

Configuring Oracle SBC with Genesys SIP Server

Technical Application Note



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.

11/1/18

Revision History

Version	Description of Changes	Date Revision Completed
1.0		06/04/20



Table of Contents

1. INTENDED AUDIENCE	4
2. DOCUMENT OVERVIEW	4
3. INTRODUCTION	4
3.1. Audience	4
3.2. Requirements	5
3.3. Architecture	5
3.4. LAB CONFIGURATION	6
4. DEPLOY THE ORACLE SBC	7
4.1. IN SCOPE	7
4.2 OUT OF SCOPE	7
4.3 BOOTING THE SBC	8
4.5. Initial Configuration	10
5. CONFIGURING SBC USING WEBGUI	11
5.1 SIP TRUNKING CONFIGURATION FOR THE ORACLE SBC	12
5.2 CONFIGURE SYSTEM ELEMENT VALUES	13
5.3 CONFIGURE PHYSICAL ELEMENT VALUES	14
5.4 Configure Network Interface	15
5.5 ENABLE MEDIA MANAGER	17
5.6. ENABLE SIP CONFIG	19
5.7 CONFIGURE REALMS	20 22
5.0 CONFIGURE STEERING FOOL	23 24
5.5 CONFIGURE SIF-INTERFACE	24 26
5.10 CONFIGURE DESIGN AGENTS	20 27
5.12. HEADER MANIPULATION RULE.	29
5.13 Session translation Rule	32
6. ENABLING REMOTE WORKER (FOR REMOTE WORKERS REGISTERING INTO GENESYS SIP	
SERVER VIA THE ORACLE SBC)	33
6.1 Realm 'remoteworker'	35
6.2. STEERING POOL ASSOCIATED WITH REALM REMOTEWORKER.	36
6.3 SIP-INTERFACE ASSOCIATED WITH REALM REMOTEWORKER	37
6.4 LOCAL-POLICY	38
7. TEST CASES REQUIRING AUTHENTICATION.	39
8. TEST PLAN EXECUTED	40
8.1 Equipment Requirements	40
8.2 DEFAULT SIP SERVER OPTIONS	41
8.3 SAMPLE EPIPHONE CONFIGURATION	41
8.3 TEST PLAN EXECUTED	43
9. CAVEATS	44



1. 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 Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Session Border Controller.

2. Document Overview

In this document we will provide the steps to navigate the Oracle SBC configuration and to configure relevant sections through the webGUI interface.

Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP is necessary to be able to utilize the document in the intended manner.

SIP Server is the Genesys software component that provides an interface between your telephony hardware and the rest of the Genesys software components in your enterprise. It translates and keeps track of events and requests that come from and are sent to the telephony device. SIP Server is a TCP/IP-based server that can also act as a messaging interface between SIP Server clients. It is the critical point in allowing your Genesys solution to facilitate and track the contacts that flow through your enterprise. This reduces the cost and complexity of extending an enterprise's telephony system outside its network borders.

Oracle Session Border Controllers (Oracle SBCs) play an important role in SIP trunking as they are used by many ITSPs and Enterprises as part of their SIP trunking infrastructure.

This application note has been prepared as a means of ensuring that SIP trunking between Genesys SIP Server, Oracle SBCs and IP Trunking services are configured in the optimal manner.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Session Border Controller and the Genesys SIP Server. There will be steps that require navigating the Oracle SBC WebGUI.

Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.



3.2. Requirements

Fully functioning Genesys SIP Server deployment, including Media Server, SIP Proxy and SIP Feature Server. Testing is performed as per below product release version.

- Genesys SIP Server, Version 8.1.1
- Genesys Media Control Platform, Version 9.0.013.61
- Genesys SIP Proxy Server, Version 8.1.100.76
- Genesys SIP Feature Server, Version 8.1.202.11
- Oracle Enterprise Session Border Controller All Oracle SBC models including Virtual Machine Edition,4600,1100,3900,6300,6350 platform running SCZ830m1p2 or above



3.3. Architecture

The Genesys SIP Server and the Oracle SBC are the edge components that form the boundary of the SIP trunk. The configuration, validation and troubleshooting of the Oracle SBC to work with the Genesys SIP Server will be described in this document.



3.4. Lab Configuration



The following diagram, similar to the Reference Architecture described earlier in this document, illustrates the lab environment created to facilitate certification testing.

All network parameters, ip addresses, hostnames etc. are specific to Oracle Labs, and cannot be used outside of the Oracle Lab environment. They are for example purposes only!!!

As per the Test Bed the connections made is as below -

- s0p3 Connection to SIP Trunk
- s0p0 Connection to Genesys SIP Server

In the setup the Oracle SBC sits in between the Genesys SIP Server and the SIP Trunk.

Client 1 and Client 2 are softphones registered on the SIP Server. The calls are made from PSTN Network which land onto the endpoints registered on Genesys SIP Server via the SBC.

We also have remote endpoints which register onto the SIP Server via the SBC which is not illustrated in the Diagram and is covered in another <u>section</u> of the documentation.

Calls made from Genesys Internal endpoints to external world are directed to SBC which then sends the call to the Trunk to terminate on PSTN Network.



4. Deploy the Oracle SBC

In this section we describe the steps for configuring an Oracle Session Border Controller, formally known as the Acme Packet Net-Net Session Director ("SBC"), for use with Genesys SIP Server in a SIP Trunking scenario.

4.1. In Scope

The following guide configuring the Oracle SBC assumes that this is a newly deployed device dedicated to a single customer. If a service provider currently has the Oracle SBC deployed and is adding SIP Server customers, then all the mentioned configuration may not be necessary and only the relevant sections must be configured.

Below are the Links to the Oracle Session Border Controller Configuration Guide which can be used as a reference point for configuring the Oracle SBC.

Web GUI User Guide

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.3.0/webgui/Oracle SBC_scz830_webgui.pdf

ACLI Configuration Guide

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.3.0/configuration/Oracle SBC_scz830_configuration.pdf

Note that Oracle offers several models of Oracle SBCs. This document covers the setup for Oracle SBC 4600 platform running SCZ830m1p2 or later. If instructions are needed for other Oracle SBC models, please contact your Oracle representative.

4.2 Out of Scope

Configuration of Network management including SNMP and RADIUS



4.3 Booting the SBC

Once the Oracle SBC is racked and the power cable connected, you are ready to set up physical network connectivity.

In the Lab environment we have setup the 4600 SBC and the below Figure illustrates the Rear view of the SBC which is used to setup Physical Connectivity of management and media cables.

The port layout may differ depending upon the SBC model being used and must be configured accordingly.



To access the console port:

Connect the serial console cable to the Oracle SBC to a workstation running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None



Power on the Oracle SBC and confirm that you see the following output from the bootup sequence.

B COM3 - PuTTY Sharing
Starting tEbmd
Starting tSipd
Starting tLrtd
Starting tH323d
Starting tH248d
Starting tBgfd
Starting tSecured
Starting tAuthd
Starting tCertd
Starting tIked
Starting tauditd
Starting tauditpusher
Starting tSnmpd
Start platform alarm
Initializing /ramdrv Cleaner
Starting tLogCleaner task
Bringing up shell
password secure mode is enabled
Admin Security is disabled
Starting SSH
SSH_Cli_init: allocated memory for 5 connections
acli: max telnet sessions: 5
Password: 0x21a059c8 (tAlarm): eth0: Link is up (1000Mb/s full duplex)

Enter the following commands to login to the Oracle SBC and move to the configuration mode. Note that the default Oracle SBC password is "acme" and the default super user password is "packet".

Password: acme Oracle SBC-Genesys > enable Password: packet Oracle SBC-Genesys # configure terminal Oracle SBC-Genesys (configure) #

You are now in the global configuration mode.



4.5. Initial Configuration

i) Assigning the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the Oracle SBC by going to

Oracle SBC-Genesys #configure terminal --- >bootparams

```
NN4600-138# conf t
NN4600-138(configure)# bootparam
'.' = clear field; '-' = go to previous field; q = quit
Boot File
                              : /boot/nnSCZ830m1p2.bz
IP Address
                             : 10.138.194.138
VLAN
                             : 0
Netmask
                             : 255.255.255.192
Gateway
                             : 10.138.194.129
IPv6 Address
IPv6 Gateway
Host IP
                             - 2
                            : vxftp
: vxftp
FTP username
FTP password
Flags
                             : NN4600-138
Target Name
Console Device
                             : COM1
Console Baudrate
                            : 115200
Other
NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.
```

A reboot is required if changes are made to the existing boot parameters.

Once you have gained access to the SBC you can further configure the system through the WEB-GUI Interface.

5. Configuring SBC using WEBGUI

There are two methods for configuring the Oracle SBC, ACLI, or GUI. For the purposes of this note, we'll be using the Oracle SBC GUI for all configuration examples.

The WebGUI can be accessed through the url :-

http://<SBC_MGMT_IP>

web-server-config is enabled by default on the Oracle SBC. If not then one can make the webserver-config on the SBC by navigating to **system> web-server-config**

web-server-config		
state	enabled	
inactivity-timeout	5	
http-state	enabled	
http-port	80	
https-state	disabled	
https-port	443	
http-interface-list		
tls-profile		
last-modified-by	admin@console	

Please refer to the Web GUI Guide for more information.

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.3.0/webgui/Oracle SBC_scz830_webgui.pdf

The expert mode is used for configuration.

Once you have accessed the Oracle SBC, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left hand side of the screen.



You may now follow the further sections of the Document to configure the SBC as desired to Connect with Genesys Pure SIP Server.

5.1 SIP Trunking Configuration for the Oracle SBC

The following section shows the Oracle SBC configuration required to work with Genesys SIP Server and the SIP trunk. The protocol used between the Oracle SBC and SIP server is UDP for signaling and RTP for media; the SIP trunk is configured for UDP in this interop testing.

It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment. The Document should be used as reference for the basic configuration objects required to interwork Oracle SBC with Genesys SIP Server.



5.2 Configure system element values

To configure system element values, use the system-config command under the system branch. Then enter values appropriate to your environment, including your default gateway IP address for your management Ethernet interface.

Here we have configured the SBC Hostname, Description and the Default Gateway. These can be used as minimal settings to configure the system-config element.

)bjects	Modify System config		
media-manager			
security	Hostname:	GenesysSBC	
session-router	Description:	SBC that interacts with Genesys SIP	
system		Server	
fraud-protection			
host-route	Location:		
network-interface	Mib system contact:		
ntp-config	Mih system name:		
pny-interface	mib system name.		
redundancy-config	Mib system location:		
sninp-continunity	Syslog servers		
spi-conng			
evetem config	Add Edit C	opy Delete	
system-config trap-receiver	Add Edit C Address	opy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	opy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	ppy Delete	
system-config trap-receiver web-server-config	Add Edit C Address	opy Delete	
system-config trap-receiver web-server-config Default gateway:	Add Edit C Address	opy Delete	
system-config trap-receiver web-server-config Default gateway:	Add Edit C Address 10.138.194.129	opy Delete	
system-config trap-receiver web-server-config Default gateway: Telnet timeout:	Add Edit C Address	(Range: 065535)	

Click the **OK** at the bottom of the screen.



5.3 Configure Physical element values

The phy-interface configuration element:

- Defines some Layers 1-2 properties (speed, half/full duplex, MAC address, and so on)
- Must be created for each physical connector that you plan to use.

To configure physical Interface values, navigate to **system->phy-interface** on the Oracle SBC Web GUI Configure the physical interface for s0p0 and s1p0 for connectivity with the Trunk and the Genesys SIP Server Environment.

As per the Test Bed the connections made is as below -

- s0p3 Connection to SIP Trunk
- s0p0 Connection to Genesys SIP Server

access-control account-config	Phy interface Securb Oritoria: 40						
filter-config	Search Chiena. An	li	Delete All L. Heleed	Deventeed		0	0
Idap-config	Auu	cuit Copy Delete	Delete All Opload	Download		Search	Search
local-policy	Name	Operation type	Port	Slot	Virtual mac	Admin state	Auto negotiation
local-routing-config	s0p0	Media	0	0		enabled	enabled
media-profile	s0p3	Media	3	0		enabled	enabled
session-agent							
session-group							
session-recording-group							
session-recording-server							
session-translation							
sip-config							
sip-feature							
sip-interface							
sip-manipulation							
sip-monitoring							
translation-rules							
system							
fraud-protection							
host-route							
network-interface							
ntp-config							



Sample physical interface configuration.

access-control	Modify Phy interface					
account-config		mouny r ny menuoe				
filter-config	Name:	2020				
Idap-config		SUPU				
local-policy	Operation type:	Media	~			
local-routing-config	Port:	0	(Range: 05)			
media-profile	Slot:	0	(Range: 02)			
session-agent	Virtual mac	<u>۲</u>	(·····g······.)			
session-group	virtual mac.					
session-recording-group	Duplex mode:	FULL	~			
session-recording-server	Speed:	100	×			
session-translation	Wancom health score:	50	(Pange: 0, 100)			
sip-config		50	[[\ange, v., [00]			
sip-feature						
sip-interface						
sip-manipulation						
sip-monitoring						
translation-rules						
system						
fraud-protection						
host-route						
network-interface						
ntp-config						
phy-interface	•					

5.4 Configure Network Interface

The network-interface configuration element:

- Must be created and refers to a specific phy-interface
- Defines Layers 2-3 properties (VLAN, IP address, mask, default gateway, and so on)

To configure network-interface, navigate to **system->Network-Interface**. Configure two interfaces, one for PSTN Trunk and one for Genesys SIP Server.

Below is the example from test bed for the network-interface configuration.

Here 2 Network interfaces are configured where-

- s0p3 Connection to SIP Trunk
- s0p0 Connection to Genesys SIP Server

local-routing-config media-profile	Network interface Search Criteria: All	ce				
session-agent	Add Ed	it Copy Delete Dele	ete All Upload Download	i -	Searc	h Se
session-group	Name	Sub port id	Description	Hostname	IP address	Pri utility addr
session-recording-group	s0p0	0			172.18.0.129	
session-recording-server	s0p3	0			192.168.1.94	
sin-config						
sip-feature						
sip-interface						
sip-manipulation						
sip-monitoring						
translation-rules						
system						
fraud-protection						

Home C	Configuration Monitor and Trace	Widgets System	
📑 <u>S</u> ave 🔅 Wizards - 🔅 Command	ds 🗸		
Objects	Modify Network interface		
media-manager			
security	Name:	s0p0	~
session-router	Sub port id:	0	(Range: 04095)
✓ system	Description:		
capture-receiver			
fraud-protection			
host-route	Hostname:		
http-client			
http-server	IP address:	172.18.0.129	
network-interface	Pri utility addr:		
network-parameters	Sec utility addr:		
ntp-config	Netmask:		
pny-interface	a i	255.255.0.0	
redundancy-config	Gateway:	172.18.0.1	
snmp-address-entry	Gw heartheat		
shimp-community	State:		
shimp-group-entry			
shimp-user-entry	Heartbeat:	0	(Range: 065535)
sninp-view-enu y	Retry count:	0	(Range: 065535)
system_access_list	Retry timeout:	1	(Range: 165535)
system-config	Health score:	0	(Pange: 0, 100)
threshold-crossing-alert-group		0	(Range: 0100)
trap-receiver	DNS IP primary:		
web-server-config	DNS ID backunds		
···· · · · · · · · · · · · · · · · · ·	DNS IP Dackup1:		
	DNS IP backup2:		
	DNS domain:		
	DNS timeout:	11	(Range: 04294967295)
	DNS max ttl:	96400	(Pango: 30, 2073600)
		00400	(Range, 502075000)
	Signaling mtu:	0	(Range: 0, 5764096)
	HIP IP list:	Add Edit Delete	



5.5 Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager and configure the below option for generating rtcp reports.

To configure navigate to Media-Manager->Media-Manager and enable the configuration.

Below is the example from test bed for the Media-Manager configuration. Just Checking on State as Yes Is sufficient for SBC to enable the Media Manager configuration and handle media traffic (RTP)

Other parameters are not required but are relevant for settings like Latching, DDOS Protection etc. to be enabled on the SBC. These parameters are outside the scope of the document and are left to their default values.

Save	3'5	Wizards -	3'5	Commands -

Objects	Modify Media manager		
media-manager	State-		
dos-alg-constraints	Flau fina limite	_	
dns-config	Flow time limit:	86400	(Range: 04294967295)
ice-profile	Initial guard timer:	300	(Range: 04294967295)
media-manager	Subsq guard timer:	300	(Range: 04294967295)
media-policy	TCP flow time limit:	86400	(Range: 04294967295)
msrp-config	TCP initial guard timer:	300	(Range: 04294967295)
realm-config	TCP subsq guard timer:	300	(Range: 04294967295)
realm-group	Hnt rtcp:		
rtcp-policy	Alad log level:	NOTIOE	
static-flow	Algulog level.	NOTICE	*
steering-pool	Mbcd log level:	NOTICE	*
tcp-media-profile	Options:	Add Edit Delete	
security			
session-router			
system			
capture-receiver			
fraud-protection			
host-route			
http.conver	Red max trans:	10000	(Range: 0.,50000)
network-interface	Red sync start time:	5000	(Range: 0, 4294967295)
network-parameters	Red sync comp time:	0000	(Decess 0, 4004007200)
ntp-config	Media a Mela	1000	(Range: 04294967295)
phy-interface	Media policing:		
redundancy-config	Max signaling bandwidth:	2500000	(Range: 7100010000000)
snmp-address-entry	Max untrusted signaling:	7	(Range: 0100)
snmp-community	Min untrusted signaling:	6	(Range: 0100)
snmp-group-entry snmp-user-entry	Tolerance window:	30	(Range: 04294967295)
snmp-view-entry	Untrusted drop threshold:	0	(Range: 0100)
spl-config	Trusted drop threshold:	0	(Range: 0.,100)
system-access-list	Acl monitor window:	30	(Range: 5, 3600)
system-config	Trap on demote to denv:		(.a.ge. 0.0000)
trap-receiver	Trap on demote to untrusted:		
web-server-config	Syslog on demote to deny:		
	Syslog on demote to untrusted:		
	Anonymous sdp:		
	Reactive transcoding:		
	Translate non rfc2833 event:		
	Xcode fax max rate:	14400	
		1400	
Show advanced		OK Delete	
Show advanced			



5.6. Enable Sip Config

SIP config enables SIP handling in the SBC. Make sure the **home realm-id**, **registrar-domain and registrar-host are configured**. Also add the options to the sip-config as shown below.

To configure sip-config navigate to Session-Router->sip-config on the Oracle SBC Web GUI.

Below are the important parameters under sip-config that need to be configured.

- Registrar-host is the Genesys SIP Server IP.
- The domain is put as * as we have not specified any specific domain on the test bed.
- The Genesys SIP Server port is configured as the Registrar-port on the Oracle SBC.
- The options "max-udp-length=0" should be configured if the SIP messages are of larger size to avoid SBC failing the calls with "513 message too large"

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 1300bytes). You can set the global SIP configuration's max-udp-length=x option for global use in your SIP configuration, or you can override it on a per-interface basis by configuring this option in a SIP interface configuration

Objects	Modify SIP config		
media-manager			
security	State:	✓	
session-router	Home Realm ID:	denesus	~
access-control	Egrada Baalm IDr	genesys	
account-config	Egress Realin ID:		¥
filter-config	Nat mode:	None	~
Idap-config	Registrar domain:	*	
local-policy	Registrar host:	170 19 0 104	
local-routing-config		172.18.0.124	
media-profile	Registrar port:	4080	(Range: 0, 102565535)
session-agent	Options:	Add Edit Delete	
session-group		max-udp-length=0	
session-recording-group		max-uup-lengui-0	
session-recording-server			
session-translation			
sip-config			
sip-feature			
sip-interface			
sip-manipulation	Refer src routing:		
sip-monitoring			
translation-rules			
system			



5.7 Configure Realms

A Ream

- Is a collection of VoIP entities residing in one or more networks.
- Typically maps to a service provider, enterprise, or end-user population environment.
- It is defined by a configuration element that contains many parameters that apply to the environment.
- Is considered as a "Layer 5" definition and a "container" of Resources.
- On the SBC, you configure realms (plus their associated configuration objects) to identify the interfaces, resources, and policies that apply to the signaling and media going through them.

To configure Realm Navigate to **realm-config under media-manager** and configure a realm as shown in the picture.

In this setup we have configured 3 Realms configured where -

'**siptrunk** is the realm for the connection to PSTN Trunk and is configured on s1p0 network interface. '**genesys'** is the Realm for connection to the to Genesys SIP Server and is configured on s0p0 network interface.

Another Realm '**remoteworker**' is configured to register remote endpoints and is described in a different section on the document.

bjects	Realm config Search Criteria: All							
media-manager	Search Chiena. All							
codec-policy	Add Edit	Copy Delete	Delete All Upload	Download		Search	Search	CI
media-manager	Identifier	Description	Addr prefix	Network interfaces		Mm		
media-policy					In realm	In network	Same ip	
realm-config	genesys		0.0.0.0	s0p0:0	enabled	enabled	enabled	
steering-pool	remoteworker		0.0.0.0	s0p0:0	disabled	enabled	enabled	
security	siptrunk		0000	s0n3:0	disabled	enabled	enabled	
session-router								
access-control								
account-config								
filter-config								
Idap-config								
local-policy								
local-routing-config								
media-profile								
session-agent								
session-group								
session-recording-group								
session-recording-server								
session-translation								
oin config								
SID-COTIIO								
sip-coniig sip-feature								

Objects	would realm coning		
media-manager			
codec-policy	Identifier:	genesys	
media-manager	Description:		
media-policy			
realm-config			
steering-pool	Network interfaces:		
security		Add Edit Delete	
session-router		s0p0:0	
access-control			
account-config			
filter-config			
Idap-config			
local-policy			
local-routing-config	Mm in realm:		
media-profile	Oo Conobles	_	
session-agent	Q03 enable.		
session-group	Media policy:	¥	
session-recording-group	Class profile:	×	
session-recording-server	In translationid:		
session-translation		¥	
sip-config	Out translationid:	change1 👻	
sip-feature	In manipulationid		
cin interface	•	OK Back	
Show advanced		Duon	

CARAR SA

2014年1月1日日

codec-policy	Out manipulationid		
media-manager	Out manipulationid:		*
media policy	Access control trust level:	high	~
	Refer call transfer:	anabled	~
realm-config			`
steering-pool	Hold refer reinvite:	\Box	
security	Dyn refer term:		
session-router	Codec policy:		
access-control			•
account-config	Codec manIP in realm:	\Box	
filter-config	RTCP policy:		~
ldap-config	Session recording server:		
local-policy			•
local-routing-config	Monitoring filters:	Add Edit Delete	
media-profile			
session-agent			
session-group			
session-recording-group			
session-recording-server			
session-translation			
sip-config			
sip-feature			
cin interface	*	OK Back	
Show advanced		Duon	

Objects	Modify Realm config	
media-manager		
codec-policy	Identifier:	siptrunk
media-manager	Description:	
media-policy		
realm-config		
steering-pool	Network interfaces:	
security		Add Edit Delete
session-router		s0p3:0
access-control		
account-config		
filter-config		
Idap-config		
local-policy		
local-routing-config	Mm in realm:	
media-profile	QoS enable:	
session-agent		0
session-group	Media policy:	~
session-recording-group	Class profile:	×
session-recording-server	In translationid:	~
session-translation	Out translationid	
sip-config	Out translationid.	×

的研究的

Mar Mark

realm-config			· ·
steering-pool	In manipulationid:		*
security	Out manipulationid:		*
session-router	Access control trust level:	none	~
access-control	Refer call transfer		
account-config	Refer can transfer.	disabled	*
filter-config	Hold refer reinvite:		
ldap-config	Dyn refer term:		
local-policy	Codec policy:		
local-routing-config			
media-profile	Codec manIP in realm:		
session-agent	RTCP policy:		~
session-group	Session recording server:		~
session-recording-group	Monitoring filters:		
session-recording-server	monitoring inters.	Add Edit Delete	
session-translation			
sip-config			
sip-feature	_		
cin interface	•	OK Back	
Show advanced			



5.8 Configure Steering Pool

The steering-pool:

- Is the SBC's media interface (for a given realm)
- Receives and transmits RTP packets
- Defines a media IP address and a pool (range) of ports from which port(s) are dynamically allocated for every established session.
- Provides call admission control (CAC) by setting a limit of sessions going into and out of a realm
- A realm can have more than one steering-pool.

To configure steering pool navigate to media-manager->steering pool.

In this setup we have configured 3 steering pool against 3 Realms.

Below is the example from test bed for the steering-pool configuration.

Objects	 Steering pool 					
media-manager	Search Criteria: All					
codec-policy	Add Edit C	Copy Delete Delete All Upload	Download		Search	Sea
media-manager	IP address	Start port	End port	Realm ID	Network inte	erface
media-policy	172.18.0.129	10000	10999	genesys		
realm-config	172.18.0.255	10000	10999	remoteworker		
security	192.168.1.94	10000	10999	siptrunk		
session-router						
access-control						
account-config						
filter-config						
Idap-config						
local-policy						

📑 Save 🙀 Wizards 🗸 🔅 Com	nmands -			Discard
Objects Media-manager codec-policy media-manager media-policy realm-config steering-pool security session-router access-control acccount-config filter-config	 Modify Steering pool IP address: Start port: End port: Realm ID: Network interface: 	172.18.0.129 10000 10999 genesys	(Range: 165535) (Range: 165535)	Show
local-policy local-routing-config				



5.9 Configure sip-interface

The sip-interface:

- Is the SBC's Edge Proxy Function
- Receives and transmits SIP signaling messages
- Provides a service pipe to the SIP daemon (sipd)
- Defines SIP signaling IP addresses, ports, transport protocols, and various SIP processing policies

To configure sip-interface, navigate to **session-router->sip-Interface**. Configure the interfaces for the PSTN and Genesys SIP Server.

Below is the example from test bed on the sip-interface configuration.

Three sip-interface are configured on the SBC where-

- sip-interface 192.168.1.94 is configured with Realm siptrunk is to route inbound traffic from Trunk to the Genesys SIP Server. Registration caching is enabled in order for SBC to cache the registration data and Route to registrar parameter is enabled to send all requests that match cached registration to the destination defined for the registrar host.
- 2. sip-interface 172.18.0.129 is configured with Realm genesys to route the outbound traffic from Genesys SIP Server to the SIP Trunk.
- 3. sip-interface 172.18.0.255 is configured with Realm remoteworker to route the registration from remote endpoint which register onto the SIP Server via the SBC. This is covered in detail another section of the document

	Search Criteria: All						
filter-config Idap-config	Add Edit	Copy Delete Delete	e All Upload Download	1		Search	Search Cl
local-policy	State	Realm ID	Description	Carriers	Trans expire	Initial inv tra	ans expire
local-routing-config	enabled	genesys				0	
media-profile	enabled	remoteworker				0	
session-agent	enabled	siptrunk				0	
session-group							
session-recording-group							
session-recording-server							
session-translation							
sip-config							

realm-config	Modity SIP interface	e					
steering-pool	Stata						
security	state:		~				
session-router	Realm ID:		siptrunk		~		
access-control	Description:						
account-config							
filter-config							
ldap-config	SIP ports						
local-policy							
local-routing-config	Add Edr	t Copy	Delete	2			
media-profile	Address	Port		Transport protocol	TLS profile	Allow anonymous	
session-agent	192.168.1.94	5060		UDP		all	
session-group	192.168.1.94	5060		TCP		all	
session-recording-group							
session-recording-server							
session-translation							
sip-config	4					•	
sip-feature	Nat traversal:		none		~		
sip-interface	Registration cachin	ng:	~				
sip-manipulation	Route to registrar:						
cin monitoring	Noute to registial.		<u> </u>				
sip-monitoring	In manipulationid:		Reject_	OPTIONS	~		
translation-rules							
translation-rules	-						

account-config	 Modify SIP interfac 	e					
filter-config Idap-config	State:						
local-policy	Realm ID:		genesys		*		
local-routing-config media-profile session-agent	Description:						
session-group	SIP ports						
session-recording-group session-recording-server	Add Ed	it Copy	Delete				
session-translation	Address	Port		Transport protocol	TLS profile	Allow anonymous	
sip-config	172.18.0.129	5060		UDP		agents-only	
sip-feature	172.18.0.129	5060		TCP		agents-only	
sip-interface sip-manipulation							
sip-monitoring	4					•	
system	Nat traversal:		none		~		
fraud-protection	Registration cachi	ng:					
host-route	Route to registrar:						
network-interface	In meninulationida						
ntp-config	in manipulationid:				~		
phy-interface	*						
			OK	Back			



5.10 Configure Session-agents

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

To Configure the session-agent for with the following parameters. Navigate to **session-router->Session-Agent.**

Below is the example from test bed for the session-agent configuration.

Here two session-agents are configured on the SBC for the trunk Side connection and other is for the Genesys SIP Server.

172.18.0.124 ----- Genesys SIP Server

192.168.1.93 ----- PSTN SIP Trunk

realm-config	 Session agent Search Criteria: All 							
security	Add Edit	Copy Delete	Delete All Upload	Download		Search	S	earch Cle
session-router	Hostname	IP address	Port	State	App protocol	Realm ID	Description	1
access-control	172.18.0.124	172.18.0.124	4080	enabled	SIP	genesys	Genesys Ag	jent
account-config	192.168.1.93	192.168.1.93	5060	enabled	SIP	siptrunk		
filter-config								
ldap-config								
local-policy								
local-routing-config								

Below is the example for the session-agent configured for Genesys SIP-server.

Objects	 Modify Session agent 			
media-manager				
security	Hostname:	172.18.0.124		
session-router	IP address:	172 18 0 124]
access-control	Port:			
account-config	Port.	4080		(Range: 0, 102565535)
filter-config	State:			
Idap-config	Transport method:	UDP	~]
local-policy	Realm ID:	Coro]
local-routing-config		Core		
media-profile	Egress Realm ID:		×	
session-agent	Description:	Genesys Agent]
session-group				
session-recording-group				
session-recording-server	Match identifier			



In the setup refer-call-transfer parameter is enabled on the SBC to locally handle the refer message for call transfer scenarios.

sip-manipulation	Rfc2833 mode:	none	¥
translation-rules	Rfc2833 payload:	0	(Range: 0, 96127)
✓ system	Codec policy:		~
fraud-protection	Refer call transfer:	enabled	~
host-route	Kpml interworking:	inherit	*
network-interface	BR it		

Certain <u>test scenarios</u> require handling of SIP Refer with replaces header. In order to complete those scenarios we also enabled option "**refer-reinvite**" on the session-agent to enable sip refer handling that contains replaces header.

The parameter should only be enabled when it is required by Oracle SBC to handle the 'refer with replaces' header and must not be configured for normal refer scenarios.

If, after the conclusion of static or dynamic REFER handling, the REFER is terminated and a new INVITE issued, users now specify a policy lookup behavior based upon either the source realm of the calling party (the INVITE originator), or the source realm of the referring party (the REFER originator).

Behavior is controlled by a 'refer-src-routing' parameter in the sip-config configuration element.

disabled, the default value, specifies that the Oracle SBC performs a policy lookup based on the source realm of the calling party.

enabled specifies that the Oracle Communications Session Border Controller performs a policy lookup based on the source realm of the referring party.

5.11 Configure Local-policy

• The Local Policy mechanism provides SIP signaling routing based on:

Ingress realm Calling and/or called number pattern Route priority (cost and availability time)

- Multiple local policies can be (and typically are) created.
- The Local Policy configuration element contains:

Matching criteria

• Zero or more "policy-attributes" sub elements, each of which defines a "route"



To configure local-policy, navigate to **session-router->local-policy**. Configure the required local policy to route the calls.

Below is an example from the test bed for the local-policy configuration. Here From address and To address * denotes calls coming from any number to any called number should be forwarded to the mentioned destination in the next hop parameter.

Objects							
objects	Modify Local policy						
 media-manager codeo policy 	From address:						
codec-policy	FIOIII audress:		Add	Edit	Delete		
media-manager			*			1	
media-policy							
realm-config							
steering-pool							
secunty							
session-router							
access-control	To address:						
account-config	To address.		Add	Edit	Delete		
titer-config			*			1	
loap-config							
local-policy							
local-routing-contig							
media-profile							
session-agent							
session-group	Source realm:			a i mani	Dataka		
session-recording-group			Add	Ealt	Delete		
session-recording-server			siptrun	k			
session-translation							
sip-conng							
sip-reature							
sip-interrace							
sip-manipulation							
sip-monitoring	Description:					1	
ansiation-rules							
fraud protection							
host-route	Policy priority:		none			1	
nost-route	Doliny attributer					1	
ntework-interface	- oncy attributes						
np-comg	Add Edit	Сору	Dele	19			
phy-interface	Next hop	Realm		Action	Cost		
recundancy-config	172.18.0.124	genesys		none	0		
sal config							
system config							
system-conig							
web server confin							
web-server-config			0	K Back			
Show advanced				Duon			



5.12. Header manipulation rule.

The following system-default Header manipulation rule is automatically applied on Genesys sipinterface involved in the test bed as an out-manipulationid.

This HMR is used for topology hiding onto the SBC and it updates Contact and From host portion with SBC outside sip-interface IP address.

ACME_NAT_TO_FROM_IP

In Juve & Mizards + & Co	minianus •					
Objects	 Modify SIP interface 	e				
media-manager						
codec-policy	State:		<			
media-manager	Realm ID:		CODASVS	~		
media-policy	Description		genesys			
realm-config	Description.					
steering-pool						
security	SID node					
session-router	SIP pons					
access-control	Add Ed	lit Copy	Delete			
account-config	Address	Port	Transport protocol	TLS profile	Allow anonymous	
filter-config	172.18.0.129	5060	UDP		agents-only	
Idap-config	172.18.0.129	5060	TCP		agents-only	
local-policy						
local-routing-config						
madia profile						
media-prome						

Objects	Modify Realm config		
media-manager codec-policy	Media policy:	Y	r
media-manager	Media sec policy:	×	•
media-policy	Class profile:	· · · · · · · · · · · · · · · · · · ·	•
realm-config	In translationid:	~	•
steering-pool security	Out translationid:	▼	•
session-router	In manipulationid:	ACME_NAT_TO_FROM_IP	·
access-control	Out manipulationid:	· · · · · · · · · · · · · · · · · · ·	•
account-config filter-config	Access control trust level:	high 🗸	•
ldap-config	Refer call transfer:	enabled 🗸	·
local-policy	Hold refer reinvite:		
local-routing-config media-profile	Dyn refer term:		
session-agent	Codec policy:	· · · · · · · · · · · · · · · · · · ·	·
session-group	Codec manIP in realm:		
session-recording-group	RTCP policy:	×	•
session-recording-server session-translation	Session recording server:	▼	-
sip-config	Monitoring filters:		
Show advanced		OK Back	



Another HMR Reject_OPTIONS is created and applied on the siptrunk sip-interface to locally respond to the SIP OPTIONS message with a 200 OK by the SBC rather than forwarding them to the Genesys SIP Server.

Objects	▲ Modify SIP interfac	e			
🔺 media-manager					
codec-policy	State:		 ✓ 		
media-manager	Realm ID:		siptrunk	*	
media-policy	Description		-4		
realm-config	buounpuoni				
steering-pool					
security	SIP norte				
session-router	on- ports				
access-control	Add Ed	it Copy	Delete		
account-config	Address	Port	Transport protocol	TLS profile	Allow anonymous
filter-config	192.168.1.94	5060	UDP		all
Idap-config	192.168.1.94	5060	TCP		all
local-policy					
local-routing-config					
media-profile					
session-agent					
session-agent session-group	Nat traversal:		none	~	
session-agent session-group session-recording-group	Nat traversal: Registration cachi	ng:	none	~	
session-agent session-group session-recording-group session-recording-server	Nat traversal: Registration cachi	ng:	none	~	
session-agent session-group session-recording-group session-recording-server session-translation	Nat traversal: Registration cachi Route to registrar:	ng:	none ✓	~	
session-agent session-group session-recording-group session-recording-server session-translation sip-config	Nat traversal: Registration cachi Route to registrar: In manipulationid:	ng:	none	~	
session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature	Nat traversal: Registration cachi Route to registrar: In manipulationid: Out manipulationid	ng: 1:	none	* *	
session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface	Nat traversal: Registration cachi Route to registrar: In manipulationid: Out manipulationid Service tag:	ng: J:	none	 	
session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation	Nat traversal: Registration cachi Route to registrar: In manipulationid: Out manipulationid Service tag:	ng: 1:	none Reject_OPTIONS	v	
session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring translation subse	Nat traversal: Registration cachi Route to registrar: In manipulationid: Out manipulationid Service tag:	ng: 1:	none Reject_OPTIONS	v	



realm-config	Modify SIP manipulation		
steering-pool	- mouny on manipulation	•	
security	Name:	Reject OPTIONS	1
session-router	Description	heleafor house	1
access-control	Description.		
account-config			
filter-config	Split headers:		1
Idap-config	opint neaders.	Add Edit Delete	
local-policy			1
local-routing-config			
media-profile			
session-agent			
session-group			
session-recording-group			
session-recording-server	Join headers:		
session-translation		Add Edit Delete	
sip-config			
sip-feature			
sip-interface			
sip-manipulation			
sip-monitoring			
translation-rules			
system	CfgRules		-
fraud-protection	Add - Edit	Copy Delete Move up Move down	
host-route	All and a second	copy score more up more down	
network-interface	Name	Element type	
ntp-config	rejectoption	header-rule	
phy-interface			
redundancy-config			
snmp-community			
spl-config			
system-config			
trap-receiver			
web-server-config	•		
Show advanced		OK Back	

🛛 <u>S</u> ave 🔅 Wizards 🗸 🏟 Comm	ands •			
realm-config steering-pool	Modify SIP manipulation / he	eader rule		
security	Name:	rejectoption		
session-router	Header name:	request-uri		
access-control account-config	Action:	reject	~	
filter-config	Comparison type:	case-sensitive	~	
Idap-config	Msg type:	request	~	
local-policy local-routing-config	Methods:	Add Edit	Delete	
media-profile		OPTIONS		
session-agent				
session-group session-recording-group				
session-recording-server				
session-translation				
sip-config	Match value:			
sip-interface	New value:			
sip-manipulation	CfgRules	L		



5.13 Session translation Rule

The following session-translation rule is configured on the SBC which strips the '+' from the called number of the request-uri as the numbers are defined without + on the SIP Server.

The session translation rule is applied as out-translationid on the genesys Realm.

i ≦ave ♀ Wizards • ♀ Commands •					🛱 Discard 🔍
bjects Translation media-manager Search Cristics	in rules eta: All	Internet Decembered			
session-router Id	Ean Copy Develo Develop Type	Add string	Add index	Delete string Delete	index
account-config account-group	Celete		U	* 0	
allowed-elements-profile class-profile					
diameter-manipulation enforcement-profile enum-confin					
filter-config h323					
home-subscriber-server http-aig					
Idap-config local-policy					
		-			
Objects		Modify Session trans	slation		
media-manager					
security		Id:		change1	
session-router		Rules calling:		Add Edit Delete	
access-contro) 			change	
account-conn	y			c	
Idan config					
local-policy					
local-routing-	config				
media-profile	Johng				
session-agen	t	Rules called:			_
session-arou	0	Nuico cuilcu.		Add Edit Delete	
session-recor	dina-aroup			change	
session-recor	ding-server				
session-trans	lation				
sip-config					
sip-feature					
sip-interface					
sip-manipulat	ion				
sip-monitoring	g				
translation-ru	les				
system					
				OK Back	
Show adva	Inced				



A basic configuration on the Oracle SBC to route calls to and from Genesys server environment is now complete. The following sections highlight some of the useful tips to configure the Oracle SBC in order to successfully resolve and overcome interoperability challenges in a SIP trunking environment between the Genesys SIP Server and Service provider network. It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

6. Enabling Remote worker (for remote workers registering into Genesys SIP server via the Oracle SBC)

A section of the testing also included remote endpoints that register through the Oracle SBC to the SIP server. This would require additional configuration to be configured on the Oracle SBC along with the SIP trunking config as mentioned in the earlier description of the test bed.

To complete the particular testing we have configured endpoints which register onto the SIP Server through the SBC.SBC terminates the call to the number based on the registration information present in the cache.

Below figure illustrates how remote workers register onto the SIP Server via the SBC





In order to achieve the requirement we have made below configuration on the Oracle SBC

Realm – remoteworker Steering Pool associated with the Realm remoteworker Sip-interface associated with the Realm remoteworker (Optional) A local-policy to route the registration requests from this Realm to the SIP Server.

Note - The local-policy element is optional as we can enable the Route to registrar parameter on the sipinterface config to route the requests to the Registrar. The registrar host and port is configured in the sipconfig element on the SBC.

The remote endpoint sends register requests from Genesys Realm onto the SBC and then SBC registers these endpoints onto the SIP Server maintaining the registration cache in its database to route inbound calls to these endpoint. Below are the snippets from the Oracle SBC WebGUI for the remote worker configuration.

6.1 Realm 'remoteworker'

the property and

11/12/18

Dbjects	Modify Realm config		
media-manager	Identifier .		
codec-policy	identifier:	remoteworker	
media-manager	Description:		
realm-config			
steering-nool			
security	Network Interfaces:	Add Edit Delete	
session-router		s0x0:0	
access-control		3000.0	
account-config			
filter-config			
Idap-config			
local-policy			
local-routing-config	Mm in realm:		
media-profile	Oo S epshie:	_	
session-agent	wosenable.		
session-group	Media policy:	¥	
session-recording-group	Class profile:	×	
session-recording-server	In translationid:	v	
session-translation	Out translationid:	· · · · · · · · · · · · · · · · · · ·	
sip-config	Out translationity.	¥	
sip-feature	In manipulationid:	¥	
sip-interface	Out manipulationid:	×	
sip-manipulation	Access control trust level:	2000a	
sip-monitoring translation-rules	Refer call fransfer:		
system	tanorot.	disabled Y	
fraud-protection	Hold refer reinvite:		
host-route	Dyn refer term:		
network-interface	Codec policy:	×	
ntp-config	Codec maniP in realm:		
phy-interface	Source manner in roami.		
redundancy-config	RTCP policy:	Y	
snmp-community	Session recording server:	*	
spl-config	Monitoring fliters:	Add Edit Delete	
system-config		Cur Doloto	
trap-receiver			
web-server-config			
Show advanced		OK Back	



6.2. Steering Pool associated with realm remoteworker.

	e Configuration Monitor and Trac	ce Widgets System		
🗐 Save 🔅 Wizards - 🔅 Con	nmands +			
 Objects media-manager 	Modify Steering pool			
codec-policy	IP address:	172.18.0.255		
media-manager	Start port:	10000	(Range: 165535)	
media-policy	End port:	10999	(Range: 1, 65535)	
realm-contig	Realm ID:	remotourodoor		
security	Network Interface:	remoteworker		
session-router	Notwork interlace.		*	
access-control				
account-config				
filter-config				
Idap-config				
local-policy				
local-routing-config				
media-profile				
session-agent				



6.3 Sip-interface associated with realm remoteworker.

Registration caching must be enabled on this sip-interface so that SBC caches the registration of the subscriber which register through this sip-interface.

Save 🔅 Wizards - 🔅 Commands						
Objects	Modify SIP interfac	е				
media-manager						
codec-policy	State:		✓			
media-manager	Realm ID:		remotev	worker	*	
media-policy	Description:					
realm-config	besonpaon.					
steering-pool						
security	SIP ports					
session-router	on ports					
access-control	Add Ed	it Copy	Dele	te		
account-config	Address	Port		Transport protocol	TLS profile	Allow anonymous
filter-config	172.18.0.255	5060		UDP		all
ldap-config						
local-policy						
local-routing-config						
media-profile	4					
session-agent	•					
session-group	Nat traversal:		none		*	
session-recording-group	Registration cachir	ng:	~			
session-recording-server	Route to registrar:		~			
session-translation	house to registrat.					
sip-config	In manipulationid:				*	
sip-teature	Out manipulationic	l:			*	
sip-interface	Service tag:					
sip-manipulation						
sip-monitoring						
translation-rules						
 system 						
heat route						
nost-route						
· -			0	Back		
Show advanced			OP	DdCK		



6.4 Local-policy

Dbjects	Modify Local policy					
🔺 media-manager						
codec-policy	From address:	From addrese:		1 Edit	Delete	
media-manager			-		201010	
media-policy			*			
realm-config						
steering-pool						
security						
session-router						
access-control						
account-config	To address:		Ad	1 Edit	Delete	
filter-config			*			
Idap-config						
local-policy						
local-routing-config						
media-profile						
session-agent						
session-group	Rouros realm:	Source realm:				
session-recording-group	source realm:			d Edit	Delete	
session-recording-server				worker		
session-translation						
sip-config						
sip-feature						
sip-interface						
sip-manipulation						
sip-monitoring	Description:					
translation-rules						
system						
fraud-protection	Policy priority:		0000			
host-route	Policy priority.		none			×
network-interface	Policy attributes					
ntp-config	Add Edit	Сору	Dele	te		
pny-interface	Next hop	Realm		Action	Co	et
redundancy-config	172.18.0.124	genesys		none	0	
snmp-community						
spi-config						
system-contig						
trap-receiver						
web-server-contig			0	R	cik	
Show advanced			0	Da	un	

7. Test cases requiring authentication.

There are two test cases that require SIP Digest authentication.

SIP Authentication for outbound calls SIP Authentication for incoming calls

The SIP Server is configured to challenge the identity of SBC when SBC sends a SIP INVITE to the SIP Server DN configured to demand authentication.

The inbound call made from PSTN to that DN. SIP Server send challenges to SBC by sending a 401 unauthorized message to the SBC.SBC further responds with a new INVITE based on the authentication attributes configured on the Session-agent. There is no configuration required for Outbound calls from Genesys SIP server.

In order to achieve the required configuration and pass the test scenarios we have configured below parameters onto the SBC for the SIP Trunk Session-agent.

bjects	 Modify Session age 	ent							
media-manager	Monitoring filters:		Add L Edit L Delate						
security				L'L'ELE					
session-router									
access-control									
account-config									
account-group									
allowed-elements-profile									
 class-profile diameter manipulation 	Audh athribuda								
enforcement-profile	Auth attribute	Auth attribute							
enum-config	Add Edi	t Copy	Delete						
filter-config	Auth realm	Username	Password	In dialog methods					
h323	Switch	user	*******	Invite					
home-subscriber-server									
http-alg									
iwf-config									
ldap-config									
local-policy	Session recording	server:							
local-response-map	a i i i			•					
local-routing-config	Session recording	required:							
media-profile	Hold refer reinvite:								
net-management-control	Send TCP fin:								
response-map	SIP recursion polic	y:		*					
service-health	Sm jesi mateh for i	Smiasi match for invite:							
session-agent	off for match for f		Add Edit	Delete					
session-agent-id-rule									
session-constraints									
session-group									
session-recording-group									
session-recording-server									



8. Test Plan Executed.

8.1 Equipment Requirements

Table below identifies equipment used for testing

Product	Version	Units	Notes
SIP Server	8.1.1	1	Standalone deployment
Resourse manager (RM)	9.0	1	
Media Control Platform (MCP)	9.0	1	
Genesys Management Framework	8.1	1	
T-Lib Client Desktop Test		1	EpiPhone application
application			
Oracle SBC SCZ830m1p2 or above		1	
SIP End Point		3	
PSTN phone		2	

Execution of test plan requires having PSTN phones and Oracle SBC to be configured with Genesys. Below figure illustrates the setup required for test bed.

Two PSTN phones representing external numbers has to be configured for accessing Genesys SIP Server through Oracle SBC, and be accessible as outbound destination from SIP Server.

2 SIP phones are configured with Sip Server as local Sip Endpoints. Genesys EpiPhone test application is configured to simulate Agent Desktops for 2 local Sip Endpoints.

Genesys EpiPhone is used to issue 3PCC Apply Treatment and Route requests. Internal SIP endpoints can be registered at SIP Server or provisioned. EpiPhone is a test tool for testing Genesys SIP Server. It provides functionality of Genesys T-Library GUI client with call/parties visualization and 3rd party call control. From EpiPhone GUI it is possible to perform all 3PCC requests required for execution of current test plan. This include Treatment request and Route requests, thus we don't need to include URS in the testing environment.



8.2 Default Sip Server Options

The default Sip Server Options configuration is as below. Configuration changes will be required on the Genesys SIP Server Trunk, DN objects as per the test case requirement in order to pass the test scenarios.

SIP Server Application Options TServer section			
SIP-hold-rfc3264=true	_		
router-timeout=30			
default-dn=			
blind-transfer-enabled=true			
resource-management-by-rm=true			
msml-support=true			
sip-enable-moh=true			

8.3 Sample EPIphone configuration

Below is the sample EPIphone configuration from the Test Bed. Here the DN's and Route Points are configured for the SBC Trunk. Please note the below configuration is just for reference as it will change with respect to each environment.



[HOME]

server = (host="\${loc_host_ip}", port=\${loc_tserv_port}) sip-proxy = \${loc_host_ip}:\${loc_sip_port};transport=udp sip-register = true dn1 = 100001, sip-port = \${sip_port_dn1}, sip=simple, play=DN1, [AA] on-invite = 486 dn2 = 100011, sip-port = \${sip_port_dn2}, sip=simple, play=DN2 dn3 = 100021, sip-port = \${sip_port_dn3}, sip=simple, play=DN3 dn4 = 17814437266, sip-port = \${sip_port_dn4}, sip=simple, play=DN4 dn5 = 100041, sip-port = \${sip_port_dn5}, sip=simple, play=DN5 dn10 = 17814437285, pool="shared" dn11 = 9001, pool="shared",script="annc=(PROMPT=(\"1\"=(INTERRUPTABLE=1,ID=1)))" dn12 = 9002, pool="shared",script="collect=(MAX_DIGITS=4,RESET_DIGITS=11,BACKSPACE_DIGITS=22,TOTA L_TIMEOUT=1000) annc=(PROMPT=(ID=1))"



8.3 Test Plan executed

The following Test Plan has been executed against this setup and results are documented below.

Scenario	Supported
Inbound Call to Agent released by caller	Yes
Inbound Call to Agent released by agent	Yes
Inbound Calls rejected	Yes
Inbound Call abandoned	Yes
Inbound Call to Route Point with Treatment	Yes
Interruptible Treatment	Yes
IVR (Collect Digit) Treatment	Yes
Inbound Call routed by using 302 out of SIP Server signaling path	Yes
1PCC Outbound Call from SIP Endpoint to external destination	Yes
3PCC Outbound Call to external destination	Yes
1PCC Outbound Call Abandoned	Yes
Caller is put on hold and retrieved by using RFC 2543 method	Yes
T-Lib-Initiated Hold/Retrieve Call with MOH using RFC 3264 method	Yes
3PCC 2 Step Transfer to internal destination by using re-INVITE method	Yes
3PCC Alternate from consult call to main call	Yes
1PCC Unattended (Blind) transfer using REFER	Yes
1PCC Attended Transfer to external destination	Yes
3PCC Two Step Conference to external party	Yes
3PCC (same as 1PCC) Single-Step Transfer to another agent	Yes
3PCC Single Step Transfer to external destination using REFER	Yes
3PCC Single Step Transfer to internal busy destination using REFER	Yes
Early Media for Inbound Call to Route Point with Treatment	Yes
Early Media for Inbound Call with Early Media for Routed to Agent	Yes
Inbound call routed outbound (Remote Agent) using INVITE without SDP	Yes
Call Progress Detection	Yes
Out of Service detection Checking MGW live status	Yes
SIP Authentication for outbound calls	Yes
SIP Authentication for incoming calls	Yes
T-Lib-Initiated Answer/Hold/Retrieve Call for Remote SIP endpoint which supports the BroadSoft SIP Extension Event Package	Yes
3PCC Outbound Call from Remote SIP endpoint to external destination	Yes
3PCC 2 Step Transfer from Remote SIP endpoint to internal destination	Yes
1PCC Attended Transfer from Remote SIP endpoint to external destination	Yes



9. Caveats

Oracle SBC does not support CPD Call Progress Detection, The functionality is available on the Genesys SIP server where Media Server (Genesys) detects the CPD and sends the result to SIP Server.

CONNECT WITH US blogs.oracle.com/oracle acebook.com/Oracle/ witter.com/Oracle pracle.com

ORACLE

Oracle Corporation, World Headquarters Worldwide Inquiries 500 Oracle Parkway Phone: +1.650.506.7000 Redwood Shores, CA 94065, USA Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615