS - SRS2 in the SRS group. Refer to [NICE Configurations for Sequential Forking](#) for additional NICE configuration changes.



With below pathcheck profile configuration, the SBC blacklists unreachable SRS servers as well as Standby SRS servers[based on 5xx response for OPTIONS]. So, the SBC is responsible for detecting SRS failures and initiating a new session to SRS for both ongoing and new calls.

In the pathcheck profile associated to SRS IP peers, we configure **failureResponseCodes** parameter to define 5xx response codes from Standby SRS server to treat as failure response. So, the SBC blacklists Standby SRS to avoid creating new recording sessions to the inactive SRS.

```
set profiles services pathCheckProfile sip_recording1 protocol sipOptions
set profiles services pathCheckProfile sip_recording1 sendInterval 10
set profiles services pathCheckProfile sip_recording1 replyTimeoutCount 3
set profiles services pathCheckProfile sip_recording1 recoveryCount 1
set profiles services pathCheckProfile sip_recording1 failureResponseCodes [ all5xx ]
set profiles services pathCheckProfile sip_recording1 transportPreference preference1 tls-tcp
comm
```

Figure 92:

The screenshot shows the configuration for an SRS Group Profile. The SRS Group Profile ID is SRSPROFILE\_1. The SRS Group Properties section shows the Number Of Simultaneous Stream set to 1 and Load Distribution set to Sequence. The SRS Server Properties section shows the Sequence Number set to 3, Trunkgroup ID set to SIPREC\_TG4, and Crypto Suite Profile set to SIPREC\_CRYPT0. The SRS Server Transport is set to TLS, and SRTTP is enabled. Below the configuration fields is a table of SRS servers.

Sequence Number	SRS IP/FQDN Address	Port	Transport	Trunkgroup ID	Crypto Suite ID
0	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
1	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
2	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
3	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0

### Parallel Forking

When the number of simultaneous stream is set to "2", the SBC sends two streams to primary[SRS1] and secondary[SRS2] SRS.Redundancy is handled by the SRS internally to detect SRS failure and handle the existing sessions. The SBC connects with SRS1 with active SDP with Active recording and SRS2 with inactive SDP.If SRS1 goes down, SRS2 sends a re-INVITE with active SDP (AIR IP details)to SBC to continue recording via SRS2. Refer [NICE Configurations for Parallel Forking](#) for additional NICE configuration changes.

In the pathcheck profile associated to SRS IP peers, the SBC blacklists only if there is no response from SRS. Any response from SRS is considered as an active response.

```

set profiles services pathCheckProfile sip_recording1 protocol sipOptions
set profiles services pathCheckProfile sip_recording1 sendInterval 10
set profiles services pathCheckProfile sip_recording1 replyTimeoutCount 3
set profiles services pathCheckProfile sip_recording1 recoveryCount 1
set profiles services pathCheckProfile sip_recording1 transportPreference preferencel tls-tcp
comm

```

**Figure 93:**

SRS Group Profile ID: SRSPROFILE\_1

Description:

SRS Group Properties

Number Of Simultaneous Stream:

Load Distribution:  Sequence  RoundRobin

SRS Server Properties

Sequence Number:

Trunkgroup ID: SIPREC\_TG4

Crypto Suite Profile: SIPREC\_CRYPTO

IPv4 Address:  .  .  .  Port V4 Number:

IPv6 Address:  :  :  :  :  :  :  :  Port V6 Number:

Server FQDN:  Port Number:

SRS Server Transport:  UDP  TCP  TLS

Enable SRTP

Sequence Number	SRS IP/FQDN Address	Port	Transport	Trunkgroup ID	Crypto Suite ID
0	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPTO
1	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPTO

## Quad Recording

TheSBC is enhanced to support simultaneously recording SIP egress and ingress legs during a session, for a total of four recordings (four simultaneous streams: two in the ingress leg, and two in the egress leg).

TheSBC provisions the SIP recordings towards all four recorders, two from Ingress tap point and another two from egress tap point. (Due to NP limitations, four simultaneous recordings cannot be triggered on the same call leg.)



- The SBC supports sending the recording streams to up to four SRS servers simultaneously.
- Each recording criteria can be configured with a Recording Cluster. A Recording Cluster can have up to four SRS Groups.
- For Quad SIPREC, there are four recordings triggered. Two recordings are triggered on the Ingress leg and two on the Egress leg.
- If there is more than one SRS Group configured, it is recommended to set `recordingType` to "both legs" or "all legs".
- When SIPREC is selected as the Recorder Type, and Recording Type is selected as both legs and all legs, the SBC by default records the ingress leg.

Create four SRS profiles with one SRS entry in each profile.



Please note we need four NICE recorder setups with all four configured SRSs running in Active mode.

**Figure 94:**

SRS Group Cluster Id: SRSCLUSTER\_1  
 Description:

Sequence Number: 3

SRS Group Id: SRSPROFILE\_4

Add/Update

Sequence Number	SRS Group Id
0	SRSPROFILE_1
1	SRSPROFILE_2
2	SRSPROFILE_3
3	SRSPROFILE_4

Figure 95:

SRS Group Profile ID: SRSPROFILE\_1  
 Description:

SRS Group Properties

Number Of Simultaneous Stream: 1

Load Distribution:  Sequence  RoundRobin

SRS Server Properties

Sequence Number: 1

Trunkgroup ID: SIPREC\_TG4

Crypto Suite Profile: SIPREC\_CRYPT0

IPv4 Address: 3 . 3 . 3 . 3 Port V4 Number: 5060

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port V6 Number: 0

Server FQDN:  Port Number: 0

SRS Server Transport:  UDP  TCP  TLS

Enable SRTP

Add/Update

Sequence Number	SRS IP/FQDN Address	Port	Transport	Trunkgroup ID	Crypto Suite ID
0	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0

## Media Encryption

The Secure Real-time Transport Protocol (Secure RTP or SRTP) is an IETF cryptographic protocol used to provide secure communications over untrusted networks as described in RFC 3711. SRTP provides confidentiality, message authentication, and replay protection to Internet media traffic such as audio and video. TheSBC SWe Core supports Secure RTP and its associated secure real-time transport control protocol (Secure RTCP) for IPv4/IPv6 addressing for both audio and video streams.

## Towards Endpoint

To enable sRTP towards endpoints, Crypto suite profiles must be configured in Packet service profiles mapped towards Ingress and Egress Trunks.

Figure 96:

Secure RTP/RTCP

Crypto Suite Profile: SIPREC\_CRYPT0

Flags

Allow Fallback  Enable SRTP

Reset ROC On Session Key Change  Reset Enc/Dec/ROC on Decryption Key Change

Update Crypto On Modify  Allow Pass Through

Add crypto suites to the crypto profile and save it.

Figure 97:

Crypto Suite Profile: SIPREC\_CRYPT0

Description:

Crypto Suites

Sequence: 0

Crypto Suite: AES CM 128 HMAC SHA1 32

Session Parameter Flags

Unauthenticated SRTP  Unencrypted SRTP

Unencrypted SRTCP

Add/Update

Sequence	Crypto Suite
0	AES CM 128 HMAC SHA1 32

## Towards NICE SIP Recorder

To enable encryption towards SIPRec, Crypto suite profiles are attached to SRS Group Profiles.

Check Enable sRTP check box in SRS Profile and select Crypto Suite Profile from the drop down list.

Figure 98:

SRS Group Profile ID: SRSPROFILE\_1

Description:

SRS Group Properties

Number Of Simultaneous Stream: 1

Load Distribution:  Sequence  RoundRobin

SRS Server Properties

Sequence Number: 3

Trunkgroup ID: SIPREC\_TG4

Crypto Suite Profile: SIPREC\_CRYPT0

IPv4 Address: 3 . 3 . 3 . 3 Port V4 Number: 5060

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port V6 Number: 0

Server FQDN: Port Number: 0

SRS Server Transport:  UDP  TCP  TLS

Enable SRTP

Add/Update

Sequence Number	SRS IP/FQDN Address	Port	Transport	Trunkgroup ID	Crypto Suite ID
0	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
1	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
2	2.2.2.2	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0
3	3.3.3.3	5060	TLS	SIPREC_TG4	SIPREC_CRYPT0

Add crypto suites to the crypto profile and attach it to the SRS group profile.

NICE supports two sRTP crypto suites AES\_CM\_128\_HMAC\_SHA1\_80 and AES\_CM\_128\_HMAC\_SHA1\_32.

Figure 99:

Crypto Suite Profile: SIPREC\_CRYPT0

Description:

Crypto Suites

Sequence: 0

Crypto Suite: AES CM 128 HMAC SHA1 32

Session Parameter Flags

Unauthenticated SRTP  Unencrypted SRTP

Unencrypted SRTCP

Add/Update

Sequence	Crypto Suite
0	AES CM 128 HMAC SHA1 32

# Ribbon SBC SWe Core High Availability

## Info

During this interop, SBC SWe was configured in HA mode with the below configuration for High Availability.

In an HA configuration, the two SBC VMs are connected to each other using the HA ports on the respective VMs. The HA logical ports must be in the same network and routable using the switch and they must be connected to a switch. Failure of the connection is via link detection and also TIPC keep-alives.

## HA Configuration Link Detection Group

The Link Detection Group allows you to group interfaces and associated Link Monitors together and track link verification failures within the group. A Link Detection Group (LDG) is configured with a unique name and a failover threshold. The LDG tracks the number of link verification failures that have occurred among the Link Monitors configured.

Create Link Detection Groups for both pkt0 and pkt1 interfaces.

```
set addressContext default linkDetectionGroup pkt0_act_ldg ceName SBCPOOJA1
set addressContext default linkDetectionGroup pkt0_act_ldg type ip
set addressContext default linkDetectionGroup pkt0_act_ldg threshold 1
set addressContext default linkDetectionGroup pkt0_act_ldg state enabled
set addressContext default linkDetectionGroup pkt0_act_ldg linkMonitor pkt0_act_lm interfaceGroup IG1
set addressContext default linkDetectionGroup pkt0_act_ldg linkMonitor pkt0_act_lm interface IF1
set addressContext default linkDetectionGroup pkt0_act_ldg linkMonitor pkt0_act_lm destination
<pkt0_default_gateway>
set addressContext default linkDetectionGroup pkt0_act_ldg linkMonitor pkt0_act_lm state enabled
set addressContext default linkDetectionGroup pkt0_stb_ldg ceName SBCPOOJA2
set addressContext default linkDetectionGroup pkt0_stb_ldg type ip
set addressContext default linkDetectionGroup pkt0_stb_ldg threshold 1
set addressContext default linkDetectionGroup pkt0_stb_ldg state enabled
set addressContext default linkDetectionGroup pkt0_stb_ldg linkMonitor pkt0_stb_lm interfaceGroup IG1
set addressContext default linkDetectionGroup pkt0_stb_ldg linkMonitor pkt0_stb_lm interface IF1
set addressContext default linkDetectionGroup pkt0_stb_ldg linkMonitor pkt0_stb_lm destination
<pkt0_default_gateway>
set addressContext default linkDetectionGroup pkt0_stb_ldg linkMonitor pkt0_stb_lm state enabled
set addressContext default linkDetectionGroup pkt1_act_ldg ceName SBCPOOJA1
set addressContext default linkDetectionGroup pkt1_act_ldg type ip
set addressContext default linkDetectionGroup pkt1_act_ldg threshold 1
set addressContext default linkDetectionGroup pkt1_act_ldg state enabled
set addressContext default linkDetectionGroup pkt1_act_ldg linkMonitor pkt1_act_lm interfaceGroup IG2
set addressContext default linkDetectionGroup pkt1_act_ldg linkMonitor pkt1_act_lm interface IF2
set addressContext default linkDetectionGroup pkt1_act_ldg linkMonitor pkt1_act_lm destination
<pkt1_default_gateway>
set addressContext default linkDetectionGroup pkt1_act_ldg linkMonitor pkt1_act_lm state enabled
set addressContext default linkDetectionGroup pkt1_stb_ldg ceName SBCPOOJA2
set addressContext default linkDetectionGroup pkt1_stb_ldg type ip
set addressContext default linkDetectionGroup pkt1_stb_ldg threshold 1
set addressContext default linkDetectionGroup pkt1_stb_ldg state enabled
set addressContext default linkDetectionGroup pkt1_stb_ldg linkMonitor pkt1_stb_lm interfaceGroup IG2
set addressContext default linkDetectionGroup pkt1_stb_ldg linkMonitor pkt1_stb_lm interface IF2
set addressContext default linkDetectionGroup pkt1_stb_ldg linkMonitor pkt1_stb_lm destination
<pkt1_default_gateway>
set addressContext default linkDetectionGroup pkt1_stb_ldg linkMonitor pkt1_stb_lm state enabled
comm
```

## NICE Configuration

For detailed NICE configurations, please visit official NICE support page <http://www.extranice.com/>.

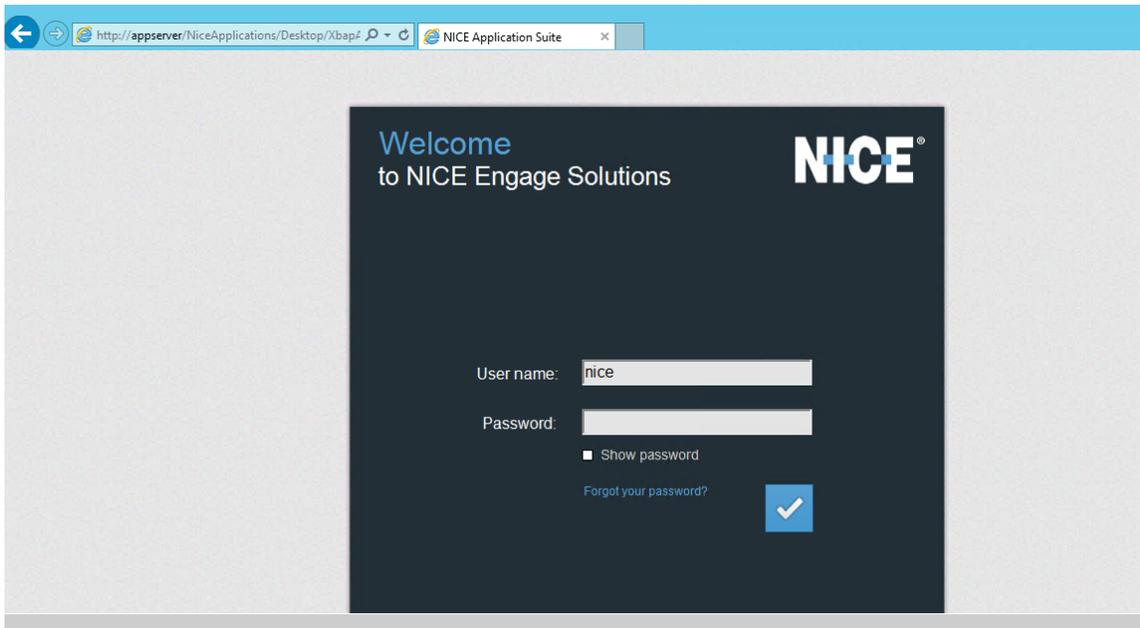
As a part of this document, we have highlighted specific NICE configuration changes that were used in our testing.

 Please note that the configurations mentioned below were used in our lab environment for testing purposes. Each customer may have unique needs and configurations. Ribbon recommends that customers work with NICE engineers for NICE configurations to best meet their requirements.

## Application Server

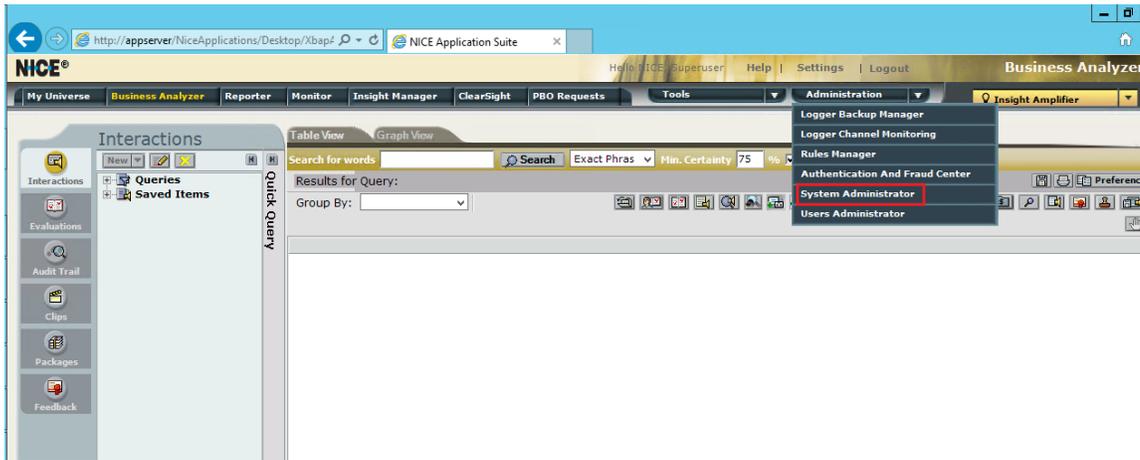
Use the below login page to access NICE application server for all the NICE configurations.

**Figure 100:**



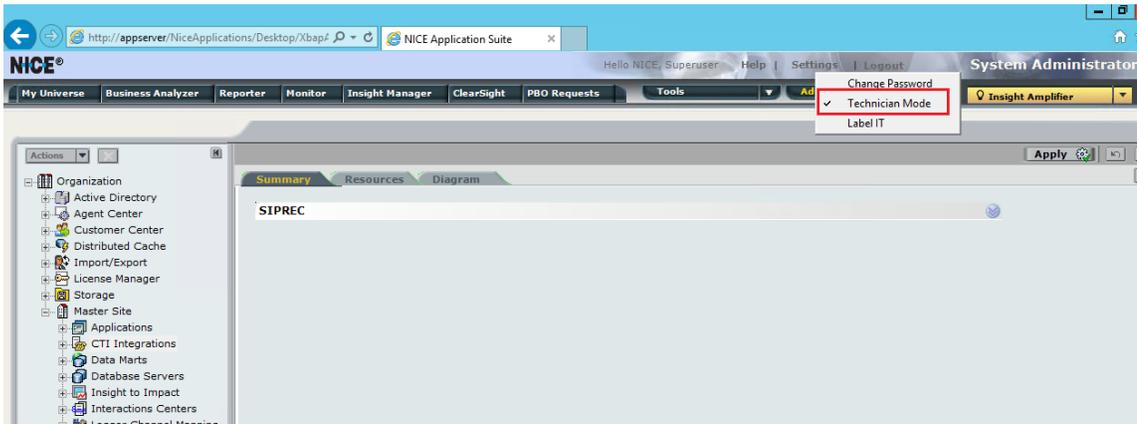
After login, Select System Administrator from the dropdown as mentioned below to check NICE configurations.

**Figure 101:**



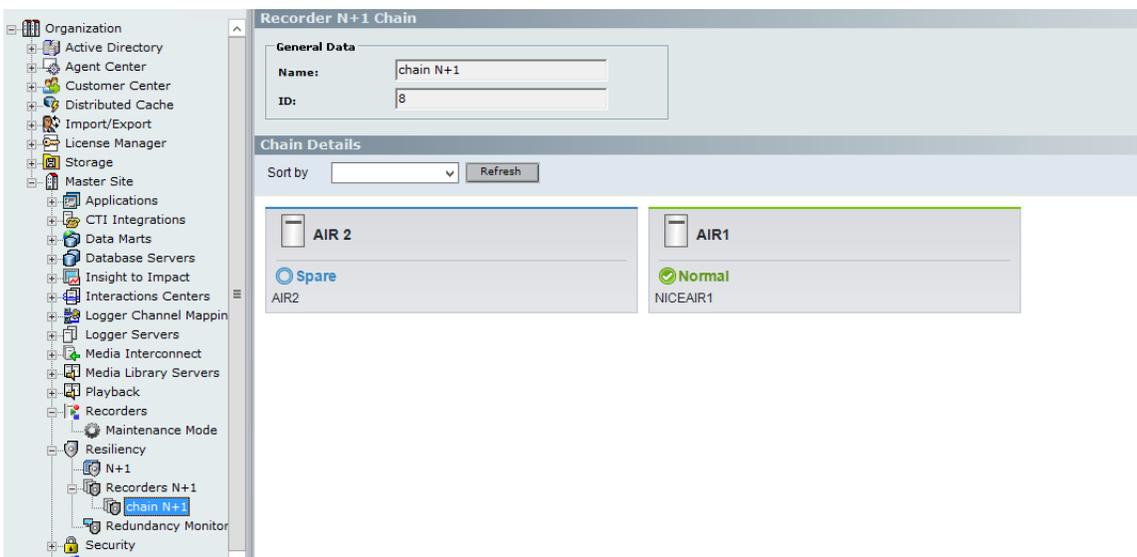
Once logged in as System Administrator, Check Enable Technician Mode from the drop down as mentioned below to edit any configurations.

**Figure 102:**



To check Active and Standby AIR servers, go to Master Site > Resiliency > Recorders N+1 > chain N+1.

**Figure 103:**



## Metadata Support

### Support for Metadata type 'sonus'

When siprecmetadata profile is not configured, by default the SBC supports backward compatibility and pre-defined metadata for passing proprietary call specific information from the SRC to the SRS.

In order to configure NICE server to support default Ribbon SBC configurations, Go to:

- Master Site > CTI Integrations > Media Provider Controllers > Additional Media Provider Controller Parameters > MetadataType > sonus
- Click Save
- In the CTI Integrations branch, click Apply



- Please repeat the above steps for both the VRSP servers.
- Restart NICE Integration Dispatch Service on both the VRSP servers.

### Support for Metadata type 'RFC7865'

When siprecmetadata profile version is set to 1, Ribbon SBC supports RFC 7865.

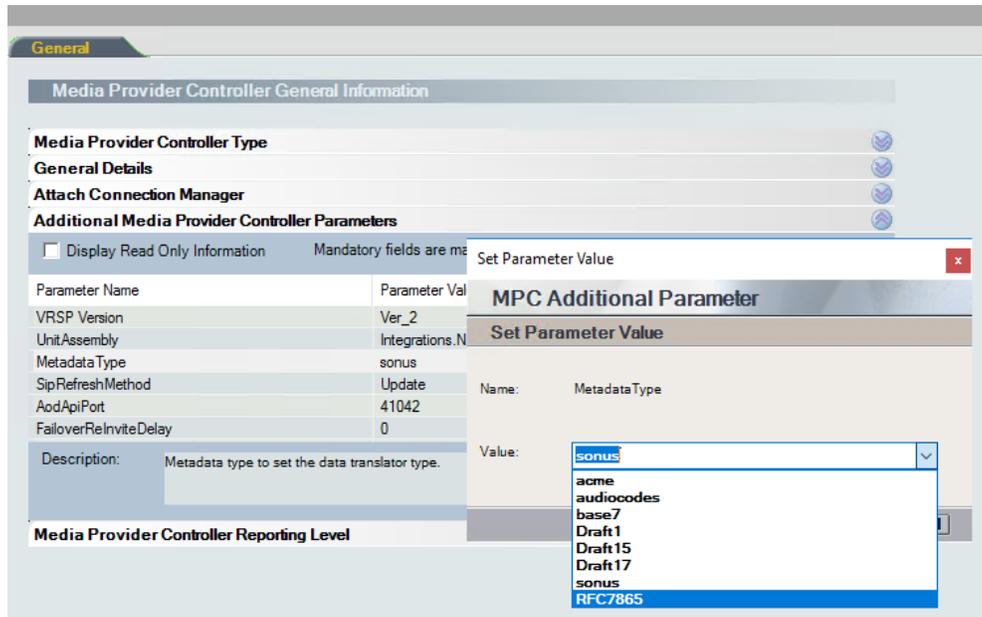
In order to configure NICE server to support RFC7865, Go to:

- Master Site > CTI Integrations > Media Provider Controllers > Additional Media Provider Controller Parameters > MetadataType > RFC7865
- Click Save
- In the CTI Integrations branch, click Apply



- Please repeat the above steps for both the VRSP servers.
- Restart NICE Integration Dispatch Service on both the VRSP servers.

Figure 104:



## VRSP NoFailback mode

In order to change configuration at NICE server, Go to:

- Master Site >CTI integration > Media Provider Controller tab > VRSP[A/S]CTI integration > Media Provider Controller tab > VRSP[A/S] > RunningMode > NOFAILBACK
- Click Save
- In the CTI Integrations branch, click Apply



- Please repeat the above steps for both the VRSP servers.
- Restart NICE Integration Dispatch Service on both the VRSP servers.

Figure 105:

<b>RedundancyIsEnabled</b>	<b>Yes</b>
<b>SrvPosition</b>	<b>Primary</b>
<b>RunningMode</b>	<b>NOFAILBACK</b>
<b>RedundancyRemoteIpAddress</b>	<b>172.16.106.221</b>
<b>RedundancyRemotePort</b>	<b>50501</b>

Figure 106:

<b>RedundancyIsEnabled</b>	<b>Yes</b>
<b>SrvPosition</b>	<b>Secondary</b>
<b>RunningMode</b>	<b>NOFAILBACK</b>
<b>RedundancyRemoteIpAddress</b>	<b>172.16.106.223</b>
<b>RedundancyRemotePort</b>	<b>50501</b>

## Transport Configurations

VRSP configurations

For UDP/TCP,Go to:

- Master Site > CTI Integrations > Media Provider Controllers > Additional Media Provider Controller Parameters > SipStackTlsEnabled > NO
- Click Save
- In the CTI Integrations branch, click Apply

For TLS, Go to:

- Master Site > CTI Integrations > Media Provider Controllers > Additional Media Provider Controller Parameters > SipStackTlsEnabled > YES
- Master Site > CTI Integrations > Media Provider Controllers > Additional Media Provider Controller Parameters > SipStackTlsCertificateSerialNumber > serial number of the NICE VRSP certificate
- Click Save
- In the CTI Integrations branch, click Apply

 • Please repeat the above steps for both the VRSP servers.

Figure 107:

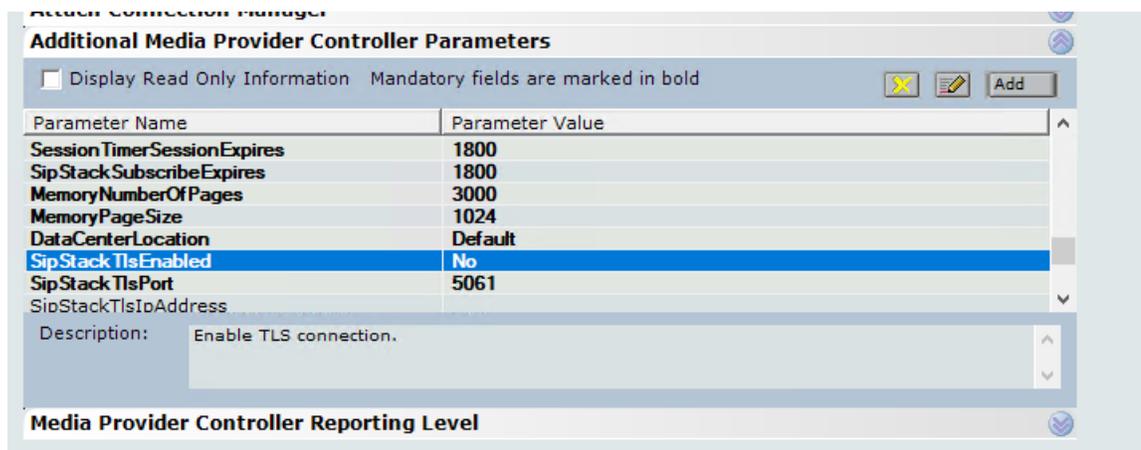
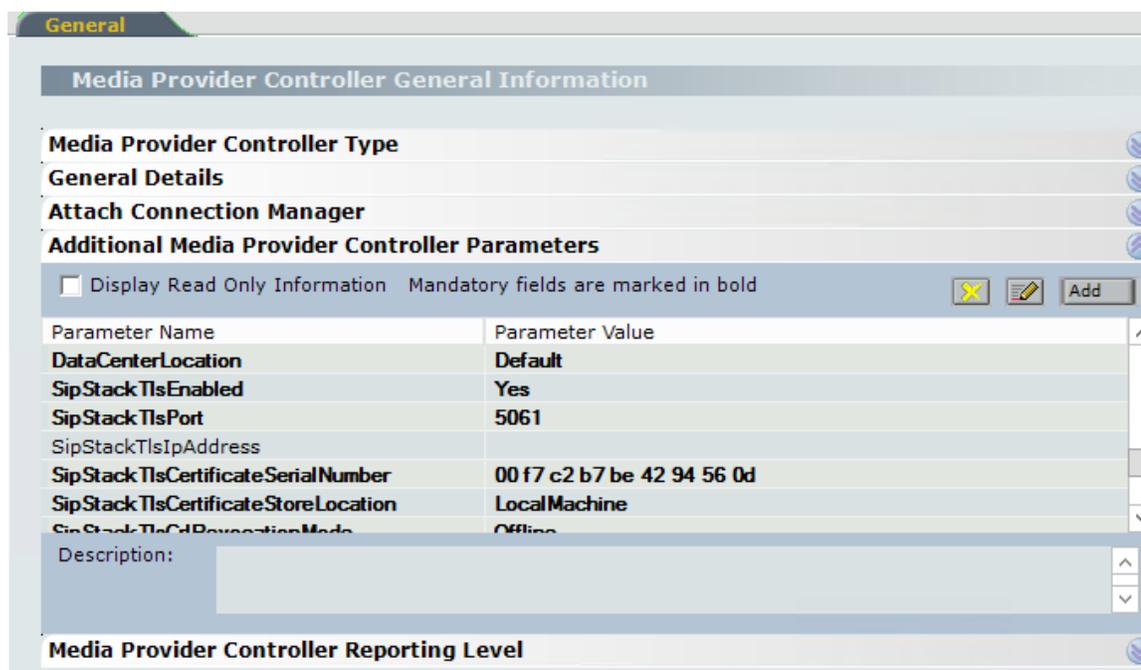


Figure 108:



## AIR configurations for UDP with RTP

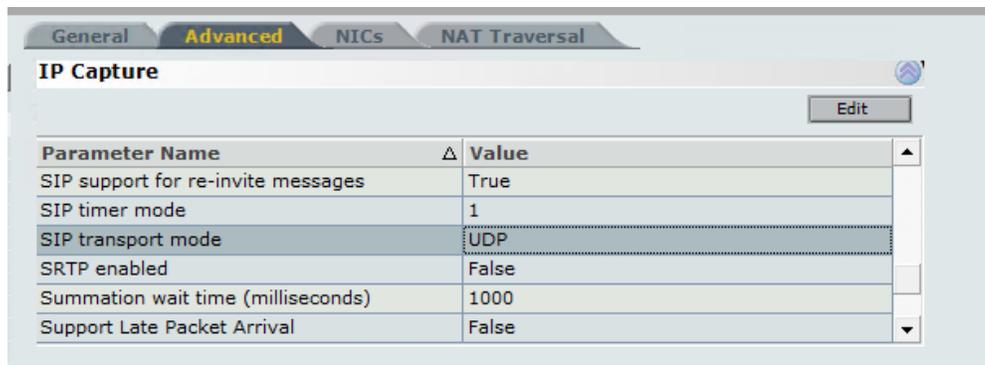
In order to change transport settings at NICE server, Go to:

- Master Site > Recorders -> AIR[A/S] > Advanced tab > IP Capture > SIP transport mode > UDP
- Master Site > Recorders -> AIR[A/S] > Advanced tab > IP Capture > SRTP enabled > False
- Click Save

- In the CTI Integrations branch, click Apply

**i** • Please repeat the above steps for both the AIR servers.

Figure 109:



### AIR configurations for TLS with sRTP

In order to change configuration at NICE server, Go to:

- Master Site > Recorders > AIR[A/S] > Advanced tab > IP Capture > SIP transport mode > TLS
- Master Site > Recorders > AIR[A/S] > Advanced tab > IP Capture > SRTP enabled > True
- Master Site > Recorders > AIR[A/S] > Advanced tab > IP Capture > Certificate serial > serial number of the NICE AIR certificate
- Click Save
- In the CTI Integrations branch, click Apply

**i** Please repeat the above steps for both AIR servers.

Figure 110:

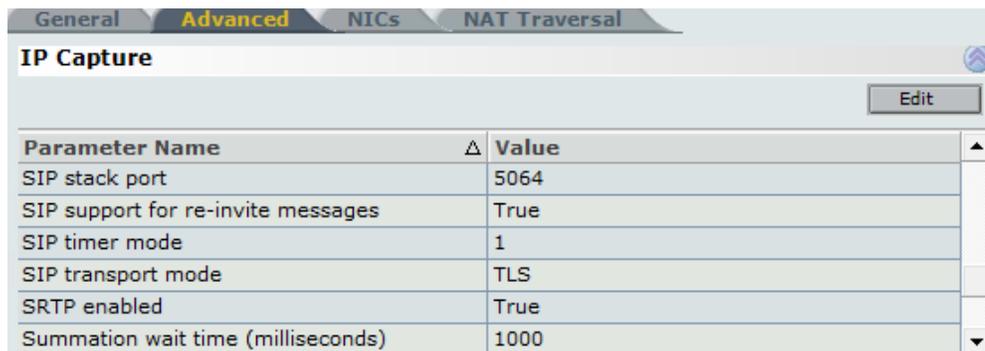
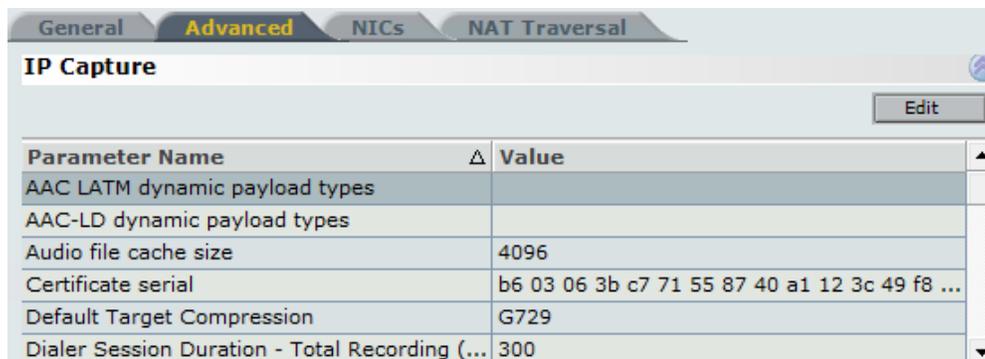


Figure 111:



**i** For Transport changes to be effective:

- Restart NICE Integration Dispatch Service on both the VRSP servers.
- Restart NICE Interactions Center RCM service on Interactions Center server.
- Restart NICE IP Capture and NICE Recorder Administrator services on both AIR servers.

## Sequential Forking

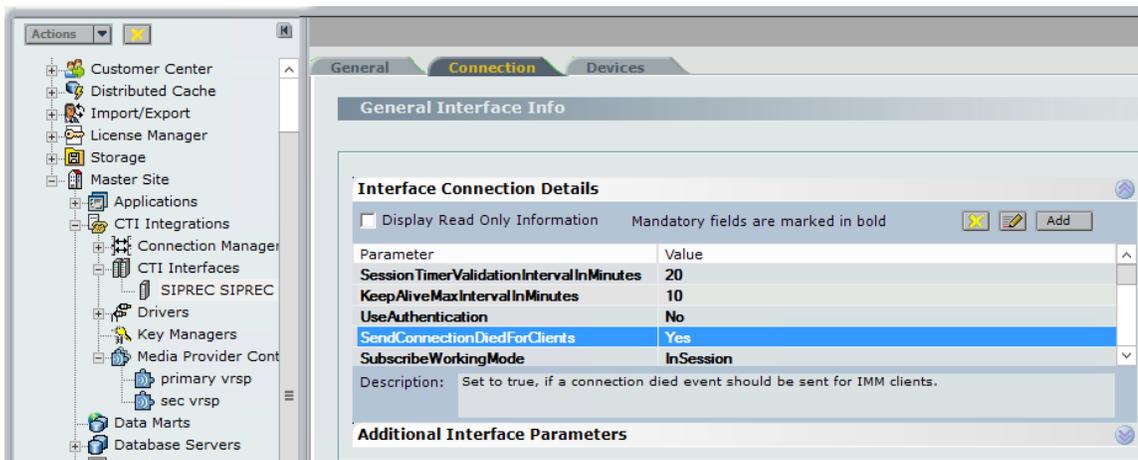
In order to change configuration at NICE server, Go to:

- Master Site > CTI Integrations > Media Provider Controller tab > VRSP[A/S] > Additional Media Provider Controller Parameters > RunningMode > NoFailback
- Master Site > CTI Integrations > CTI Interfaces > Connection > Interface Connection Details > SendConnectionDiedForClients > Yes
- Click Save
- In the CTI Integrations branch, click Apply

**i** For Transport changes to be effective:

- Restart NICE Integration Dispatch Service on both the VRSP servers.
- Restart NICE IP Capture and NICE Recorder Administrator services on both AIR servers.

Figure 112:



## Parallel Forking

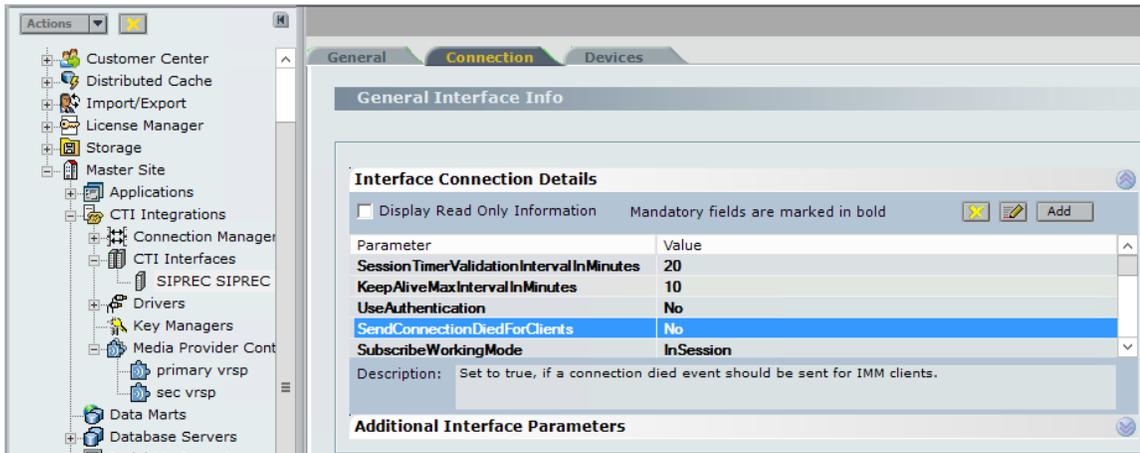
In order to change configurations at NICE server, Go to:

- Master Site > CTI Integrations > Media Provider Controller tab > VRSP[A/S] > Additional Media Provider Controller Parameters > RunningMode > NoFailback
- Master Site > CTI Integrations > CTI Interfaces > Connection > Interface Connection Details > SendConnectionDiedForClients > No
- Master Site > Integration Centers > IC\_Server > Configuration > Call Server > op\_MaxOpenCallDuration /op\_MaxOpenCompoundCallDuration > Desired timeout for long call duration.
- Click Save
- In the CTI Integrations branch, click Apply

**i** For Transport changes to be effective:

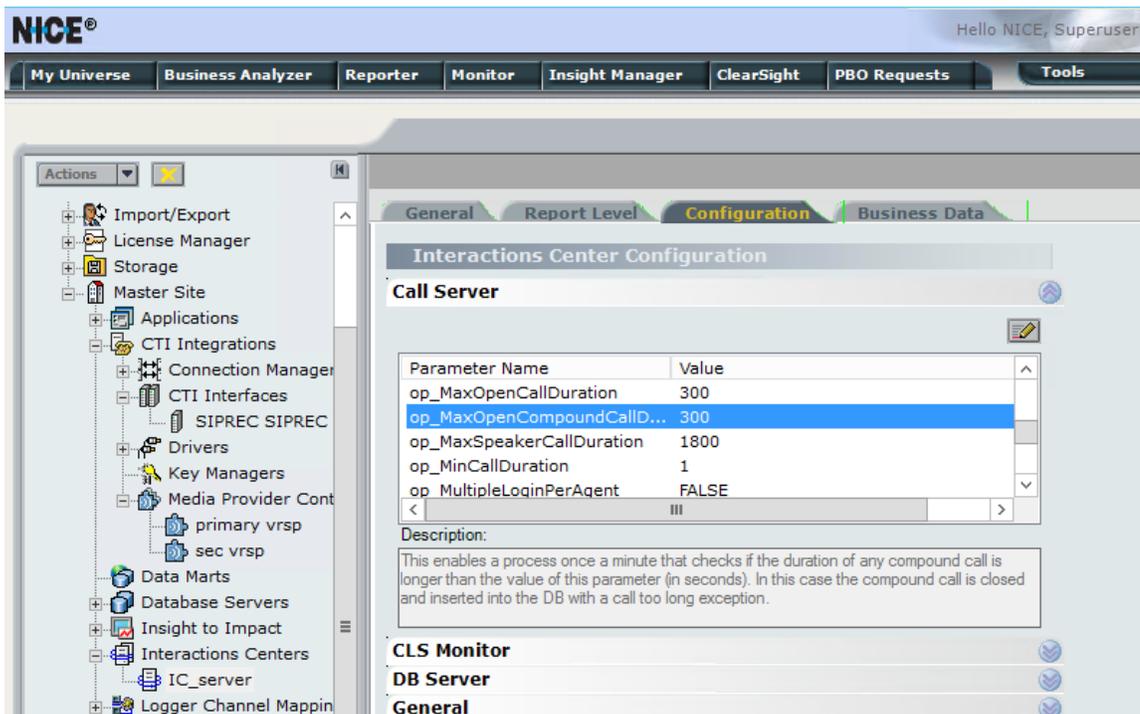
- Restart NICE Integration Dispatch Service on both the VRSP servers.
- Restart NICE Interactions Center Core and NICE Interactions Center RCM services on Interactions Center server.
- Restart NICE IP Capture and NICE Recorder Administrator services on both AIR servers.

Figure 113:



**i** Please note the timeouts captured in the snapshots were configured solely for the purpose of testing. Please tune this timeout as per specific business needs.

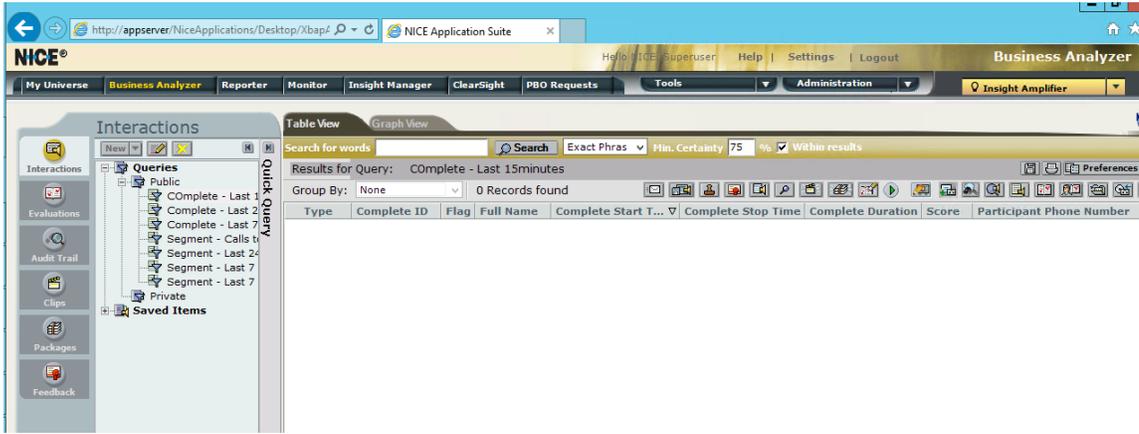
Figure 114:



## NICE Business Analyzer

Use NICE Business Analyzer to view/query/listen to recordings created.

Figure 115:



## 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	Call Recording via CLI	✓
3	DTMF - RFC2833/ Inband	✓
4	DTMF - SIP INFO	✗
5	Call Hold/ Resume	✓
6	Call Transfer (Blind/ Unattended)	✓
7	Call Transfer (Attended)	✓
8	Session Refresh	✓
9	Call Forward No Answer	✓
10	Conference	✓
11	Transcoding	✓
12	Music On Hold	✓
13	TLS with SRTP	✓
14	SIPRec Call Forking	✓
15	Quad Recording	✓
16	HA SBC switchover	✓
17	SRS Redundancy - Sequential Forking	✓
18	SRS Redundancy - Parallel Forking	✓

### Legend

Supported	✓
-----------	---

Not Supported



## Caveats

---

Ribbon:

- SIPRec leg goes to Inactive state after call transfer with REFER processed on SBC while recording type is set to either "Egress" or "Ingress."
- SBC sends two different session\_id's for single call towards Active and Standby NICE SRS servers. During NICE VRSP failover scenarios, NICE recorder is unable to map the two sessions to a single interaction. As a workaround to avoid any recording loss, at NICE, we configure op\_MaxOpenCompoundCallDuration/op\_MaxOpenCallDuration". NICE will push open interactions handled by failed SRS server to NBA as a new file after this configured timeout [default 5 hours].

Nice:

- Upon NICE VRSP failover, it may take up to three minutes (default) for AIR to refresh the session and retrieve keys from secondary VRSP. This may result in failure to decrypt and open any new calls for up to three minutes ("white noise" + exception on the interaction).

## Support

---

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

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

## References

---

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

## Conclusion

---

This Interoperability Guide describes successful configuration of Ribbon SBC SWe Core& PSX with NICE SIP Recorder.

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.