Oracle SBC integration with Assertion SecureVoice

Technical Application Note

ORACLE

COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.

Revision History

Version	**Description of Changes**	**Date Revision Completed**
1.0	Initial Draft	12th December 2024

1 Table of Contents

2 Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It's assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with integrating UC and CC systems, Sip Trunking Services and Assertion Secure Voice.

3 Document Overview

This Application Note guides users through the process of configuring Oracle SBC to integrate with Assertion's SecureVoice. The document covers the full operational configuration of the Oracle SBC, including network settings, service parameters, and security configurations. The solution has been validated using Oracle Communication SBC with OS930p1

4 About Assertion SecureVoice

Assertion SecureVoice (hereafter referred also as Assertion Defender in this document) protects your enterprise contact center and SIP Remote Workers from Scam, Robo, Junk Calls and any voice threats. Assertion SecureVoice detects, reports and blocks voice threats in real time and SecureVoice works with almost all CC and UC vendors**.**

The Key features of Assertion SecureVoice is listed below:

- Detect number spoofing attempts to protect from ransomware attack and voice phishing (scam).
- Targeted routing of suspicious scam calls to trained agents / attendants.
- Detect and block brute force, extension enumeration and other attacks on the SIP remote worker infrastructure.
- TDoS protection to safeguard from call spikes which could result in customers not being able to connect to you.
- Monitor usage, choking and rejections in outbound and inbound traffic to provide an early warning to ensure smooth operations.

In addition, it should be noted that the configuration provided in this guide focuses mainly on the Oracle SBC related parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

For additional information on **Assertion SecureVoice**, please visit,

https://assertion.cloud/securevoice/

5 Introduction

5.1 Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Oracle Enterprise SBC. There will be steps that require navigating the Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

5.2 Requirements

- Fully functioning UC/CC Platform.
- Fully functioning Assertion SecureVoice (Assertion Defender and Scanner) Software.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.3.0 version.

Note: For deployment and configuration of Assertion Defender and Scanner, please contact your Assertion Account team. The Assertion team will provide necessary guidance and support throughout the process.

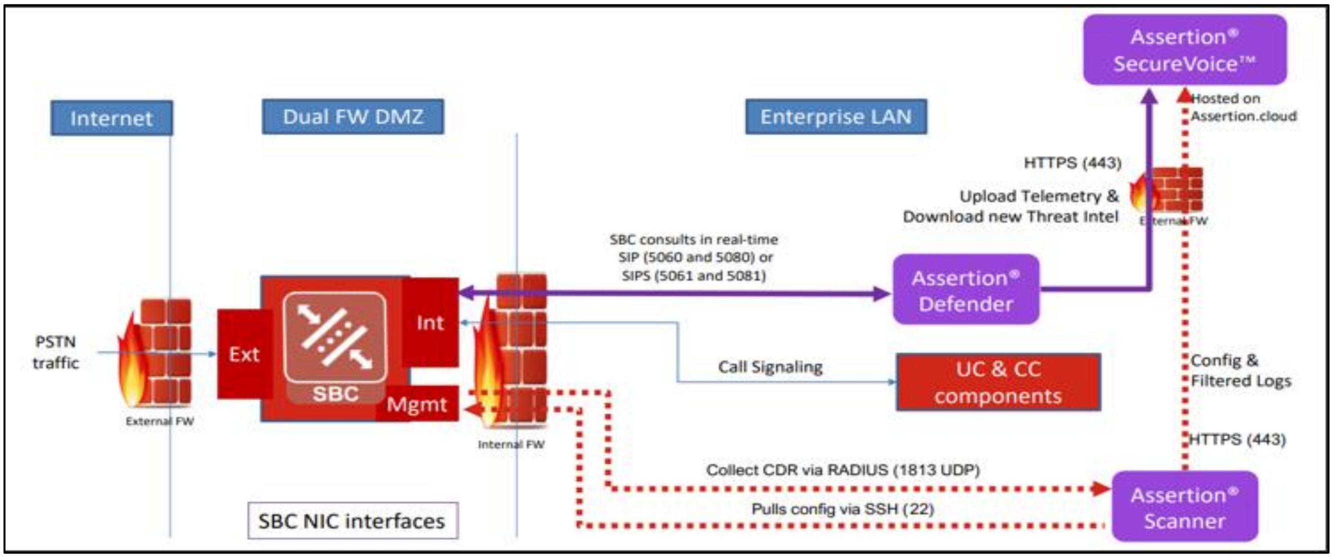
The below revision table explains the versions of the software used for each component:
This table is Revision 1 as of now:

Software Used	SBC Version
Revision 1	9.3.0

5.3 Architecture

Security Scan Approach

Assertion SecureVoice uses two on-prem components; Assertion Scanner to collect the CDR from Oracle SBC and Assertion Defender to provide real-time session enforcement. The Scanner and the Defender send data to the cloud for advanced analytics.



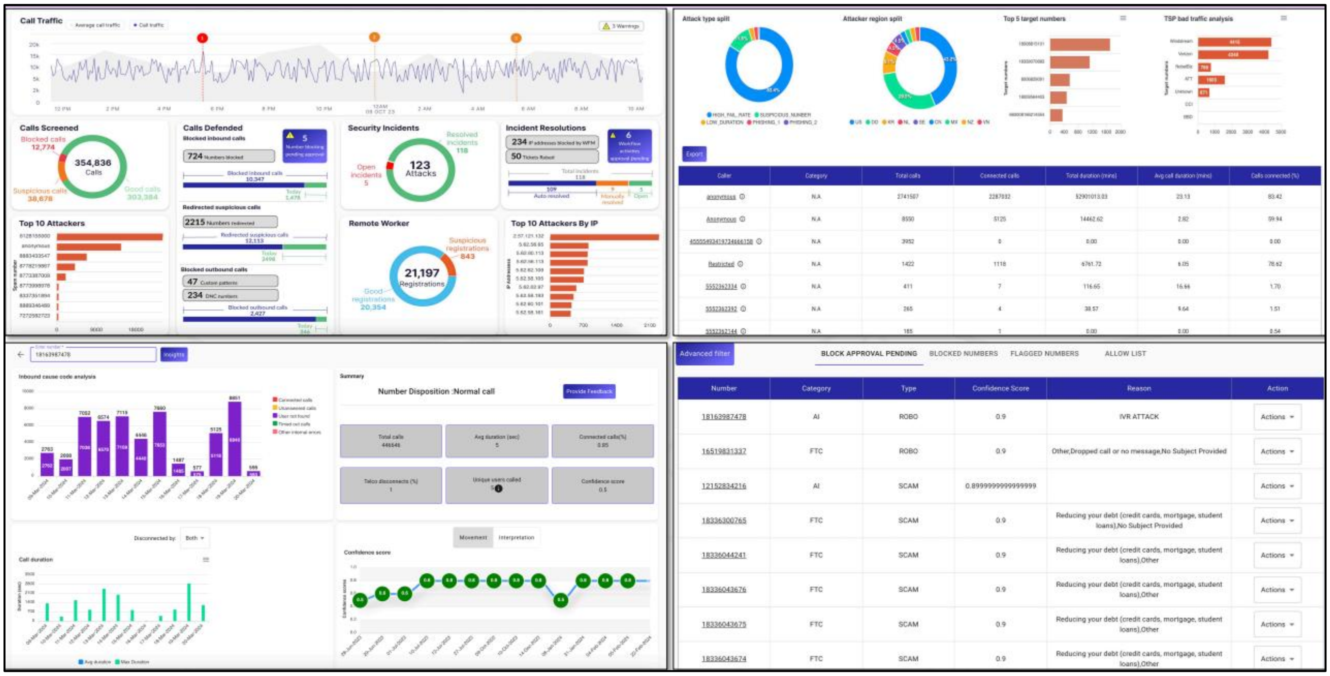
Defender is consulted during call setup and "redirects" acceptable calls. It is not on the signaling path of connected calls and never in the media path.

5.4 Assertion Hardware, Software and Network Requirements

Minimum 2 VMs - 1 Scanner and 1 Defender

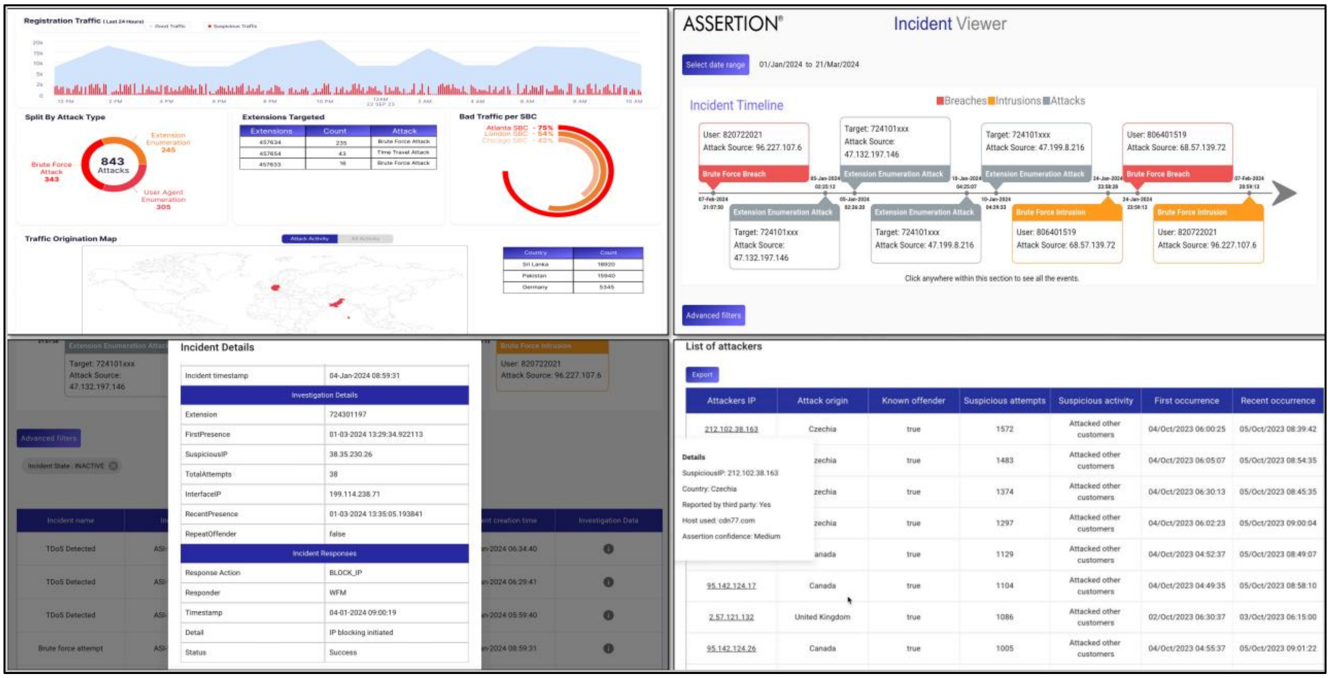
- Assertion Scanner has the following requirements:
- — Hardware requirements – VM with 8GB RAM, 4 vCPU * 2.2GHz, free disk space of 150 GB.
- — Software requirements – OVA provided with RHEL 8.x/9.x. Customer to provide license.
- — Network – 2 NIC cards, 1Gbps
- Assertion Defender has the following requirements:
- — Hardware requirements – VM with 8GB RAM, 4 vCPU * 2.2GHz, free disk space of 150 GB.
- — Software requirements – OVA provided with RHEL 8.x/9.x. Customer to provide license.
- — Network – 2 NIC cards, 1Gbps

5.5 Assertion Portal Product Screens



Caller	Category	Total calls	Connected calls	Total duration (mins)	Avg call duration (mins)	Calls connected (%)
anonymous ⓘ	N.A	2741507	2287032	52901013.03	23.13	83.42
Anonymous ⓘ	N.A	8550	5125	14462.62	2.82	59.94
4555549341973466158 ⓘ	N.A	3952	0	0.00	0.00	0.00
Restricted ⓘ	N.A	1422	1118	6761.72	6.05	78.62
5552362334 ⓘ	N.A	411	7	116.65	16.66	1.70
5552362392 ⓘ	N.A	265	4	38.57	9.64	1.51
5552362144 ⓘ	N.A	185	1	0.00	0.00	0.54

Number	Category	Type	Confidence Score	Reason	Action
18163987478	AI	ROBO	0.9	IVR ATTACK	Actions ▾
16519831337	FTC	ROBO	0.9	Other,Dropped call or no message,No Subject Provided	Actions ▾
12152834216	AI	SCAM	0.8999999999999999		Actions ▾
18336300765	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),No Subject Provided	Actions ▾
18336044241	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾
18336043676	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾
18336043675	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾
18336043674	FTC	SCAM	0.9	Reducing your debt (credit cards, mortgage, student loans),Other	Actions ▾



Extensions Targeted

Extensions	Count	Attack
457634	235	Brute Force Attack
457654	43	Time Travel Attack
457633	16	Brute Force Attack

Country	Count
Sri Lanka	18920
Pakistan	15940
Germany	5345

01/Jan/2024 to 21/Mar/2024

- 07-Feb-2024 21:07:50 – Brute Force Breach – User: 820722021 Attack Source: 96.227.107.6
- 05-Jan-2024 00:35:13 – Extension Enumeration Attack – Target: 724101xxx Attack Source: 47.132.197.146
- 05-Jan-2024 02:26:20 – Extension Enumeration Attack – Target: 724101xxx Attack Source: 47.132.197.146
- 10-Jan-2024 04:25:07 – Extension Enumeration Attack – Target: 724101xxx Attack Source: 47.199.8.216
- 10-Jan-2024 04:29:33 – Extension Enumeration Attack – Target: 724101xxx Attack Source: 47.199.8.216
- 24-Jan-2024 23:58:28 – Brute Force Intrusion – User: 806401519 Attack Source: 68.57.139.72
- 24-Jan-2024 23:58:13 – Brute Force Breach – User: 806401519 Attack Source: 68.57.139.72
- 07-Feb-2024 20:58:13 – Brute Force Intrusion – User: 820722021 Attack Source: 96.227.107.6

Click anywhere within this section to see all the events.

Incident Details

Incident timestamp	04-Jan-2024 08:59:31
Investigation Details	
Extension	724301197
FirstPresence	01-03-2024 13:29:34.922113
SuspiciousIP	38.35.230.26
TotalAttempts	38
InterfaceIP	199.114.238.71
RecentPresence	01-03-2024 13:35:05.193841
RepeatOffender	false
Incident Responses	
Response Action	BLOCK_IP
Responder	WFM
Timestamp	04-01-2024 09:00:19
Detail	IP blocking initiated
Status	Success

Incident name	In	nt creation time	Investigation Data
TDoS Detected	ASI	n-2024 06:34:40	ⓘ
TDoS Detected	ASI	n-2024 06:29:41	ⓘ
TDoS Detected	ASI	n-2024 05:59:40	ⓘ
Brute force attempt	ASI	n-2024 08:59:31	ⓘ

List of attackers

Attackers IP	Attack origin	Known offender	Suspicious attempts	Suspicious activity	First occurrence	Recent occurrence
212.102.38.163	Czechia	true	1572	Attacked other customers	04/Oct/2023 06:00:25	05/Oct/2023 08:39:42
	zechia	true	1483	Attacked other customers	04/Oct/2023 06:05:07	05/Oct/2023 08:54:35
	zechia	true	1374	Attacked other customers	04/Oct/2023 06:30:13	05/Oct/2023 08:45:35
	zechia	true	1297	Attacked other customers	04/Oct/2023 06:02:23	05/Oct/2023 09:00:04
	anada	true	1129	Attacked other customers	04/Oct/2023 04:52:37	05/Oct/2023 08:49:07
95.142.124.17	Canada	true	1104	Attacked other customers	04/Oct/2023 04:49:35	05/Oct/2023 08:58:10
2.57.121.132	United Kingdom	true	1086	Attacked other customers	02/Oct/2023 06:30:37	03/Oct/2023 06:15:00
95.142.124.26	Canada	true	1005	Attacked other customers	04/Oct/2023 04:55:37	05/Oct/2023 09:01:22

Details
SuspiciousIP: 212.102.38.163
Country: Czechia
Reported by third party: Yes
Host used: cdn77.com
Assertion confidence: Medium

6 Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC to integrate Assertion SecureVoice with a PSTN service and UC/CC platform.

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons. The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 9.3 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950
- AP 4900
- VME

7 New SBC configuration

If the customer is looking to setup a new SBC from scratch, please follow the sections given below.

As there are many ways to install the SBC (purpose-built appliance, VM, and public cloud deployment), please follow the link given below for the type of install base used to deploy the Oracle SBC.

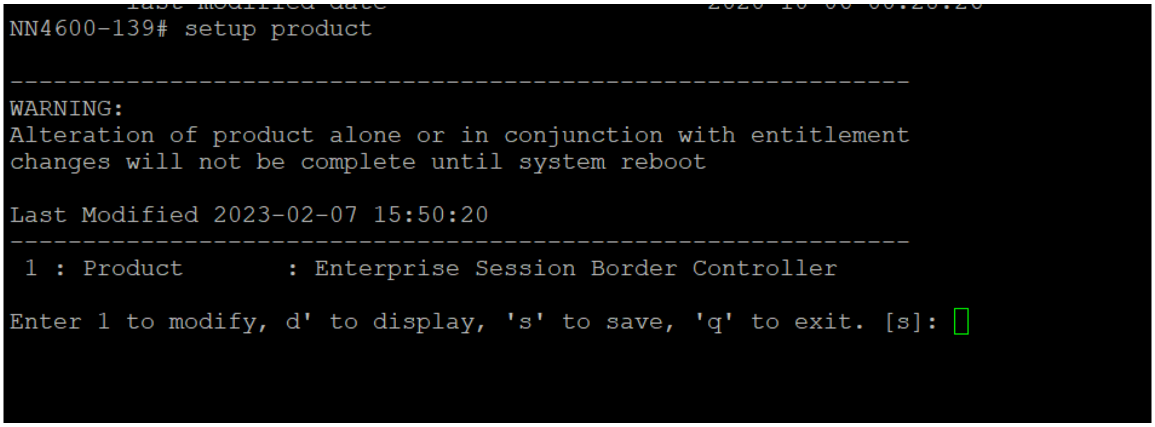
https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/installation/index.html

Once the SBC is installed and logged in, please follow the steps given below.

7.1 Setup product

Setup product type to Enterprise Session Border Controller as shown below.

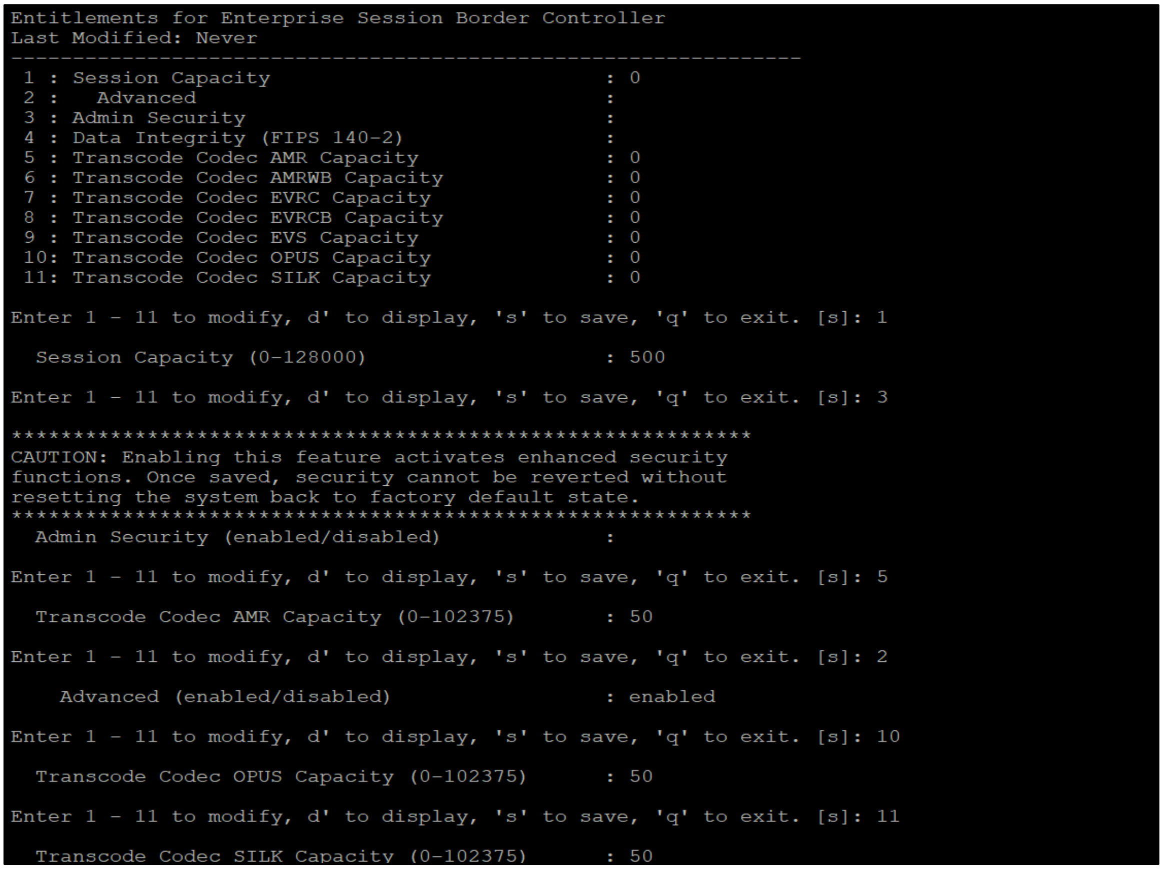
To configure product type, type in “*setup product*” in the terminal



```
NN4600-139# setup product

--------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2023-02-07 15:50:20
--------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]:
```

7.2 Setup Entitlements

Enable features for the ESBC using the “*setup entitlements*” command as shown below.



```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                          : 0
 2 :   Advanced                                :
 3 : Admin Security                            :
 4 : Data Integrity (FIPS 140-2)               :
 5 : Transcode Codec AMR Capacity              : 0
 6 : Transcode Codec AMRWB Capacity            : 0
 7 : Transcode Codec EVRC Capacity             : 0
 8 : Transcode Codec EVRCB Capacity            : 0
 9 : Transcode Codec EVS Capacity              : 0
 10: Transcode Codec OPUS Capacity             : 0
 11: Transcode Codec SILK Capacity             : 0

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-128000)                  : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

************************************************************
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
************************************************************
  Admin Security (enabled/disabled)            :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5

  Transcode Codec AMR Capacity (0-102375)      : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)                : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10

  Transcode Codec OPUS Capacity (0-102375)     : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11

  Transcode Codec SILK Capacity (0-102375)     : 50
```

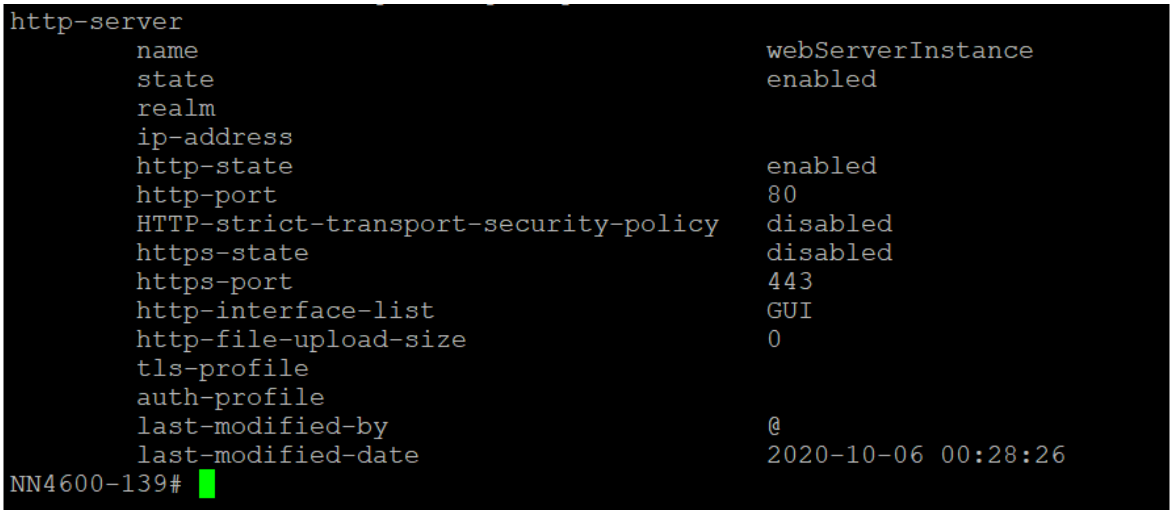
Save changes and reboot the SBC.

The SBC comes up after reboot and is now ready for configuration.

7.3 Enable Management GUI

ALCI Path: config t→system→http-server

Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.



```
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               80
        HTTP-strict-transport-security-policy   disabled
        https-state                             disabled
        https-port                              443
        http-interface-list                     GUI
        http-file-upload-size                   0
        tls-profile
        auth-profile
        last-modified-by                        @
        last-modified-date                      2020-10-06 00:28:26
NN4600-139#
```

7.4 Configure SBC using Web GUI

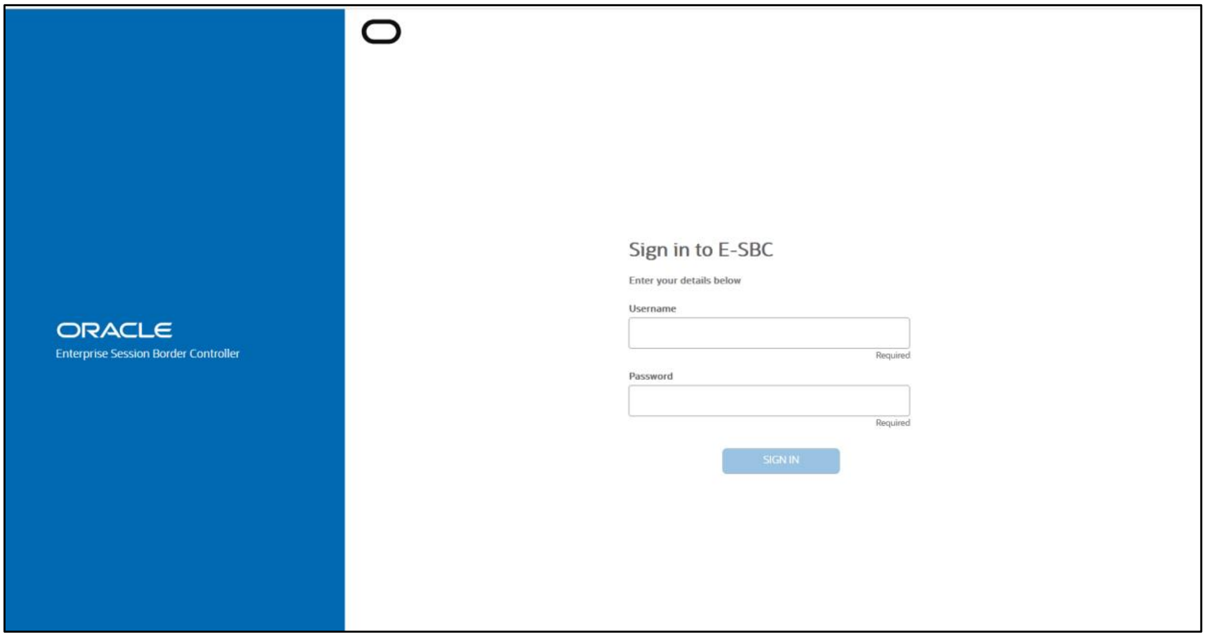
There are two methods for configuring the SBC, ACLI or GUI. For the purposes of this note, we'll be using the SBC GUI for all configuration examples. We will however provide the ACLI path to each element.

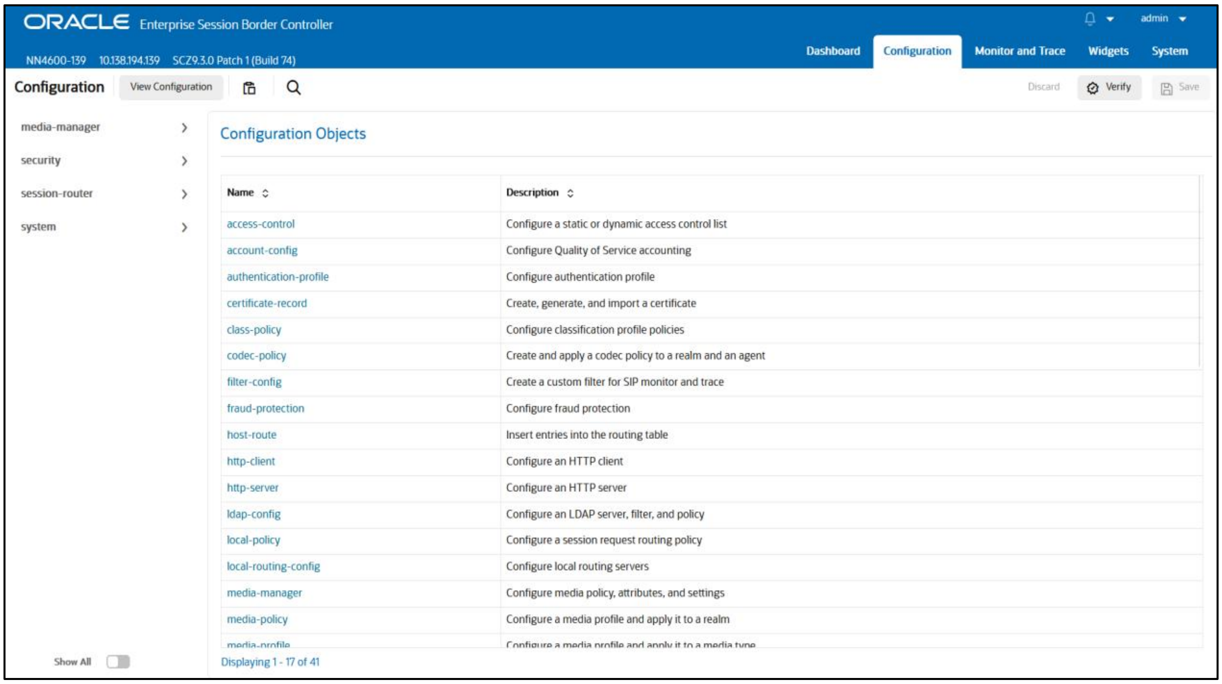
To access the SBC GUI, enter the management IP address into a web brower. When the login screen appears, enter the username and password to access the SBC.

Once you have access to the SBC GUI, at the top, click the Configuration Tab. This will bring up the SBC Configuration Objects List on the left-hand side of the screen.

Any configuration parameter not specifically listed below can remain at the SBC default value and does not require a change for the connection to Assertion Secure Voice to function properly.

Note: the configuration examples below were captured from a system running the latest GA software, 9.3.0





Configuration Objects

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server
ldap-config	Configure an LDAP server, filter, and policy
local-policy	Configure a session request routing policy
local-routing-config	Configure local routing servers
media-manager	Configure media policy, attributes, and settings
media-policy	Configure a media profile and apply it to a realm
media-profile	Configure a media profile and apply it to a media type

Displaying 1 - 17 of 41

Refer to the SBC GUI User Guide for more information:

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/webgui/web-gui-guide.pdf

Note: Expert Mode is used when adding or modifying the SBC configuration

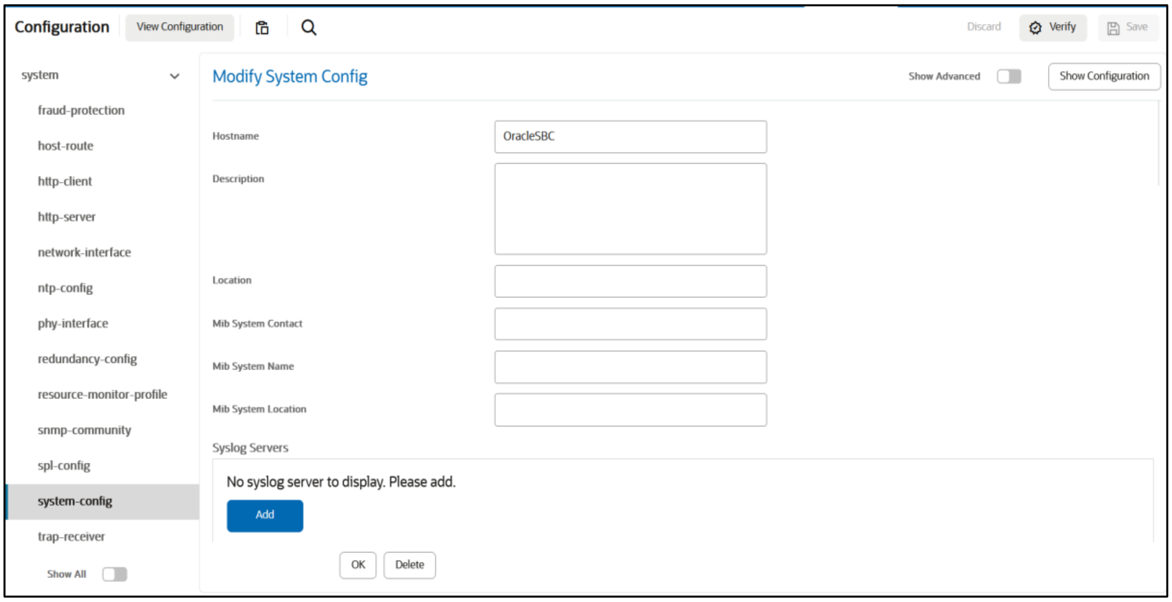
Tip: To make this configuration simpler, directly search the element to be configured from the Objects tab available.

7.5 System-Config

To enable system level functionality for the OCSBC, you must first enable the system-config

GUI Path: system/system-config

ACLI Path: config t→system→system-config



Modify System Config

Hostname: OracleSBC

Description:

Location:

Mib System Contact:

Mib System Name:

Mib System Location:

Syslog Servers

No syslog server to display. Please add.

If media transcoding is required in your environment and the SBC is deployed as VME SBC or in a public cloud, you'll need to enable transcoding cores under the system config element. Please see the document below for more information:

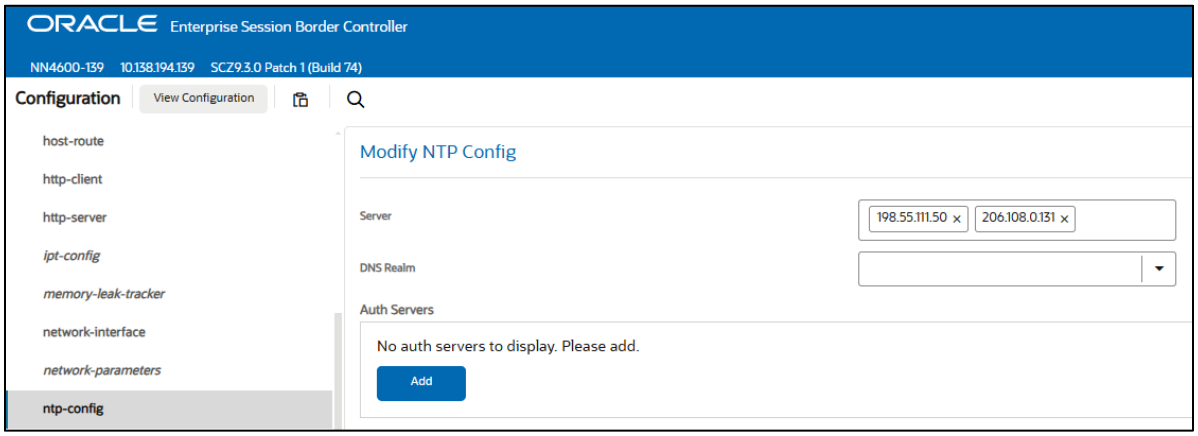
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/releasenotes/esbc-release-notes.pdf

7.5.1 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration but recommended.

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-sync



Modify NTP Config

Server: 198.55.111.50 × 206.108.0.131 ×

DNS Realm:

Auth Servers

No auth servers to display. Please add.

- Select OK at the bottom

Now we'll move on configuring network connections on the SBC.

7.6 Networking configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure three physical interfaces, and three network interfaces. One to communicate with Assertion Secure Voice Platform, one to connect to PSTN Network and a third connection to the UC/CC platform.

Note: The slots and ports used in this example may be different from your network setup.

7.6.1 Physical Interfaces

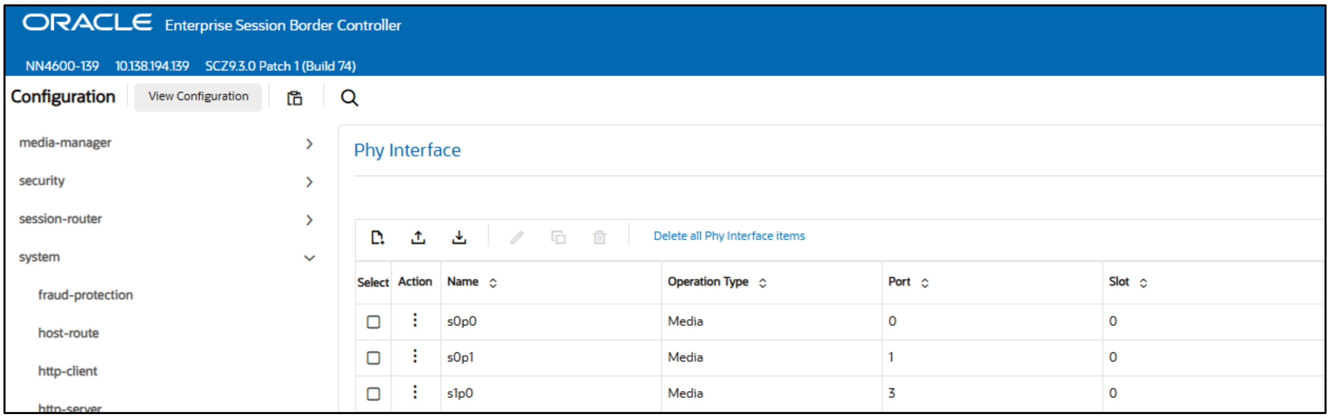
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

- Click Add, use the following table as a configuration example:

Config Parameter	Assertion	PSTN	UC/CC Platform
Name	s1p0	s0p0	s0p1
Operation Type	Media	Media	Media
Slot	1	0	0
Port	0	0	1

Note: Physical interface names, slot and port may vary depending on environment



ORACLE Enterprise Session Border Controller

NN4600-139 10.138.194.139 SCZ9.3.0 Patch 1 (Build 74)

Configuration | View Configuration

media-manager
security
session-router
system
fraud-protection
host-route
http-client
http-server

Phy Interface

Delete all Phy Interface items

Select	Action	Name	Operation Type	Port	Slot
□	⋮	s0p0	Media	0	0
□	⋮	s0p1	Media	1	0
□	⋮	s1p0	Media	3	0

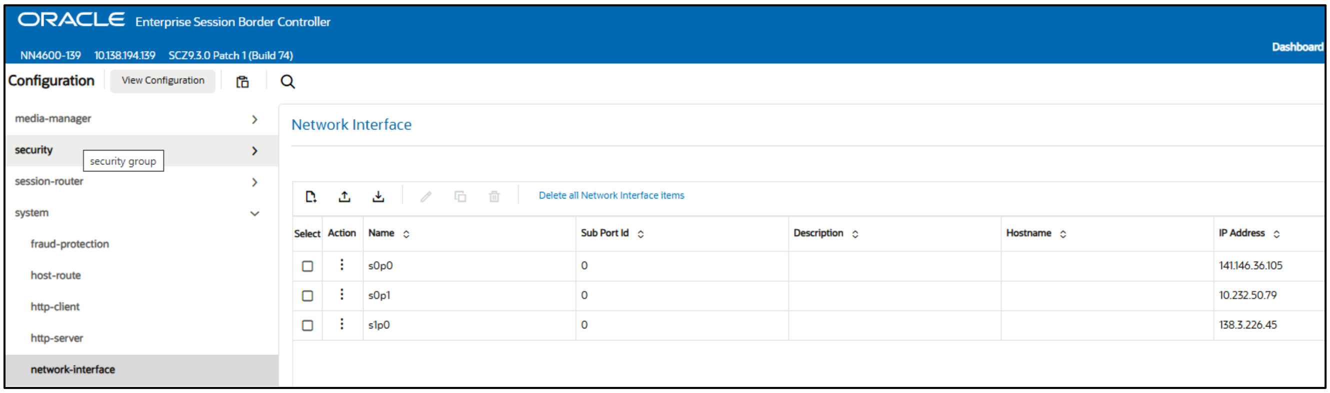
7.6.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

- Click Add, use the following table as a configuration example:

Config Parameter	Assertion	PSTN	UC/CC Platform
Name	s1p0	s0p0	s0p1
IP Address	138.3.226.45	141.146.36.105	10.232.50.79
Netmask	255.255.255.224	255.255.255.192	255.255.255.0
Gateway	138.3.226.33	141.146.36.65	10.232.50.1



Select	Action	Name	Sub Port Id	Description	Hostname	IP Address
□	⋮	s0p0	0			141.146.36.105
□	⋮	s0p1	0			10.232.50.79
□	⋮	s1p0	0			138.3.226.45

Click OK at the bottom of each after entering the config information.

Next we'll configure the necessary elements to setup Media on the SBC.

7.7 Media Configuration

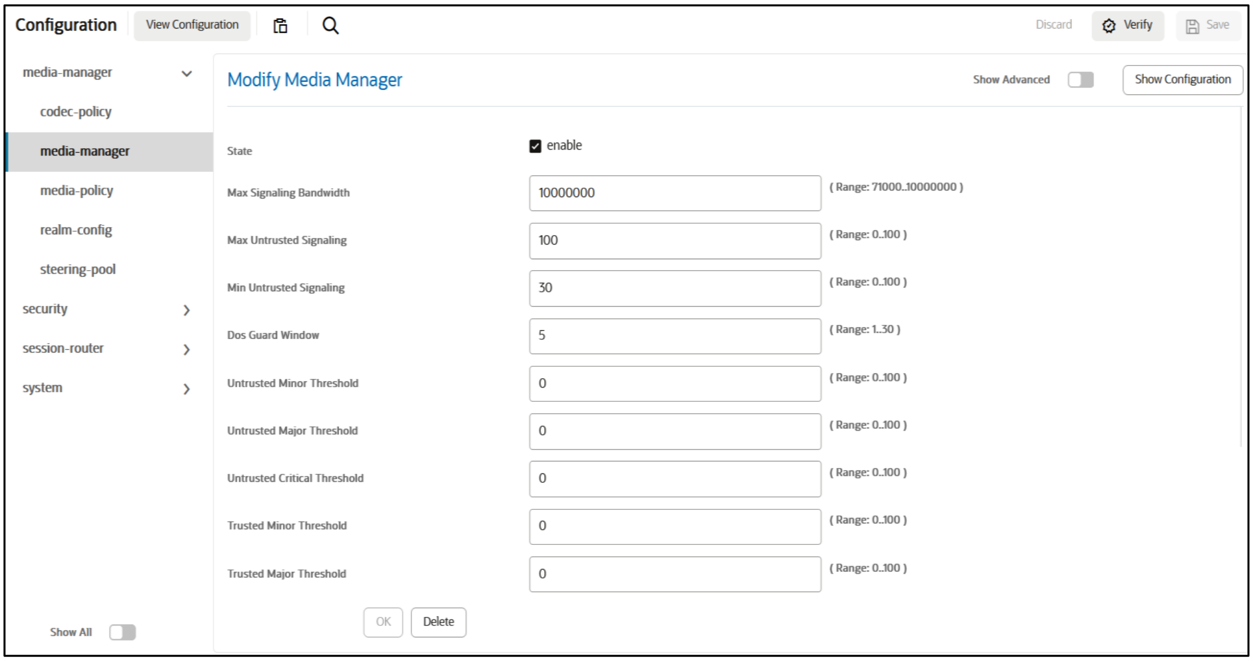
This section will guide you through the configuration of media manager, realms, and steering pools, all of which are required for the SBC to handle signaling and media flows through the SBC.

7.7.1 Media Manager

To configure media functionality on the SBC, you must first enable the global media manager

GUI Path: media-manager/media-manager

ACLI Path: config t→media-manager→media-manager-config



State: ☑ enable

Max Signaling Bandwidth: 10000000 (Range: 71000..10000000)

Max Untrusted Signaling: 100 (Range: 0..100)

Min Untrusted Signaling: 30 (Range: 0..100)

Dos Guard Window: 5 (Range: 1..30)

Untrusted Minor Threshold: 0 (Range: 0..100)

Untrusted Major Threshold: 0 (Range: 0..100)

Untrusted Critical Threshold: 0 (Range: 0..100)

Trusted Minor Threshold: 0 (Range: 0..100)

Trusted Major Threshold: 0 (Range: 0..100)

- Click OK at the bottom.

7.7.2 Realm Config

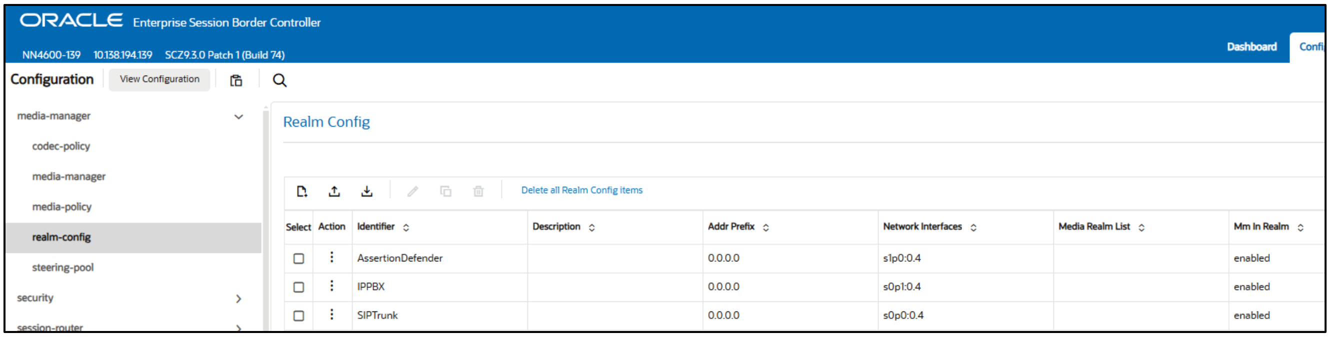
Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

GUI Path; media-manger/realm-config

ACLI Path: config t→media-manger→realm-config

Click Add and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

Config Parameter	Assertion	PSTN	UC/CC Platform
Identifier	Assertion Defender	SIPTrunk	IPPBX
Network Interface	s1p0	s0p0	s0p1
MM in Realm		☑	☑
Access Control trust level	High	High	High



Select	Action	Identifier	Description	Addr Prefix	Network Interfaces	Media Realm List	Mm In Realm
□	⋮	AssertionDefender		0.0.0.0	s1p0:0.4		enabled
□	⋮	IPPBX		0.0.0.0	s0p1:0.4		enabled
□	⋮	SIPTrunk		0.0.0.0	s0p0:0.4		enabled

- Select OK at the bottom of each.

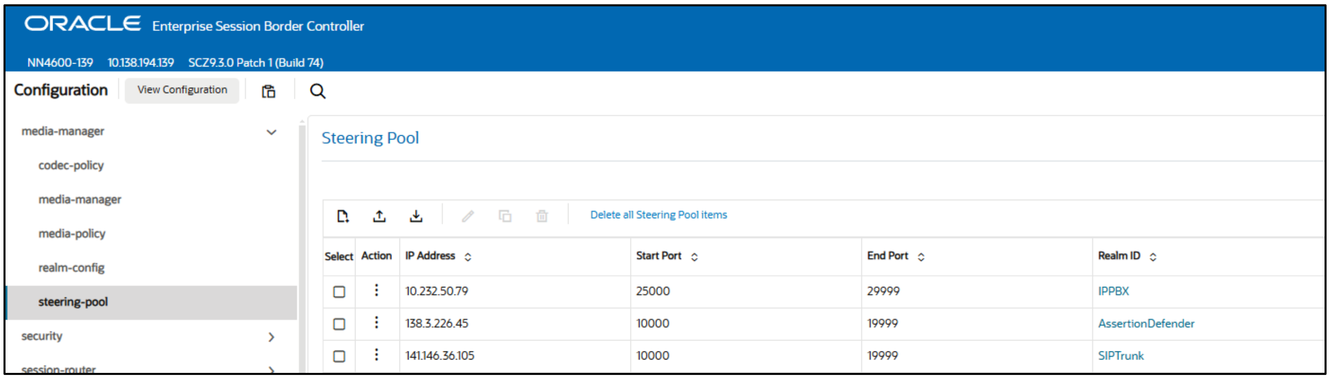
7.7.3 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system. We configure one steering pool for each configured realm:

GUI Path: media-manger/steering-pool

ACLI Path: config t→media-manger→steering-pool

- Click Add and use the below examples to configure.



Steering Pool

Select	Action	IP Address	Start Port	End Port	Realm ID
□	⋮	10.232.50.79	25000	29999	IPPBX
□	⋮	138.3.226.45	10000	19999	AssertionDefender
□	⋮	141.146.36.105	10000	19999	SIPTrunk

Select OK at the bottom of each.

We'll now work through configuring what is needed for the SBC to handle SIP Signaling.

7.8 Sip Configuration

This section outlines the configuration parameters required for processing, modifying, and securing sip signaling traffic.

7.8.1 Sip-Config

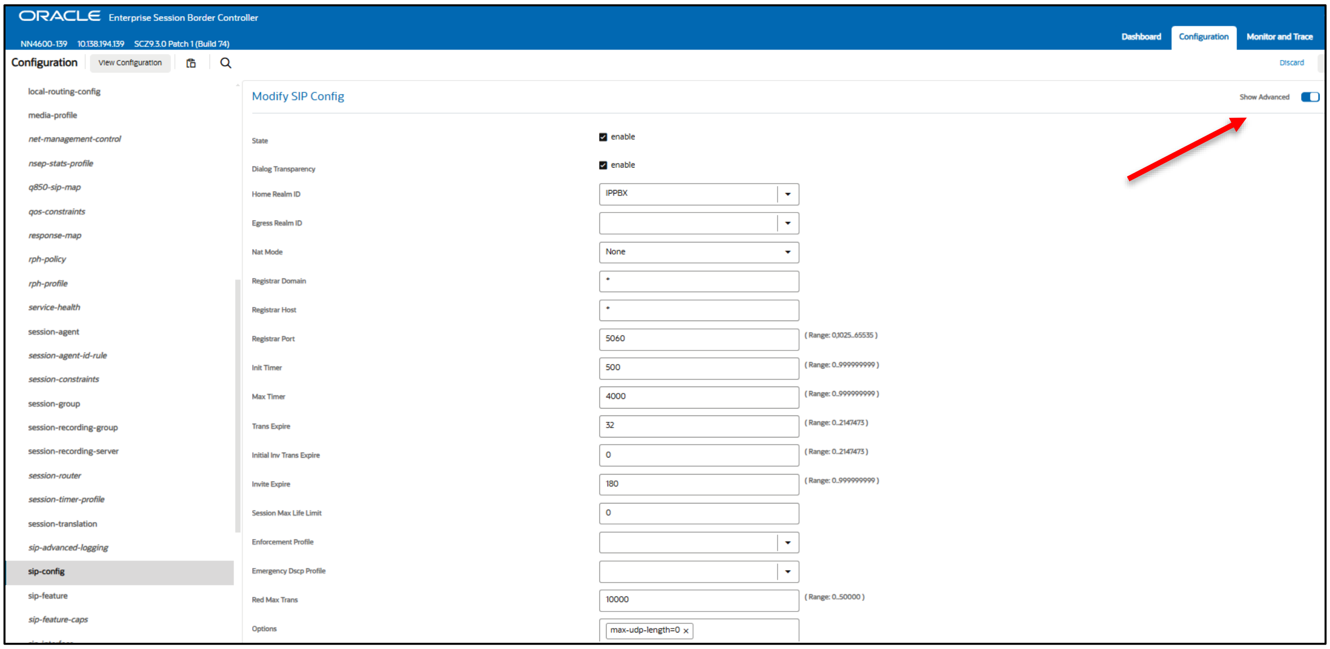
To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config
ACLI Path: config t→session-router→sip-config

There are only two recommended and one optional changes/additions to the global Sip Config.

- Set the home realm ID parameter to IPPBX Realm, and add the following hidden option:
- Max-udp-length=0: Setting this option to zero (0) forces sipd to send fragmented UDP packets. Using this option, you override the default value of the maximum UDP datagram size (1500 bytes; sipd requires the use of SIP/TCP at 1300 bytes).
- Enable sag-lookup-on-redirect if using a session agent group for your UC/CC platform

Note: toggle show advanced to expose the "Option" parameter



Modify SIP Config

State ☑ enable

Dialog Transparency ☑ enable

Home Realm ID: IPPBX

Egress Realm ID:

Nat Mode: None

Registrar Domain: *

Registrar Host: *

Registrar Port: 5060 (Range: 0,1025..65535)

Init Timer: 500 (Range: 0..999999999)

Max Timer: 4000 (Range: 0..999999999)

Trans Expire: 32 (Range: 0..2147473)

Initial Inv Trans Expire: 0 (Range: 0..2147473)

Invite Expire: 180 (Range: 0..999999999)

Session Max Life Limit: 0

Enforcement Profile:

Emergency Dscp Profile:

Red Max Trans: 10000 (Range: 0..50000)

Options: max-udp-length=0

- Select OK at the bottom.

7.8.2 Sip-Manipulations

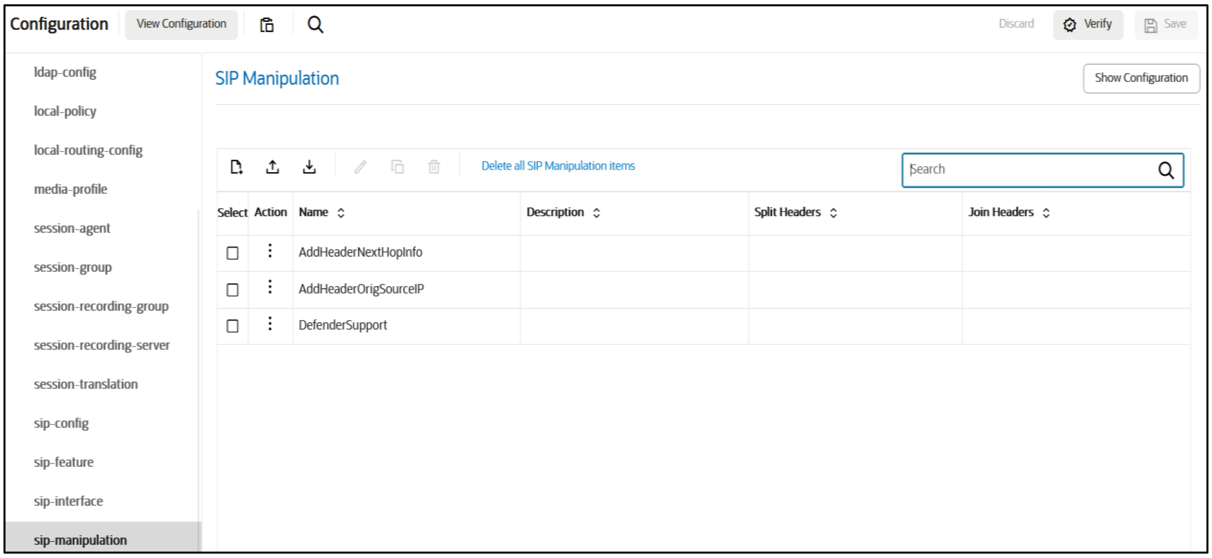
To successfully integrate Assertion Defender with the SBC, three sip manipulations need to be configured:

1. Name: AddHeaderNextHopInfo
   - Adds custom sip header to Invite “Next Hop Info” with the Session Agent IP and port.
2. Name: AddHeaderOrigSourceIP
   - Adds custom sip header to Invite “OrigSourceInfo” with the Remote IP of PSTN service.
3. Name: DefenderSupport
   - Updates the from header display-uri and To user-uri
   - Deletes the maddr parameter from the Request URI header.

Sip Manipulations can be configured through the SBC’s management GUI, we are displaying the complete manipulations with output from the ACLI for ease of viewing.

GUI Path: session-router/sip-manipulation

ACLI Path: config t→session-router→sip-manipulation



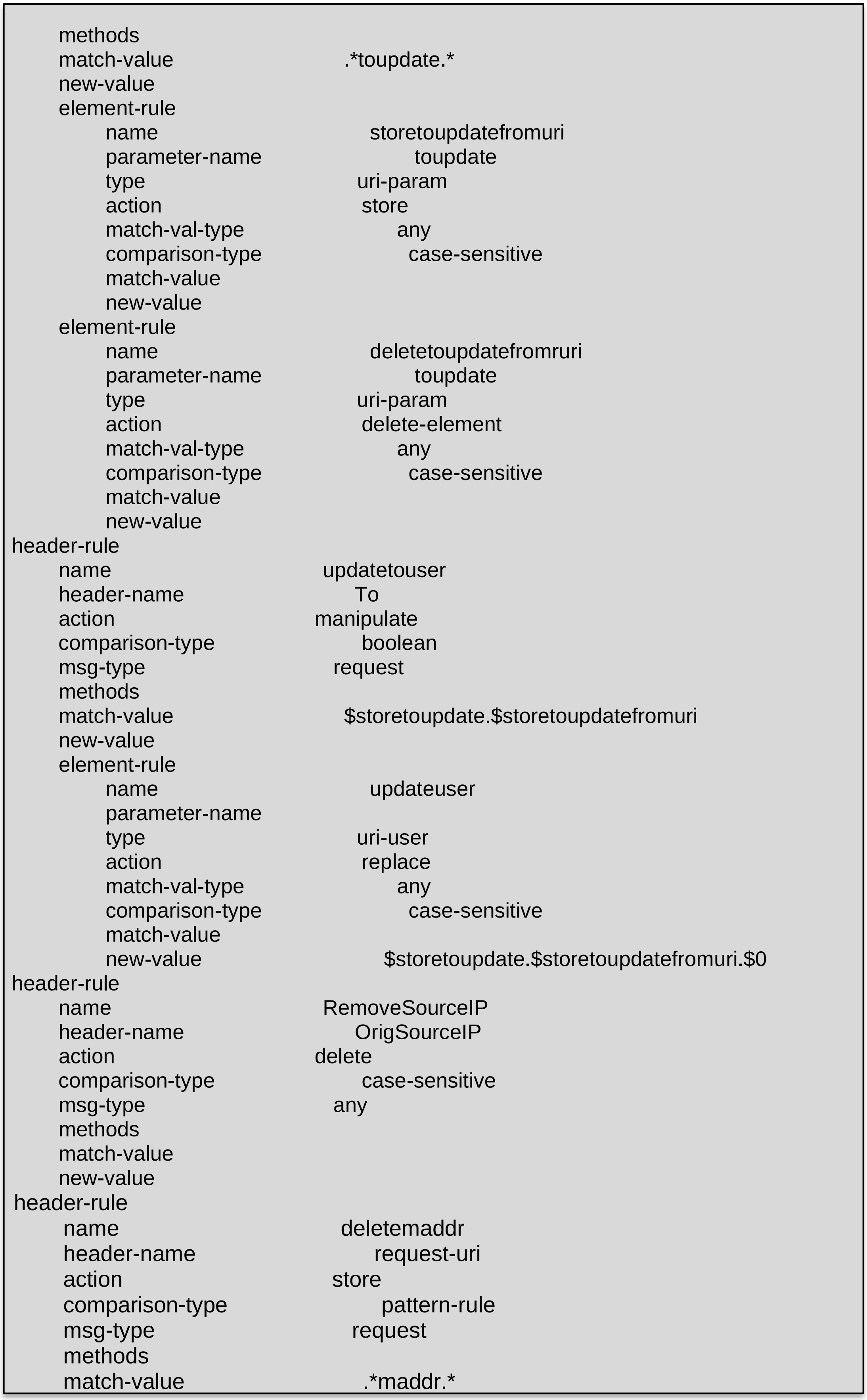
Select	Action	Name	Description	Split Headers	Join Headers
□	⋮	AddHeaderNextHopInfo			
□	⋮	AddHeaderOrigSourceIP			
□	⋮	DefenderSupport			

```
sip-manipulation
        name                                AddHeaderNextHopInfo
        description
        split-headers
        join-headers
        header-rule
                name                                InboundNextHopInfo
                header-name                              NextHopInfo
                action                             add
                comparison-type                           case-sensitive
                msg-type                             request
                methods                              INVITE
                match-value
                new-value                             "<Session_Agent_IP>:<Port>"
```

```
       sip-manipulation
        name                                AddHeaderOrigSourceIP
        description
        split-headers
        join-headers
        header-rule
                name                                AddTrunkIp
                header-name                              OrigSourceIP
                action                             add
                comparison-type                           case-insensitive
                msg-type                             request
                methods                              INVITE
                match-value
                new-value                             $REMOTE_IP
```

Note: If using a Session Agent Group for your UC/CC platform, modify the '*new-value'* in the *"AddHeaderNextHopInfo"* manipulation above to *"<DefenderIP>;maddr=<sag>"*

```
sip-manipulation
 name                         DefenderSupport
 description
 split-headers
 join-headers
 header-rule
      name                      storedisplay
      header-name                  request-uri
      action                   store
      comparison-type               pattern-rule
      msg-type                   request
      methods
      match-value                 .*displayupdate.*
      new-value
      element-rule
          name                       storedisplayfromuri
          parameter-name                 displayupdate
          type                      uri-param
          action                    store
          match-val-type                any
          comparison-type                case-sensitive
          match-value
          new-value
      element-rule
          name                       deletefromruri
          parameter-name                 displayupdate
          type                      uri-param
          action                    delete-element
          match-val-type                any
          comparison-type                case-sensitive
          match-value
          new-value
 header-rule
      name                      updatefromdisplay
      header-name                  From
      action                   manipulate
      comparison-type               boolean
      msg-type                   any
      methods
      match-value                 $storedisplay.$storedisplayfromuri
      new-value
      element-rule
          name                       updatedisplay
          parameter-name
          type                      uri-display
          action                    replace
          match-val-type                any
          comparison-type                case-sensitive
          match-value
          new-value                   $storedisplay.$storedisplayfromuri.$0
 header-rule
      name                      storetoupdate
      header-name                  request-uri
      action                   store
       comparison-type               pattern-rule
      msg-type                   request
```



```
    methods
    match-value                 .*toupdate.*
    new-value
    element-rule
        name                        storetoupdatefromuri
        parameter-name                  toupdate
        type                      uri-param
        action                    store
        match-val-type                  any
        comparison-type                   case-sensitive
        match-value
        new-value
    element-rule
        name                        deletetoupdatefromruri
        parameter-name                  toupdate
        type                      uri-param
        action                    delete-element
        match-val-type                  any
        comparison-type                   case-sensitive
        match-value
        new-value
header-rule
    name                        updatetouser
    header-name                     To
    action                    manipulate
    comparison-type                 boolean
    msg-type                    request
    methods
    match-value                 $storetoupdate.$storetoupdatefromuri
    new-value
    element-rule
        name                        updateuser
        parameter-name
        type                      uri-user
        action                    replace
        match-val-type                  any
        comparison-type                   case-sensitive
        match-value
        new-value                       $storetoupdate.$storetoupdatefromuri.$0
header-rule
    name                        RemoveSourceIP
    header-name                     OrigSourceIP
    action                    delete
    comparison-type                 case-sensitive
    msg-type                    any
    methods
    match-value
    new-value
header-rule
    name                        deletemaddr
    header-name                     request-uri
    action                    store
    comparison-type                   pattern-rule
    msg-type                    request
    methods
    match-value                   .*maddr.*
```

```
      new-value
      element-rule
            name                          deletemaddr
            parameter-name                     maddr
            type                        uri-param
            action                       delete-element
            match-val-type                     any
            comparison-type                      case-sensitive
            match-value
            new-value
```

7.8.3 Sip Interface

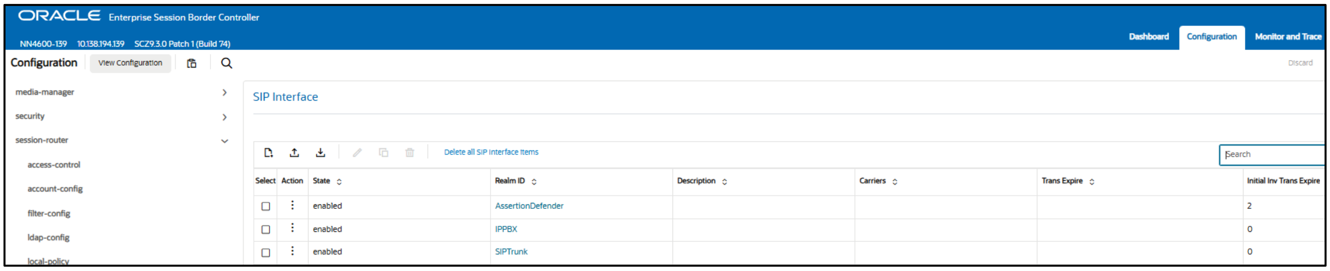
The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages. Configure three sip interfaces, one associated with PSTN Realm, one associated with Assertion SecureVoice and a third for the UC/CC platform.

GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

Click Add, and use the table below as an example to configure:

Config Parameter	Assertion Defender	SIPTrunk	IPPBX
Realm ID	AssertionDefender	SIPTrunk	IPPBX
in-manipulationid		AddHeaderOrigSourceIP	
out-manipulationid			DefenderSupport
initial-inv-trans-expire	2		
Sip Port Config Parameter	**Assertion Defender**	**SIPTrunk**	**IPPBX**
Address	138.3.226.45	141.146.36.105	10.232.50.79
Port	5060	5060	5060
Transport	TCP	UDP	TCP
Allow Anonymous	agents-only	agents-only	agents-only



Select	Action	State	Realm ID	Description	Carriers	Trans Expire	Initial Inv Trans Expire
□	⋮	enabled	AssertionDefender				2
□	⋮	enabled	IPPBX				0
□	⋮	enabled	SIPTrunk				0

Notice this is where we assign two of the three sip manipulations configured under the Sip Manipulation section of this guide.

- Select OK at the bottom of each when applicable

7.8.4 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path.

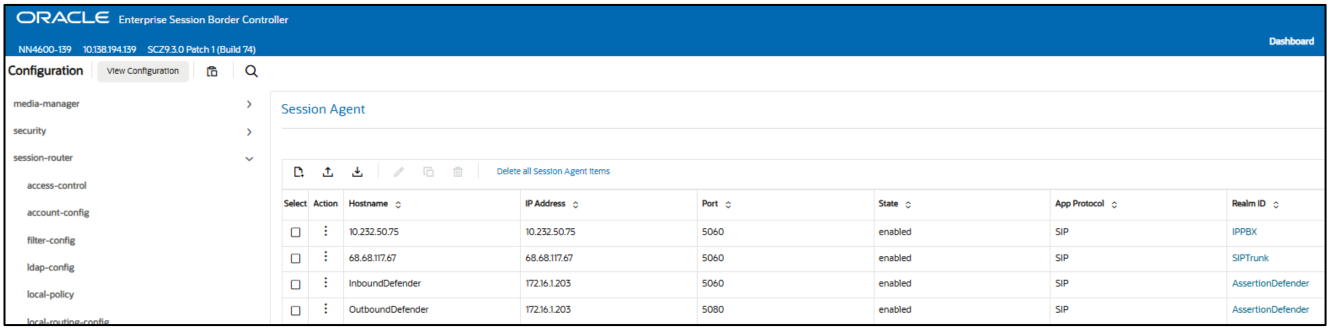
GUI Path: session-router/session-agent

ACLI Path: config t→session-router→session-agent

In this configuration example, we'll configure four session agents on the SBC. Two for Assertion SecureVoice, One for Sip Trunk and one for the UC/CC platform:

- Click Add, and use the table below to configure:

Config Parameter	Assertion Inbound	Assertion Outbound	SIPTrunk	IP-PBX
Hostname	InboundDefender	OutboundDefender	68.68.117.67	10.232.50.75
IP Address	172.16.1.203	172.16.1.203	68.68.117.67	10.232.50.75
Port	5060	5080	5060	5060
Transport Method	StaticTCP	StaticTCP	UDP	StaticTCP
Realm ID	AssertionDefender	AssertionDefender	SIPTrunk	IPPBX
Redirect Action	Recurse			
Ping Method	OPTIONS		OPTIONS	OPTIONS
Ping Interval	120		30	30
Out ManipulationID	AddHeaderNextHopInfo			



Session Agent

Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID
□	⋮	10.232.50.75	10.232.50.75	5060	enabled	SIP	IPPBX
□	⋮	68.68.117.67	68.68.117.67	5060	enabled	SIP	SIPTrunk
□	⋮	InboundDefender	172.16.1.203	5060	enabled	SIP	AssertionDefender
□	⋮	OutboundDefender	172.16.1.203	5080	enabled	SIP	AssertionDefender

Note: redirect action is only required if using a SAG to connect to your UC/CC platform

- Select OK at the bottom.

7.9 Routing Configuration

Now that most of the system, signaling, and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls to and from Assertion SecureVoice platform, the Sip trunk and UC/CC system.

7.9.1 Local Policy

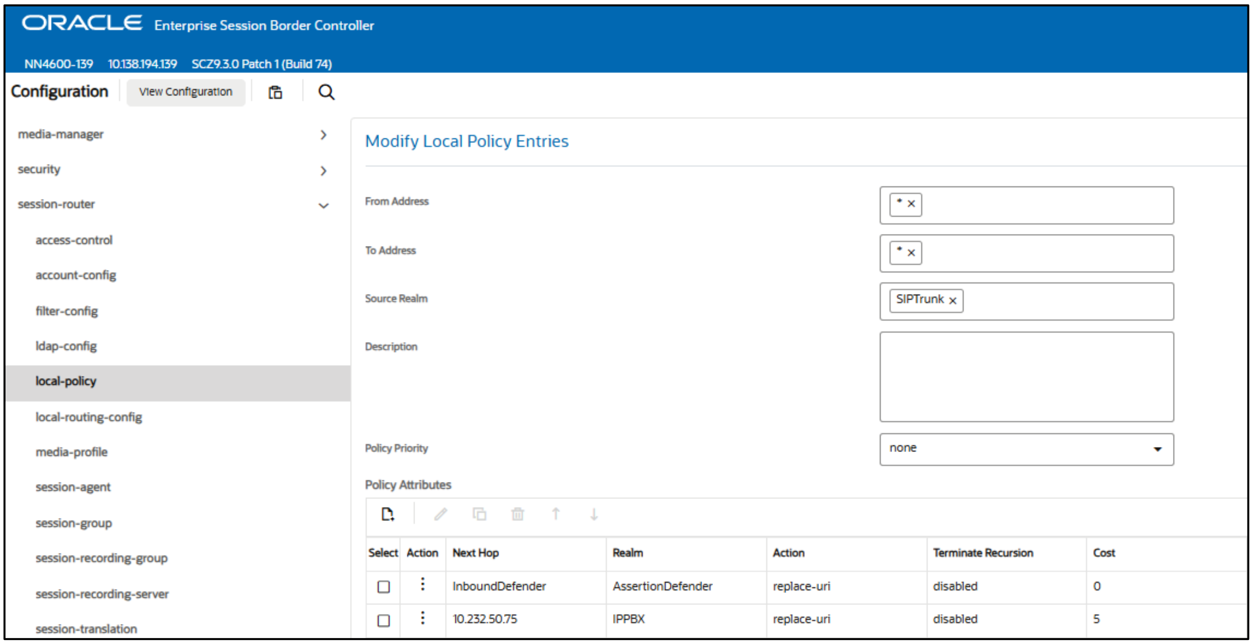
GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy

Configure two local policies to route calls from PSTN to Assertion and from IP-PBX to Assertion. Each local policy will have two possible routes. We leverage the SBC's least cost routing to prioritize each next hop.

Note: The second policy attribute routes calls to sip-trunk or UC/CC platform if there is no response from Assertion Defender for more than 2 secs (which we configured previously in the sip-interface config).

1. Route Calls from SIPTrunk to Assertion SecureVoice Inbound, with a second route to the UC/CC platform:



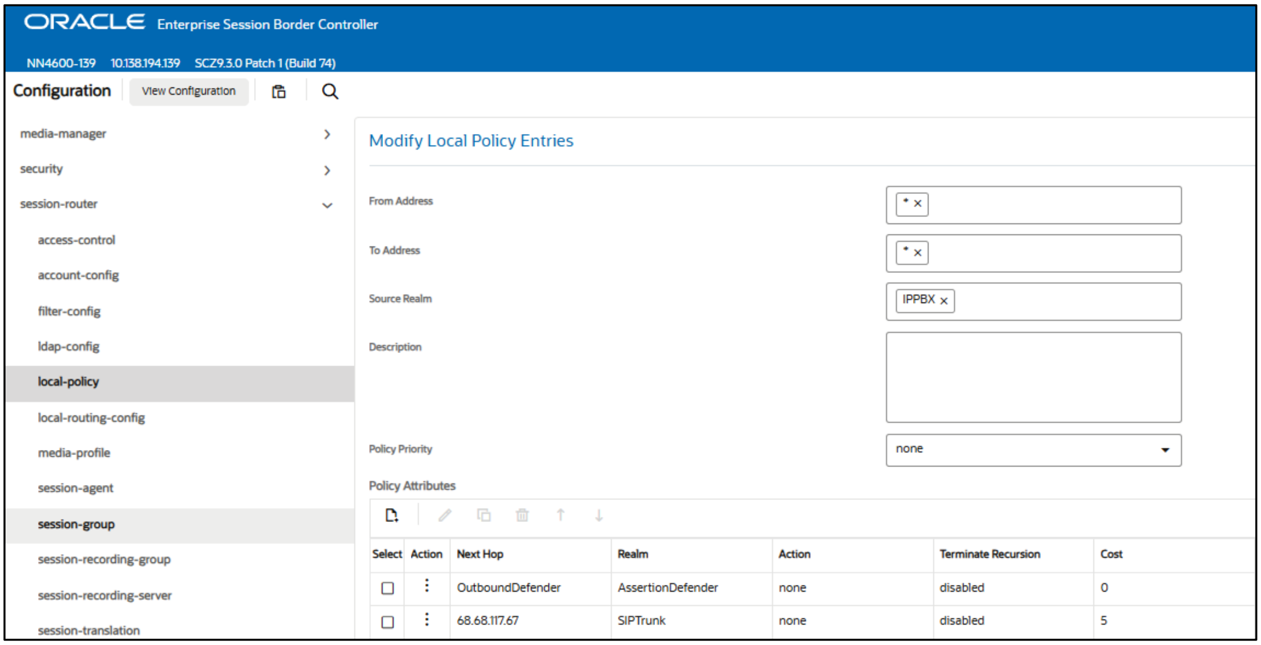
Modify Local Policy Entries

From Address	*
To Address	*
Source Realm	SIPTrunk
Description	
Policy Priority	none

Policy Attributes

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost
□	⋮	InboundDefender	AssertionDefender	replace-uri	disabled	0
□	⋮	10.232.50.75	IPPBX	replace-uri	disabled	5

2. Route calls from the UC/CC platform to Outbound Defender with a second route to SipTrunk.



Modify Local Policy Entries

From Address	*
To Address	*
Source Realm	IPPBX
Description	
Policy Priority	none

Policy Attributes

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost
□	⋮	OutboundDefender	AssertionDefender	none	disabled	0
□	⋮	68.68.117.67	SIPTrunk	none	disabled	5

- Click OK at the bottom of each when applicable.

7.10 Access Controls

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

Please note, DDOS values are specific to platform and environment. For more detailed information please refer to the Oracle Communications SBC Security Guide.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/security/index.html

However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high

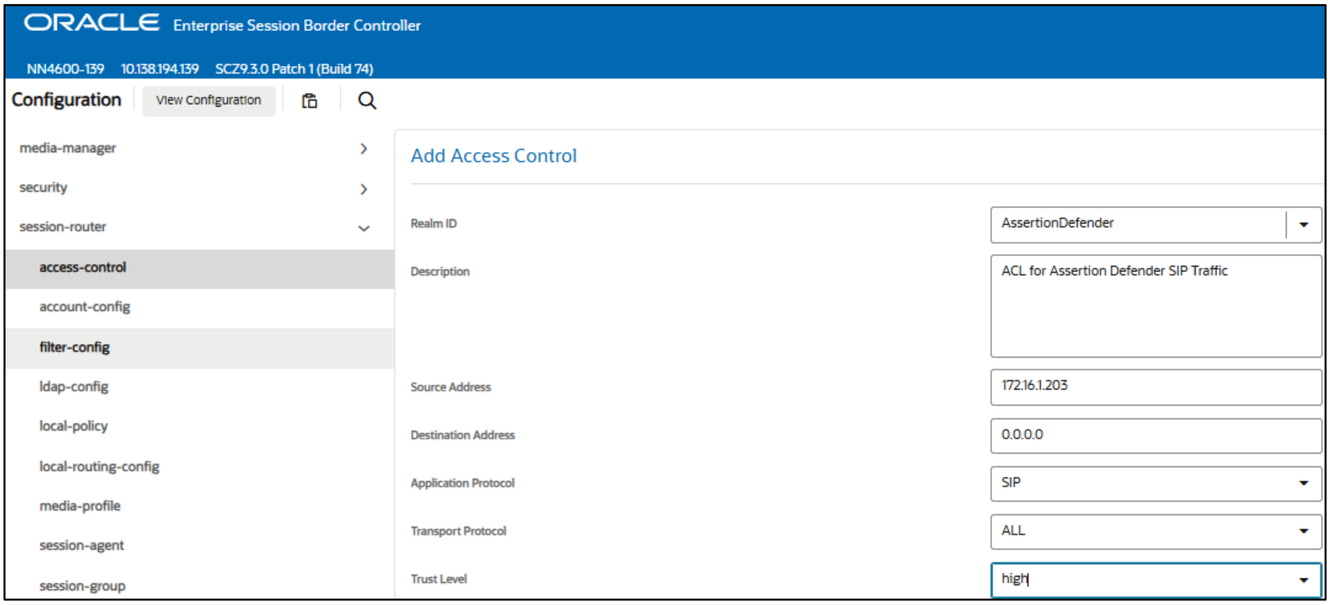
2. Set the access control trust level on public facing realms to HIGH

In this configuration example, Assertion SecureVoice has one IP address that must be allowed to send traffic to the SBC, 172.16.1.203. This must be configured as an access control on the Oracle SBC and associated with the realm facing Assertion.

GUI Path: session-router/access-control

ACLI Path: config t→session-router→access-control

Click Add and use this example to create ACL's for all of your public facing interface, ie…SIPTrunk, etc..



Add Access Control

Realm ID: AssertionDefender

Description: ACL for Assertion Defender SIP Traffic

Source Address: 172.16.1.203

Destination Address: 0.0.0.0

Application Protocol: SIP

Transport Protocol: ALL

Trust Level: high

- Click OK at the bottom.

Now we'll move on to configuring the SBC for Radius Accounting and CDR push to the Assertion Scanner.

7.11 Accounting Configuration

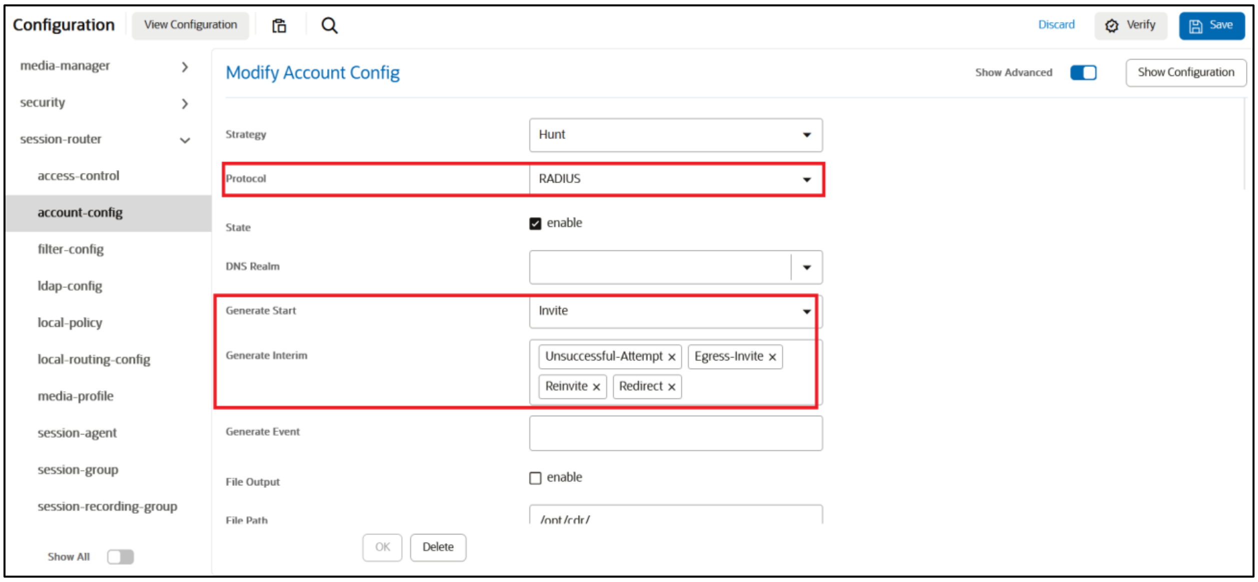
Assertion SecureVoice uses two on-prem components; Assertion Scanner to collect the CDR from Oracle SBC and Assertion Defender to provide real-time session enforcement.

In this section, we'll configure the SBC's account config and account servers to push CDR from the Oracle SBC to the Assertion Scanner.

GUI Path: session-router/account-config

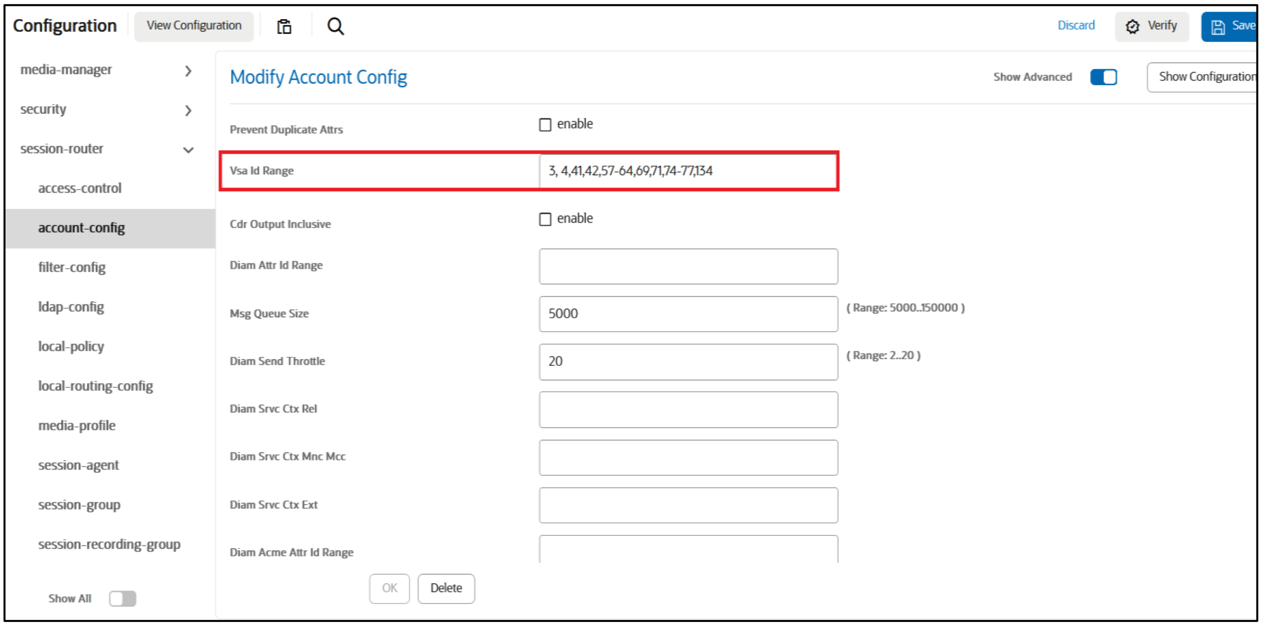
ACLI Path: config t→session-router→account-config

- Click add, and use the following example to configure the account config:



Modify Account Config

Strategy	Hunt
Protocol	RADIUS
State	☑ enable
DNS Realm	
Generate Start	Invite
Generate Interim	Unsuccessful-Attempt × Egress-Invite × Reinvite × Redirect ×
Generate Event	
File Output	☐ enable
File Path	/opt/cdr/



Modify Account Config

Prevent Duplicate Attrs	☐ enable
Vsa Id Range	3, 4,41,42,57-64,69,71,74-77,134
Cdr Output Inclusive	☐ enable
Diam Attr Id Range	
Msg Queue Size	5000 (Range: 5000..150000)
Diam Send Throttle	20 (Range: 2..20)
Diam Srvc Ctx Rel	
Diam Srvc Ctx Mnc Mcc	
Diam Srvc Ctx Ext	
Diam Acme Attr Id Range	

7.11.1 Account Server Configuration

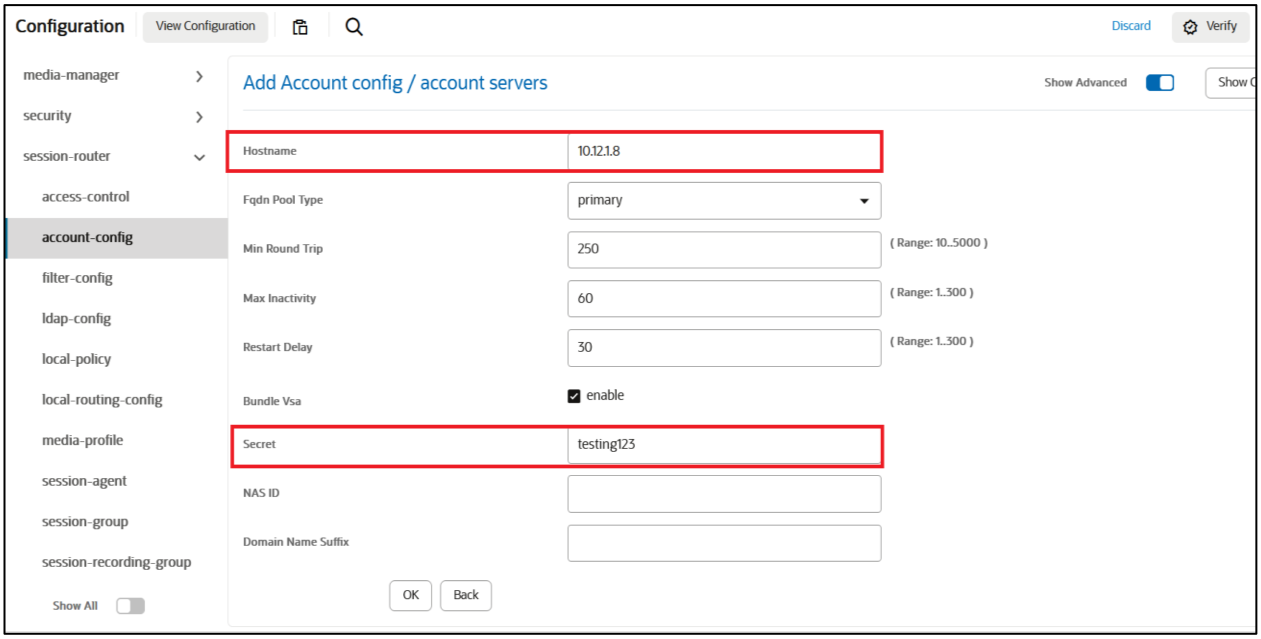
For the CDR Collection using RADIUS, we need to enable and configure an account server, which is a subset of the account-config outlined above.

GUI Path: session-router/account-config/account servers

ACLI Path: config t→session-router→account-config→account-servers

The following need to be configured for the SBC to properly communicate with the Radius Server:

- Hostname: Enter the hostname/IP address of the Radius server
- Secret: Type the secret to use with Radius server
- Click Add, and use the following example to configure your account server:



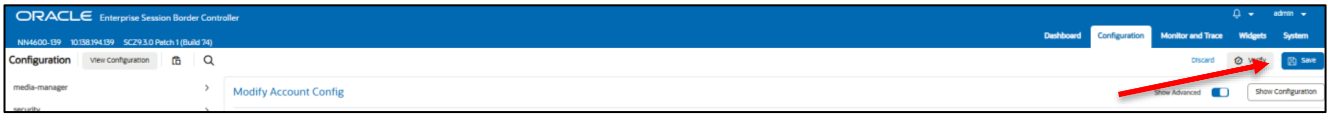
Add Account config / account servers

Hostname: 10.12.1.8
Fqdn Pool Type: primary
Min Round Trip: 250 (Range: 10..5000)
Max Inactivity: 60 (Range: 1..300)
Restart Delay: 30 (Range: 1..300)
Bundle Vsa: ☑ enable
Secret: testing123
NAS ID:
Domain Name Suffix:

- Click OK at the bottom when complete.

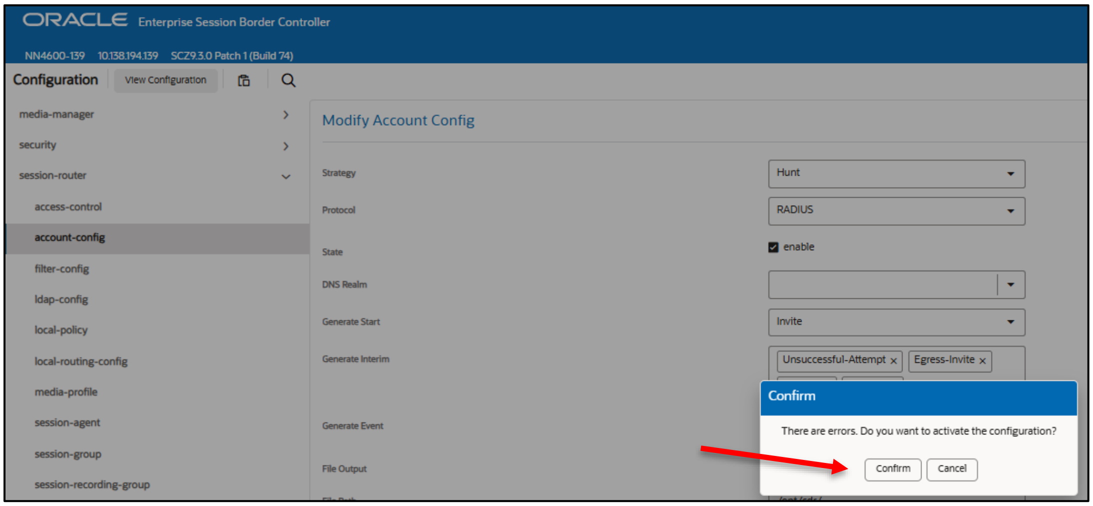
7.12 Save and Activate

7.12.1 Save Config



Modify Account Config

7.12.2 Activate Config



Modify Account Config

Strategy: Hunt

Protocol: RADIUS

State: ☑ enable

DNS Realm:

Generate Start: Invite

Generate Interim: Unsuccessful-Attempt × Egress-Invite ×

Confirm

There are errors. Do you want to activate the configuration?

This concludes the minimum required configuration to successfully integrate Assertion SecureVoice platform with your Oracle Session Border Controller.

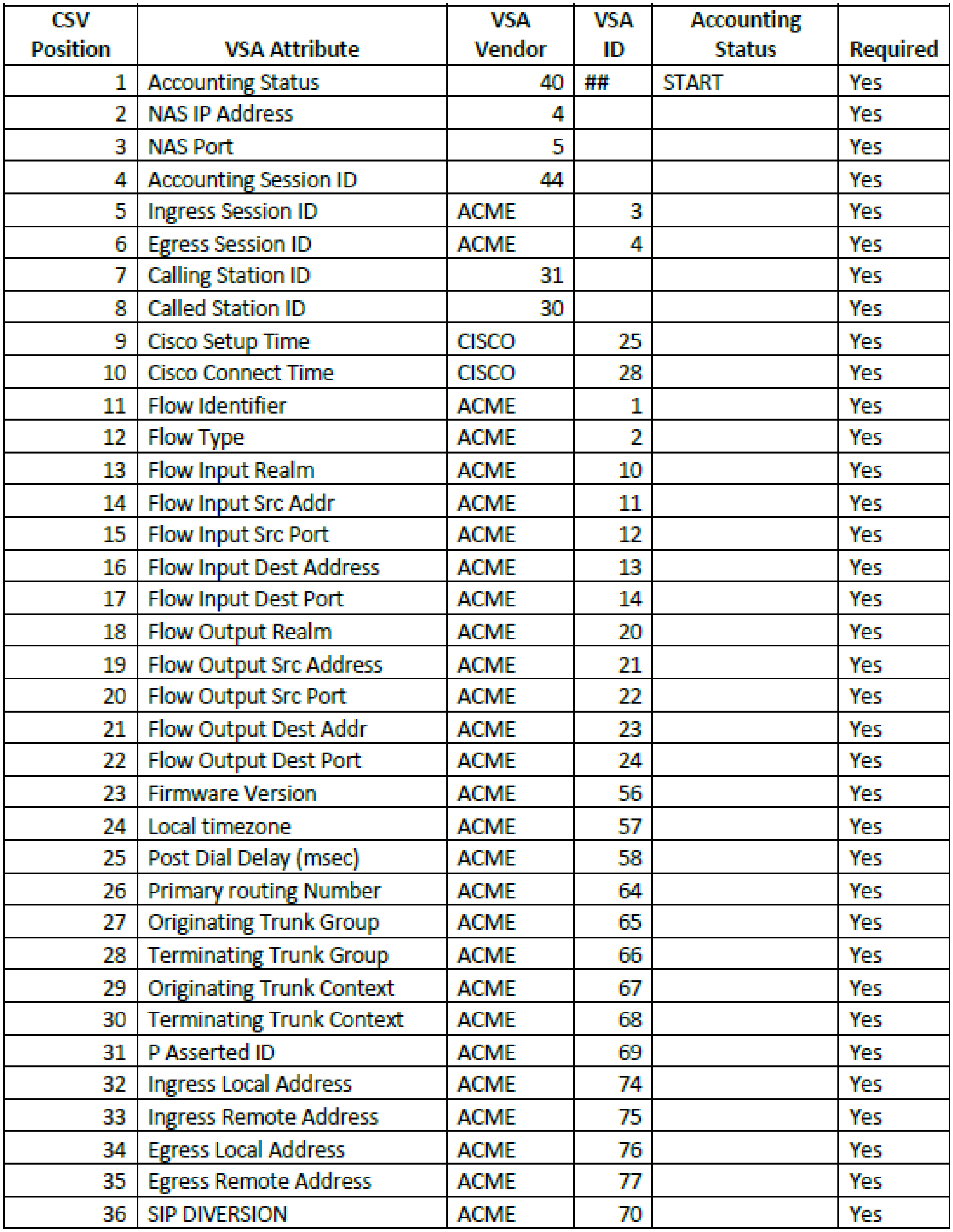
8 Existing SBC configuration

If your environment has an Oracle SBC deployed with a fully functional configuration, the following configuration elements are required to integrate Assertion SecureVoice into your existing config.

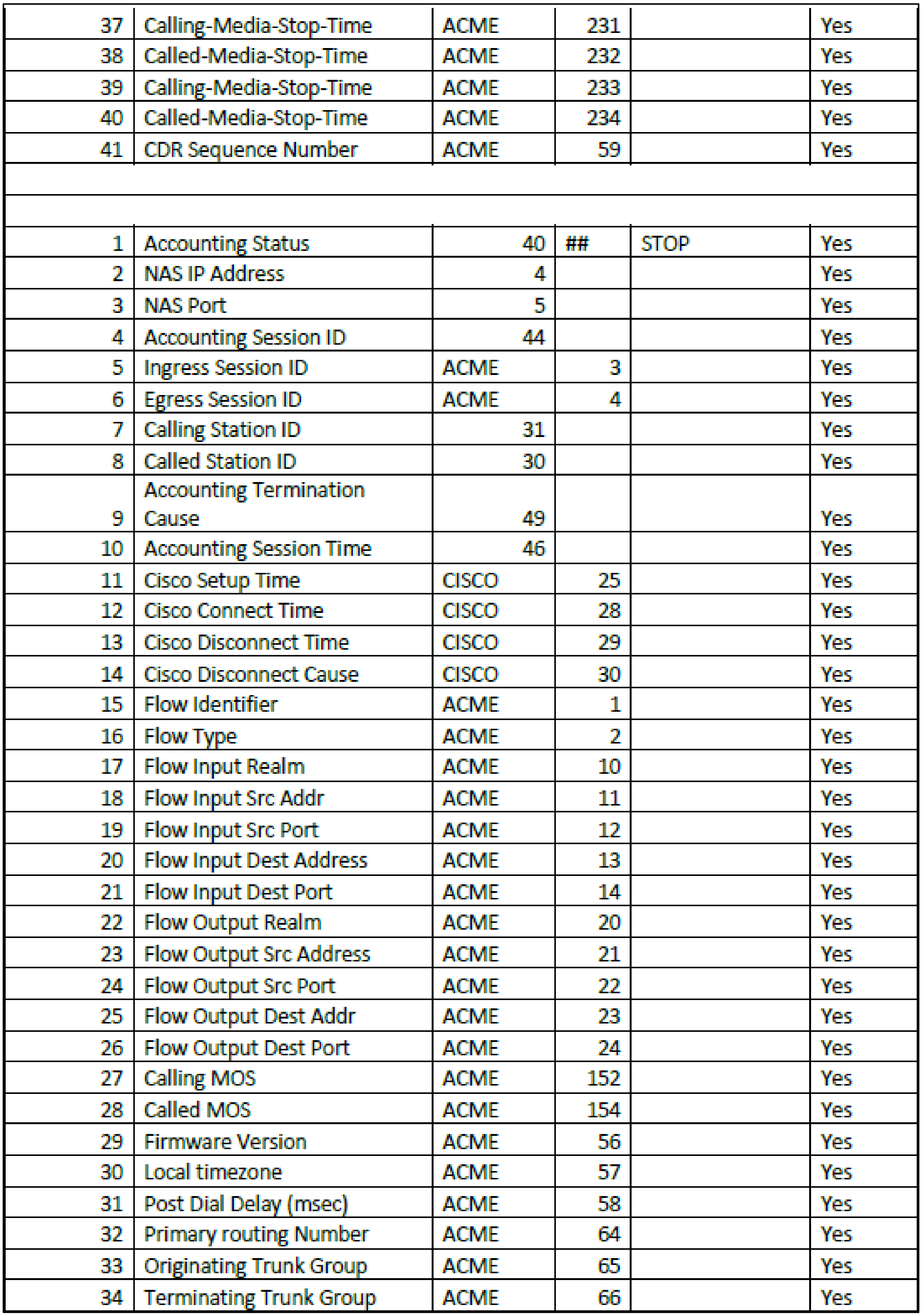
- New realm-config
- New sip-interface
- New session-agent
- New steering-pools
- New local-policy
- New sip-manipulation
- New account-config

9 Appendix A

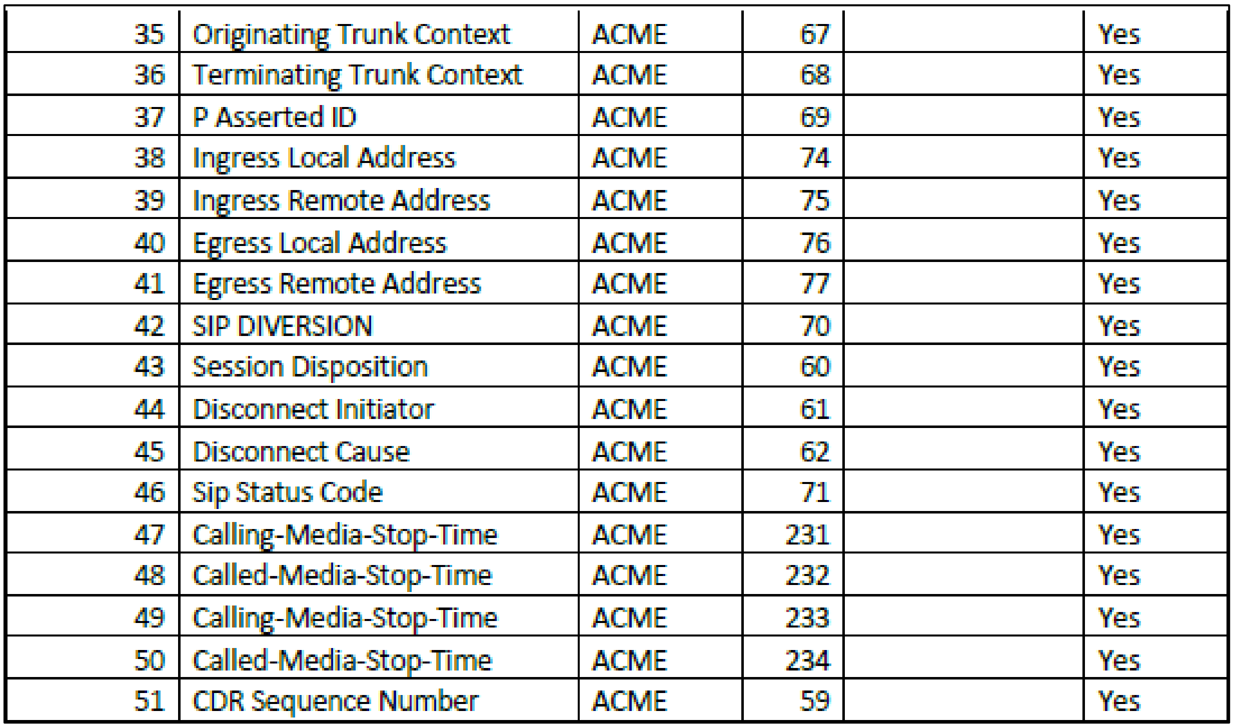
9.1 CDR vsa-id Mapping



CSV Position	VSA Attribute	VSA Vendor	VSA ID	Accounting Status	Required
1	Accounting Status	40	##	START	Yes
2	NAS IP Address	4			Yes
3	NAS Port	5			Yes
4	Accounting Session ID	44			Yes
5	Ingress Session ID	ACME	3		Yes
6	Egress Session ID	ACME	4		Yes
7	Calling Station ID	31			Yes
8	Called Station ID	30			Yes
9	Cisco Setup Time	CISCO	25		Yes
10	Cisco Connect Time	CISCO	28		Yes
11	Flow Identifier	ACME	1		Yes
12	Flow Type	ACME	2		Yes
13	Flow Input Realm	ACME	10		Yes
14	Flow Input Src Addr	ACME	11		Yes
15	Flow Input Src Port	ACME	12		Yes
16	Flow Input Dest Address	ACME	13		Yes
17	Flow Input Dest Port	ACME	14		Yes
18	Flow Output Realm	ACME	20		Yes
19	Flow Output Src Address	ACME	21		Yes
20	Flow Output Src Port	ACME	22		Yes
21	Flow Output Dest Addr	ACME	23		Yes
22	Flow Output Dest Port	ACME	24		Yes
23	Firmware Version	ACME	56		Yes
24	Local timezone	ACME	57		Yes
25	Post Dial Delay (msec)	ACME	58		Yes
26	Primary routing Number	ACME	64		Yes
27	Originating Trunk Group	ACME	65		Yes
28	Terminating Trunk Group	ACME	66		Yes
29	Originating Trunk Context	ACME	67		Yes
30	Terminating Trunk Context	ACME	68		Yes
31	P Asserted ID	ACME	69		Yes
32	Ingress Local Address	ACME	74		Yes
33	Ingress Remote Address	ACME	75		Yes
34	Egress Local Address	ACME	76		Yes
35	Egress Remote Address	ACME	77		Yes
36	SIP DIVERSION	ACME	70		Yes



37	Calling-Media-Stop-Time	ACME	231		Yes
38	Called-Media-Stop-Time	ACME	232		Yes
39	Calling-Media-Stop-Time	ACME	233		Yes
40	Called-Media-Stop-Time	ACME	234		Yes
41	CDR Sequence Number	ACME	59		Yes
1	Accounting Status	40	##	STOP	Yes
2	NAS IP Address	4			Yes
3	NAS Port	5			Yes
4	Accounting Session ID	44			Yes
5	Ingress Session ID	ACME	3		Yes
6	Egress Session ID	ACME	4		Yes
7	Calling Station ID	31			Yes
8	Called Station ID	30			Yes
9	Accounting Termination Cause	49			Yes
10	Accounting Session Time	46			Yes
11	Cisco Setup Time	CISCO	25		Yes
12	Cisco Connect Time	CISCO	28		Yes
13	Cisco Disconnect Time	CISCO	29		Yes
14	Cisco Disconnect Cause	CISCO	30		Yes
15	Flow Identifier	ACME	1		Yes
16	Flow Type	ACME	2		Yes
17	Flow Input Realm	ACME	10		Yes
18	Flow Input Src Addr	ACME	11		Yes
19	Flow Input Src Port	ACME	12		Yes
20	Flow Input Dest Address	ACME	13		Yes
21	Flow Input Dest Port	ACME	14		Yes
22	Flow Output Realm	ACME	20		Yes
23	Flow Output Src Address	ACME	21		Yes
24	Flow Output Src Port	ACME	22		Yes
25	Flow Output Dest Addr	ACME	23		Yes
26	Flow Output Dest Port	ACME	24		Yes
27	Calling MOS	ACME	152		Yes
28	Called MOS	ACME	154		Yes
29	Firmware Version	ACME	56		Yes
30	Local timezone	ACME	57		Yes
31	Post Dial Delay (msec)	ACME	58		Yes
32	Primary routing Number	ACME	64		Yes
33	Originating Trunk Group	ACME	65		Yes
34	Terminating Trunk Group	ACME	66		Yes



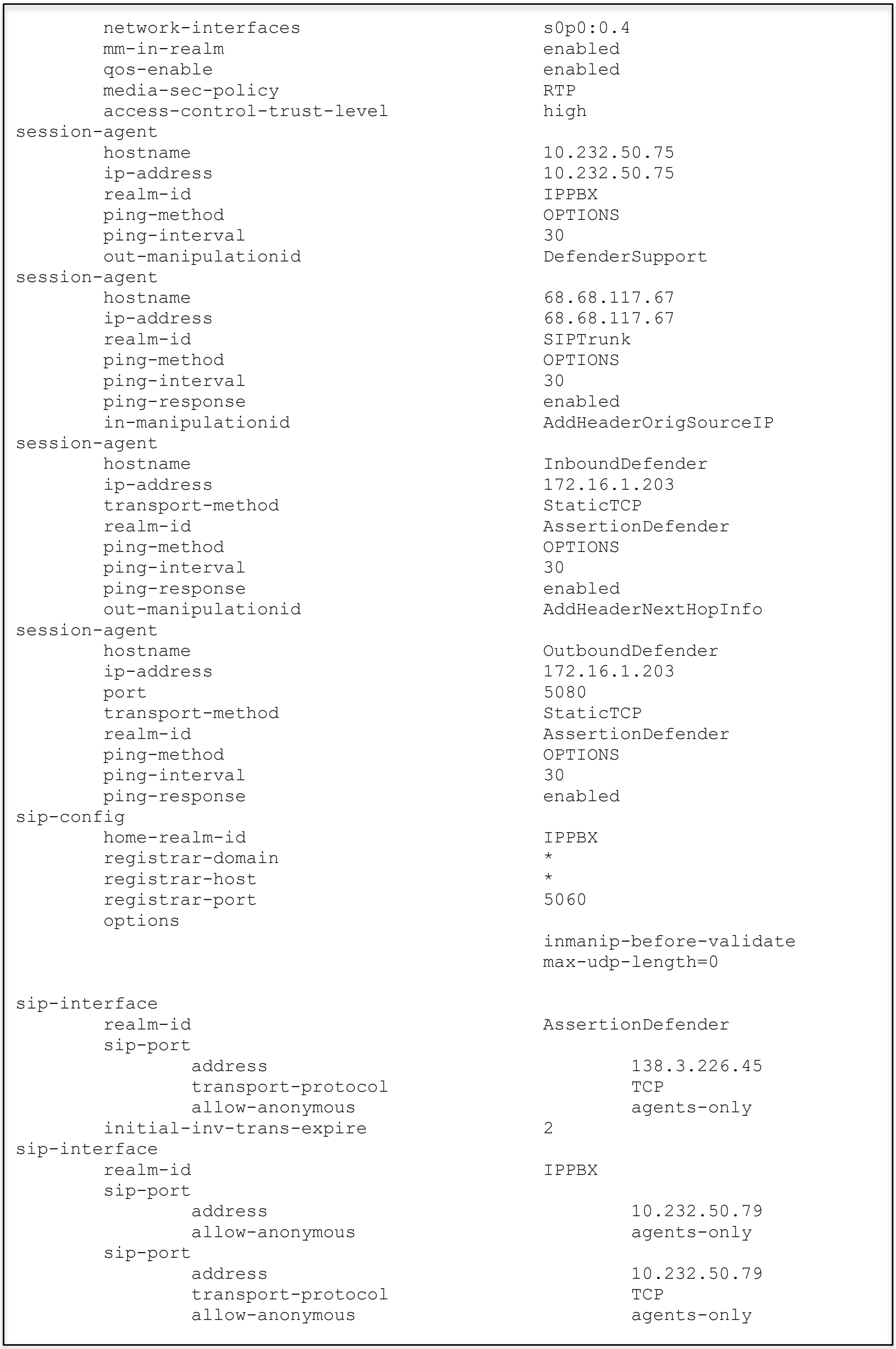
35	Originating Trunk Context	ACME	67		Yes
36	Terminating Trunk Context	ACME	68		Yes
37	P Asserted ID	ACME	69		Yes
38	Ingress Local Address	ACME	74		Yes
39	Ingress Remote Address	ACME	75		Yes
40	Egress Local Address	ACME	76		Yes
41	Egress Remote Address	ACME	77		Yes
42	SIP DIVERSION	ACME	70		Yes
43	Session Disposition	ACME	60		Yes
44	Disconnect Initiator	ACME	61		Yes
45	Disconnect Cause	ACME	62		Yes
46	Sip Status Code	ACME	71		Yes
47	Calling-Media-Stop-Time	ACME	231		Yes
48	Called-Media-Stop-Time	ACME	232		Yes
49	Calling-Media-Stop-Time	ACME	233		Yes
50	Called-Media-Stop-Time	ACME	234		Yes
51	CDR Sequence Number	ACME	59		Yes

10 Appendix B

10.1 SBC ALCI Running Config

```
access-control
        realm-id                                AssertionDefender
        description                             ACL for Assertion Defender SIP Traffic
        source-address                          172.16.1.203
        application-protocol                    SIP
        trust-level                             high
account-config
        generate-start                          Invite
        generate-interim                        Unsuccessful-Attempt
                                                Egress-Invite
                                                Reinvite
                                                Redirect
        account-servers
                hostname                                10.12.1.8
                secret                                  testing123
        vsa-id-range                            3, 4,41,42,57-64,69,71,74-77,134
filter-config
        name                                    all
        user                                    *
http-server
        name                                    webServerInstance
        http-interface-list                     GUI
local-policy
        from-address                            *
        to-address                              *
        source-realm                            IPPBX
        policy-attribute
                next-hop                                InboundDefender
                realm                                   AssertionDefender
        policy-attribute
```

```
                next-hop                                68.68.117.67
                realm                                   SIPTrunk
                cost                                    5
local-policy
        from-address                            *
        to-address                              *
        source-realm                            SIPTrunk
        policy-attribute
                next-hop                                InboundDefender
                realm                                   AssertionDefender
                action                                  replace-uri
        policy-attribute
                next-hop                                10.232.50.75
                realm                                   IPPBX
                action                                  replace-uri
                 cost                                    5
media-manager
network-interface
        name                                    s0p0
        ip-address                              141.146.36.105
        netmask                                 255.255.255.192
        gateway                                 141.146.36.65
        dns-ip-primary                          8.8.8.8
        dns-ip-backup1                          8.8.4.4
        dns-domain
network-interface
        name                                    s0p1
        ip-address                              10.232.50.79
        netmask                                 255.255.255.0
        gateway                                 10.232.50.1
network-interface
        name                                    s1p0
        ip-address                              138.3.226.45
        netmask                                 255.255.255.224
        gateway                                 138.3.226.33
ntp-config
        server                                  198.55.111.50
                                                206.108.0.131
phy-interface
        name                                    s0p0
        operation-type                          Media
phy-interface
        name                                    s0p1
        operation-type                          Media
        port                                    1
phy-interface
        name                                    s1p0
        operation-type                          Media
        port                                    3
realm-config
        identifier                              AssertionDefender
        network-interfaces                      s1p0:0.4
        mm-in-realm                             enabled
        qos-enable                              enabled
        media-sec-policy                        RTP
        access-control-trust-level              high
realm-config
        identifier                              IPPBX
        network-interfaces                      s0p1:0.4
        mm-in-realm                             enabled
        media-sec-policy                        RTP
        access-control-trust-level              high
realm-config
        identifier                              SIPTrunk
```



```
        network-interfaces                      s0p0:0.4
        mm-in-realm                             enabled
        qos-enable                              enabled
        media-sec-policy                        RTP
        access-control-trust-level              high
session-agent
        hostname                                10.232.50.75
        ip-address                              10.232.50.75
        realm-id                                IPPBX
        ping-method                             OPTIONS
        ping-interval                           30
        out-manipulationid                      DefenderSupport
session-agent
        hostname                                68.68.117.67
        ip-address                              68.68.117.67
        realm-id                                SIPTrunk
        ping-method                             OPTIONS
        ping-interval                           30
        ping-response                           enabled
        in-manipulationid                       AddHeaderOrigSourceIP
session-agent
        hostname                                InboundDefender
        ip-address                              172.16.1.203
        transport-method                        StaticTCP
        realm-id                                AssertionDefender
        ping-method                             OPTIONS
        ping-interval                           30
        ping-response                           enabled
        out-manipulationid                      AddHeaderNextHopInfo
session-agent
        hostname                                OutboundDefender
        ip-address                              172.16.1.203
        port                                    5080
        transport-method                        StaticTCP
        realm-id                                AssertionDefender
        ping-method                             OPTIONS
        ping-interval                           30
        ping-response                           enabled
sip-config
        home-realm-id                           IPPBX
        registrar-domain                        *
        registrar-host                          *
        registrar-port                          5060
        options
                                                inmanip-before-validate
                                                max-udp-length=0

sip-interface
        realm-id                                AssertionDefender
        sip-port
                address                                 138.3.226.45
                transport-protocol                      TCP
                allow-anonymous                         agents-only
        initial-inv-trans-expire                2
sip-interface
        realm-id                                IPPBX
        sip-port
                address                                 10.232.50.79
                allow-anonymous                         agents-only
        sip-port
                address                                 10.232.50.79
                transport-protocol                      TCP
                allow-anonymous                         agents-only
```

```
sip-interface
        realm-id                                SIPTrunk
        sip-port
                address                                 141.146.36.105
                allow-anonymous                         agents-only
        sip-port
                address                                 141.146.36.105
                transport-protocol                      TCP
                allow-anonymous                         agents-only
sip-manipulation
        name                                    AddHeaderNextHopInfo
        header-rule
                name                                    InboundNextHopInfo
                header-name                             NextHopInfo
                action                                  add
                msg-type                                request
                methods                                 INVITE
                new-value                               "<Session_Agent_IP>:<Port>"
sip-manipulation
        name                                    AddHeaderOrigSourceIP
        header-rule
                name                                    AddTrunkIp
                header-name                             OrigSourceIP
                action                                  add
                comparison-type                         case-insensitive
                msg-type                                request
                methods                                 INVITE
                new-value                               $REMOTE_IP
sip-manipulation
        name                                    DefenderSupport
        header-rule
                name                                    storedisplay
                header-name                             request-uri
                action                                  store
                comparison-type                         pattern-rule
                msg-type                                request
                match-value                             .*displayupdate.*
                element-rule
                        name                                    storedisplayfromuri
                        parameter-name                          displayupdate
                        type                                    uri-param
                        action                                  store
                element-rule
                        name                                    deletefromruri
                        parameter-name                          displayupdate
                        type                                    uri-param
                        action                                  delete-element
        header-rule
                name                                    updatefromdisplay
                header-name                             From
                action                                  manipulate
                comparison-type                         boolean
                match-value                             $storedisplay.$storedisplayfromuri
                element-rule
                        name                                    updatedisplay
                        type                                    uri-display
                        action                                  replace
                        new-value                     $storedisplay.$storedisplayfromuri.$0
        header-rule
                name                                    storetoupdate
                header-name                             request-uri
                action                                  store
                comparison-type                         pattern-rule
                msg-type                                request
                match-value                             .*toupdate.*
                element-rule
                        name                                    storetoupdatefromuri
                        parameter-name                          toupdate
                        type                                    uri-param
                        action                                  store
                element-rule
                        name                                    deletetoupdatefromruri
                        parameter-name                          toupdate
                        type                                    uri-param
                        action                                  delete-element
        header-rule
                name                                    updatetouser
                header-name                             To
                action                                  manipulate
                comparison-type                         boolean
                msg-type                                request
                match-value                            $storetoupdate.$storetoupdatefromuri
                element-rule
                        name                                    updateuser
                        type                                    uri-user
                        action                                  replace
                        new-value                   $storetoupdate.$storetoupdatefromuri.$0
        header-rule
                name                                    RemoveSourceIP
                header-name                             OrigSourceIP
                action                                  delete
        header-rule
                name                                    deletemaddr
                header-name                             request-uri
                action                                  store
                comparison-type                         pattern-rule
                msg-type                                request
                match-value                             .*maddr.*
                element-rule
                        name                                    deletemaddr
                        parameter-name                          maddr
                        type                                    uri-param
                        action                                  delete-element
sip-monitoring
        match-any-filter                        enabled
        monitoring-filters                      *
steering-pool
        ip-address                              10.232.50.79
        start-port                              25000
        end-port                                29999
        realm-id                                IPPBX
steering-pool
        ip-address                              138.3.226.45
        start-port                              10000
        end-port                                19999
        realm-id                                AssertionDefender
steering-pool
        ip-address                              141.146.36.105
        start-port                              10000
        end-port                                19999
        realm-id                                SIPTrunk
system-config
        system-log-level                        NOTICE
        default-gateway                         0.0.0.0
        source-routing                          disabled
        snmp-agent-mode                         v1v2
```

ORACLE

Oracle Corporation, World Headquarters
2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries
Phone: +1.650.506.7000 or
Phone: +1.800.392.2999

CONNECT WITH US

- blogs.oracle.com
- facebook.com/oracle
- twitter.com/oracle
- oracle.com/

Integrated Cloud Applications & Platform Services