

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.

11/10

Revision History

Version	Description of Changes	Date Revision Completed
1	Initial publication	6/4/2020
2	Configuration included for remote worker registration over a secured connection.	6/26/2020
3	Updated after testing with 900p3 version	1/7/2022



Table of Contents

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	5
3. INTRODUCTION	5
3.1. AUDIENCE	
3.2. REQUIREMENTS	
3.3. ARCHITECTURE	
3.4. LAB CONFIGURATION	
4. DEPLOY THE ORACLE SBC	8
4.1. IN SCOPE	
4.2 Out of Scope	
4.3 BOOTING THE SBC	9
4.5. Initial Configuration	
5. CONFIGURING SBC USING WEBGUI	12
5.1 SIP TRUNKING CONFIGURATION FOR THE ORACLE SBC	13
5.2 CONFIGURE SYSTEM ELEMENT VALUES	14
5.3 CONFIGURE PHYSICAL ELEMENT VALUES	
5.4 Configure Network Interface	16
5.5 ENABLE MEDIA MANAGER	18
5.6. ENABLE SIP CONFIG	20
5.7 Configure Realms	
5.8 Configure Steering Pool	
5.9 CONFIGURE SIP-INTERFACE	
5.10 CONFIGURE SESSION-AGENTS	
5.11 CONFIGURE LOCAL-POLICY	
5.12. HEADER MANIPULATION RULE	
5.13 Session translation Rule	33
6. ENABLING REMOTE WORKER (FOR REMOTE WORKERS REGISTERING INTO GENESYS SIP	
SERVER VIA THE ORACLE SBC)	
6.1 Realm 'remoteworker'	
6.2. STEERING POOL ASSOCIATED WITH REALM REMOTEWORKER.	
6.3 SIP-INTERFACE ASSOCIATED WITH REALM REMOTEWORKER.	
6.4 LOCAL-POLICY	
7. TEST CASES REQUIRING AUTHENTICATION.	40
8. TEST PLAN EXECUTED	41
8.1 Equipment Requirements	
8.2 DEFAULT SIP SERVER OPTIONS	42
8.3 SAMPLE EPIPHONE CONFIGURATION	
8.3 TEST PLAN EXECUTED	44
9. ENABLING REMOTE WORKER (FOR REMOTE WORKERS REGISTERING INTO GENESYS SIP	
SERVER VIA THE ORACLE SBC OVER SECURE CONNECTION)	
9.1 SIGNALING SECURITY CONFIGURATION	
9.1.1 Certificate Records	
9.1.2 GENERATE CERTIFICATE SIGNING REQUEST	
9.1.3 IMPORT CERTIFICATES TO SBC	53



9.1.4 TLS PROFILE	
9.2 MEDIA SECURITY CONFIGURATION	
9.2.1 SDES-PROFILE	
9.2.2 Media Security Policy	
9.3 CHANGES TO SBC CONFIGURATION.	
9.31. CHANGE TO THE SIP-INTERFACE CONFIGURATION OBJECT	
9.3.2 CHANGE TO THE REALM-CONFIG CONFIGURATION OBJECT	
9.3.3 CHANGE TO THE SESSION-AGENT CONFIGURATION OBJECT.	
9.3.4 LOCAL-POLICY	
9.5 GENESYS SIDE CONFIGURATION	
9.5.1 Prerequisites.	
9.5.2 GENERATE CERTIFICATE	
9.5.3 GENESYS SIP SERVER CONFIGURATION.	
9.5.4 TRUNK CONFIGURATION	
9.5.5 SRTP BETWEEN AGENT AND SBC	
10.CAVEATS	70



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.

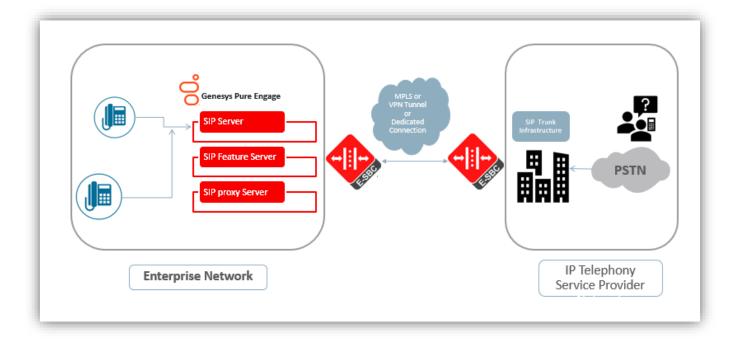
Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.



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,4600,1100,3900,6300,6350,3950,4950 platform running SCZ900p3 or above

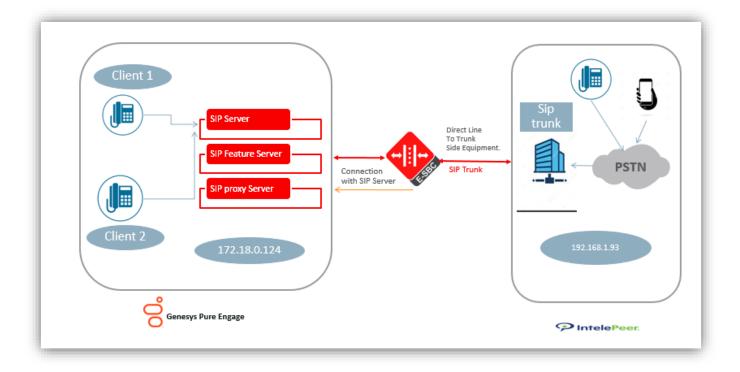


3.3. Architecture

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 SCZ900p3 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

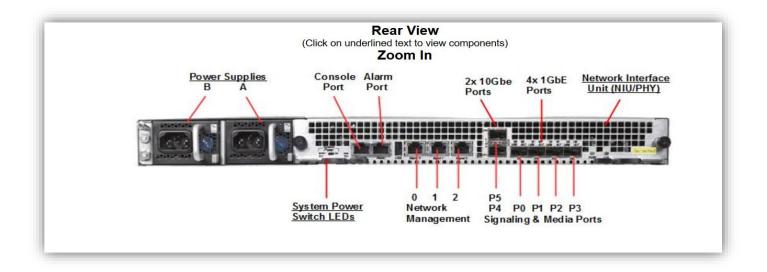


4.3 Booting the SBC

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	🔄 🔹 Currently Sharing 💼 📼 💌
Starting tEbmd	A
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	E
Password: 0x21a059c8 (tAlarm): eth0: Link is up (10	000Mb/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**

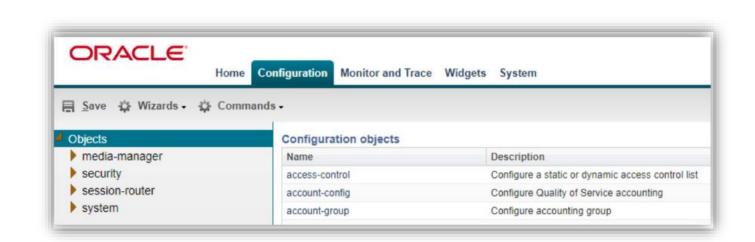
web-server-config		
state	enabled	
inactivity-timeout	5	
http-state	enabled	
http-port	80	
https-state	disabled	
https-port	443	
http-interface-list		
tls-profile		
last-modified-by	admin@console	

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.

Objects	Modify System config		
 media-manager security session-router system fraud-protection host-route network-interface ntp-config phy-interface redundancy-config snmp-community spl-config system-config trap-receiver web-server-config 	Hostname: Description: Location: Mib system contact: Mib system name: Mib system location: Syslog servers Add Edit O Address	GenesysSBC SBC that interacts with Genesys SIP Server	

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 Search Criteria: All 						
filter-config Idap-config		dit Copy Delete	Delete All Upload	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.

accept config		Modify Phy interface			
account-config filter-config					
Idap-config		Name:	s0p0		
local-policy		Operation type:	Media	~	
local-routing-config		Port:	0	(Range: 05)	
media-profile		Slot:	-	(Range: 02)	
session-agent			0	(Range: 02)	
session-group		Virtual mac:			
session-recording-group		Duplex mode:	FULL	~	
session-recording-server		Speed:	100	v	
session-translation		Wancom health score:	50	(Range: 0100)	
sip-config			50	(Range: 0100)	
sip-feature					
sip-interface					
sip-manipulation					
sip-monitoring					
translation-rules					
🖌 system					
fraud-protection					
host-route					
network-interface					
ntp-config					
phy-interface	•		OK		

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

session-recording-group sop0 0 172.18.0.129 0 sip-config sop3 0 192.168.1.94 0 sip-config sip-feature sip-monitoring translation-rules 192.168.1.94 0 sip-monitoring translation-rules translation-rules translation-rules translation-rules translation-rules translation-rules	local-routing-config media-profile	Network interfa Search Criteria: Al					
session-recording-group session-recording-server session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring translation-rules system fraud-protection Name IP address Pri utility at some	session-agent	Add E	dit Copy Delete Dele	te All Upload Download	d	Searc	ch S
session-recording-group sop0 0 172.18.0.129 session-ranslation sop3 0 192.168.1.94 sip-cnfig sip-interface sip-manipulation sip-monitoring translation-rules system fraud-protection		Name	Sub port id	Description	Hostname	IP address	Pri utility addr
session-translation s0p3 0 192.168.1.94 sip-config sip-feature 192.168.1.94 sip-interface sip-manipulation 192.168.1.94 sip-monitoring translation-rules 192.168.1.94 system sip-monitoring 192.168.1.94		s0p0	0			172.18.0.129	
sip-config sip-feature sip-interface sip-manipulation sip-monitoring translation-rules system fraud-protection		s0p3	0			192.168.1.94	
sip-feature sip-interface sip-manipulation sip-monitoring translation-rules system fraud-protection							
sip-interface sip-manipulation sip-monitoring translation-rules system fraud-protection							
sip-manipulation sip-monitoring translation-rules system fraud-protection	•						
sip-monitoring translation-rules system fraud-protection							
system fraud-protection							
fraud-protection	translation-rules						
	system						
host-route	fraud-protection						
	host-route						
	nto config						

📑 Save 👙 Wizards - 👙 Comman	ids -		
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	IP address:		
http-server		172.18.0.129	
network-interface	Pri utility addr:		
network-parameters	Sec utility addr:		
ntp-config phy-interface	Netmask:	255.255.0.0	
redundancy-config	Gateway:		
snmp-address-entry	Gateway.	172.18.0.1	
snmp-community	Gw heartbeat		
snmp-group-entry	State:		
snmp-user-entry	Heartbeat:	2	(Range: 065535)
snmp-view-entry		0	
spl-config	Retry count:	0	(Range: 065535)
system-access-list	Retry timeout:	1	(Range: 165535)
system-config	Health score:	0	(Range: 0100)
threshold-crossing-alert-group			
trap-receiver	DNS IP primary:		
web-server-config	DNS IP backup1:		
	DNS IP backup2:		
	DNS domain:		
	DNS timeout:	11	(Range: 04294967295)
	DNS max ttl:	86400	(Range: 302073600)
	Signaling mtu:	0	(Range: 0, 5764096)
	HIP IP list:	·	1



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.

Objects	Modify Media manager		
media-manager	mouny mount manager		
codec-policy	State:	*	
dns-alg-constraints	Flow time limit:	88400	(Range: 04294967295)
dns-config	Initial guard timer:	300	(Range: 04294967295)
ice-profile	Subsq guard timer:		
media-manager		300	(Range: 04294967295)
media-policy	TCP flow time limit:	86400	(Range: 04294967295)
msrp-config playback-config	TCP initial guard timer:	300	(Range: 04294967295)
realm-config	TCP subsq guard timer:	300	(Range: 04294967295)
realm-group	Hnt rtcp:		
rtcp-policy	Algd log level:	NOTICE	*
static-flow			
steering-pool	Mbcd log level:	NOTICE	~
tcp-media-profile	Options:	Add Edit Delete	
security			
session-router			
system			
capture-receiver			
fraud-protection			
host-route			
http-client	Red max trans:	10000	(Range: 050000)
http-server network-interface	Red sync start time:		
network-parameters		5000	(Range: 04294967295)
ntp-config	Red sync comp time:	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	Tolerance window:	-	
snmp-user-entry		30	(Range: 04294967295)
snmp-view-entry	Untrusted drop threshold:	0	(Range: 0100)
spl-config	Trusted drop threshold:	0	(Range: 0100)
system-access-list system-config	Acl monitor window:	30	(Range: 53600)
threshold-crossing-alert-group	Trap on demote to deny:		
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:		

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:	genesys	~
access-control	Egress Realm ID:	genesys	
account-config	-		*
filter-config	Nat mode:	None	*
Idap-config	Registrar domain:	*	
local-policy	Registrar host:	172.18.0.124	
local-routing-config	-	172.18.0.124	
media-profile	Registrar port:	4080	(Range: 0, 102565535)
session-agent	Options:	Add Edit Delete	2
session-group		max-udp-length=0	
session-recording-group		max-dup-length=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.

Objects d media-manager	 Realm config Search Criteria: All 							
codec-policy	Add Edit	Copy Delete	Delete All Upload	Download		Search	Search	Clea
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		0.0.0.0	s0p3:0	disabled	enabled	enabled	
session-router								
access-control								
account-config								
filter-config								
niter-coning								
Idap-config								
Idap-config								
Idap-config local-policy								
Idap-config local-policy local-routing-config								
Idap-config local-policy local-routing-config media-profile								
Idap-config local-policy local-routing-config media-profile session-agent								
Idap-config Iocal-policy Iocal-policy Iocal-routing-config media-profile session-agent session-agent								
Idap-config Iocal-policy Iocal-routing-config media-profile session-agent session-group session-recording-group								
Idap-config local-policy local-policy media-profile session-agent session-recording-group session-recording-server session-recording-server								
Idap-config local-policy local-routing-config media-profile session-agent session-agent session-recording-group session-recording-server								

Objects	 Modify Realm config 	
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	QoS enable:	
session-agent		
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		

CARARISAN

的现在分词是非常的

andra policy			
codec-policy	Out manipulationid:		*
media-manager	Access control trust level:	high	~
media-policy	Defense il transferi	-	
realm-config	Refer call transfer:	enabled	*
steering-pool	Hold refer reinvite:		
security	Dyn refer term:		
session-router			
access-control	Codec policy:		*
account-config	Codec manIP in realm:		
filter-config	RTCP policy:		~
ldap-config			•
local-policy	Session recording server:		*
local-routing-config	Monitoring filters:	Add Edit De	elete
media-profile			
session-agent			
session-group			
session-recording-group			
session-recording-server	-		
session-translation			
sip-config			
sip-feature	*		
Show advanced		OK Back	
chen autanoou			

Objects	 Modify Realm config 	
🔺 media-manager		
codec-policy	Identifier:	siptrunk
media-manager	Description:	
media-policy		
realm-config		
steering-pool	Network interfaces:	Add Edit Delete
security		
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		
session-group	Media policy:	×
session-recording-group	Class profile:	~
session-recording-server	In translationid:	
session-translation	Out translationide	
sip-config	Out translationid:	×

See progest

Di el des

realm-config			
steering-pool	In manipulationid:		*
security	Out manipulationid:		~
session-router	Access control trust level:	none	~
access-control	Refer call transfer:		
account-config		disabled	*
filter-config	Hold refer reinvite:		
Idap-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	Ŧ	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	Copy Delete Delete All Up	oad Download		Search	Sear
media-manager	IP address	Start port	End port	Realm ID	Network int	terface
media-policy	172.18.0.129	10000	10999	genesys		
realm-config	172.18.0.255	10000	10999	remoteworker		
steering-pool security session-router	192.168.1.94	10000	10999	siptrunk		
access-control						
account-config						
filter-config						
Idap-config						
local-policy						

🗎 Save 🌣 Wizards - 🌣 Comman	nds •			Discard
Objects media-manager codec-policy media-manager media-policy realm-config steering-pool security session-router access-control account-config filter-config local-policy local-policy	Modify Steering pool IP address: Start port: End port: Realm ID: Network interface:	172.18.0.129 10000 10999 genesys	(Range: 165535) (Range: 165535)	Shor



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

account-config	 SIP interface Search Criteria: All 						
filter-config	Add Edit	Copy Delete Delete	All Upload Download	i		Search	Search Cl
Idap-config local-policy	State	Realm ID	Description	Carriers	Trans expire	Initial inv trans	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 sip-feature							

realm-config	Modify SIP interface	e					
steering-pool			_				
security	State:		✓				
session-router	Realm ID:		siptrunk		~		
access-control	Description:						
account-config							
filter-config							
ldap-config	SIP ports						
local-policy							
local-routing-config	Add Edi	t Copy	Delete				
media-profile	Address	Port	1	Fransport protocol	TLS profile	Allow anonymous	
session-agent	192.168.1.94	5060	l. l	JDP		all	
session-group	192.168.1.94	5060	1	TCP		all	
session-recording-group							
session-recording-server							
session-translation							
sip-config	•					•	
sip-feature	Nat traversal:		none		~		
sip-interface	Registration cachin	a:	~				
sip-manipulation	Route to registrar:	-	~				
sip-monitoring							
translation-rules	In manipulationid:		Reject_O	PTIONS	~		
translation-rules							
system	•						

account-config	Modify SIP interface	Modify SIP interface						
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	Add Ed	it Copy	Delete					
session-recording-server session-translation	Address	Port	Tr	ansport protocol	TLS profile	Allow anonymous		
sip-config	172.18.0.129	5060	U	DP		agents-only		
sip-feature	172.18.0.129	5060	т	CP		agents-only		
sip-interface								
sip-manipulation								
sip-monitoring	•					۱.		
translation-rules	Nat traversal:		none		~			
system fraud-protection	Registration cachi	na:						
host-route		-						
network-interface	Route to registrar:							
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 steering-pool	Session agent Search Criteria: All							
security	Add Edit	Copy Delete	Delete All Upload	Download		Search		Search C
session-router	Hostname	IP address	Port	State	App protocol	Realm ID	Descripti	on
access-control	172.18.0.124	172.18.0.124	4080	enabled	SIP	genesys	Genesys	Agent
account-config	192.168.1.93	192.168.1.93	5060	enabled	SIP	siptrunk		
filter-config								
Idap-config								
local-policy								
local-routing-config								
media-profile								

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:	0.000	~
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 sip-monitoring	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			

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	Modify Local policy					
media-manager	mouny coour poncy					
codec-policy	From address:		Add	Edit	Delete	1
media-manager			Aug	Luit	D01010	
media-policy			*			
realm-config						
steering-pool						
security						
session-router						
access-control						
account-config	To address:		Add	Edit	Delete	
filter-config			*			
Idap-config						
local-policy						
local-routing-config						
media-profile						
session-agent						
session-group	Source realm:					
session-recording-group	avarue realit.		Add	Edit	Delete	
session-recording-server			siptrunk	(
session-translation						
sip-config						
sip-feature						
sip-interface						
sip-manipulation						
sip-monitoring	Description:					
translation-rules						
system						
fraud-protection	Policy priority:		none		~	
host-route network-interface	Policy attributes					1
ntp-config						
phy-interface	Add Edit	Copy	Delet	Ð		
redundancy-config	Next hop	Realm		Action	Cost	
snmp-community	172.18.0.124	genesys		none	0	
spl-config						
system-config						
trap-receiver						
web-server-config						
-			OK	Back		
Show advanced						



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

Objects	Modify SIP interface	e				
🔺 media-manager						
codec-policy	State:		✓			
media-manager	Realm ID:		genesys	*		
media-policy	Description:		gonosys			
realm-config	Description.					
steering-pool						
security	SIP ports					
session-router						
access-control	Add Ed	it Copy	Delete			
account-config	Address	Port	Transport protocol	TLS profile	Allow anonymous	
	470.40.0.400	5060	UDP		agents-only	
filter-config	172.18.0.129					
Idap-config	172.18.0.129	5060	TCP		agents-only	
ldap-config local-policy		5060	TCP		agents-only	
ldap-config local-policy local-routing-config		5060	TCP		agents-only	
Idap-config local-policy		5060	ТСР		agents-only	

Objects	 Modify Realm config 		
media-manager codec-policy	Media policy:		•
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:		V
session-recording-server session-translation	Session recording server:		•
sin-config	Monitoring filtors:		
cip comig	~	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 interfact 	e			
🔺 media-manager					
codec-policy	State:		 ✓ 		
media-manager	Realm ID:		siptrunk	~	
media-policy	Description:		oprunk		
realm-config	Description.				
steering-pool					
security	SIP ports				
session-router					
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
ldap-config	192.168.1.94	5060	TCP		all
local-policy					
local-routing-config					
media-profile	1				
session-agent	•				
session-group	Nat traversal:		none	~	
session-recording-group	Registration cachi	ng:	 ✓ 		
	Route to registrar:				
session-recording-server session-translation		In manipulationid:			
session-translation sip-config	In manipulationid:		Reject_OPTIONS	*	
session-translation sip-config sip-feature	In manipulationid: Out manipulationid		Reject_OPTIONS	~	
session-translation sip-config sip-feature sip-interface	Out manipulationic		Reject_OPTIONS		
session-translation sip-config sip-feature sip-interface sip-manipulation			Reject_OPTIONS		
session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring	Out manipulationic		Reject_OPTIONS		
session-translation sip-config sip-feature sip-interface sip-manipulation	Out manipulationic		Reject_OPTIONS		



realm-config	Modify SIP manipulation		
steering-pool			
security	Name:	Reject_OPTIONS	
session-router	Description:		
access-control			
account-config			
filter-config	Split headers:		
ldap-config		Add Edit Delete	
local-policy			
local-routing-config			
media-profile			
session-agent			
session-group			
session-recording-group			
session-recording-server	Join headers:	Add Edit Delete	
session-translation		· · · · ·	
sip-config			
sip-feature			
sip-interface			
sip-manipulation sip-monitoring			
translation-rules			
system	01 D 1		
fraud-protection	CfgRules		
host-route	Add - Edit	Copy Delete Move up Move 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	

realm-config	Modify SIP manipulation	header rule	
steering-pool			
security	Name:	rejectoption	
session-router	Header name:	request-uri	
access-control account-config	Action:	reject	~
filter-config	Comparison type:	case-sensitive	~
ldap-config	Msg type:	request	~
local-policy local-routing-config	Methods:	Add Edit De	lete
media-profile		OPTIONS	
session-agent session-group			
session-recording-group			
session-recording-server			
session-translation			
sip-config sip-feature	Match value:		
sip-interface	New value:		
sip-manipulation	CfgRules		



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.

iects media-manager security ession-router access-control account-config account-group allowed-elements-profile	Translation rules Search Criteria: All Add Edit Copy Delete Delete All Id Type				
session-router access-control account-config account-group					
access-control account-config account-group				Table addre	Search Search
account-group	change delete	Add string	Add index 0	Delete string +	Delete index 0
class-profile					
diameter-manipulation enforcement-profile enum-config					
filter-config					
h323 home-subscriber-server http-alg					
iwf-config Idap-config					
local-policy					
Objects		Modify Session tr	ranslation		
media-mana	ager	,,			
security	-	ld:	1	change1	
session-rou	ter	Rules calling:		Add Edit Delete	
access-c					
account-	-			change	
filter-cont	-				
Idap-cont	-				
local-poli					
media-pr	ting-config				
session-a		Rules called:			
session-g		Nules called.		Add Edit Delete	
	recording-group			change	
	recording-server				
session-t	translation				
sip-config	g				
sip-featu					
sip-interfa					
sip-mani					
sip-monit	-				
translatio	on-rules				
system					
Show	advanced			OK Back	



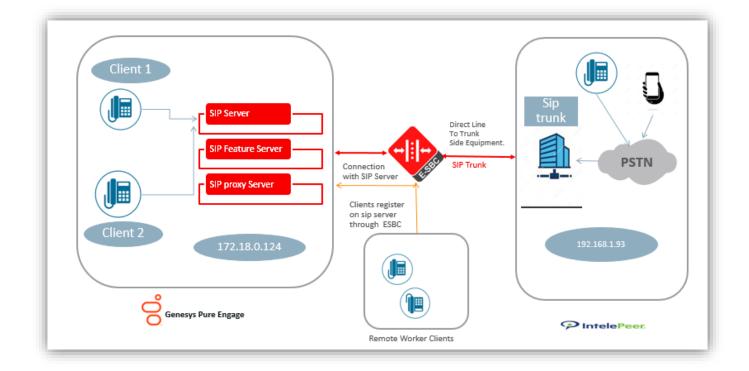
A basic configuration on the Oracle SBC to route calls to and from Genesys server environment is now complete. The following sections highlight some of the useful tips to configure the Oracle SBC in order to successfully resolve and overcome interoperability challenges in a SIP trunking environment between 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'

Objects	Modify Realm config	
media-manager	mouny ream comig	
codec-policy	Identifier:	remoteworker
media-manager	Description:	
media-policy	Description.	
realm-config		
steering-pool	Network Interfaces:	
security	Hetwork Interlaces.	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	Qo S enable:	
session-agent		
session-group	Media policy:	×
session-recording-group	Class profile:	×
session-recording-server	In translationId:	×
session-translation	Out translationid:	· · · · · · · · · · · · · · · · · · ·
sip-config		
sip-feature sip-interface	in manipulationid:	¥
sip-interface sip-manipulation	Out manipulationid:	×
sip-monitoring	Access control trust level:	none
translation-rules	Refer call transfer:	
system		
fraud-protection	Hold refer reinvite:	
host-route	Dyn refer term:	
network-interface	Codec policy:	×
ntp-config	Codec maniP in realm:	
phy-interface		
redundancy-config	RTCP policy:	Y
snmp-community	Session recording server:	¥
spl-config	Monitoring fliters:	Add Edit Delete
system-config	-	Add Cuir Delete
trap-receiver		
web-server-config		
Show advanced		OK. Back

11772/118



6.2. Steering Pool associated with realm remoteworker.

	ne Configuration Monitor and Trac	e Widgets System		
🗐 Save 🔅 Wizards - 🔅 Con	mmands -			
 Objects media-manager 	Modify Steering pool			
codec-policy	IP address:	172.18.0.255		
media-manager	start port:	10000	(Range: 165535)	
media-policy realm-config	End port:	10999	(Range: 165535)	
steering-pool	Realm ID:	remoteworker	*	
security	Network Interface:		~	
session-router				
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.

Objects Modify SIP interface media-manager State: media-manager Realm ID: media-noing Description: steering-pool Security secense-control access-control account-config Add filter-config Aldow anonyn idap-config all local-policy all	/mc
media-manager Realm ID: remoteworker media-policy Description: realm-config Image: Config access-control account-config access-control account-config Add Edit Copy Delete Address Port Transport protocol TLS profile Aldress Port Idap-config ail	/mou
media-policy realm-config steering-pool Description: security SIP ports access-control account-config filter-config ldap-config local-policy Add	/mous
media-policy Description: realm-config Description: setering-pool SIP ports session-router Add access-control Add edit cognot Port Transport protocol TLS profile Aldoress Port Transport protocol TLS profile Aldoress Port Idap-config 172.18.0.255 local-policy ODP	/mous
realm-config steering-pool security SIP ports access-control account-config filter-config local-policy difference and an analysis of the security of the security sec	mous
security session-router access-control account-config filter-config local-policy	mous
SIP ports access-control account-config filter-config local-policy Add Edit Copy Delete Address Port Transport protocol TLS profile Allow anonyn Idap-config	/mous
session-router Add Edit Copy Delete access-control Address Port Transport protocol TLS profile Allow anonyn filter-config 172.18.0.255 5060 UDP all	/mous
account-config filter-config ldap-config local-policy	mous
filter-config Idap-config Iocal-policy	ymous
Idap-config local-policy	
local-policy	
local-routing-config	
media-profile	
session-agent	
session-group Nat traversal: none 🗸	
session-recording-group Registration caching:	
session-recording-server Route to registrar:	
session-manistation	
sip-reature Out manipulationid:	
sip-manipulation Service tag:	
sip-manipulation	
translation-rules	
system	
fraud-protection	
host-route	
network-interface	
OK Back	



6.4 Local-policy

Objects	Modify Local policy					
🔺 media-manager						
codec-policy	From address:		Add	Edit	Delete	
media-manager						
media-policy			*			
realm-config						
steering-pool						
security						
session-router						
access-control						
account-config	To address:		Add	Edit	Delete	
filter-config			*			_
Idap-config						
local-policy						
local-routing-config						
media-profile						
session-agent						
session-group	Source realm:					
session-recording-group	addree realm.		Add	Edit	Delete	
session-recording-server			remote	vorker		
session-translation						
sip-config						
sip-feature						
sip-interface						
sip-manipulation						
sip-monitoring	Description:					-
translation-rules						
✓ system						
fraud-protection	Policy priority:		none			~
host-route			none			¥
network-interface	Policy attributes					
ntp-config	Add Edit	Сору	Delet	9		
phy-interface	Next hop	Realm		Action	Cost	t
redundancy-config	172.18.0.124	genesys		none	0	
snmp-community						
spl-config						
system-config						
trap-receiver						
web-server-config			04	Ba	sik	
Show advanced				Da		

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.

Dbjects	Modify Session age	ent			
media-manager	Monitoring filters:		Add Edit	Delete	
security			- Logit	and the second s	
session-router					
access-control					
account-config					
account-group allowed-elements-profile					
class-profile					
diameter-manipulation	Auth attribute				
enforcement-profile	Add Ed	it Copy	Delete		
enum-config	Auth realm	Username	Password	In dialog methods	
filter-config h323	Switch	user	*******	Invite	
home-subscriber-server					
http-alg					
iwf-config					
Idap-config					
local-policy					
local-response-map	Session recording			*	
local-routing-config	Session recording	required:			
media-profile	Hold refer reinvite:				
net-management-control	Send TCP fin:				
qos-constraints	SIP recursion polic				
response-map				*	
service-health session-agent	Sm icsi match for i	nvite:	Add Edit	Delete	
session-agent-id-rule					
session-agent-id-rule session-constraints					
session-agent-id-rule session-constraints session-group					
session-agent-id-rule session-constraints					



8. Test Plan Executed.

8.1 Equipment Requirements

Table below identifies equipment used for testing

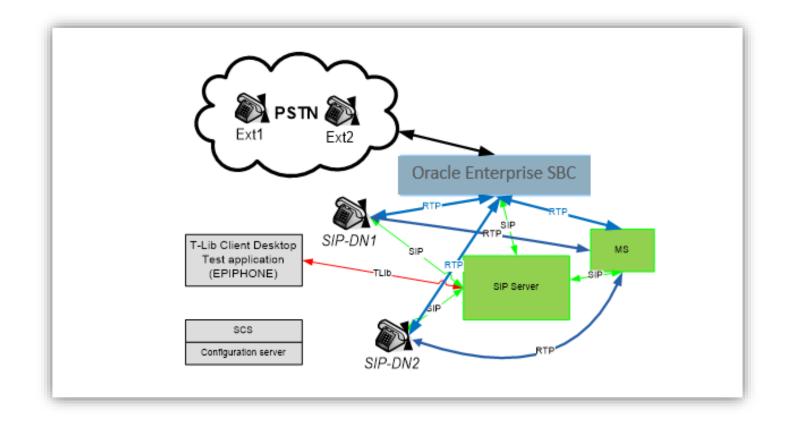
Product	Version	Units	Notes
SIP Server	8.1.1	1	Standalone deployment
Resourse manager (RM)	9.0	1	
Media Control Platform (MCP)	9.0	1	
Genesys Management Framework	8.1	1	
T-Lib Client Desktop Test		1	EpiPhone application
application			
Oracle SBC SCZ900p3 or above		1	
SIP End Point		3	
PSTN phone		2	

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_dn3}, 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. Enabling Remote worker (for remote workers registering into Genesys SIP server via the Oracle SBC over secure connection)

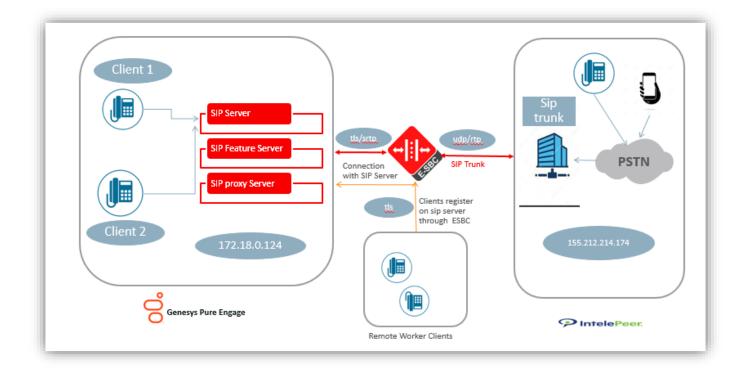
-///

Testing is performed for Genesys remote Agents to connect to the Oracle SBC over a secure connection. Agents register and make calls over a secure connection through the Oracle SBC.

In order to perform the testing we have used TLS/SRTP protocol between the SIP server and the SBC. This requires additional configuration/configuration changes to the configuration mentioned in <u>section</u> 6 of the document.

Below figure illustrates how remote workers register onto the SIP Server via the SBC over a secure connection.

Endpoints register onto SIP server via SBC over a TLS connection. The audio on inbound calls and outbound calls from the endpoints is secured via SRTP.





The following additional configuration objects are configured on the Oracle SBC to create a secured connection between Genesys side and the SBC.

- Signaling Security configuration
- Media Security configuration

9.1 Signaling Security configuration

9.1.1 Certificate Records

"**Certificate-records**" are configuration elements on Oracle SBC which captures information for a TLS certificate such as common-name, key-size, key-usage etc.

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC's configuration.

GUI Path: security/certificate-record ACLI Path: config t->security->certificate-record

For the purposes of this application note, we'll create three certificate records on the Oracle SBC. They are as follows:

SBC Certificate (end-entity certificate) Genesys Endpoint Certificate Root CA certificate

The SBC's end entity certificate is what is presented to Genesys signed by your CA authority.

For Testing we have created a Certificate Authority (CA) on the Windows Server that is running the Genesys Framework components in our Lab Server. For the purpose of App note we have signed the SBC end entity certificate and the Genesys Endpoint Certificate from the same CA.



To configure the certificate record:

Click Add, and configure the SBC certificate as shown below:

tlscert – is the name of SBC endpoint certificate record created on the SBC.

Objects	Modify Certificate record	
media-manager		
security	Name:	liscert
admin-security	Country:	US
auth-params authentication	State:	california
authentication-profile	Locality:	Redwood
cert-status-profile	Organization:	Engineering
certificate-record	Unit:	
 ike ipsec 	Common name:	sbcinternal
media-security	Key size:	2048
password-policy	Alternate name:	
public-key security-config	Trusted:	
ssh-config	Key usage list:	Add Edit Delete
tls-global		digitalSignature
tls-profile		keyEncipherment
session-router		
▶ system		
		ОК Васк
Show advanced		Dack

Objects	Modify Certificate record		
media-manager			
security			
admin-security	Extended key usage list:		
auth-params	Extended key usage list.	Add Edit Delete	
authentication		serverAuth	
authentication-profile			
cert-status-profile			
certificate-record			
🕨 ike			
ipsec			
media-security	Key algor:	C2	
password-policy		154	
public-key	Digest algor:	sha256	r
security-config	Ecdsa key size:	p256 🗸	
ssh-config	Cert status profile list:	Add Edit Delete	
tls-global		Add Edit Delete	
tls-profile			
session-router			
system			
Show advanced		OK Back	

11772711

Click **OK** at the bottom

2///

Using this same procedure, configure certificate records for **Root CA** and **Genesys Endpoint** Certificate.



genesysep: - is the name of Genesys Endpoint Certificate which is created for communication between the SBC and Genesys Sip Server.

Objects	Modify Certificate record	
media-manager		
security	Name:	genesysep
admin-security	Country:	US
auth-params	State:	
authentication		MA
authentication-profile	Locality:	Burlington
cert-status-profile	Organization:	Engineering
certificate-record	Unit:	
▶ ike	Common name:	
▶ ipsec	Common name.	WINGENPE
media-security	Key size:	1024 💌
password-policy	Alternate name:	
public-key	Trusted:	
security-config		_
ssh-config	Key usage list:	Add Edit Delete
tls-global		digitalSignature
tls-profile		keyEncipherment
session-router		
system		
		OK Back
Show advanced		Dack

Objects	Modify Certificate record		
media-manager			
security	Extended key usage list:	Add Edit Dele	to
admin-security		· · · · ·	LG
auth-params		clientAuth	
authentication		serverAuth	
authentication-profile			
cert-status-profile			
certificate-record			
🕨 ike			
ipsec	Key algor:	rsa	~
media-security	Digest algor:	sha1	~
password-policy			
public-key	Ecdsa key size:	p256	~
security-config	Cert status profile list:	Add Edit Dele	te
ssh-config			
tls-global			
tls-profile			
session-router			
system			
Show advanced		OK Back	



genesysca :- is the name of certificate record created for certificate authority which is used to sign the certificates.

Objects	Modify Certificate record	
media-manager		
security	Name:	genesysca
admin-security	Country:	US
auth-params	State:	
authentication		MA
authentication-profile	Locality:	Burlington
cert-status-profile	Organization:	Engineering
certificate-record	Unit:	
▶ ike	Common name:	
ipsec	Common name:	WINGENPE-CA-1
media-security	Key size:	2048 💌
password-policy	Alternate name:	
public-key	Trusted:	
security-config		
ssh-config	Key usage list:	Add Edit Delete
tls-global		digitalSignature
tls-profile		keyEncipherment
session-router		
system		
		OK Back
Show advanced		Duok



Objects Media-manager	Modify Certificate record		
security			
 admin-security 	Extended key usage list:	Add Edit Delet	e
auth-params		serverAuth	
authentication			
authentication-profile			
cert-status-profile			
certificate-record			
ike			
ipsec	Key algor:		
media-security		rsa	*
password-policy	Digest algor:	sha256	×
public-key	Ecdsa key size:	p256	~
security-config	Cert status profile list:	•	
ssh-config		Add Edit Delet	e
tis-global			
tls-profile			
session-router			
system			
		OK Back	

9.1.2 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. This is not required for the Genesys Endpoint Certificate and the CA certificate that have been created.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:



Objects media-manager	Certificate record Search Criteria: All			Į				
security	Add Edit	Copy Delete	e Delete All Upload	Download Generate	Import		Search Se	arch Clear
admin-security	Name	Country	State	Locality	Organization	Unit	Common na	me
auth-params	genesysca	US	MA	Burlington	Engineering		WINGENPE-	CA-1
authentication	genesysep	US	MA	Burlington	Engineering		WINGENPE	
authentication-profile cert-status-profile	tiscert	US	california	Redwood	Engineering		sbcinternal	
certificate-record								
ike								
ipsec								
media-security								
password-policy								
public-key								

A window as show below will pop up.

Copy the following information and send to a CA a	uthority
BEGIN CERTIFICATE REQUEST MIIC7TCCAdUCAQAwdTELMAkGA1UEBhMCVVMxC MwEQYDVOQH	zAJBgNVBAgTAk1BMR
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbr EAxMIY3Vz	mVlcmluZzEuMCwGA1U
dG9tZXJzLnRlbGVjaGF0Lm8tdGVzdDA2MTYxOTc3L ZlhvcN	
AQEBBQADggEPADCCAQoCggEBAKYzWQF5/+hu6 njns4+Dul	
S5deNI0pWT5fX9oja4Ks0fL9qWhGIAD0gLAQ9SRkO9 suC52	dLQpuVWNvvRB9NL+9
pDPSIQNFthXxSI2QVUoQx+LQGBe4HvNjyIHi0ICE0c wVKwE	NNS9wEQKvKStqXen8
3txwuw5ehHEdepbg8geiXat47SCcyFZ5H/wwEk55Wk paL	
pU73vRn3JDJqPVNa4IXt7wXC5uhDdw5805bhCM5Tc Ytu	HsX0IR+dk/S7OLgfyDy/

Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

Also note, at this point, a save and activate is required before you can import the certificates to each certificate record created above.



9.1.3 Import Certificates to SBC

Once certificate signing request has been completed – import the signed certificate to the SBC. Please note – all certificates including **Root CA and Genesys Endpoint certificates** are required to be imported to the SBC.

Click import and that will open the window to import the certificate. You can either specify the certificate file path or copy the certificate contents and paste on the window.

Once all certificates have been imported, issue save/activate from the WebGUI.

Add Edit Copy Delete Delete All Delete Delete Dele	Objects	Certificate record							
• winis-security authenication authenication or status-profile certificate record • ke • posc • media-security authenication • attentication • attentication-profile certificate record • ke • posc • media-security authenication-profile certificate record • ke • posc • media-security authenication • attentication • attentication-profile certificate record • ke • posc • media-security authenication • attentication-profile certificate record • ke • posc • media-security authenication • ker Vistards - Certificate record • Ke • posc • media-security authenication • ker Certificate record • Ke • posc • media-security authenication • port Import certificate • file • paster • post • file • paster • post • file • paster • post • file • paster • post • modia-security • attentication • port • file • post • modia-security • pastord-policy • public-key • security-config •	Media-manager	Search Criteria: All				•			
authentication-profile Vince Vi		Add Edit	Copy Delete	e Delete All Upload	Download Generate	Import	Sei	arch	Search Cle
authentication entristatus-portile entristatus-p		Name	Country	State	Locality	Organization	Unit		
authentication-profile etc: security-posting media-security authentication-profile certificate record we security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile ession-router sthere security-config ssh-config tis-profile ession-router security-config ssh-config tis-profile t		genesysca	US	MA	Burlington	Engineering		WINGENF	PE-CA-1
ectificate record us u		genesysep	US	MA	Burlington	Engineering		WINGENF	ΡE
economicate record Pase Pase Pase Pase control Pase control Pase control Pase control Pase control Commands - ects Certificate record Security control Certificate record auth-params Comment control auth-params Use control auth-params Use control certificate record Prime genesysca Use control certificate-record Browse paseword-policy Public-key security control Esconomicate record pase control Esconomicate record retificate-record Use control retificate-record Import retificate-record Import retificate-record Import retificate-record Import		tiscert	US	california	Redwood	Engineering		sbcinterna	l
we psec psec psec predia-security psecvity-config auteritation Certificate record Search Criteria All Add Edit Cop Name Comat: interaction mort method: authentication Search Criteria All interaction-profile Mane certificate record Search Criteria All interaction-profile Mane certificate record Search Criteria All interaction-profile Import method: certificate-record Search Criteria All interaction-profile Import method: certificate-record Import method: iscent US genesysca Import method: iscent US pspc media-secunty pasword-policy <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
<pre>prec media-security public-key security-config seturt-ocofig security-config seturt-ocofig seturt-ocofig security-config seturt-params authentication authentication authentication peresysca ect-status-profile cert-status-profile security password-policy public-key security-config security-confi</pre>									
Import Certificate ects ecta auth-security auth-security auth-security auth-security authentication authentication authentication penesysep uscertificate ispeci media-security password-policy public-key security-config is-polie wession-router									
security-config security-config tartificate-record kee is-security authentication-profile certificate-record kee ispec media-security password-policy public-key security-config ssh-config tis-profile tis-profil									
security-config ave Vizards Vizards Commands Certificate record ects necia-manager ecurity admin-security authentication-profile cert-status-profile cert-status-profile certificate record i ke password-policy public-key security-config ssh-config tis-profile ession-router	password-policy								
ave ♣ Wizards + ♣ Commands - ects needia-manager ecurity admin-security auth-params authentication authentication-profile certificate-record ke ipsec media-security public-key security-config ts-profile ts-profile ession-router	public-key								
ave ♣ Wizards + ♣ Commands - ects hedia-manager ecurity auth-params authentication authentication cert-status-profile certificate-record ke pisec hedia-security password-policy public-key security password-po	security-config								
cts Search Criteria: All Add Edit admin-security Add auth-params genesysca authentication genesysca authentication-profile Certificate record cert-status-profile Certificate file: certificate-record Import certificate file: ike ipsec media-security password-policy public-key security ssh-config ssh-config tts-global tts-global tts-global tts-profile									
cts Search Criteria: All Add Edit genesysca Us genesysca Us itscert Us itscert Us itscert Us isseconfly enering adit-security neering password-policy public-key security-config ssh-config tis-gobal tis-gobal tis-gobal Import tis-gobal Import <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
cels Search Criteria: All edia-manager cecurity admin-security auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config tts-global tts-global tts-profile	ave 🗱 Wizards - 🛱 Co	mmands -							
edia-manager edia-manager edia-manager edia-manager admin-security auth-params authentication genesysca g				Import certificat	<u>م</u>				
Add Edit Cor admin-security Name Cor auth-params genesysca US authentication genesysep US tscert US tscert US tscert/staus-profile certificate-record ike ipsec media-security password-policy public-key security-config ts-config ts-profile t				mport certinicat	-				
Add Edit Cop admin-security Name Cot auth-params genesysca US authentication-profile genesysep US certificate-record tiscert US ike ipsec import ipsec media-security password-policy public-key public-key security-config ssh-config tis-profile tis-global tis-profile		Jearch Ch	iteria. Ali	Format:	try-all		~		
auth-params auth-params authentication authentication-profile certificate-record ike ipsec media-security password-policy public-key security-config tls-pofile tls-pofile ession-router	ecurity	Add	Edit	Cop	uy un				
auth-params genesysca US ineering authentication genesysep US genesysep US ineering cert-status-profile itscert US certificate-record iscert US ike ipsec ineering media-security password-policy ineering public-key security-config integration ssh-config its-profile integration tis-global tis-profile integration ession-router integration integration				Import methods	Cila O Dacta			anization	Un
authentication genesysep US genesysep US certificate-record itscert ike ipsec media-security password-policy public-key security-config ssh-config tis-profile tis-profile use	admin-security	Namo							
authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tis-global tis-profile tis-profile Import Cancel									UI
cert.status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tls-global tls-profile ession-router	auth-params						Browse		01
cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tis-global tis-profile tis-profile tis-profile	auth-params authentication	genesys	ca	US Certificate file:			Browse	ineering	0
ike ipsec media-security password-policy public-key security-config ssh-config tis-global tis-profile tession-router	auth-params authentication	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
ipsec media-security password-policy public-key security-config ssh-config tis-global tis-profile tession-router	auth-params authentication authentication-profile	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
 ipsec media-security password-policy public-key security-config ssh-config tis-global tis-profile ession-router 	auth-params authentication authentication-profile cert-status-profile	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
media-security password-policy public-key security-config ssh-config tls-global tls-profile ession-router	auth-params authentication authentication-profile cert-status-profile certificate-record	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
password-policy public-key security-config ssh-config tis-global tis-profile Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
public-key security-config ssh-config tis-global tis-profile Import Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record kike ipsec	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
security-config ssh-config tls-global tls-profile Import Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
security-config ssh-config tis-global tis-profile Import Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
ssh-config tls-global tls-profile Import Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
tls-global tls-profile Import Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record kike ipsec media-security password-policy public-key	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
tls-profile Import Cancel	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
ession-router	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
ession-router	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tls-global	genesyse genesyse	ca ep	US Certificate file:			Browse	ineering ineering	
ystem	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tls-global	genesyse genesyse	ca ep	US Certificate file:		Cancel	Browse	ineering ineering	
	auth-params authentication authentication-profile cert-status-profile certificate-record kke ipsec media-security password-policy public-key security-config ssh-config tls-global tls-profile	genesyse genesyse	ca ep	US Certificate file:		Cancel	Browse	ineering ineering	
	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tls-global tls-profile ession-router	genesyse genesyse	ca ep	US Certificate file:		Cancel	Browse	ineering ineering	
Show advanced Displaying 1 - 3 of 3	auth-params authentication authentication-profile cert-status-profile certificate-record ike ipsec media-security password-policy public-key security-config ssh-config tls-global tls-profile ession-router	genesyse genesyse	ca ep	US Certificate file:		Cancel	Browse	ineering ineering	



9.1.4 TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile ACLI Path: config t->security->tls-profile

Click Add, use the example below to configure

Here **genesystls** is the name of the tls-profile that has been created for the use encryption with Genesys side.

📑 Save 🛟 Wizards - 😫 Commande	S •		
 Objects media-manager 	Modify TLS profile		
security	Name:	genesystis	
admin-security	End entity certificate:	tiscert	
auth-params authentication	Trusted ca certificates:	Add Edit Delete	
authentication-profile		genesysca	_
cert-status-profile		genesysep	
certificate-record			
▶ ike			
ipsec			
media-security			
password-policy public-key	Cipher list:	Add Edit Delete	
security-config		ALL	
ssh-config			
tls-global			
tls-profile			
session-router			
system			
	Verify depth:	10	(Range: 0 10)
Show advanced		OK Back	

Click **OK** at the bottom



9.2 Media Security Configuration

This section outlines how to configure support for media security between the Oracle SBC and Sip Server/Agent Endpoints.

9.2.1 sdes-profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

GUI Path: security/media-security/sdes-profile ACLI Path: config t->security->media-security->sdes-profile

Click Add, and use the example below to configure

rtcp-policy	 Modify Sdes profile 	
static-flow		
steering-pool	Name:	sdes1
tcp-media-profile security	Crypto list:	Add Edit Delete
admin-security		AES_CM_128_HMAC_SHA1_32
auth-params		AES_CM_128_HMAC_SHA1_80
authentication		ARIA_CM_192_HMAC_SHA1_32
authentication-profile		ARIA_CM_192_HMAC_SHA1_80
cert-status-profile		
certificate-record		
▶ ike	Srtp auth:	
ipsec	Srtp encrypt:	
media-security	SrTCP encrypt:	
dtls-srtp-profile		
media-sec-policy	Mki:	
sdes-profile	Egress offer format:	same-as-ingress
sipura-profile	Use ingress session params:	Add Edit Delete
password-policy public-key		Find Lone Doloto
security-config		
ssh-config		
Show advanced	Ť	OK Back

Click **OK** at the bottom



9.2.2 Media Security Policy

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used.

In this example, we are configuring two media security policies. One to secure and decrypt media toward Genesys side and other for non-secure media facing PSTN side.

GUI Path: security/media-security/media-sec-policy ACLI Path: config t->security->media-security->media-sec-policy

Click Add, use the examples below to configure.

msp1 is the name of the media-sec-policy for the secured side.

rtcp-policy	 Modify Media sec policy 		
static-flow			
steering-pool	Name:	msp1	
tcp-media-profile	Pass through:		
security	Options:		
admin-security	Options.	Add Edit Delete	
auth-params			
authentication			
authentication-profile			
cert-status-profile			
certificate-record			
) ike			
) ipsec			
media-security	Inbound Profile:		
dtls-srtp-profile		sdes1 👻	
media-sec-policy	Mode:	srtp 👻	
sdes-profile	Protocol:	sdes 💌	
sipura-profile	Hide egress media update:		
password-policy public-key			
dtls-srtp-profile	Outbound		
media-sec-policy	Profile:	sdes1	×
sdes-profile	Mode:		
sipura-profile	Mode:	srtp	*
password-policy	Protocol:	sdes	~
public-key		<u>(</u>	
security-config			
ssh-config	-		
Show advanced		OK Back	



removecrypto is the name of the media-sec-policy for the non-secured side.

rtcp-policy	 Modify Media sec policy 		
static-flow			
steering-pool	Name:	rempovecrypto	
tcp-media-profile	Pass through:		
security	Options:		
admin-security	Options.	Add Edit Delete	
auth-params			
authentication			
authentication-profile			
cert-status-profile			
certificate-record			
ike			
• ipsec			
media-security	🛋 Inbound		
dtls-srtp-profile	Profile:	×	
media-sec-policy	Mode:	rtp 🗸	
sdes-profile	Protocol:		
sipura-profile			
password-policy	Hide egress media update:		
dtls-srtp-profile	Outbound		
media-sec-policy	Profile:		
sdes-profile		~	
sipura-profile	Mode:	rtp 🗸	•
password-policy	Protocol:	none	•
public-key			
security-config			
ssh-config	*		
		OK Back	

9.3 Changes to SBC configuration.

The following changes are made to the SBC to the SBC configuration objects to incorporate the tls/srtp related parameters functionality.



9.31. Change to the sip-interface configuration object

Sip-port '**5061**' for tls is added on the sip-interfaces facing the Genesys side.

Idap-config	Modify SIP interfa	ce				
local-policy						
local-response-map	State:		✓			
local-routing-config	Realm ID:		genesys	~		
media-profile net-management-control	Description:		genesys			
gos-constraints						
response-map						
service-health	SIP ports					
session-agent	Add Ed	lit Copy	Delete			
session-agent-id-rule	Address	Port	Transport prote	ocol TLS profile	Allow anonymous	
session-constraints	10.232.50.50	5061	TLS	genesystls	all	
session-group	10.232.50.50	5060	UDP		all	
session-recording-group						
session-recording-server						
session-timer-profile						
session-translation	4				۱.	
sip-advanced-logging	Initial inv trans ex	pire:	0	(Range:	0999999999)	
sip-config	Session max life I	imit:	0			
sip-feature			0			
sip-feature-caps	Proxy mode:			*		
sip-interface	-					



local-response-map	Modify SIP inter	face			
local-routing-config					
media-profile	State:		✓		
net-management-control	Realm ID:				
qos-constraints	Realin ID.		remoteworker	*	
response-map	Description:				
service-health					
session-agent					
session-agent-id-rule	SIP ports				
session-constraints	Add	Edit Copy	Delete		
session-group	Address	Port	Transport protoc	TLS profile	Allow anonymous
session-recording-group	10.232.50.60	5061	TLS	genesystis	all
session-recording-server	10.232.50.60	5080	UDP	genesysus	all
session-timer-profile	10.232.30.00	5060	UDF		aii
session-translation					
sip-advanced-logging					
sip-config	4				4
sip-feature	Initial inv trans	oxpiro			
sip-feature-caps			0	(Range	: 0999999999)
sip-interface	Session max life	e limit:	0		
sip-manipulation	Proxy mode:			~	
				l	

Registration caching must enabled on the sip-interface associated with realm 'remoteworker'.

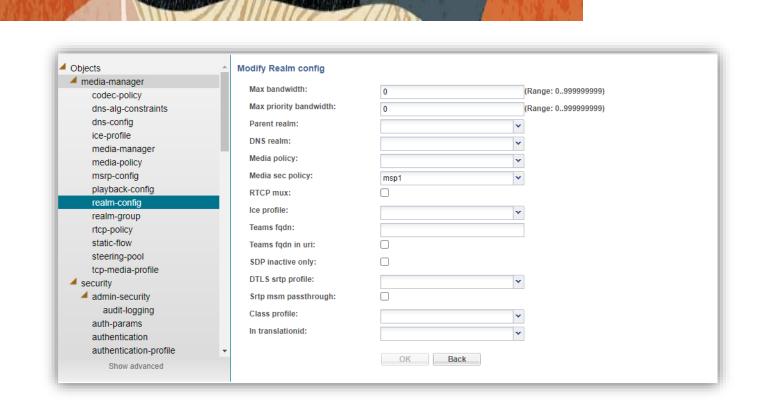
local-response-map	 Modify SIP interface 		
local-routing-config			
media-profile	4		•
net-management-control	Initial inv trans expire:	0	(Range: 099999999)
qos-constraints	Session max life limit:	0	
response-map	Proxy mode:	•	
service-health	Proxy mode.		*
session-agent	Redirect action:		v
session-agent-id-rule	Nat traversal:	none	v
session-constraints	Nat interval:	22	(Danger 0, 4204067205)
session-group		30	(Range: 04294967295)
session-recording-group	TCP nat interval:	90	(Range: 04294967295)
session-recording-server	Registration caching:		
session-timer-profile	Min reg expire:	300	(Range: 099999999)
session-translation		300	(Range: 0999999999)
sip-advanced-logging	Registration interval:	3600	(Range: 04294967295)
sip-config	Route to registrar:	 ✓ 	
sip-feature	Secured network:		
sip-feature-caps	Uri fada domain		
sip-interface	Uri fqdn domain:		
sip-manipulation	Options:	Add Edit Delete	
sip-monitoring	-		
Show advanced		OK Back	



9.3.2 Change to the realm-config configuration object

Media-sec-policy **msp1** is added to the realms facing Genesys side to secure the media towards sip server. The policy is added on realms **genesys** and **remoteworker**.

bjects	 Modify Realm config 		
media-manager			
codec-policy	Identifier:	genesys	
dns-alg-constraints	Description:		
dns-config			
ice-profile			
media-manager	Addr prefix:	0.0.0.0	
media-policy		0.0.0.0	
msrp-config	Network interfaces:	Add Edit Delete	
playback-config		M10:0.4	
realm-config			
realm-group			
rtcp-policy			
static-flow			
steering-pool			
tcp-media-profile	Mm in realm:		
security			
admin-security	Mm in network:		
audit-logging	Mm same ip:		
auth-params	QoS enable:		
authentication			
authentication-profile	•		
Show advanced		OK Back	



L.S. LI BRAKE

Objects	Modify Realm config	
media-manager		
codec-policy	Identifier:	remoteworker
dns-alg-constraints	Description:	
dns-config		
ice-profile		
media-manager	Addr prefix:	0.0.0.0
media-policy	Network interfaces:	0.0.0
msrp-config	Network Interfaces:	Add Edit Delete
playback-config		M10:0.4
realm-config		
realm-group		
rtcp-policy		
static-flow		
steering-pool		
tcp-media-profile	Mm in realm:	\square
security		
admin-security	Mm in network:	
audit-logging	Mm same ip:	
auth-params	QoS enable:	
authentication		0

RACE	NAMES OF THE OWNER OWNER OF THE OWNER OWN	Andread

ice-profile	QoS enable:	
media-manager media-policy	Max bandwidth:	0 (Range: 0999999999)
msrp-config	Max priority bandwidth:	0 (Range: 0999999999)
playback-config	Parent realm:	×
realm-config	DNS realm:	×
realm-group rtcp-policy	Media policy:	×
static-flow	Media sec policy:	msp1 💌
steering-pool	RTCP mux:	
tcp-media-profile security	Ice profile:	v
admin-security	Teams fqdn:	
audit-logging	Teams fqdn in uri:	
auth-params	SDP inactive only:	
authentication authentication-profile	DTI & erto profilo:	
Show advanced		OK Back

Media-sec-policy **removecrypto** is added to the realm facing the PSTN side **SIPtrunk** to remove the crypto attributes towards the PSTN side. This change is made because the sip trunk only supports UDP/RTP protocols.

ojects	 Modify Realm config 	
media-manager		
codec-policy	Identifier:	SIPTrunk
dns-alg-constraints	Description:	
dns-config		
ice-profile		
media-manager	Addr prefix:	
media-policy		0.0.0.0
msrp-config	Network interfaces:	Add Edit Delete
playback-config		M00:0
realm-config		
realm-group		
rtcp-policy		
static-flow		
steering-pool		
tcp-media-profile	Mm in realm:	
security		
admin-security	Mm in network:	
audit-logging	Mm same ip:	
auth-params	QoS enable:	
authentication		_
authentication-profile	-	OK Bask
Show advanced		OK Back

Objects	Modify Realm config		
media-manager	wim in realm:	1	
codec-policy dns-alg-constraints	Mm in network:		
dns-config	Mm same ip:		
ice-profile	QoS enable:		
media-manager media-policy	Max bandwidth:	0	(Range: 0999999999)
msrp-config	Max priority bandwidth:	0	(Range: 099999999)
playback-config	Parent realm:		•
realm-config	DNS realm:		
realm-group rtcp-policy	Media policy:		•
static-flow	Media sec policy:	rempovecrypto	r
steering-pool	RTCP mux:		
tcp-media-profile	Ice profile:		•
 admin-security 	Teams fqdn:		
audit-logging	Teams fqdn in uri:		
auth-params	SDP inactive only:		
authentication authentication-profile	DTI 6 erto profilo:		-
Show advanced		OK Back	



9.3.3 Change to the session-agent configuration object.

The session-agent configured for Genesys sip server is modified to reflect the tls port on the sip server and the transport protocol of tls.

h323 home-subscriber-server	 Session agent Search Criteria: All 							
http-alg	Add Edit	Copy Delete	Delete All Upload	Download		Search	Search	Clea
iwf-config	Hostname	IP address	Port	State	App protocol	Realm ID	Description	
Idap-config	172.18.0.124	172.18.0.124	5069	enabled	SIP	genesys	Genesys Agent	
local-policy	172.18.0.133	172.18.0.133	5060	enabled	SIP	genesys		
local-response-map	68.68.117.67	68.68.117.67	5060	enabled	SIP	SIPTrunk		
local-routing-config								
media-profile								
net-management-control								
qos-constraints								
response-map								
response-map service-health								

h323	 Modify Session agent 		
home-subscriber-server			
http-alg	Hostname:	h72.18.0.124	
iwf-config	IP address:	172.18.0.124	
Idap-config	Port:	5069	(Range: 0, 102565535)
local-policy	State:	✓	
local-response-map			
local-routing-config	App protocol:	SIP	~
media-profile	App type:		~
net-management-control	Transport method:	StaticTLS	*
qos-constraints		StaticTLS	•
response-map	Realm ID:	genesys	*
service-health	Egress Realm ID:		v
session-agent	Description:	Genesys Agent	
session-agent-id-rule		Control / Ngoni	
session-constraints			
session-group	Match identifier		
session-recording-group			
session-recording-server	Add Edit	Copy Delete	
session-timer-profile	Identifier rule	Match v	value
session-translation			
sip-advanced-logging	•	OK Back	
Show advanced		DACK	



9.3.4 Local-policy

There is no change made to the local-policy and a local-policy like below is configured to route registrations from realm **remoteworker** to the sip server on realm **genesys**. Alternatively route-to-registrar parameter can also be used on the remoteworker sip-interface to route the register request to sip-server.

class-profile	Modify Local policy
diameter-manipulation	
enforcement-profile	From address: Add Edit Delete
enum-config	Add Edit Delete
filter-config	*
h323	
home-subscriber-server	
http-alg	
iwf-config	
Idap-config	
local-policy	To address: Add Edit Delete
local-response-map	*
local-routing-config	
media-profile	
net-management-control	
qos-constraints	
response-map	
service-health	
session-agent	Source realm: Add Edit Delete
session-agent-id-rule	remoteworker
session-constraints	
session-group	
Show advanced	OK Back
h323	Description:
home-subscriber-server	
http-alg	
iwf-config	State:
Idap-config	Policy priority:
local-policy	Policy attributes
local-response-map local-routing-config	Add Edit Copy Delete
media-profile	Next hop Realm Action Terminate recursion Cost
net-management-control	172.18.0.124 genesys none disabled 0
qos-constraints	
response-map	
service-health	
session-agent	
session-agent-id-rule	4 F
session-constraints session-group	



9.5 Genesys side configuration.

The following configuration is required on the Genesys side for the successful implementation.

Note: All the Genesys components of the Lab are running on Windows Server 2012. The steps differ when the Genesys applications are running on Unix based systems. For the purpose of App note we have provided steps required to be configured for Windows based Genesys application. These steps may vary depending upon your implementation type and changes should be made accordingly to your setup. Steps below are for the use of simple TLS and additional steps need to be configured if mutual authentication is required.

9.5.1 Prerequisites.

Before starting to configure your secure connections with TLS, you must have done the following:

Generated certificates, with associated private and public keys, and CRLs. Made certificates available for applications on hosts.

TLS certificates must be generated and installed appropriately on any host that runs Genesys applications that utilize TLS secure connections. A certificate is generated and signed using a certification authority (CA) entity, which is able and authorized to issue certificates signed with its own name.



9.5.2 Generate Certificate

Generate a certificate on a computer that is running the Windows Server operating system, and has Windows Certificate Services installed and configured. Configure your Windows Server to act as a certificate authority.

-		MMC - [C	onsole Root\Certification Authorit	y (Local)]		_ 0 ×
File Action View Favorites	· · · · · · · · · · · · · · · · · · ·					_ & ×
🗢 🔿 🙍 🗔 🗟 🖬 👂						
Console Root	Name	Description				Actions
⊿ Gertificates (Local Computer) ⊿ Certificates (Local Computer)	J WINGENPE-CA-1	Certification Authority				Certification Authority (Local)
Certificates						More Actions
Trusted Root Certification.						
Enterprise Trust Intermediate Certification						
Intermediate Certification J Trusted Publishers						
Untrusted Certificates						
Third-Party Root Certificat						
Trusted People Client Authentication Issue						
Client Authentication issue Other People						
BitLocker Drive Encryption						
Remote Desktop						
Certificate Enrollment Requip Smart Card Trusted Roots						
Trusted Devices						
Web Hosting						
Certificates - Current User						
Certification Authority (Local)						
					Activate Windo	WS
< III >					Go to System in Cor	rol Panel to activate Windows.
= 🐺 占 🕻) 🛛 🛃 💈	- 🔤 🔏 🤅	2. 🗹 🔚 💊			▲ 🍡 🔁 🌗 10:33 PM 6/25/2020

- Open a web browser, and enter the following URL: http://<server-name>/certsrv where <server-name> is the server that runs the Windows Server operating system, and on which Windows Certificate Services is installed and configured.
- On the Microsoft Certificate Services Welcome page, click Request a certificate.
- On the Request a Certificate page, click Advanced certificate request.
- Create a certificate signing request and submit the request to CA for approval. Make sure to include the following extended key attributes on your certificate request. (Client Authentication and Server Authentication)

Ce	rtificate	× MMC - [Console Roo	ot\Certificates (Local	Computer)\Person	al\Certificates]			-
eneral Details Certification Pat	h	_						, <u> </u>
Show: <all></all>	~	sued By	Expiration Date	Intended Purposes	Friendly Name	Status Certificate Te	Actions	
Field	Value	INGENPE INGENPE-CA-1	1/1/2099 6/18/2025	Server Authenticati	<none> <none></none></none>		Certificates	
Signature hash algorithm	sha1	INGENPE-CA-1	6/19/2021	Server Authenticati			More Actions	
Issuer	WINGENPE	MSvc-WINGENPE	10/8/2029	Server Authenticati			WINGENPE	
Valid from Valid to	Saturday, January 1, 2000 12 Thursday, January 1, 2099 12 =						More Actions	
Subject	WINGENPE							
Public key	RSA (1024 Bits)							
Enhanced Key Usage	Server Authentication (1.3.6							
Authority Key Identifier	KeyID=6b 55 44 43 3d 33 87 🗸							
1	tidt Properties Copy to File OK	Ī						
III >>	<		ш			Activate Win	dows Gruol Panel to activat	e Windows.
nal store contains 4 certificates.								
			× 🖂 📼					m من 10:41
- 写 📥 🔇	🔈 🛛 🛃 🖆	7 🔤 🥢 🤻	2. 🔟 📋				* 😼	行 (10:4 6/25

- After you submit the certificate request, the confirmation page appears, followed by the Certificate Issued page.
- On the Certificate Issued page, click Install this certificate.

9.5.3 Genesys sip server configuration.

The figure below illustrates the tls related configurations performed on the Genesys sip server.

sip-port-tls is the tls port configured for the Genesys Sip Server. We have used port 5069 for the tls communication.

sip-tls-cert – is the thumbprint of the certificate which is created for the use of tls on sip server. Since we are using simple TLS, **sip-tls-mutual** is set to false.



Senesys	Genesys /	Administro	ator				Tenant:	Environment	P New V	Vindow Log out	🗇 • 🔞
MONITORING PROVISIONING	OPERATIONS										
ROVISIONING > Environment > /	Applications > SIPSer	ver									
Navigation 🔍	SIPServer - Star	ted - Primary - \Appl	ications\								
🙀 Search 🛛 🛨	🗙 Cancel 📄 Save &	Close 🛃 Save 🛃 Sa	ve & New 🛛 😹 Reload 🛛	🔿 Start 🔳 Stop	Grace	ful Stop					
😹 Environment 📃	Configuration	Options	Permissions	Dependencies	,	Alarms	Logs				
🙀 Alarm Conditions	New 🔂 Delete 🚽	Export 🐺 Import	u						View: Advanced Vi	iew (Options)	
🔂 Scripts							Option	Value			
Application Templates	Y tis			Section Option Filter Filter			Filter				
Applications	TServer (8 Items))									
Hosts	TServer/sip-port-tis				TServer sip-port-tis		sip-port-tis	5069			
Solutions	TServer/sip-tls-cer	t			TServer		sip-tls-cert fa d8 e5 11 dd 74 f4 4c 96		74 f4 4c 96 7d d1 2a e	3 3f 29 95 dd 32 82	0a
📑 Time Zones	TServer/sip-tls-cer	-			TServer		sip-tls-cert-key				
Business Units/Sites	TServer/sip-tls-cipl	her-list			TServer		sip-tls-cipher-list				
📑 Tenants	TServer/sip-tls-crl TServer/sip-tls-mu	4			TServer TServer		sip-tls-crl sip-tls-mutual	false			
Table Access Points	TServer/sip-tis-tiar				TServer		sip-tis-target-name-check				
Formats	TServer/sip-tis-true	-			TServer		sip-tis-trusted-ca				
📑 Fields											
😹 Switching 🛛 🛨											
Routing/eServices +											
😝 Desktop 🛛 🛨											
🛃 Accounts 🛛 🕒											
Noice Platform								Activate Wi	ndows		
a Outbound Contact 🛛 🛨	A Page 1 o	f 1 🕨 🕅 🍣 👘								- Displaying of	biacto 1 - 9 of



9.5.4 Trunk configuration

On the SBC trunk the following options is modified for the use of tls on Sip server.

Senesys [®]	C	Senesys Admi	his						ant	nvironment P	New V	Vindow Log out 🍈 🕶 🌘
		DN - \Switches\Switch\DNs\Local DN\ Cancel J Save & Close J Save Save New										
MONITORING PROVISIONING OPERATIONS												
ROVISIONING > Switching > Switches > Switch		Configuration Options Permissions Dependencies					-					
lavigation		Switch - \Switches		New 🙀 Delete 🚽			View: Advanced	Mew (Anney)	~			Tasks
Search 📑	Ð	🕻 Cancel 📕 Save & Close 📕 S			Export & import			1	· ·			Create
Environment		Configuration Options		Name 🔺		Section	Option	Value				Course Dance of
Switching		🗅 🔻 📄 New 💁 New Folder	T	Filter		Filter	Filter	Filter			65	Create Range of DNs
DN Groups		Number .	•	TServer (5 Items)					_			
Places		Filter		TServer/contact		TServer	contact	10.232.50.50:5061;transport=tis				Orchestration
Place Groups		iew: 🔄 Switch > 🦳 DNs :		TServer/oos-check		TServer	oos-check	10				V Load Application
*		100001		TServer/oos-force		TServer	oos-force	5				Unload Application
Switching Offices	Þ	100011		TServer/record		TServer	record	false				
Switches		100021		TServer/refer-enabl	ed	TServer	refer-enabled	true				Routing
G IVRs		100031										W Load Strategy
	Þ	100041										Vilload Strategy
		1234567890										
		17814437266										CSV Bulk Processing
		17814437285										🐼 DN Import
		17814437293										DN Export
		17814437386										
		9000										Multi Update 🔺
Routing/eServices		9001										🧭 Manage Annex
Desktop	1	9002										Manage Manage
		911 DMSML										Permissions
		DN								A stimute MAGes at		
,		VN ↓ ↓ Page 1 of 1 ↓ ↓			1 🕨 🕅 🍣 -			Displaying objects 1 - 5	of 5	Activate Windows	*	Copy Object

9.5.5 SRTP between Agent and SBC

From the SIP Server perspective there is no configuration required for SRTP for secured media to work. SRTP is negotiated like any other media is negotiated with other party you will be interfacing with.

So in this scenario SBC performs the SRTP SDP negotiation with the B party and secured media is sent based on negotiated information. SIP server only relays the information to the Agent

10.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.

ORACLE

CONNECT WITH US
blogs.oracle.com/oracle
facebook.com/Oracle/

twitter.com/Oracle

oracle.com

Oracle Corporation, World HeadquartersWorldwide Inquiries500 Oracle ParkwayPhone: +1.650.506.7000Redwood Shores, CA 94065, USAFax: +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