

Oracle SBC integration with Genesys PureCloud BYOC and Verizon Business IP Trunking

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.

Version History

As a best practice always follow the latest Application note available on the Oracle TechNet Website. https://www.oracle.com/technical-resources/documentation/acme-packet.html

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Genesys PureCloud and Verizon Business IP Trunk	09 Sep 2021
1.1	Oracle Public IP Address masked	18 Nov 2021
1.2	New Section added- Genesys PureCloud Configuration Assistant.	03 Feb 2022

Table of Contents

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	
2.1 VERIZON BUSINESS IP TRUNKING	
2.2 GENESYS PURECLOUD	
2.3 ORACLE SBC	5
3. VALIDATED ORACLE VERSIONS	
4. ARCHITECTURE.	
5. CONFIGURE GENESYS PURECLOUD	
5.1 EXTERNAL TRUNK CONFIGURATION	
5.1.1 CREATE A NEW EXTERNAL TRUNK	
5.1.2 SET INBOUND SIP TERMINATION IDENTIFIER	
5.1.3 SET OUTBOUND SIP SERVERS OR PROXIES	
5.1.4 SET CALLING ADDRESS.	
5.1.5 SET SIP ACCESS CONTROL	
5.1.6 ENABLE E.164 FORMAT 5.2 SITE CONFIGURATION	
5.2.1 CREATE A NEW SITE	
5.2.1 CREATE A NEW SITE	
5.2.2 NUMBER FLANS & CLASSIFICATIONS	
5.2.4 PHONE CONFIGURATION	
5.2.5 SIMULATE CALL	
5.2.5 SIMULATE CALL	
5.3.1 CREATE DID RANGE	
5.3.2 Assign DID to User	
5.4. ARCHITECT FLOW FOR INBOUND WELCOME PROMPT	
6. CONFIGURING THE SBC	15
6.1 NEW SBC CONFIGURATION	
6.1.1 ESTABLISHING A SERIAL CONNECTION TO THE SBC	
6.1.2 CONFIGURE SBC USING WEB GUI	
6.2. CONFIGURE SYSTEM-CONFIG	
6.3. CONFIGURE PHYSICAL INTERFACE VALUES	
6.3. Configure Network Interface values	
6.4. ENABLE MEDIA MANAGER	
6.5. ENABLE SIP-CONFIG	
6.6. CONFIGURE REALMS	
6.7. Configure SIP Interfaces	
6.8. CONFIGURE SESSION-AGENT	
6.9. CONFIGURE SESSION-AGENT GROUP	
6.10. Configure steering-pool	
6.11. SIP SECURITY CONFIGURATION	
6.11.1 CONFIGURING CERTIFICATES	
6.11.1.1 END ENTITY CERTIFICATE	
6.11.1.2 IMPORT CA CERTIFICATE	
6.11.2 TLS-PROFILE	
6.12. MEDIA SECURITY CONFIGURATION.	
6.12.1 CONFIGURE SDES PROFILE.	
6.12.2. CONFIGURE MEDIA SECURITY PROFILE.	
6.13 IKE/IPSEC CONFIG	
6.13.1 IKE CONFIG	
6.13.1.1 IKE INTERFACE	

7777

1111

6.13.1.2 IKE SAINFO	40
6.13.2 SECURITY POLICY	
6.14. CONFIGURE LOCAL-POLICY	
6.15. CODEC POLICIES	
6.16 QOS MARKING	
6.17. ENABLE PING-RESPONSE	
6.18. ACCESS CONTROL	
6.19. SBC BEHIND NAT SPL CONFIGURATION	
7. SYNTAX EXAMPLES	50
8. CONFIGURING THE ORACLE SBC THROUGH CONFIG ASSISTANT	53
SECTION OVERVIEW AND REQUIREMENTS	
INITIAL GUI ACCESS	
PURECLOUD CONFIGURATION ASSISTANT	
PAGE 1- PURECLOUD NETWORK	
PAGE 2 - IMPORT DIGICERT TRUSTED CA CERTIFICATE FOR PURECLOUD	
PAGE 3 - SBC CERTIFICATES FOR PURECLOUD SIDE	
PAGE 4 – PURECLOUD SIDE TRANSCODING	
PAGE 5 – VERIZON RETAIL IP TRUNK NETWORK	
PAGE 6 – VERIZON RETAIL IP TRUNK SESSION AGENT	
PAGE 7 - PSTN SIDE TRANSCODING	
REVIEW	
Download and/or Apply	
CONFIGURATION ASSISTANT ACCESS	
9. TEST PLAN EXECUTED	62

1111

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 Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Genesys PureCloud and how SIP Trunking is implemented.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Genesys PureCloud and Verizon Business IP Trunk.

It should be noted that the SBC configuration provided in this guide focuses strictly on the Genesys PureCloud and Verizon Business IP Trunk related parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

Related documentation can be found below -

2.1 Verizon Business IP Trunking

https://www.verizon.com/business/products/voice-collaboration/voip/ip-trunking/

2.2 Genesys PureCloud

The Genesys PureCloud solution provides flexibility and interoperability to the PureCloud suite of voice services by allowing you to define SIP trunks between the PureCloud AWS-based Edge and Media Tier and third-party carriers over the public Internet. https://help.mypurecloud.com/articles/about-byoc-cloud/

2.3 Oracle SBC

- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- Oracle® Enterprise Session Border Controller Security Guide

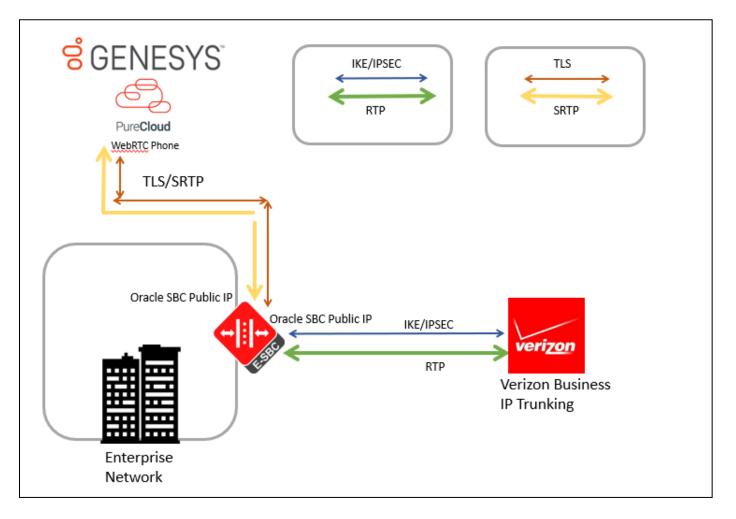
3. Validated Oracle Versions

We have successfully conducted testing with the Oracle Communications SBC versions: SCZ840p5a

These software releases with the configuration listed below can run on any of the following products:

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

4. Architecture.



Above figure illustrates the connection between Genesys PureCloud, Oracle SBC and Verizon Business IP Trunk. Both PureCloud and Verizon Trunk are connected to the Oracle SBC Public FQDN /IP. The connection between PureCloud and Oracle SBC is TLS/SRTP and between Verizon SIP Trunk and Oracle SBC is IPSEC/RTP. Oracle SBC is used to steer the signaling, media to, and From the PureCloud to Verizon SIP Trunk.

The configuration, validation and troubleshooting are the focus of this document and will be described in two phases -

Phase 1 – Configuring Genesys PureCloud

Phase 2 – Configuring Oracle Session Border Controller.

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

5. Configure Genesys PureCloud

Note: The document only includes the steps required on Genesys PureCloud to communicate with Oracle SBC as an External Trunk. Additional configuration may apply which may not be covered in this document. Please work with your Genesys representative for the most optimal Pure Cloud configuration as per your requirement.

To implement PureCloud BYOC with Oracle SBC, you use the Telephony Admin UI to create SIP trunks between the PureCloud Media Tier resources in AWS and the Oracle SBC.

The Oracle Enterprise SBC will act as an intermediary between the Verizon Trunk and Genesys PureCloud. The SBC is configured to broker calls as a back-to-back user agent (B2BUA) between the two systems. The Verizon DIDs are assigned to users on PureCloud System who can originate and accept the calls. These calls traverse through Oracle SBC with which we can implement several security and additional features as per our requirement.

For the purpose of this Application note, the connection between Oracle SBC and Genesys PureCloud is set over a Secure TLS 1.2 and SRTP based connection.

5.1 External Trunk Configuration

A trunk connects a communication service to a PureCloud telephony connection option and facilitates point-to-point communication. We will configure Oracle Enterprise SBC as an external Trunk on the PureCloud Portal. Detailed steps to configure the external trunk can be found here-

https://help.mypurecloud.com/articles/create-a-byoc-cloud-trunk/

To configure the external Trunk, Navigate to

Admin> Telephony>Trunks> External Trunks > Create New.

5.1.1 Create a new External Trunk

Type: BYOC Carrier Trunk

Protocol: TLS (TCP and UDP are also available)

5.1.2 Set Inbound SIP Termination Identifier

Inbound SIP Termination Identifier – is the DNS Name we will configure on the Oracle SBC and will be used to route calls towards PureCloud. Here a vanity FQDN **byoc-voxai.byoc.mypurecloud.com** is generated with the inbound sip termination identifier as byoc-voxai. This FQDN resolves to the following IP Addresses of the PureCloud AWS US Data Centers.

Inbound SIP Termination Identifier: byoc-voxai

Ex: INVITE <u>sip:+xxxxxxxx@byoc-voxai.byoc.mypurecloud.com</u> Protocol: TLS Genesys Reference - <u>https://help.mypurecloud.com/articles/tls-trunk-transport-protocol-specification/</u>

Genesys Cloud IP List

IP AddressesLoad Balancer DNS Names52.203.12.137b01.byoc.us-east-1.mypurecloud.com54.82.241.192b02.byoc.us-east-1.mypurecloud.com54.82.241.68b03.byoc.us-east-1.mypurecloud.com54.82.188.43b04.byoc.us-east-1.mypurecloud.com

Topology Metrics Trunks Sites Edge Groups	External Trunk Name Oracle BYOC POC		Status Type Metrics Inbound Calls Outbound Calls QoS Mismatches	 Operational Generic BYOC Carrier 0 0 0 0 0 	
Edges	Trunk State 😧		Protocol 😗		د د
Phone Management Certificate Authorities	In Service		TLS		-
DID Numbers Extensions	Inbound / Termination Inbound SIP Termination Identifier @	5	Inbound SIP Termination	n Header 😧	
	DNIS Replacement Routing Disabled				
		Inbound Reques	st-URI Reference		
	FQDN Method			urecloud.com :ontext=byoc.mypurecloud.com@lb01.byoc.us-	

5.1.3 Set Outbound SIP Servers or Proxies

Outbound SIP Termination FQDN is the Public FQDN of the Oracle SBC.

Edge Groups	Outbound	
Idges	Outbound SIP Termination FQDN 😧	c
Phone Management	solutionslab.cgbubedford.com	
	Outbound SIP TGRP Attribute O	TGRP Context-ID O
Certificate Authorities		
DID Numbers	Outbound SIP DNIS O	
Extensions		
		Outbound Request-URI Reference
		INVITE sip+xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
		In the spont concerning prevent make agreement work (1)

5.1.4 Set Calling Address

Topology	Calling				
Metrics	Address 😧	c	Address Override Method 😧		
Trunks	19729132636		Always		
Sites	Name 😧		Name Override Method 📀		
			Always		
ge Groups	SIP Access Control 😧				
pes	Allow the Following Addresses ()				
one Management		÷			
tificate Authorities					
Numbers		ê			
ensions	Add an IP or CIDR address	+			
	External Trunk Configuration			Expand All	Collapse All
	▶ General				
	► Transport				
	 Identity 				
	➤ Media				
	 Protocol 				
	 Diagnostics 				
	► Custom				
	Save External Trunk Cancel				

The Calling Address is the default number used as an outbound ANI when a call is placed on the Trunk. In case a user has assigned the optionally DID that number can be used in place of the default number.

5.1.5 Set SIP Access Control

Whitelist the Oracle SBC IP addresses under the SIP Access Control. (DNS name not supported)

Edge Gr			
Edges		IP Access Control 😧 Allow the Following Addresses 😧	
Phone M	Management	141.146.36.69	ŧ
Certifica	cate Authorities	141.146.36.68	*
DID Nun	imbers	141.140.30.00	
Extensio	ions	Add an IP or CIDR address	+

5.1.6 Enable E.164 format

By default, calls sent out of trunks do not include the "+" prefix, to enable E.164 number formatting disable omitting the "+". The settings can be found in the external trunk configuration, under the Identity Section. This setting is available for both inbound and outbound calls.

Address Digits Length 😧	Address Omit + Prefix 😧 🍤
0	Disabled

5.2 Site Configuration.

A site is a list of rules for routing calls. Objects such as phones associated with a site share the same rules. When a user makes a call from a phone, the system looks up the site and the call type in order to route the call to the best outbound phone line, or endpoint. Phones that are associated with a site are usually located in the same general area and have the same general purpose. A site is used to link trunk with Pure Cloud Edge(s).

Detailed steps to configure the Site can be found here-

https://help.mypurecloud.com/articles/create-site-genesys-cloud-voice/

5.2.1 Create a New Site

To Create a site, Navigate to Admin>Telephony>Sites> Create New. Type a name into the Site Name box. From the Location list, select a location for your site. From the Time Zone list, select your time zone. Under Media Model, select Cloud. Click Create Site.

Topology	General Number Plans Outbo	und Routes Simulate Call					
Metrics	Site Name						
Trunks	BYOC_Oracle		Default Site	Make this site the default site			
Sites	Description		Type Media Model	 Branch Site Cloud 			
Edge Groups			Phones	1			
Edges	Location		Edge Group	 Restart all phones assigned to this Site PureCloud Voice - AWS 			
Phone Management	C Test location	-	Topology Diagram	🛔 Show Topology			
Certificate Authorities							
	Media 😯						
DID Numbers	Geo-Lookup TURN @						
Extensions	Disabled						
	Automatic Updates 😯						
	Recurrence Type		Time Zone				
	Daily	~	America/Chicago (-05:00)			
	Time						
	 All day Range 						
	Start Time	End Time					
	2 : 00 AM	5 : 00 AM					
	Save Site Cancel						

5.2.2 Number Plans & Classifications

PureCloud provides a set of default number plans that work for most users. We can modify this numbering Plan as per our specific need. We have created a new Numbering Plan "BYOC" where we will define the Numbers that take the route associated with this trunk. You can assign specific numbers, a range or numbers or even use Regex for routing.

Telephony / Sites / Edit	Site								
Topology	General Nur	mber Plans	Outbound Routes	Simulate Call					
Metrics	 Number Plans a 	are evaluated fr	om top to bottom. Or	der can be change	d by dragging and drop	pping	number plans.		
Trunks	+ New Number	Plan					Ŵ	Delete Number Pl	lan
Sites	1 BYOC		Number Plar	n Name					
Edge Groups	1 Emergency		BYOC						
Edges	1 Extension		Match Type						
Phone Management	1 National		E.164 Num	iber List				Q	1
Certificate Authorities	•		Digit Lengt	h					
DID Numbers	1 International		E.164 Num						
Extensions	1 Network		Intra-Count	-					
Extensions			Number Lis						
			Regular Exp	pression					_
			+1 203-87	71-0043		-	+1 203-871-0043	×	
			+1 781-44	43-7247] -	+1 781-443-7247	×	
			+1 888-23	36-2427] →	+1 888-236-2427	×	

5.2.3 Configure outbound route

The Outbound route binds the numbering plans with the trunk. The classification created in numbering plan should be assigned to the Outbound Route associated with the external trunk.

Telephony / Sites / Edit S	Site				
pology	General Number Pla	ns Outbound Routes	Simulate Call		
etrics					
nks	 New Outbound Route 	Outbound R	oute Name	Distribution Pattern	🛍 Delete Outbound Route
5	Default Outbound Route	Default Ou	utbound Route	Sequential O Rand	om
e Groups		Description		External Trunks 😧	
88				🛧 🔸 🔴 OracleSolu	ntionsLabBYOCSBC 🗎
ne Management		State Enabled			
ficate Authorities		Classificatio	ons	Select External Trunks	*
lumbers		Emergency			
isions		Network 36	BYOC x		
	Save Outbound Routes	Cancel			

5.2.4 Phone configuration

Below is an example of a WebRTC Phone configuration which will be used for calling purpose and is assigned to the Users. The WebRTC Phone is assigned to the Oracle BYOC Site.

Topology	Phone
Metrics	Phone Name
Trunks	Status Unmanaged Make and Model Genesys Cloud WebRTC Phone
Sites	Base Settings 🕖 In Use By
Edge Groups	WebRTC Cloud P+ Log off Default For None
Edges	BYOC_Oracle Primary Edge O virtual-edge+0e97fcbda24ea3d49
Phone Management	Person Secondary Edge O virtual-edge+03e78d824757a3555
Certificate Authorities	· ·
DID Numbers	
Extensions	Phone Configuration Expand All Collapse All
	General
	▶ Media
	Network
	+ Custom
	Save Phone Cancel

5.2.5 Simulate call

Genesys PureCloud provides a neat feature to test and validate the routing of calls for troubleshooting purpose. Below is an example for a call to BYOC type number classification on this Site. Success indicates a successful routing response.

■ Telephony / Sites /	Edit Site
Topology	General Number Plans Outbound Routes Simulate Call
Metrics	6 Simulate call will use settings from the "General", "Number Plans", and "Outbound Routes" tabs. You do not need to save before simulating a call. This allows
runks	you to test before applying the changes.
ites	+12038710043 Simulate Call
dge Groups	✓ Success
dges	Normalized Number 🚱 🖌 🖌 tel:+12038710043
	Number Plan 🧿 🖌 🧹 BYOC
hone Management	Classification 😢 🖌 BYOC
ertificate Authorities	Outbound Route 2 Default Outbound Route
ID Numbers	External Trunks 😧
rtensions	OracleSolutionsLabBYOCSBC This Trunk is operational on all of the associated Edge interfaces.
	Preferred Edges 📀
	None
	Additional Edges
	 virtual-edgei-0561cfbbc881e3384 - Port 1 (WAN) (PureCloud Voice - AWS) virtual-edgei-0290074b4eb1c255a - Port 1 (WAN) (PureCloud Voice - AWS)
	► Log

5.3 DID Assignment

5.3.1 Create DID Range

To create a New DID Range or Number Navigate to Admin.> Telephony > DID Numbers> Create Range. Provide the DID range and Service Provider name and Click Save

Topology	DID Assignments DID Ranges			
Metrics	Create Range			Create Range
Trunks	DID Range	Service Provider	Comments	DID Start
Sites	+1 203-871-0043 → +1 203-871-0043	Twilio	PurecloudtoTwilioviaOracleSBC	== +1 • +12038710043
Edge Groups	+1 415-230-2042 → +1 415-230-2042	Twilio	Ecosystem Testing	DID End
Edges	+1 415-326-7696 → +1 415-326-7696			+1 ▼ +12078710053
Phone Management	+1 415-895-9907 → +1 415-895-9907	Twilio		Service Provider
	+1 415-909-3170 → +1 415-909-3170	Twilio		Twilio
Certificate Authorities	+1 602-428-9752 → +1 602-428-9752	Twilio	Chunder 2	Comments
DID Numbers	+1 602-883-7410 → +1 602-883-7410	Twilio	Chunder 1	PurecloudtoTwilioviaOracleSBC
Extensions	+1 781-313-1033 → +1 781-313-1033	byoc		
	+1 781-443-7266 → +1 781-443-7266	byoc		
	+1 928-275-4426 → +1 928-275-4426	Twilio	Andi Dev?	

5.3.2 Assign DID to User

On users' profile field, one of the DID can be assigned to PureCloud User as Other Number. The Oracle SBC is configured to send calls from external world to this DID number which will terminate to the user on PureCloud.

	 OracleSolutionslab 			
Email	Work Personal			
	Other			
Phone	Work	• (201) 555-0123	ext.	Ŀ
	Cell	• (201) 555-0123	ext.	
	Home	• (201) 555-0123	ext.	B
	Other	• (781) 349-6949	ext.	
Links	External System	http(s)://www.external-system-url.com		

5.4. Architect flow for inbound welcome prompt

Below is an example for an Architect Flow for inbound Voice Prompt which will be used for inbound calls from Verizon Business Trunk to Genesys PureCloud via Oracle SBC.

Second Second Call Flow					
Oracle_BYOC_Welcome Home					
션 Save As 션 Version 1.0 🛽 Export 👻 Validate	e 🗦 👻 🕀 Print 🖋 Edit This flow is not currently open for edit.				
Starting Menu <	🗏 10 Main Menu 📀				
▼ 10 Image: Main Menu Image: Ima	Initial Greeting				
Settings	😐 Hello, Welcome to Voxai and Oracle BYOC Testing 💿				
S Actions	Menu Prompt				
🛷 Event Handling	□ You are at the Main Menu, press 9 to disconnect				
E Menus	Default Menu Choice				
Supported Languages	None (disconnect the interaction)				
Speech Recognition	Menu Options				
Resources ~	r Menu Options				
🔁 Data	Speech Recognition Options				
💬 Prompts 🗘 Dependencies					
Reusable Menus 🗸 🗸					
Reusable Tasks 🗸					

6. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for Genesys PureCloud and Verizon IP Trunk.

6.1 New SBC configuration

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

6.1.1 Establishing a serial connection to the SBC

Note: The below method is applicable to the SBCs running on Hardware Platforms. For VME and Cloud SBCs the method of configuration will be different to as shown below. Follow the appropriate documentation or contact your Oracle representative for details about how to configure the VME and Cloud SBC platforms.

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on 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

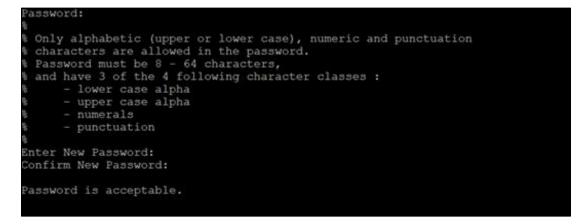
Power on the SBC and confirm that you see the following output from the boot-up sequence

Starting	
Starting	tServiceHealth
Starting	tCollect
Starting	tAtcpd
Starting	tAsctpd
Starting	tMbcd
Starting	tCommMonitord
Starting	tFped
Starting	tAlgd
Starting	tRadd
Starting	tEbmd
Starting	tSipd
Starting	tH323d
Starting	tbfdd
Starting	tIPTd
Starting	tSecured
Starting	tAuthd
Starting	tCertd
Starting	tIked
Starting	tTscfd
Starting	tFcgid
Starting	tauditd
Starting	tauditpusher
Starting	tSnmpd
Starting	tIFMIBd
Start pla	tform alarm
Starting	display manager
[nitializ	ing /opt/ Cleaner
Starting	tLogCleaner task
3ringing	up shell
Starting	acliMgr
bassword	secure mode is enabled
Admin Sec	writy is disabled
Password:	

Enter the default password to log in to the SBC. Note that the default SBC password is "acme" and the default super user password is "packet" for the Hardware and VME Platform.

Follow the appropriate documentation or contact your Oracle representative for details about how to configure the Cloud SBC platforms.

Both passwords must be changed according to the rules shown below.



Now set the management IP of the SBC by setting the IP address in bootparam.

To access bootparam. Navigate to Configure terminal->bootparam.

NN4600-139# conf t NN4600-139(configure)# b	ootparam
'.' = clear field; '-';	= go to previous field; q = quit
Boot File	: /boot/nnSCZ840p3B.bz
IP Address	: 10.138.194.139
VLAN	
Netmask	: 255.255.255.192
<u> </u>	: 10.138.194.129
IPv6 Gateway	
Host IP	
FTP username	
FTP password	: vxftp
Flags	
Target Name	
Console Device	
Console Baudrate	: 115200
Other	
	meters will not go into effect until reboot. boot parameters may also be changed through
PHY and Network Interfac	e Configurations.
ERROR : space	in /boot (Percent Free: 40)
NN4600-139(configure)#	

Note: There is no management IP configured by default.

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

To configure product type, type in setup product in the terminal



Save the changes and reboot the SBC.

Entitlements for Enterprise Session Bor Last Modified: Never	der Controller
1 : Session Capacity 2 : Advanced	: 0
3 : Admin Security	:
4 : Data Integrity (FIPS 140-2)	
5 : Transcode Codec AMR Capacity	: 0
6 : Transcode Codec AMRWB Capacity	: 0
7 : Transcode Codec EVRC Capacity	: 0
8 : Transcode Codec EVRCB Capacity	: 0
9 : Transcode Codec EVS Capacity	: 0
10: Transcode Codec OPUS Capacity	: 0
11: Transcode Codec SILK Capacity	: 0
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 1
Session Capacity (0-128000)	: 500
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 3
*****	******
CAUTION: Enabling this feature activate functions. Once saved, security cannot resetting the system back to factory de ************************************	be reverted without fault state.
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 5
Transcode Codec AMR Capacity (0-10237	5) : 50
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 2
Advanced (enabled/disabled)	: enabled
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 10
Transcode Codec OPUS Capacity (0-1023	75) : 50
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 11
Transcode Codec SILK Capacity (0-1023	75) : 50

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

Navigate to configure terminal->system->http-server-config.

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

p-server	
name	webServerInstance
state	enabled
realm	
ip-address	
http-state	enabled
http-port	80
https-state	disabled
https-port	443
http-interface-list	REST,GUI
http-file-upload-size	0
tls-profile	
auth-profile	
last-modified-by	Ð
last-modified-date	2021-01-25 00:16:28

6.1.2 Configure SBC using Web GUI

In this app note, we configure SBC using the WebGUI.

The Web GUI can be accessed through the URL <u>http://<SBC_MGMT_IP</u>>.

	0		
		Sign in to E-SBC	
		Enter your details below	
ORACLE Enterprise Session Border Controller		Username 	Required
		Password	
		SIGN IN	Required

The username and password are the same as that of CLI.

Highest task CPU usage		Current memory usage		Historical memory usage	
100 80 60 40 20 0 452060 102060 552060 102060 552060 102060 102060 102060 Time	 sipd03 tSSH-1 tConsole atcpd01 xserv 	20.0%	Allocated Free	3235M 3235M 3234M 3234M 3233M 3232M 00000000000000000000000000	 Memory usage (, Trend (rate:4.04 -)
Alarms					

Navigate to Configuration as shown below, to configure the SBC.

			Dashboard	Configuration	Monitor and Trace	Widgets	System
🗘 Wizards 👻	Commands 💌				Save Verify	Discard	Searc
media-manager	•	Configuration Objects					
security	Þ						
session-router	•	Name	Description				
strong main (access-control	Configure a static or dynamic access control list				-
system	•	account-config	Configure Quality of Service accounting				
		authentication-profile	Configure authentication profile				
		certificate-record	Create, generate, and import a certificate				
		class-policy	Configure classification profile policies				
		codec-policy	Create and apply a codec policy to a realm and an agent				
		filter-config	Create a custom filter for SIP monitor and trace				
		fraud-protection	Configure fraud protection				
		host-route	Insert entries into the routing table				
		http-client	Configure an HTTP client				
		http-server	Configure an HTTP server				-

Kindly refer to the GUI User Guide given below for more information.

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

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

6.2. Configure system-config

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

Navigate to system->system-config ACLI Path: config t->system->system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)

	Session Border Controller					admi
			Dashboard	Configuration	Monitor and Trace	Widgets Sy
🐼 Wizards 👻					Save Verify	Discard
http-client	Modify System Config					Show Configura
http-server network-interface ntp-config phy-interface redundancy-config	Hostname Description	OracleS8C				
snmp-community	Location Mib System Contact					
system-config	Mib System Name Mib System Location					
tdm-config trap-receiver	Acp TLS Profile	Delete				

Please enter the default gateway value in the system config page.

	erprise S	ession Border Controller						adn
					Dashboard	Configuration	Monitor and Trace	Widgets S
🔅 Wizards 👻	ands 👻						Save Verify	Discard
http-client	^	Modify System Confi	S					Show Configu
http-server		Displaying 0 - 0 of 0 Options						
network-interface		6 H.T.						
ntp-config		Call Trace	enable					
phy-interface		Default Gateway	10.138.194.129					
redundancy-config		Restart	🖌 enable					
snmp-community		Telnet Timeout	0	(Range: 065535)				
spl-config		Console Timeout	0	(Range: 065535)				
system-config		HTTP Timeout	5	(Range: 020)				
		Alarm Threshold						
tdm-config		Add						
trap-receiver	~	OF	C Delete					
Show All								

For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration.

If there is no transcoding involved, then the above step is not needed.

6.3. Configure Physical Interface values

To configure physical Interface values, Navigate to System->phy-interface. ACLI Path: config t->system->phy-interface Here we have configured, phy-interface M00 for Verizon Trunk and M10 for PureCloud.

Parameter Name	Verizon (M00)	PureCloud (M10)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Configure **M00** interface as per example shared below.

	prise Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🚯 Wizards 👻 🏟 Command	ds 💌					Save Verify
host-route	Add Phy Interface					
http-client	Name					
http-server		M00				
network-interface	Operation Type	Media	•			
	Port	0	(Range: 05)			
ntp-config	Slot	0	(Range: 02)			
phy-interface	Virtual Mac					
redundancy-config	Admin State	✓ enable				
snmp-community	Auto Negotiation	v enable				
spl-config	Duplex Mode	FULL	V			
system-config	Speed	100	Ψ.			
trap-receiver	·	OK Back				

Configure M10 interface as per example shared below -

				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻	5 💌					Save Verify
session-router	Add Phy Interface					
system 🗸	Name	M10				
fraud-protection host-route	Operation Type	Media 👻				
http-client	Port Slot	0	(Range: 05) (Range: 02)			
http-server	Virtual Mac					
network-interface	Admin State	✓ enable				
ntp-config	Auto Negotiation	✓ enable				
phy-interface	Duplex Mode	FULL				
redundancy-config	Speed	100 🗸				
snmp-community	ОК	Back				
Show All						

6.3. Configure Network Interface values

To configure network-interface, Navigate to system->Network-Interface.

ACLI Path: config t->system->network-interface

The table below lists the parameters, to be configured for both the interfaces.

Note: The provided network IP addresses are given for example purpose only. In the real-world scenario We cannot use same networks on two network-interfaces hence make sure you use a different IP range for each Network-interface.

In this Setup we are using Google Public DNS to resolve the DNS names to IP Addresses.

Parameter Name	Verizon	PureCloud Network interface
Name	M00	M10
Host Name		solutionslab.cgbubedford.com
IP address		
Netmask	255.255.255.192	255.255.255.192
Gateway		
dns-ip-primary		8.8.8.8
dns-ip-backup1		8.8.8.4
Dns-domain		solutionslab.cgbubedford.com

Configure network interface M00 as below

Configuration View Conf	Configuration View Configuration Q						
media-manager	•	Modify Network Interface	e de la companya de l				
security	•						
session-router	ж.,	Name	M00 v				
system	•	Sub Port Id	0	(Range: 0_4095)			
fraud-protection		Description					
host-route							
http-client		Hostname					
http-server		IP Address					
network-interface		Pri Utility Addr					
ntp-config		Sec Utility Addr					
phy-interface		Netmask	255.255.255.192				
redundancy-config		Gateway					
snmp-community		⊿ Gw Heartbeat					
spl-config		State	enable				
system-config Show All	*	ок	Back				

Similarly, configure network interface $\ensuremath{\textbf{M10}}$ as below

Configuration View	Configuration	۹		
media-manager	•	Modify Network Interface		
security	- F -			
session-router	- F	Name	M10 💌	
system		Sub Port Id	0	(Range: 0.4095)
fraud-protection		Description		
host-route				
http-client		Hostname	solutionslab.cgbubedford.com	
http-server		IP Address		
network-interface		Pri Utility Addr		
ntp-config		Sec Utility Addr		
phy-interface		Netmask	255.255.255.192	
redundancy-config	- 11	Gateway		
snmp-community		⊿ Gw Heartbeat		
spl-config	-	~ · ·		
Show All		OK	Back	

6.4. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below. In addition to the above config, please set the max and min untrusted signaling values to one.

Navigate to Media->Manager->Media-Manager

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

ORACI	_E Enterprise	Session Border Controller		20		0	
				Dashboard	Configuration	Monitor and Trace	Widgets
🚯 Wizards 🔻	🔅 Commands 🔻					Save Verify	Discard
media-manager codec-policy	•	Modify Media Manager	ŗ				
media-manage	r-	State	✓ enable				
media-policy		Flow Time Limit	86400	(Range: 04294967295)			
realm-config		Initial Guard Timer	300	(Range: 04294967295)			
		Subsq Guard Timer	300	(Range: 04294967295)			
steering-pool		TCP Flow Time Limit	86400	(Range: 04294967295)			
security	•	TCP Initial Guard Timer	300	(Range: 04294967295)			
session-router	•	TCP Subsq Guard Timer	300	(Range: 04294967295)			
system	•	Hnt Rtcp	enable				
		Algd Log Level	NOTICE				
		Mbcd Log Level	NOTICE				
		OK	Delete				
Show All							

					Dashboard Configu	ration Monitor and Trace Widget
Wizards 🔻	Commar	nds 🔻				Save Verify Discar
media-manager	•	^	Modify Media Manager			
codec-policy				1000	[minBer on 161 1101613]	
media-manager			Media Policing	✓ enable		
media-policy			Max Arp Rate	10	(Range: 0.100)	
media-policy			Max Signaling Packets	0	(Range: 04294967295)	
realm-config			Max Untrusted Signaling	1	(Range: 0100)	
steering-pool			Min Untrusted Signaling	1	(Range: 0100)	
ecurity	•		Tolerance Window	30	(Range: 04294967295)	
ession-router	•		Untrusted Drop Threshold	0	(Range: 0.100)	
			Trusted Drop Threshold	0	(Range: 0.100)	
ystem	•		Acl Monitor Window	30	(Range: 53600)	
fraud-protection			Trap On Demote To Deny	enable	(million success)	
host-route				enable		
		~	ОК	Delete		
Show All						

6.5. Enable sip-config

SIP config enables SIP handling in the SBC.

To configure sip-config, Navigate to Session-Router->sip-config ACLI Path: config t->session-router->sip-config

Add the below options in the sip-config options

- inmanip-before-validate
- max-udp-length=0

Configuration View Configuration	Q		
account-config	Modify SIP Config		
filter-config	Charles		
ldap-config	State	enable	
local-policy	Dialog Transparency	✓ enable	
local-routing-config	Home Realm ID	byoc-voxai 💌	
media-profile	Egress Realm ID	.	
session-agent	Nat Mode	None 💌	
session-group	Registrar Domain	*	
session-recording-group	Registrar Host		
	Registrar Port	5091	(Range: 0,102565535)
session-recording-server	Init Timer	500	(Range: 04294967295)
session-translation	Max Timer	4000	(Range: 04294967295)
sip-config	Trans Expire	32	(Range: 04294967295)
sip-feature	Initial Inv Trans Expire Invite Expire	0	(Range: 0.999999999)
sip-interface	Carrier Man Life Limit	180	(Range: 04294967295)
Show All	ОК	Delete	
Configuration View Configuration	Q		
Conngulation view connigulation	<u>х</u>		
account-config	Modify SIP Config		
filter-config		ΙΟΟΟΟ	(Kange: 0
Idap-config	Options	inmanip-before-validate 🗙	
local-policy		max-udp-length=0 🗙	
local-routing-config	SPL Options		
media-profile	SIP Message Len	0	(Range: 065535)
session-agent	Enum Sag Match	enable	
session-group	Extra Method Stats	v enable	
session-recording-group	Extra Enum Stats	enable	
	Registration Cache Limit	0	(Range: 0999999999)
session-recording-server	Register Use To For Lp	enable	
session-translation	Refer Src Routing	enable	
sip-config	Atcf Stn Sr		

6.6. Configure Realms

Navigate to media-manager -> realm-config ACLI Path: config t->media-manger->realm-config

The name of the Realm can be any relevant name according to the user convenience. Use the following table as a configuration example for the three realms used in this configuration:

Config Parameter	Verizon	Pure Cloud Realm	
Identifier	Verizon	GenesysCloud	
Network Interface	M00	M10	
Mm in realm	Ŋ	V	
Access Control Trust Level	High	High	
Media Sec policy	RTP	sdespolicy	
Codec Policy	OptimizeCodecs		
Media Policy	VerizonQOS		

Configure Realm for Verizon Trunk as below -

Configuration	View Configuration	۹.		
media-manager	•	Modify Realm Config		
codec-policy				
media-manager		Identifier	Verizon	
media-policy		Description		
realm-config				
steering-pool		Addr Prefix	0.0.0.0	
security	•	Network Interfaces	M00:0 ×	
session-router	•	Media Realm List		
system	•	Mm In Realm	enable	
		Mm in Network	✓ enable	
		Mm Same Ip	✓ enable	
		QoS Enable	✓ enable	
		Max Bandwidth	0	(Range: 0999999999)
		Max Priority Bandwidth	0	(Range: () 000000000)
Configuration	View Configuration	Q		
media-manager	•	Modify Realm Config		
codec-policy		Parent Realm		
media-manager		DNS Realm		v
media-policy				•
realm-config		Media Policy	VerizonQOS	v
steering-pool		Media Sec Policy	RTP	T
security	•	RTCP Mux	enable	

Configure Realm for Genesys PureCloud as below -

Configuration	View Configuration	Q		
media-manager	•	Modify Realm Config		
codec-policy				
media-manager		Identifier	GenesysCloud	
media-policy		Description		
realm-config				
steering-pool		Addr Prefix	0.0.0.0	
security	•	Network Interfaces	M10:0.4 ×	
session-router	•	Media Realm List		
system	•			
		Mm In Realm	enable	

realm-config steering-pool			Media Policy Media Sec Policy				· ·		
security		►	RTCP Mux		sdesPolicy		•		
session-router		F	Ice Profile		enable		•		
system		•	Teams Fqdn						
			Teams Fqdn In Uri		enable				
			SDP Inactive Only		enable				
ORACL	LE Enter	prise Sess	sion Border Controller				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻	🔅 Comman	ds 🔻							Save Verify
media-manager	•	A	dd Realm Config						
codec-policy media-manager		0	ut Translationid			•			
media-policy		In	Manipulationid			•			
		O	ut Manipulationid			•			
realm-config		A	verage Rate Limit	0			(Range: 04294967295)		
steering-pool		A	ccess Control Trust Level	high		•			
security	•	In	valid Signal Threshold	0			(Range: 04294967295)		
session-router	•	М	aximum Signal Threshold	0			(Range: 04294967295)		
system	•	U	ntrusted Signal Threshold	0			(Range: 04294967295)		
fraud-protectior	n		at Trust Threshold	0			(Range: 065535)		
host-route		×.4	av Endnainte Dar Mat						
Show All			OK Ba	ack					

We have set Access Control Trust Level on the Reams to High as we have static access-control configured and this is a peering enviorment.

For more information on Access Control Trust Level, please refer to SBC Security guide link given below:

https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc_scz840_security.pdf

6.7. Configure SIP Interfaces

Navigate to session-router-> sip-interface and configure the sip-interface as shown below. ACLI Path: config t->session-router->sip-interface

Configure sip-interface for the PureCloud as below-

- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the Session agents added to the SBC.

Configure sip-interface for Genesys PureCloud and Verizon Business Trunk as below -

Configuration Ves Configuration	Q							Decerd 🛛 🕲 Verity 💽 Save
account-config	Modify	SIP Interface						show configuration
filter-config	State							
losg-config	Realm ID		💌 enable					
local-policy			GenesysCito	w w				
local-routing-config	Descriptio	n						
media-profile								
session-agent	SIP Ports							
session-group		/ 6 8						
session-recording-group	Action	Select Address		Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
session-recording-server	1			9060	TLS	PureCloudTLS	al	
session-translation								
sip-config								
sip-texture								
sip-interface								

onfiguration Vev C										Droved 🖉 Verty	
local-policy	-	Modify	SIPIn	terface						Show Co	ufbrazou
local-routing-config		State			🖌 erable						î.
media-profile		Realm ID			Vertzon	-					- 1
session-agent		Descriptio									- 1
session-group											
session-recording-group											
session-recording-server	- 11	SIP Ports									
session-translation		C	2.3	6 🐵							
sig-config		Action	Select	Address		Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs	
sig-feature		1			_	5060	UDP		agents-only		
sip-interface						5060	TCP		agents-only		
sig-manipulation											
sip-moniforing											
translation-rules											

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

6.8. Configure session-agent

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

Navigate to session-router->Session-Agent ACLI Path: config t->session-router->session-agent

Configure the session-agents for the Genesys Pure Cloud

- Host name to "byoc-voxai.byoc.mypurecloud.com"
- port to 5061
- realm-id needs to match the realm created for the Genesys Pure Cloud
- transport set to "staticTLS"

ping-method – send OPTIONS message to PureCloud to check health ping-interval to 30 sec

Configuration	View Configuration	Q			Discard	🖄 Verify 📙 Save
media-manager	► [▲]	Modify Session Agent				Show Configuration
security	•					
session-router	•	Hostname	byoc-voxai.byoc.mypurecloud.com			
access-control		IP Address				
account-config		Port State	5061	(Range: 0,102565535)		
filter-config		App Protocol	✓ enable			
ldap-config		Appriotocor	SIP 💌			
local-policy		Арр Туре	Ŧ			
local-routing-co	nfig	Transport Method	StaticTLS 👻			
media-profile		Realm ID Egress Realm ID	GenesysCloud 👻			
session-agent		Description	v			
session-group		Description				
session-recordin	ng-group					
session-recordin	ng-server	Match Identifier				
session-translat	ion •					-

Configure the session-agents for the Verizon Business Trunk as below Table.

-

Config Parameter	Verizon 1	Verizon2
Hostname	<verizon 1="" fqdn=""></verizon>	<verizon 2="" fqdn=""></verizon>
IP-Address	<ipv4 address=""></ipv4>	<ipv4 address=""></ipv4>
Port	5201	6292
Transport method	UDP	UDP
Realm ID Verizon	Verizon	
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Refer Call Transfer	enabled	enabled
Ping Response	\checkmark	\checkmark

Verizon Session Agent 1

Configuration v	lew Configuration	٩		
media-manager	*	Modify Session Agent		
security	► I			
session-router	•	Hostname	sce10001.1259031211.globalipcom.com	
access-control		IP Address	152.188.29.19	
account-config		Port	6292	(Range: 0,102565535)
filter-config		State	✓ enable	
ldap-config		App Protocol	SIP	
local-policy		Арр Туре	•	
local-routing-config		Transport Method	UDP 🔻	
media-profile		Realm ID	Verizon 💌	
session-agent		Egress Realm ID	•	
session-group		Description		
session-recording-g	roup			
session-recording-se	erver	Match Identifier		

711

1100

1///

Verizon Session Agent 2

Configuration View Configuration	Q		
media-manager	Modify Session Agent		
security			
session-router 🗸	Hostname	sce10002.1259031211.globalipcom.com	r
access-control	IP Address	152.188.28.147	
account-config	Port	5201	(Range: 0,102565535)
filter-config	State	✓ enable	
ldap-config	App Protocol	SIP 👻	
local-policy	Арр Туре	•	
local-routing-config	Transport Method	UDP 🔻	
media-profile	Realm ID	Verizon 👻	
session-agent	Egress Realm ID		
session-group	Description		
session-recording-group			
session-recording-server	Match Identifier		
session-translation •	ОК	Back	

6.9. Configure session-agent group

A session agent group allows the SBC to create a load balancing model. Navigate to Session-Router->Session-Group. ACLI Path: config t->session-router->session-group

Please configure the following group for Verizon Session Agents

Configuration Vie	w Configuration	۲.	
media-manager	► *	Modify Session Group	
security	•		
session-router	•	Group Name	VerizonGrp
access-control		Description	
account-config			
filter-config		State	✓ enable
ldap-config		App Protocol	SIP v
local-policy		Strategy	RoundRobin 👻
local-routing-config		Dest	sce10001.1259031211.globalipcom.con
media-profile			×
session-agent			sce100021259031211.globalipcom.cor
session-group			
session-recording-gro	pup	Trunk Group	
session-recording-ser	rver	Sag Recursion	✓ enable
session-translation		Stop Sag Recurse	401,407
slp-config		SIP Recursion Policy	v
slp-feature	-		
Show All	\supset	ОК	Back

6.10. Configure steering-pool

Steering-pool config allows configuration to assign IP address(s), ports & a realm. They define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

Navigate to GUI Path: media-manger->steering-pool ACLI Path: config t->media-manger->steering-pool

Configure PureCloud Steering pool as below -

	138.194.139 SCZ8.4.0	ision Border Controller Patch 5 (Build 332)				Dashboard
Configuration	View Configuration	Q				
media-manager	¥ *	Modify Steering Poo	1			
codec-policy						
media-manager		IP Address				
media-policy		Start Port	20000		(Range: 0,165535)	
realm-config		End Port	40000		(Range: 0,1_65535)	
	_	Realm ID	GenesysCloud	*		
steering-pool	_	Network Interface		Ŧ		
security						
session-router						

Configure Verizon Business Trunk Steering Pool as below -

Configuration Vi	ew Config	uration	Q			
media-manager	•	^	Modify Steering Pool			
codec-policy						
media-manager			IP Address			
media-policy			Start Port	10000		(Range: 0,165535)
			End Port	10999		(Range: 0,165535)
realm-config			Realm ID	Verizon	-	
steering-pool			Network Interface			
security	•				•	
session-router	•					
access-control						

6.11. SIP Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Genesys Pure Cloud and and IKE/IPSEC to connect to Verizon Business IP Trunk

Genesys Purecloud supports TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities. Similarly, Verizon Business requires a secure, IPSEC tunnel be established between the Oracle SBC and the VZB network. You must obtain the IPSEC Template from your Verizon Business account team before configuring IKE/IPSEC on the Oracle SBC.

6.11.1 Configuring Certificates

This section describes how to configure the SBC for TLS and SRTP communication for **PureCloud**. It requires a certificate signed by one of the trusted Certificate Authorities.

"Certificate-records" are configuration elements on Oracle SBC which captures information for a TLS certificate such as commonname, 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 certificate records as below.

- SBC Certificates (end-entity certificate)
- DigiCert Root CA
- DigiCert Intermidiate Cert (this is optional only required if your server certificate is signed by an intermediate)
- DigiCertEVRootCA (Genesys PureCloud)

Supported CA for Genesys PureCloud BYOC

Genesys Pure Cloud signs the BYOC Cloud endpoints with X.509 certificates issued by DigiCert, a public Certificate Authority. More specifically, the root certificate authority that signs the BYOC Cloud endpoints is the DigiCert High Assurance EV Root CA.

https://help.mypurecloud.com/articles/tls-trunk-transport-protocol-specification/

Note Genesys PureCloud uses subject name validation to ensure that the remote endpoint identifies itself as the expected target. If a server certificate does not contain the name to which the client is connected as either the common name or the subject alternate name, the connection is refused.

Below Table 1 is for reference. Modify the configuration according to the certificates in your environment.

Config Parameter	SBC Certificate(P ureCloud)	DigiCertEV RootCA	DigiCert Root CA	DigiCert Intermediat e
Name	SBCCert	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Common Name	solutionslab.cgb ubedford.com	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Key Size	2048	2048	2048	2048
Key-Usage-List	0 0		digitalSignature keyEncipherme nt	digitalSignature keyEncipherme nt
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa

Digest-algor	Sha256	Sha256	Sha256	Sha256
--------------	--------	--------	--------	--------

6.11.1.1 End Entity Certificate

The SBC's end entity certificate is what is presented to PureCloud signed by your CA authority, in this example we are using Digicert as our signing authority.

Here in this setup, We wil create two end entity certificates for PureCloud.

Common name: (solutionslab.cgbubedford.com) for PureCloud

Step 1 Configure SBC Certificate Record

To Configure the certificate record:

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

Configuration View Configuration	Q			
media-manager	•	Modify Certificate Record		
security				
authentication-profile		Name	SBCPureCloudCert	
certificate-record		Country	US	
tis-global		State	California	
tls-profile		Locality	Redwood City	
session-router	•	Organization	Oracle Corporation	
system	►	Unit		
		Common Name	solutionslab.cgbubedford.com	
		Key Size	2048 💌	
		Alternate Name		
		Trusted	✓ enable	
		Key Usage List	digitalSignature 🗙	
			keyEncipherment 🗙	
		Extended Key Usage List	serverAuth 🗙 clientAuth 🗙	
		Key Algor	rsa 🔻	
		Digest Algor	sha25ó 💌	
		Ecdsa Key Size	p25ó 💌	
		Cert Status Profile List		
Show All		ок	Back	

Step 2 – Generating a certificate signing request

Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- Select the certificate and generate certificate on clicking the "Generate" command.
- The Step must be performed for SBCPureCloudCert.
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.

Configuration Vev Configuration	Q											Distant (Q) Ver	ny 🔅 Seve
media-manager	•	Certific	ate Re	cord									
security	*												
authentication-profile					1.4	0 0 0 0						Search	Q
certificate-record		D 0	Select			Country	State	Locality	Organization	Unit		Common Name	ų
tis-global		PRESIDENT		BaltimoreRoot		US	144	Burlington	Engineering	Urin.		Baltimore CyberTrust	Beat
tis-profile		:		and the second									
session-router		1		DigiCertinter		Ų\$	MA	Burlington	Engineering			DigiCert SHA2 Secure	e Server CA
system		1		DigiCenRoot		US	MA	Burlington	Engineering			DigiCent Global Root	CA
		1	~	SBCPureCoudCert	Edit	16	California	Redwood City	Oracle Corporation			solutionslab.cgbubed	find.com
		1		TeamsEnterpriseCent	Copy		California	Redwood City	Oracle Corporation			telechat.o-test061617	77.com
v ∰ Commands v nager ▶ ^	Cer	rtificate	e Rec			certificate respo				×			Save
	Cer	rtificate	e Rec	ord Copy	/ the follo BEGIN C C32CCAC	owing information and s CERTIFICATE REQUEST	send to a CA authority	BAgTCKNhbGlmb3JuaWEx		×			Save
nager	Cer	rtificate		ord Copy	r the follo BEGIN (C3ZCCAC (TBgNVB 9uMSQW (GSIb3DQ	owing information and s CERTIFICATE REQUEST CCAQAWfDELMAkGAIU AACTDFJIZHdvb2QgQ2l JIgYDVQQDExt02WXIV2 ZEBAQUAA4IBDwAwgg	send to a CA authority JEBhMCVVMxEzARBgNV 0eTEbMBkGAIUEChMST3 zhhdCSVLXRIc3QwNJE2M JEKAOIBAQDX+fmN6hilb	3JhY2xliENvcnBvcmF0 Tk3Ny5jb20wggEIMA0G Pcdu26HyGu7VYwgtijq		×			Save
nager				Ord Copy Mill FTA Delete LpD MH	r the follo BEGIN (C3ZCCAC TBgNVB 9UMSQW QGSIb3DQ 22WY+3KI 6XVVUUD	owing information and CERTIFICATE REQUEST CCAQAW/DELMAKGAIL MACTDFJIZHdvb2QgQ2l MACTDFJIZHdvb2QgQ2l MACTDFJIZHdvb2QgQ2l MACTDFJIZHAW QEBAQUAA4IBDWAWgg ILLSyEJSG3PUBSPRO0 355saIWewgTLGAR2	send to a CA authority UEBINCVVMxEZARBgNV/ OPTEbMBKGAIUECHMST3 ZhihdCsVLXRIc3QUWIĘZM/ ZEKAOBAQDX+fmN6hilbF MLEJXAOUG66KUZ3ISDV SKTIapOh6-hmMft/K4305	3Jh72xllENvcnBvcmF0 Tk3NySjb20wggEIMA0G Pcdu26HyGu7VVwgti]q VktM1g7f075c/z7k stqh66gmkk9m02JTZ0		×	: Co	orrmon Name	
nager	N	Add		Delete Copy Delete LpC MH 10B B174	y the follo BEGIN (C3ZCCAC (TBgNVB 9UMSQW QGSIb3DQ 22WY+3KI (6X)VUUD V2UZfXn+ 4qQZtdxV	owing information and s CERTIFICATE REQUEST CCAQAW/DELMAkGAIL AACTDFIZHOKO2QQ2I JIGYDVQQDEXt0ZVIXIY2 ZEBAQUAA4IBDWAWg2 ZEBAQUAA4IBDWAWg LILSYEISC3PWEWWQTLGAgU2 HEXXGWJNKPUTPMISBQ JUOJFOWANAWKLBDTM	send to a CA authority DEBIMCVVMxE2ARBgNV OETEbMBKGAIUEChMST3 ZhIdGSVLREGQWIEZW ZEKA0BAQDX+fmklohilb EMLEJXA0uG66Ku23ISDV SKTiap9N+nm4jrK4X5pp Z3L32Xn+b4Hpv+IcoFu5 E0qkvRB/inuBg/C12qHP	3JhV2xllENvcnBvcmF0 TK3Ny5jb20wggEIMA0G Podu26HyGwg7VYwgtIjq VktM1g7f075c/z7k atqh6ogmkK9m02JT20 3E4WD7KHL9pDTsAR YCV2IQQ0LFLguVhgk		×			search
nager	N	Add	ter	Delete Copy Delete LpC MIII Delete HA	y the follo BEGIN (C C32CCAO (TBgNVB) 9UMSQW 9UMSQW 1GSIb3DC 02Wy+3KI 16XyvUUp 16XyvUUp 16XyvUUp 14Q2tdXV HGdjKGn .cBgkqhk	wing information and : cccr.2nqAwfDeLMAkGAIL AcTOP12Hdvb2QgQ2U AgVDVQDextDeXt02WdV2 QEBAQUAA4IBDWAWg2 DS5sa1WewwqTLGAgK2 HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJhKPUTPM58g HEXKGWJHKPUTPM58g	send to a CA authority DEBhMCVVMxE2ARBgNV OFTEbhBkGAIUEChMST BkGAUCHCMA BkGAUCHCMA BkGAUCHCMA SkTlap9hb+nm4[rk4/Spa 28.32Nh94hgHr4C6/U23 SkTlap9hb+nm4[rk4/Spa 28.32Nh94hgHr4C6/ShAP VCBHyGK6H2N07bCQ0 VCBHyGK6H2N07bCQ0 SkTla09MC6H2N07bCQ0 SkT	3JhY2vlijlENvcnBvcmF0 TK3Ny5b20wggEIMA0G Pcdu2ehyGu7Vwgt11q vktM1g7f075c/27k stqh65gmkk9m023TZO SE4WD7KL9pDTSAR YCV21QQU.FLguVngk /2L4ZmmAJEtAgMBAAGg BjkqhlkG9W0BAQSFAAOC		×	DI	ommon Name	search
nager	N D	Add Iame DigiCertint	ter bot	ord Copy Milk FTA W Delete B77 HIA B17 HIA AQ 4Tf	v the follo BEGIN (C32CCAC TBgNVB 9UMSQW 1GSIb3DC 2009 1400 1500 1400 1	wing information and : CCCTAQAW/DELMAkGAII ACTOPI2Hdvb2QQQ2U AQUVAQDEAUAA4IBDWAWg2 DEAQUAA4IBDWAWg2 DEAQUAA4IBDWAWg2 DEAQUAA4IBDWAWG2 DEACUAA4 HEXXXXXIIHWWWTLGAgU2 HEXXXXIIHWWWTLGAgU2 HEXXXXIIHWWWTLGAgU2 HEXXXXIIIHWWWTLGAgU2 HEXXXXIIIHWWWTLGAgU2 HEXXXXIIIHWWWTLGAgU2 HEXXXXIIIHWWWTLGAgU2 HEXXXIIIIHWWWTLGAgU2 HEXXXIIIIHWWWTLGAgU2 HEXXXIIIIHWWWTLGAgU2 HEXXXIIIIIHWWWTLGAgU2 HEXXXIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	send to a CA authority UEBhMCVV/McE2ARBgN/U oeTEMbHKsAULKRICSQUNIE23M BMLEJXAOUG64KUZ3ISQM BMLEJXAOUG64KUZ3ISQM SMTap0h0-mml(rk4Xpa Z3L3ZNH04HQH/C4CFUS Z3L3ZNH04HQH/C4CFUS CGM/RB/MUBS/CJBAPF VCBH/gKAH2X0TbCQQ SGMUGDWQEAWFDDANB (ToTIg2ALEW2hyOV)RB4HH [ToTIg2ALEW2hyOV)RB4HH	3JhY2ullENvcnBvcmP0 TK3Ny5jb2owgElMADG Pcdu2eHyGu7VwgU1g (ktMt1g7075c/27k 354W07XHL9DT3AR 354W07XHL9DT3AR QKdh1G90wBAQSFAAQC mY8BR0Tv6bvnImh7s4 Y6SnotV1E0KHPuf		×	DI	ommon Name IgiCert SHA2 Secure Serve	search er CA
nager	N D G	Add Iame NgiCertint NgiCertRo	ter bot nter	ord Copy MII(FIA WP Delete CS NH UD B174 HIA AQ 4TT rk44 xz2	v the follo BEGIN (C3zCCAc TBgIN/B 9UMSQW 9GSIb3DQ 22/vy+3KI 65/yvuUp y2uzfXn-4 40QztdX/ HGdJKGn i.cBgkqhk EAZRWqV 2vngPNL 969(S4N) 869(S4N)	owing information and : CERTIFICATE REQUEST SCCAQAWDEL MAKGAIL NACTOFIZHOHOZOWICH NACTOFIZHOHOZOWICH INFORMATION DEBAQUAA1BROWNE DEBAQUAA1BROWNE DESAUTOFICA DESAUTOFICA DESAUTOFICA USIO DESAUTOFICA USIO DESAUTOFICA DISCOMPTONIC DISCOMPTON	send to a CA authority 	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Eyu/Vngk KginktiGK00wBG/SFADC W18BR0KJ6DV/ADV/TFEOH MSBR0KJ6V/ADV/M QCts//mtaNH/KIL/M walqaDCT9FE/FEOH		×	D1 D1 GC	ommon Name IglCert SHA2 Secure Serve IglCert Global Root CA	search er CA
nager	N D G G	Add lame VigiCertInt VigiCertRo GoDaddyir	ter bot nter toot	ord Copy 	r the follo BEGIN (C3zCCAc TBgNVB 9uMSQw 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 4QQztdxV HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGN .cBgkqhk HGdJKGN .cBgkqhk .c	wing information and CERTIFICAT EQUEST CCAQANDELMAKGAIL ANTOFIZ-HAVAGQQQI (grDYQQQEHCQXMV) EBAQUAAHBDWANgg (BAQUAHBDWANgQCSAU EBAQUAAHBDWANG SSANIWWQT ICAQE2 - IEXXGWINK-UIPNSG - IEXXG	send to a CA authority UEBNMCVVN/kEZARBg/V/ OeTENMBK6.autuchMST3 zhld/SLN,URIC3QUNIE3M MLEJXA0UGoKHZ3ISOV STIAp0h0-mml/KK3Xpg ZL3ZXh1b4Hg/VCFNUS ZL3ZXh1b4Hg/VCFNUS Scaludb/Vg/Sk1HF0ANB (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H LT01gALEw2hyOV)RB4H DITECLYPSCRXL/UK8UF	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Eyu/Vngk KginktiGK00wBG/SFADC W18BR0KJ6DV/ADV/TFEOH MSBR0KJ6V/ADV/M QCts//mtaNH/KIL/M walqaDCT9FE/FEOH		×	DI DI GC	ommon Name IgiCert SHA2 Secure Serve IgiCert Global Root CA oDaddy Secure Server CA	search rr CA
nager	N D G G	Add lame NgICertInt NgICertRo ioDaddyIr ioDaddyR	ter bot nter toot	ord Copy 	r the follo BEGIN (C3zCCAc TBgNVB 9uMSQw 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 4QQztdxV HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGN .cBgkqhk HGdJKGN .cBgkqhk .c	owing information and CERTIFICAT BEQUEST CCAQAwfDELMAKGAIL MATDFIJ2HM20202011 288AQUAA4BD/MWg1 CAA4BD/	send to a CA authority UEBNMCVVN/kEZARBg/V/ OeTENMBK6.autuchMST3 zhld/SLN,URIC3QUNIE3M MLEJXA0UGoKHZ3ISOV STIAp0h0-mml/KK3Xpg ZL3ZXh1b4Hg/VCFNUS ZL3ZXh1b4Hg/VCFNUS Scaludb/Vg/Sk1HF0ANB (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H LT01gALEw2hyOV)RB4H DITECLYPSCRXL/UK8UF	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Eyu/Vngk KginktiGK00wBG/SFADC W18BR0KJ6DV/ADV/TFEOH MSBR0KJ6V/ADV/M QCts//mtaNH/KIL/M walqaDCT9FE/FEOH		×	DI DI GC	IglCert SHA2 Secure Serve IglCert SHA2 Secure Serve IglCert Global Root CA oDaddy Secure Server CA oDaddy Class2 Root CA	search rr CA
nager	N D G G	Add lame NgICertInt NgICertRo ioDaddyIr ioDaddyR	ter bot nter toot	ord Copy 	r the follo BEGIN (C3zCCAc TBgNVB 9uMSQw 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 4QQztdxV HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGN .cBgkqhk HGdJKGN .cBgkqhk .c	wing information and CERTIFICAT EQUEST CCAQANDELMAKGAIL ANTOFIZ-HAVAGQQQI (grDYQQQEHCQXMV) EBAQUAAHBDWANgg (BAQUAHBDWANgQCSAU EBAQUAAHBDWANG SSANIWWQT ICAQE2 - IEXXGWINK-UIPNSG - IEXXG	send to a CA authority UEBNMCVVN/kEZARBg/V/ OeTENMBK6.autuchMST3 zhld/SLN,URIC3QUNIE3M MLEJXA0UGoKHZ3ISOV STIAp0h0-mml/KK3Xpg ZL3ZXh1b4Hg/VCFNUS ZL3ZXh1b4Hg/VCFNUS Scaludb/Vg/Sk1HF0ANB (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H LT01gALEw2hyOV)RB4H DITECLYPSCRXL/UK8UF	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Egu/Vngk Kglighki0G/W08G/SFADC W18BR0KJ6D/Vdk/FM/ QCts//mtaNH/KIL/M walqaDCT9FE/FEbh+		×	DI DI GC	IglCert SHA2 Secure Serve IglCert SHA2 Secure Serve IglCert Global Root CA oDaddy Secure Server CA oDaddy Class2 Root CA	search rr CA
nager	N D G G	Add lame NgICertInt NgICertRo ioDaddyIr ioDaddyR	ter bot nter toot	ord Copy 	r the follo BEGIN (C3zCCAc TBgNVB 9uMSQw 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 4QQztdxV HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGN .cBgkqhk HGdJKGN .cBgkqhk .c	wing information and CERTIFICAT EQUEST CCAQANDELMAKGAIL ANTOFIZ-HAVAGQQQI (grDYQQQEHCQXMV) EBAQUAAHBDWANgg (BAQUAHBDWANgQCSAU EBAQUAAHBDWANG SSANIWWQT ICAQE2 - IEXXGWINK-UIPNSG - IEXXG	send to a CA authority UEBNMCVVN/kEZARBg/V/ OeTENMBK6.autuchMST3 zhld/SLN,URIC3QUNIE3M MLEJXA0UGoKHZ3ISOV STIAp0h0-mml/KK3Xpg ZL3ZXh1b4Hg/VCFNUS ZL3ZXh1b4Hg/VCFNUS Scaludb/Vg/Sk1HF0ANB (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H LT01gALEw2hyOV)RB4H DITECLYPSCRXL/UK8UF	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Egu/Vngk Kglighki0G/W08G/SFADC W18BR0KJ6D/Vdk/FM/ QCts//mtaNH/KIL/M walqaDCT9FE/FEbh+		×	DI DI GC	IglCert SHA2 Secure Serve IglCert SHA2 Secure Serve IglCert Global Root CA oDaddy Secure Server CA oDaddy Class2 Root CA	search rr CA
nager	N D G G	Add lame NgICertInt NgICertRo ioDaddyIr ioDaddyR	ter bot nter toot	ord Copy 	r the follo BEGIN (C3zCCAc TBgNVB 9uMSQw 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 4QQztdxV HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGN .cBgkqhk HGdJKGN .cBgkqhk .c	wing information and CERTIFICAT EQUEST CCAQANDELMAKGAIL ANTOFIZ-HAVAGQQQI (grDYQQQEHCQXMV) EBAQUAAHBDWANgg (BAQUAHBDWANgQCSAU EBAQUAAHBDWANG SSANIWWQT ICAQE2 - IEXXGWINK-UIPNSG - IEXXG	send to a CA authority UEBNMCVVN/kEZARBg/V/ OeTENMBK6.autuchMST3 zhld/SLN,URIC3QUNIE3M MLEJXA0UGoKHZ3ISOV STIAp0h0-mml/KK3Xpg ZL3ZXh1b4Hg/VCFNUS ZL3ZXh1b4Hg/VCFNUS Scaludb/Vg/Sk1HF0ANB (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H LT01gALEw2hyOV)RB4H DITECLYPSCRXL/UK8UF	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Egu/Vngk Kglighki0G/W08G/SFADC W18BR0KJ6D/Vdk/FM/ QCts//mtaNH/KIL/M walqaDCT9FE/FEbh+		×	DI DI GC	IglCert SHA2 Secure Serve IglCert SHA2 Secure Serve IglCert Global Root CA oDaddy Secure Server CA oDaddy Class2 Root CA	search rr CA
nager	N D G G	Add lame NgICertInt NgICertRo ioDaddyIr ioDaddyR	ter bot nter toot	ord Copy 	r the follo BEGIN (C3zCCAc TBgNVB 9uMSQw 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 1GSIb3DC 4QQztdxV HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGn .cBgkqhk HGdJKGN .cBgkqhk HGdJKGN .cBgkqhk .c	wing information and CERTIFICAT EQUEST CCAQANDELMAKGAIL ANTOFIZ-HAVAGQQQI (grDYQQQEHCQXMV) EBAQUAAHBDWANgg (BAQUAHBDWANgQCSAU EBAQUAAHBDWANG SSANIWWQT ICAQE2 - IEXXGWINK-UIPNSG - IEXXG	send to a CA authority UEBNMCVVN/kEZARBg/V/ OeTENMBK6.autuchMST3 zhld/SLN,URIC3QUNIE3M MLEJXA0UGoKHZ3ISOV STIAp0h0-mml/KK3Xpg ZL3ZXh1b4Hg/VCFNUS ZL3ZXh1b4Hg/VCFNUS Scaludb/Vg/Sk1HF0ANB (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H (LT01gALEw2hyOV)RB4H LT01gALEw2hyOV)RB4H DITECLYPSCRXL/UK8UF	SIIVIZAILENvcnBercmFO TRAVISIEZOVEREIMAGG Feduzeh-HGUTV-Wegtig kinktig/TOTS-K/TK stqh/Gagmkki0m02JTZO SE4W/DT/KIL-0pDTsAR CU-ZQUDL-Egu/Vngk Kglighki0G/W08G/SFADC W18BR0KJ6D/Vdk/FM/ QCts//mtaNH/KIL/M walqaDCT9FE/FEbh+		×	DI DI GC	IglCert SHA2 Secure Serve IglCert SHA2 Secure Serve IglCert Global Root CA oDaddy Secure Server CA oDaddy Class2 Root CA	search rr CA

- 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.

Step 3 Import Certificates to the SBC

Once certificate signing request have been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue **save/activate** from the WebGUI

Configuration View Configurat	tion Q										Discard 🖉 Verity 🔚 Sar
media-manager	•	Certific	ate R	ecord							
security	*										
authentication-profile		-	_								
certificate-record			₿ <u>1</u>		PKCS12						Search Q
tis-global		Action	Select	Name		Country	State	Locality	Organization	Unit	Common Name
tis-profile		÷		Baltimore	Root	US	MA	Burlington	Engineering		Baltimore CyberTrust Root
session-router	•			DigiCerth	nter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
system	•	:	•	DigiCert	Edit	US	MA	Burlington	Engineering		DigiCert Global Root CA
		:		SBCPure	Сору	US	California	Redwood City	Oracle Corporation		solutionslab.cgbubedford.com
		:		TeamsEi	Delete Generate	US	California	Redwood City	Oracle Corporation		telechat.o-test06161977.com
					Sort						

🚯 Wizards 👻	ands 💌						
media-manager	•	Certificate Record		Import certificate	×		
security				Format	v		
authentication-profile		Add Delete All	Upload		pkcs		
certificate-record		Name	Country	Import method	x509 try-all	Unit	Common
tls-global		DigiCertinter	US		Paste		DigiCert S
tls-profile		DigiCertRoot	US	Certificate file	No file chosen,		DigiCert G
session-router		GoDaddyInter	US	Certificate me	Tupload No file chosen.		GoDaddy
		GoDaddyRoot	US				GoDaddy
system		SBCEnterpriseCert	US				telechat.o
fraud-protection							
host-route							
http-client							
http-server					Import Cancel		
network-Interface					Import Cancel		
ntp-config							

6.11.1.2 Import CA Certificate

Repeat the steps provided Step 3 to import all the root and intermediate CA certificates into the SBC as mentioned in Table 1. At this stage, all the required certificates SBC certificates have been imported to the SBC

6.11.2 TLS-Profile

A TLS profile configuration on the SBC allows specific certificates to be assigned. Navigate to security-> TLS-profile config element and configure the tls-profile as shown below ACLI Path: config t->security->tls-profile

TLS-Profile - Genesys PureCloud

PureCloud BYOC only supports endpoints using the TLS version 1.2 protocol. Supported TLS ciphers include:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

TLS-only listeners are available on host port 5061.

Configuration View Configuration Q				
media-manager	Modify TLS Profile			
security 💌				
authentication-profile	Name	TLSPureCloud		
certificate-record	End Entity Certificate	SBCPureCloudCert 🛛		
tis-global	Trusted Ca Certificates	BaltimoreRoot 🗙		
tls-profile		DigiCertRoot 🗙		
session-router 👻		DigiCertInter 🗙		
access-control	Cipher List	TLS_RSA_WITH_AES_256_CBC_SHA2	56 X TLS_RSA_WITH_AES_256_CBC_SHA X	
account-config	Verify Depth	10	(Range: 010)	1
filter-config	Mutual Authenticate	v enable		
ldap-config	TLS Version	tlsv12 v		
local-policy	Options			
local-routing-config	Cert Status Check			
media-profile		enable		
session-agent	Cert Status Profile List			
session-group	Ignore Dead Responder	enable		
session-recording-group	Allow Self Signed Cert	✓ enable		
session-recording-server				
Show All	ОК	Back		

6.12. Media Security Configuration.

This section outlines how to configure support for media security between the ORACLE SBC and Genesys PureCloud.

6.12.1 Configure 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.

Navigate to ->Security -> Media Security ->sdes profile and create the policy as below. ACLI Path: config t->security->media-security->sdes-profile

dd Sdes Profile		Dashboard	Configuration	Monitor and Trace Save Verify	Widgets Discard
dd Sdes Profile				Save Verify	Discard
dd Sdes Profile					
me	SDES				
/pto List	AES_CM_128_HMAC_SHA1_80 X				
	AES_CM_128_HMAC_SHA1_32 X				
p Auth	✓ enable				
p Encrypt	v enable				
CP Encrypt	✓ enable				
ä	enable				
ress Offer Format	same-as-ingress 🔹				
e Ingress Session Params					
ОК Ва	ack				
p rC ri	Encrypt IP Encrypt ss Offer Format Ingress Session Params	Encrypt P Encrypt P Encrypt enable enable sso Offer Format same-as-ingress Ingress Session Params	Encrypt enable P Encrypt enable enable ss Offer Format same-as-ingress v	Encrypt enable P Encrypt enable enable enable sss Offer Format same-as-ingress Ingress Session Params	Encrypt enable enable ss Offer Format same-as-ingress fingress Session Params

6.12.2. Configure Media Security Profile

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 PureCloud, the other for non-secure media facing Verizon Business Trunk.

Navigate to ->Security -> Media Security ->media Sec policy and create the policy as below: ACLI Path: config t->security->media-security->media-sec-policy

Create Media Sec policy with name SDES, which will have the sdes profile, created above.

Assign this media policy to PureCloud Realm.

ORAC	LE E	nterprise S	Session Border Controller						a
						Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	🔅 Com	mands 🔻						Save Verify	Discard
certificate-reco		^	Add Media Sec Policy						
ike	•		Name	SDES					
ipsec	►		Pass Through	enable					
local-accounts			Options						
media-security	· •		Inbound						
dtls-srtp-pro	ofile		Profile	SDES 💌					
media-sec-p	olicy		Mode	srtp	•				
sdes-profile			Protocol	sdes	•				
sipura-profil	e	11	Hide Egress Media Update	enable					
password-polic	E y		Outbound						
Show All		~	ОК Е	Back					

Create another Media Sec Policy RTP as shown below. This policy will be applied to the Verizon Ream facing the Verizon Business SIP Trunk.

🔅 Wizards 👻 📢	🐉 Commands	•			
admin-security	▶	^	Modify Media Sec Policy		
auth-params			Name	RTP	
authentication			Pass Through	enable	
authentication-pro	ofile		Options		
cert-status-profile	•				
certificate-record			▲ Inbound		
factory-accounts			Profile	•	
			Mode	rtp	•
ike	•		Protocol	none	•
ipsec	Þ		Hide Egress Media Update	enable	
local-accounts					
media-security	•		✓ Outbound Profile		
dtls-srtp-profile			Mode	rtp	
media-sec-polic	sy.	-			•
Show All		Ţ	ОК	Back	

6.13 IKE/IPSEC Config

The configuration elements required for IKE are not available via the Oracle ESBC GUI and must be configured via ACLI.

Note : Verizon does not necessarily use IPSEC and IKE for Trunks and it could be UDP or TCP.IPSEC configuration is only required if the setup requires the Trunk to communicate over IPSEC.

Note: The examples provided will only display the parameters of each element that have been changed. All others can be left at default values unless required to be changed for your specific purposes:

6.13.1 IKE Config

ACLI Path: config t->security->ike->ike-config

Type Select and use the below example to configure the global lke configuration on the SBC.

ike-config	
ike-version	1
log-level	NOTICE
phase1-dh-mode	dh-group2
phase2-exchange-mode	dh-group2

6.13.1.1 Ike Interface

ACLI Path: config t->security->ike->ike-interface

ike-interface	
ike-version	1
address	
realm-id	Verizon
ike-mode	initiator
shared-password	* * * * * * *
sd-authentication-method	shared-password

6.13.1.2 lke Salnfo

ACLI Path: config t->security->ike->ike-sainfo

ike-sainfo	
name	VZ1
auth-algo	md5
encryption-algo	3des
tunnel-local-addr	
tunnel-remote-addr	152.188.29.84
ike-sainfo	
name	VZ2
auth-algo	md5
encryption-algo	3des
tunnel-local-addr	
tunnel-remote-addr	152.188.28.212

6.13.2 Security Policy

Security Policies are part of the IPSEC configuration on the SBC, and this is available through the GUI.

GUI Path: security/ipsec/security policy

ACLI Path: config t->security->ipsec->security-policy

Use the below table as an example to configure security policies on the SBC toward Verizon Business:

Function	IPSEC	SIP	IPSEC	SIP
Name	Verizon- Security- Policy-1	Verizon- Security- Policy-1A	Verizon- Security- Policy-2	Verizon- Security- Policy-2A
Vetwork-Interface	S1p0:0	S1p0:0	S1p0:0	S1p0:0
Priority	0	1	2	3
.ocal IP addr match				
Remote ip addr match	<vz-ipsec-ip></vz-ipsec-ip>	<vz-sip-ip></vz-sip-ip>	<vz-ipsec-ip></vz-ipsec-ip>	<vz-sip-ip></vz-sip-ip>
.ocal port match	500	0	500	0
Remote port match	500	0	500	0
.ocal IP Mask	255.255.255.0	255.255.255.255	255.255.255.0	255.255.255.255
Remote IP mask	255.255.255.224	255.255.255.255	255.255.255.224	255.255.255.255
ke- <u>sainfo</u> -name		VZ1		VZ2
Action	Allow	IPSEC	Allow	IPSEC
outbound-sa-fine-grained-mask				
ocal ip mask	255.255.255.255	255.255.255.0	255.255.255.255	255.255.255.0
Remote in mask	255.255.255.255	255,255,255,224	255,255,255,255	255.255.255.224

name	Verizon-Security-Policy-1				
network-interface	M00:0				
local-ip-addr-match					
remote-ip-addr-match	152.188.29.84				
local-port-match	500				
remote-port-match	500				
local-ip-mask	255.255.255.192				
remote-ip-mask	255.255.255.224				
action	allow				
ecurity-policy					
name	Verizon-Security-Policy-1A				
network-interface	M00:0				
priority	1				
local-ip-addr-match					
remote-ip-addr-match	152.188.29.19				
ike-sainfo-name	VZ1				
outbound-sa-fine-grained-mask					
local-ip-mask	255.255.255.192				
remote-ip-mask	255.255.255.224				

security-policy							
name	Verizon-Security-Policy-2						
network-interface	M00:0						
priority	2						
local-ip-addr-match							
remote-ip-addr-match	152.188.28.212						
local-port-match	500						
remote-port-match	500						
local-ip-mask	255.255.255.192						
remote-ip-mask	255.255.255.224						
action	allow						
security-policy							
name	Verizon-Security-Policy-2A						
network-interface	M00:0						
priority	3						
local-ip-addr-match							
remote-ip-addr-match	152.188.28.147						
ike-sainfo-name	VZ2						
outbound-sa-fine-grained-mask							
local-ip-mask	255.255.255.192						
remote-ip-mask	255.255.255.224						

6.14. Configure local-policy

Local policy config allows the SBC to route calls from one end of the network to the other based on routing criteria.

To configure local-policy, Navigate to Session-Router->local-policy. ACLI Path: config t->session-router->local-policy

Following local-policy routes the calls from Genesys PureCloud to Verizon Business IP Trunk which are then terminated towards PSTN.

Following local-policy routes the calls from Verizon Business Trunk which are then routed to Genesys PureCloud from the SBC.

Configuration View Configuration	Q											Di	scard 🖉 Verit	fy 🕒 Save
media-manager	*	Modify	/ Local	Policy										
security >														*
session-router 💌		From Address			* ×									
access-control		To Address		* X									- 1	
account-config		Source Re	alm		byoc-	voxal 🗙								
filter-config		Descriptio	n											- 1
Idap-config														- 1
local-policy														- 1
local-routing-config		State			🖌 enat	ble								- 1
media-profile		Policy Priority			none		v							- 1
session-agent		Policy Attr	ributes											- 1
session-group		D	<i>o</i> (õ õ										
session-recording-group		Action	Select	Next Hop	i	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key	
session-recording-server				sag:VertzonGrp	N N	Verizon	replace-url	disabled	0	enabled		single		
session-translation														
stp-config	-													-
Show All				OK	Back									

Configuration Verticengation media-manager security secson-router access-control access-control access-control access-control access-control access-control idap-confg idap-confg	Configuration View Configuration	Q													Discard	🙆 Verify	ID s
security session-router access-control access-control access-control account-config fiter-config idap-config idap-config local-policy local-policy local-policy media-profile Policy Priority none				· · · · · · · · · · · · · · · · · · ·									Discard	Q verity	_ EI 38		
session-router session-router access-control access-control account-config source Realm verizon X itter-config bescription local-routing-config State source media-profile Policy Priority	media-manager 🕨		Mod	ify Lo	ocal	Policy											
session-router Address X access-control To Address 	security 🕨																
account-config Source Realm fitter-config Description Idap-config Description Idap-config State Iocal-policy State Iocal-policy Policy Priority	session-router v		From /	From Address		* >	<										
Idep-config Description Idep-config Description Iocal-policy State Iocal-routing-config State media-profile Policy Priority	access-control		To Add	To Address		* >	<									- 1	
Idap-config Description Iocal-policy State Iocal-routing-config State media-profile Policy Priority	account-config		Source			Ver	1zon ×										
Idap-config Idap-config Iocal-policy State Iocal-routing-config State media-profile Policy Priority	filter-config		Descri	otion													- 1
local-routing-config State media-profile Policy Priority	Idap-config																
media-profile Policy Priority none v	local-policy																
neus-prone • none •	local-routing-config		State	State			🗸 er	nable									
session-agent Policy Attributes	media-profile		Policy	Priority	У		none	2	•								. 1
	session-agent		Policy	Attribu	ites												. 1
session-group Ct / P To @	session-group		D	0	6	i 🖻											- 12
session-recording-group Action Select Next Hop Realm Action Terminate Recursion Cost State App Protocol Lookup Next Key	session-recording-group		Actio	n Se	elect	Next Hop		Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	N	ext Key	
session-recording-server	session-recording-server					OracleSBCPureCl	oudT	PureCloud	none	disabled	0	enabled		single			
session-translation	session-translation																
stp-config	stp-config																

6.15. Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the OCSBC the ability to add, strip, and reorder codecs for SIP sessions

Note: This is an optional configuration. Only configure codec policies if deemed necessary in your environment

GUI Path: media-manager/codec-policy

ACLI Path: config t->media-manager->codec-policy

Some SIP trunks may have issues with codec being offered by Genesys PureCloud, specifically Verizon requested the SBC try to offer only one codec when possible. For this reason, we have created a codec policy "OptimizeCodecs" for the Verizon SIP trunk to remove the codecs that are not required or supported.

• Click Add, and use the examples below to configure

Configuration View Config	guration	C	2	
media-manager	•	•	Modify Codec Policy	
codec-policy				
media-manager			Name	OptimizeCodecs
media-policy			Allow Codecs	PCMU 🗙 Telephone-Event 🗙
realm-config				
steering-pool			Add Codecs On Egress	PCMU ×
security	•		Order Codecs	
authentication-profile			Packetization Time	20
certificate-record			Force Ptime	enable
tls-global			Secure Dtmf Cancellation	enable
tls-profile			Dtmf In Audio	disabled 👻
session-router	•		Tone Detection	
system	•	•		
Show All			ОК	Jack

6.16 QOS Marking

QoS marking allows you to apply a set of TOS/DiffServ mechanisms that enable you to provide better service for selected networks

GUI Path: media manager->media policy

ACLI Path: config t->media-manager->media-policy

Configuration View Configuration C	ξ.					Discard 🖉 Verify 🖺 Save					
media-manager 👻 🌋	Modify	Medi	a Policy			Show Configuration					
codec-policy											
media-manager	Name		VerizonQOS	VerizonQOS							
media-policy	Tos Settin	gs									
realm-config	D	/	ā 🛍								
	Action	Select	Media Type	Media Sub Type	Tos Value	Media Attributes					
steering-pool	:		audio		0xb8						
security 👻											
authentication-profile	:		message	sip	0x68						
certificate-record											
tls-global											
tls-profile											
session-router											
system 🕨 👻						-					
Show All			OK Back								

6.17. Enable Ping-response

The option is found under the **Session agent** configuration element and will be enabled on all session agents configured for Verizon Trunk and Genesys PureCloud .

Below is an example of the parameter **Ping response** enabled on PureCloud Session-Agent. Similarly, the parameter should be enabled for Verizon Business Session Agents.

Configuration View Configuration Q			
media-manager	Modify Session Agent		
security >			
session-router 💌	Hostname	byoc-voxai.byoc.mypurecloud.com	
access-control	IP Address		
account-config	Port	50ó1 (Ran	ange: 0,102565535)
filter-config	State	enable	
ldap-config	App Protocol	SIP 💌	
local-policy	Арр Туре	•	
local-routing-config	Transport Method	StaticTLS 👻	
media-profile	Realm ID	GenesysCloud v	
media-manager 🕨	Modify Session	Agent	
security •	· · · · · · · · · · · · · · · · · · ·		
session-router 👻	SPL Options		
access-control	Media Profiles		
account-config	In Translationid		v
filter-config	Out Translationid	toPSTN	v
ldap-config	Trust Me	enable	
local-policy	Local Response Map	enable	
local-routing-config			•
media profile	Ping Response	enable	

6.18. Access Control

To enhance the security of your Oracle Session Border Controller, we recommend configuration access controls to limit traffic to only trusted IP addresses on all public facing interfaces

GUI Path: session-router/access-control

Please use the example below to configure access controls in your environment for both PureCloud IP's, as well as SIP Trunk IP's (if applicable).

byoc.mypurecloud.com resolves to the following load balancer IP Addresses

- 52.203.12.137 <u>lb01.byoc.us-east-1.mypurecloud.com</u>
- 54.82.241.192 <u>lb02.byoc.us-east-1.mypurecloud.com</u>
- 54.82.241.68 Ib03.byoc.us-east-1.mypurecloud.com
- 54.82.188.43 <u>lb04.byoc.us-east-1.mypurecloud.com</u>

Configure access-control for each IP PureCloud IP Address as shown in the below example.

Configuration View Configuration	Q			
media-manager	-	Modify Access Control		
security				
authentication-profile		Realm ID	GenesyCloud v	
certificate-record		Description		
tis-global				
tis-profile		Source Address	34.211.206.63	
session-router	·	Destination Address		
access-control		Application Protocol	SIP 👻	
account-config		Transport Protocol	ALL 👻	
filter-config		Access	permit 👻	
Idap-config		Average Rate Limit	0	(Range: 0.4294967295)
local-policy		Trust Level	none v	
local-routing-config		Minimum Reserved Bandwidth	0	(Range: 0.4294967295)
media-profile		Invalid Signal Threshold	0	(Range: 0.4294967295)
session-agent		Maximum Signal Threshold	0	(Range: 0.4294967295)
session-group		Untrusted Signal Threshold Deny Period	0	(Range: 04294967295)
session-recording-group		Nat Trust Threshold	30	(Range: 0.4294967295) (Range: 0.65535)
session-recording-server		Max Endpoints Per Nat	0	(Range: 0.65535)
Show All	*	ОК В	ack	

Similarly create ACL entries for each Verizon Trunk as shown in the below example.

Configuration View Configuration	Q		
media-manager	Modify Access Con	trol	
session-router v	Realm ID Description	Verizon 💌	
access-control	Description	VerizonSIP	
account-config			
filter-config	Source Address	152.188.0.0/16	
Idap-config	Destination Address	0.0.0.0	
local-policy	Application Protocol	SIP 💌	
local-routing-config	Transport Protocol	ALL 👻	
media-profile	Access	permit 💌	
session-agent	Average Rate Limit	0	(Range: 04294967295)
session-group	Trust Level	high 💌	
session-recording-group	Minimum Reserved Bandw	idth 0	(Range: 04294967295)
session-recording-server	Invalid Signal Threshold	0	(Range: 04294967295)
session-translation	Maximum Signal Threshold	0	(Range: 04294967295)
stp-config	Untrusted Signal Threshold	0 30	(Range: 04294967295) (Range: 04294967295)
slp-feature	•	50	[naile: 0.4674701673]
Show All		OK Back	

Notice the trust level on this ACL is set to high. When the trust level on an ACL is set to the same value of as the access control trust level of its associated realm, this create an implicit deny, so only traffic from IP addresses configured as ACL's with the same trust level will be allowed to send traffic to the SBC. For more information about trust level on ACL's and Realms, please see the <u>SBC Security Guide, Page 3-10</u>

6.19. SBC Behind NAT SPL configuration

This configuration is needed when your SBC is behind a NAT device. This is configured to avoid loss in voice path and SIP signaling.

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call.

For example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One publicprivate address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the PureCloud side SIP interface.

To configure SBC Behind NAT SPL Plug in,

Navigate to session-router->SIP-interface->spl-options and input the following value, save, and activate.

HeaderNatPublicSIPIflp=52.151.236.203,HeaderNatPrivateSIPIflp=10.0.4.4

Here HeaderNatPublicSIPIfIp is the public interface ip and HeaderNatPrivateSIPIfIp is the private ip.

media-manager	•	Modify Realm Config		
codec-policy		Early Media Allow		
media-manager		Early Media Allow	•	
media-policy		Enforcement Profile	•	
realm-config		Additional Prefixes		
steering-pool		Restricted Latching	none 👻	
security	•	Options		
session-router	•	SPL Options	HeaderNatPublicSiPlfip=52.151.236.20	
system	•	Delay Media Update	enable	
		Refer Call Transfer	disabled 🔹	
		Hold Refer Reinvite	enable	
		Refer Notify Provisional	none 💌	
		Dyn Refer Term	enable	
		Orden Delter	Back	
Show All				

This configuration would be applied to each SIP Interface in the ORACLE SBC configuration that was deployed behind a Nat Device.

7. Syntax Examples

Picture 1 -Sample SIP INVITE from PureCloud to Oracle SBC

```
2021-09-01 02:00:43.658
INVITE sip:+16174261400@customers.telechat.o-test06161977.com:5061;transport=tls SIP/2.0
Record-Route: <sip:54.244.22.120:5061;r2=on;transport=tls;ftag=Yn0Sy7I;lr>
Record-Route: <sip:10.87.16.129:5060;r2=on;ftag=Yn0Sy7I;lr>
To: "Boston MA" <sip:+16174261400@customers.telechat.o-test06161977.com>
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@54.244.22.120>;tag=Yn0Sy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
Via: SIP/2.0/TLS 54.244.22.120:5061;branch=z9hG4bKb5f7.5310eb26.0
Via: SIP/2.0/UDP 10.87.209.169:6060; branch=z9hG4bKb5f7.eecf4c36.0
CSeq: 1 INVITE
Max-Forwards: 67
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO
Supported: norefersub, timer
Accept: application/sdp, application/dtmf-relay
Contact: <sip:+17812032806@10.87.209.169:6060;did=42f.a8a5bde5>
x-inin-cnv: 238493bd-87d6-443e-a548-69b57deb5edd
x-pcv-domain: customers.telechat.o-test06161977.com
Content-Type: application/sdp
User-Agent: GENESYS-SIPSERVICE/1.0.0.4186
Content-Length: 357
```

Picture 2 – Sample 200 OK response to PureCloud .

```
SIP/2.0 200 OK
To: "Boston MA" <sip:+16174261400@customers.telechat.o-test06161977.com>;tag=111331881-
1630475903588
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@54.244.22.120>;tag=YnOSy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
Via: SIP/2.0/TLS 54.244.22.120:5061;branch=z9hG4bKb5f7.5310eb26.0
Via: SIP/2.0/UDP 10.87.209.169:6060;branch=z9hG4bKb5f7.eecf4c36.0
CSeq: 1 INVITE
Record-Route: <sip:54.244.22.120:5061;r2=on;transport=tls;ftag=Yn0Sy7I;lr>
Record-Route: <sip:10.87.16.129:5060;r2=on;ftag=YnOSv7I;lr>
Supported:
Contact: <sip:+161742614000
                                       5061;transport=tls>
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY
Accept: application/media control+xml, application/sdp
Content-Type: application/sdp
Content-Length: 371
```

Picture 3- Sample SIP INVITE from Oracle SBC to VZB Trunk

From Header:

• Must contain a Verizon DID that is associated with the trunk group

. Must Contain the SBC local Sip Interface IP address and port

To Header

. Must Contain the Verizon Sip IP address or Hostname, and port

```
INVITE sip:+16174261400@sce10002.1259031211.globalipcom.com:5201 SIP/2.0
Via: SIP/2.0/UDP
                               5060;branch=z9hG4bK74nmnd1040vst8j4los0.1
To: "Boston MA" <sip:+16174261400@152.188.28.147:5201>
From: "OracleSolutionsLabBYOCSBCTest" <sip:+178120328060
                                                                :5060>;tag=Yn0Sy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
CSeq: 1 INVITE
Max-Forwards: 66
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO
Supported: norefersub, timer
Accept: application/sdp, application/dtmf-relay
Contact: <sip:+178120328060
                                         5060;did=42f.a8a5bde5;transport=udp>
x-inin-cnv: 238493bd-87d6-443e-a548-69b57deb5edd
x-pcy-domain: customers.telechat.o-test06161977.com
Content-Type: application/sdp
User-Agent: GENESYS-SIPSERVICE/1.0.0.4186
Content-Length: 274
```

Picture 4 – Sample 200 OK from Verizon Trunk to Oracle SBC

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP :5060;branch=z9hG4bK74nmnd1040vst8j4los0.1
To: "Boston MA" <sip:+16174261400@152.188.28.147:5201>;tag=111331881-1630475903588
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@ 5060>;tag=YnOSy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
CSeg: 1 INVITE
Supported:
Contact: <sip:+16174261400@152.188.28.147:5201;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 288
```

Picture 5- Sample SIP INVITE from Oracle SBC to PureCloud

```
INVITE
 sip:7812032802@OracleSBCPureCloudTesting.byoc.usw2.pure.cloud:5061;user=phone;transport=tls
 SIP/2.0
 Via: SIP/2.0/TLS
                               5061;branch=z9hG4bKb12kh020007rgur17460.1
 From: <sip:+918130313388@solutionslab.cgbubedford.com;user=phone>;tag=2139011582-1630461859974-
 To: "ORACLESOLLAB ."<sip:7812032802@
                                                    ;user=phone>
 Call-ID: BW020419974010921419608329@63.77.76.250
 CSeq: 260885572 INVITE
 Contact: <sip:+918130313388@solutionslab.cgbubedford.com:5061;transport=tls>
 Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
 Accept: application/media control+xml, application/sdp, multipart/mixed
 Supported:
 Max-Forwards: 68
 Content-Type: application/sdp
 Content-Disposition: session; handling=required
 Content-Length: 467
X-MS-SBC: Oracle/NN4600/8.4.0p5A
```

Picture 6- Sample 200 OK from PureCloud to Oracle SBC

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS
          :5061; rport=8196; received=
                                           ;branch=z9hG4bKb12kh020007rgur17460.1
Record-Route: <sip:10.87.41.109:5060;r2=on;ftag=2139011582-1630461859974-;lr>
Record-Route: <sip:52.32.193.99:5061;r2=on;transport=tls;ftag=2139011582-1630461859974-;lr>
To: "ORACLESOLLAB ."<sip:7812032802@1
                                               ;user=phone>;tag=VNWwS6k
From: <sip:+918130313388@solutionslab.cgbubedford.com;user=phone>;tag=2139011582-1630461859974-
Call-ID: BW020419974010921419608329@63.77.76.250
CSeq: 260885572 INVITE
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO
Supported: norefersub, timer
Accept: application/sdp, application/dtmf-relay
Contact: <sip:7812032802@10.87.254.136:6060;did=eae.9ca6723>
Content-Type: application/sdp
Date: Wed, 01 Sep 2021 02:04:20 GMT
User-Agent: GENESYS-SIPSERVICE/1.0.0.4186
```

8. Configuring the Oracle SBC through Config Assistant

When you first log on to the Oracle SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the SBC provides the Configuration Assistant. The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic. You can use the Configuration Assistant for the initial set up to make to the basic configuration. Please check "Configuration Assistant Operations" in the Web GUI User Guide and "Configuration Assistant Workflow and Checklist" in the <u>ACLI Configuration</u> Guide

Please note, applying a configuration to the SBC via the Configuration Assistant will overwrite any existing configuration currently applied to the SBC. We highly recommend this only be used for initial setup of the SBC. This feature is not recommended to be used to make changes to existing configurations.

Configuration package is available starting in release nnSCZ840p7 and nnSCZ900p2.

Section Overview and Requirements

This section describes how to use our Configuration Assistant feature as a quick and simple way to configure the Oracle SBC for integration with Genesys PureCloud. We will choose Verizon Retails IP Trunk on the other Side for Carrier Connectivity.

The pre-requisites are given below.

- SBC running release SCZ840p7 or later which will have this template package by default added to the SBC code.
- TLS certificate for the SBC preferably in PKCS format, or access to PureCloud supported CA to sign certificate once CSR is generated by the SBC.

The following outline assumes you have established initial access to the SBC via console and completed the following steps:

- Configured boot parameters for management access
- Setup Product
- Set Entitlements
- Configured HTTP-Server to establish access to SBC GUI

Initial GUI Access

The Oracle SBC WebGui can be accessed by entering the following in your web browser. http(s)://<SBC Management IP>.

The username and password are the same as that of the CLI.

If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below

PureCloud Configuration Assistant

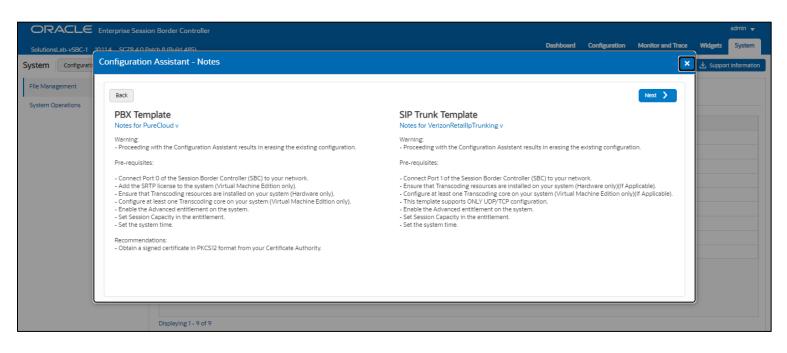
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:

	1.4 SC28.4.0 Patch 8 (Build 485)		Dashbourd	comparadon	Monitor and Trace	
System Configuration A	Configuration Assistant - Select Deployment				×	🛃 Support Informatio
File Management						
System Operations	Select a PBX Template	Select a SIP Trunk Template			Next >	
	Microsoft ACS	Select PBX Template to list the corresponding SIP Side template				
	Cisco					
	Avaya Session Manager					
	GenericPBX					
	GenesysPureEngage					
	PureCloud					
	Five9					
	Upload a Configuration	Upload a Template Package				
	Drag and Drop Select a file or drop one nere.	Drag and Drop Select a file or drop one here.	+			
	Please click below link for additional template packages. https://www.orade.com/technical-resources/documentation/acme-packet.html					

Under PBX template, we'll select PureCloud template. This brings up a list of available sip trunk templates.

	erprise Session Border Controller					admin 👻
SolutionsLab-vSBC-1 10.11.4	4 SC28.4.0 Patch 8 (Build 485)		Dashboard	Configuration	Monitor and Trace	Widgets System
System Configuration Ass	Configuration Assistant - Select Deployment			×	A Support Information	
File Management System Operations	Select a PBX Template	Select a SIP Trunk Template			Next >	
	Microsoft ACS ·	VerizonRetaillpTrunking				
	Cisco	TwilioSIPTrunking				
	Avaya Session Manager	GenericSipTrunk				
	GenericPBX	IntelepeerSipTrunking ·				
	GenesysPureEngage	ATTIPtrunking				
	PureCloud	BellCanadatrunking				
	PureCloud v [PureCloudOnly.gz] Description : PureCloud template anables you to configure and connect your Session Border Controller to Genergya PureCloud.	OrangeBTIP				
	Upload a Configuration	Upload a Template Package				
	Drag and Drop + Select a file or drop one here.	Drag and Drop Select a file or drop one here.	+			
	Flesse click below link for additional template packages. https://www.oracle.com/technical-resources/documentation/acme-packet.html					

Select Verizon Retail IP trunk template and click Next at the top to access the Notes page. Pay close attention to the information here, as this is a list of warnings, pre-requisites, and recommendations:



Clicking "Next" on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page providing the opportunity to setup entitlements, add license keys, etc. before moving on to the configuration.

Once all requirements for your selected templates have been satisfied, you can proceed to the configuration pages.

Page 1- PureCloud Network

Page 1 of the template is where you will configure the network information to connect to PureCloud Network.

Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each filed. Also, pay close attention to which fields are listed as "required".

										~	
ORACLE	Enterprise Session Bo	order Controller									admin 👻
SolutionsLab-vSBC-1	10114 SC78 4 0 Patch 8	3 (Build 485)					Da	shboard Configuration	on Monitor and Trace	Widgets	System
System Configuration	Configuration As	sistant - PureCloud	Network						×	🛃 Support	t Information
File Management System Operations	< Back	< 1	2			5	(6)	7	Skip 💙		
System operations		PureCloud Network	Root Trusted Certificate	SBC Certificate	Genesys Purecloud Transcoding	Verizon IP Trunk Network	Verizon Session Agent	Transcoding			
			Let's cor	nfigure the inter	face that commu	nicates with Pur	reCloud				
				Realm Name 🗇							
						Required					
				Enter PureCloud	Session Agent hostname	here					
						Required					
				Enter the PureClo	ud IP here 🕐						
				Port Number @					-		
						-					
	D	isplaying 1 - 9 of 9									

Page 2 - Import DigiCert Trusted CA Certificate for PureCloud

Page 2 of this template is where the SBC will import the **DigiCert High Assurance EV Root Cert CA** certificate, which PureCloud uses to sign the certificates it presents to the SBC during the TLS handshake.

Importing the PureCloud Root CA certs is enabled by default.

Configuration Assi	stant Root Hust								×
K Back	O	2	3		5	6	- 7	Next >	
	PureCloud Network	Root Trusted Certificate	SBC Certificate	Genesys Purecloud Transcoding	Verizon IP Trunk Network	Verizon Session Agent	Transcoding		
		Let's st	art provisioning	the root trusted co	ertificate for Pure	eCloud.			
		OU=v	giCert Inc www.digicert.com)igiCert High Assurance	EV/ Poot CA					•
		Validity Not B		2006 GMT					11
			giCert Inc						н
		CN=E X509v3	www.digicert.com JigiCert High Assurance extensions:	EV Root CA					
		Dig X509	v3 Key Usage: critical ital Signature, Certifica v3 Basic Constraints: cr						
		X509 B1:3		:D4:98:26:1A:08:02:EF:63:	64:2B:C3				
			v3 Authority Key Identi	fier:					-

By default, the SBC is set to import a certificate in PKCS12 format. This is the simplest and recommended way to add a certificate to the Oracle SBC. Using this method, you will add the SBC's hostname under "FQDN or Common Name" field, upload a certificate signed from one of the PureCloud Supported CA Vendors, and enter the certificates password.

ORACLE	Enterprise Session Bo	order Controller									
SolutionsLab-vSBC-1	10.1.1.4 SCZ8.4.0 Patch 8	8 (Build 485)					Das	hboard Configuratio	n Monitor and Trace	Widgets	System
System Configuration	Configuration As	sistant - SBC Certifi	cate						×	날 Suppor	t Information
File Management	K Back		0		(4)	(5)	(6)	(7)	skip 义		
System Operations		PureCloud Network	Root Trusted Certificate	SBC Certificate Let's start prov Certificate prov PKCS12 Fully Qualified I	Genesys Purecloud Transcoding risioning certificat isioning type Domain Name or Commo Domain Name or Commo tet (.p12 or .pfx)	Verizon IP Trunk Network es for the SBC	Verizon Session Agent	Transcoding			
	D	isplaying 1 - 9 of 9									

Certificate Signing Request (CSR)

The alternative to importing a PKCS12 certificate to the SBC is to configure a certificate and generate a certificate signing request that you will have signed by a PureCloud supported CA. Same as PKCS12, you will enter the SBC's hostname under "FQDN or Common Name" and "Country" field (required) and answer the remaining question presented on this page (optional).

	Enterprise Session Bor									4	Δ 🚽	admin 🚽
							P~	shboard Configu	ration Monitor and Tr		Widgets	System
	10.1.1.4 SCZ8.4.0 Patch 8						Dias	anooaro Coringo	ration monitor and fr	ace	Middera	System
System Configuration	Configuration Ass	istant - SBC Certific	cate							×	🛃 Suppor	t Information
File Management System Operations	K Back	Ø	0	3	(4)	5		(7)	Skip >			
		PureCloud Network	Root Trusted Certificate	SBC Certificate	Genesys Purecloud Transcoding	Verizon IP Trunk Network	Verizon Session Agent	Transcoding				
				Let's start prov	visioning certificat	es for the SBC						
				Certificate provis	ioning type ⑦				*			
				CSR		*						
				Fully Qualified Do	omain Name or Common	Required						
				Country 🗇		Required						
				State ①								
				Locality 🕲					•			
	Dis	playing 1 - 9 of 9										

Page 4 – PureCloud side Transcoding

Page 4 is where you will be able to configure transcoding between the SBC and PureCloud.

Once transcoding features is set to "yes", you will then have an option to select additional media codecs you want included in offers/answers toward PureCloud. If you select yes to either question regarding media codecs, you will be presented with a required drop down.

You can select as many codecs from the list presented.

	terprise Session Borde	er Controller									admin 👻
SolutionsLab-vSBC-1 10.1.1	.4 SCZ8.4.0 Patch 8 (Bi	uild 485)					Das	hboard Configuratio	n Monitor and Trace	Widgets	System
System Configuratic Co	onfiguration Assis	stant - Genesys Pu	recloud Transo	coding					×	🛃 Suppo	rt Information
File Management	K Back	0	0	0	4	(5)	(6)	- 7	Next >		
System Operations	(Duck	PureCloud Network	Root Trusted Certificate	SBC Certificate	Genesys Purecloud Transcoding	Verizon IP Trunk Network	Verizon Session Agent	Transcoding			
							-				
			Le	et's configure trai	nscoding for Gene	sys Purecloud si	de				_
				Do you want to select m PureCloud)?	edia codecs (SBC to	No Yes Y Yes Y Yes Y					
										-	
	4-14		_			_	_				

Page 5 – Verizon Retail IP Trunk Network

Page 5 of the template is where you will configure the network information to connect to Verizon Retail SIP trunk Network. Please fill the required fields and Press Next.

ORACLE Enterprise Session Bor	der Controller							▼ ac	ámin 👻
SolutionsLab-vSBC-1 10.1.1.4 SCZ8.4.0 Patch 8	(Build 485)				Dashi	board Configurati	on Monitor and Trace	Widgets	System
System Configuratic Configuration Ass	istant - Verizon IP Trun	k Network					×	🛃 Support In	formation
File Management System Operations	PureCloud Network Re	ot Trusted SBC Certificate	Genesys Purecloud Transcoding	5 Verizon IP Trunk Network	Verizon Session Agent	Transcoding	Stap 💙		
	Let's	configure the interface that	t communicates w	ith your Verizor	n Retail IP Trunk				
		Realm Name 🕲		Required			*		
		Port Number 🕲		Required					
		Port 1		w					
		Slot Number ®		Required					
		Slot 0		*					
		Network IP Addre	ss @	Required					
				Required			•		
Dis	playing 1 - 9 of 9								

Page 6 – Verizon Retail IP Trunk Session Agent

Page 6 of the template is where you will configure the Verizon Retail IP Trunk Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your PSTN SIP trunk.

ORACLE	Enterprise Session Bord	er Controller									admin 🔫
SolutionsLab-vSBC-1	10.1.1.4 SCZ8.4.0 Patch 8 (B	luild 485)					Dasi	hboard Configu	ration Monitor and Trac	Widgets	s System
System Configuration	Configuration Assis	stant - Verizon Ses	sion Agent							× 土 Supp	port Information
System configuration	Configuration Assis	PureCloud Network	Root Trusted Certificate	SBC Certificate Let's configure Verizon Session Agent In Verizon Session Agent IP Verizon Session Agent P Did Verizon provide a sec address for Sip Signaling	R Address O ort O cond Hostname/IP	Verizon IP Trunk Network nt for Verizon equired equired	4 Verizon Session Agent	(7) Transcoding	Sktp 🔪		
	Displ	aying 1 - 9 of 9									

Please fill the required fields and click Next.

Page 7 - PSTN side Transcoding

Page 7 is where you will be able to configure transcoding between the SBC and Verizon Retail IP Trunk.

Once transcoding features is set to "yes", you will then have an option to select additional media codecs you want included in offers/answers towards Verizon Retail IP trunk. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.

ORACLE	Enterprise Session Border C	ontroller										admin 👻
SolutionsLab-vSBC-1 10	0.1.1.4 SCZ8.4.0 Patch 8 (Build	485)					1	Dashboard	Configuration	Monitor and Trace	Widgets	System
System Configuration	Configuration Assistar	nt - Transcoding								×	🛃 Suppo	t Information
File Management System Operations	K Back	PureCloud Network	Root Trusted Certificate		dia codecs between SBC	⑦ No Yes	Verizon Session Agent	n Tra	2 anscoding	Review		
	Displayin	g1-9cf9	_	G729 G722 PCMU PCMA					_			

Review

At the end of the template, you will notice in the top right, a "*Review*" tab. If all 8 pages presented across the top are showing green, indicting there are no errors with the information entered, click on the "Review" tab.

										0	S I Sand
ORACLE	Enterprise Session Border	Controller									admin 🔻
SolutionsLab-vSBC-1 1	10.1.1.4 SCZ8.4.0 Patch 8 (Buil	ld 485)					Dash	board Configura	tion Monitor and Trace	Widgets	System
System Configuration	Configuration Assist	ant - Transcoding							×	🛃 Suppor	rt Information
		1995) 1997									
File Management	< Back	0	0		0	O	0	7	Review		
System Operations		PureCloud Network	Root Trusted Certificate	SBC Certificate	Genesys Purecloud Transcoding	Verizon IP Trunk Network	Verizon Session Agent	Transcoding	_		
				Let's o	onfigure transcoo	ling					
			Do	you want to enable tra C?	nscoding features on the	1 No Yes					
			Do	you want to select mee d Verizon?	lia codecs between SBC	1 No Yes					
			Se	lect media codecs (SBC	to Verizon) 🕐						
				PCMU 🗙							

The screen looks like below after clicking the Review Tab. The left side of the review page contains all of the entries added on each page and allows for editing each page individually if necessary.

The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.

ORACLE	Enterprise Session Border Controller				🚨 👻 admin 👻
SolutionsLab-vSBC-1	10.1.1.4 SCZ8.4.0 Patch 8 (Build 485)			Dashboard Configuration Monitor and Tra	ice Widgets System
System Configuration	Configuration Assistant - Sumn	nary			X Support Information
File Management System Operations				Download w Apply	
	PureCloud Network	/ Edit	Co	infiguration	
	Realim Name PureCloud Enter the PureCloud IP here Slot 0 Network IP subnet mask 255.255.255.192 Primary DNS server IP Address	Enter PureCloud Session Agent hostname here pureCloud.com Port Number Port O Network IP Address 141146.36.69 Network Gateway IP Address 141346.36.65 DNS Domain	certificate-record name common-name certificate-record name state locality organization unit common-name codec-policy name allow-codecs	DigiCertHighAssuranceEVRoot DigiCert High Assurance EV Root CA PureCloudCSR california Redwood City oracle Corporation oracle CORD-AS BOSTON telechat.o-test06161977.com VerizonCodecPolicy	
	Root Trusted Certificate Do you consent to installing the DigiCe enabled	rt High Assurance EV Root Cert	add-codecs-on-egress http-server name local-policy from-address to-address source-realm	PCMU webServerInstance * Purecloud	
	Displaying 1 - 9 of 9				

On the left side of the review contains the entries for each page. Each page has an "*Edit*" tab that can be used to make changes to the information entered on that specific page without having to go through the entire template again.

On the right side of the review page, under the "*Configuration*" tab is the ACLI output from the SBC. This is the complete configuration of the SBC based on the information entered throughout the template. Also on the right side of the review page you may see another tab, "*CSR*".

On Page 3 of the template, if you chose CSR from the drop-down menu instead of PKCS, the SBC configures a certificate record and generates a certificate signing request for you.

ORACLE	Enterprise Session Border Cont	troller							
SolutionsLab-vSBC-1	10.1.1.4 SCZ8.4.0 Patch 8 (Build 485	5)			Dashboard	Configuration	Monitor and Trace	Widgets	System
System Configurat	Configuration Assistant	- Summary					ډ	🛃 🛃 Suppo	rt Information
File Management System Operations						Download	d 💌 Apply		
	PureCloud Network		🥒 Edit	Configuration	Pu	reCloudCSR CSR			
	Realim Name PureCloud Enter the PureCloud IP here Slot Number Slot 0 Network IP subnet mask 255.255.255.192 Primary DNS server IP Addre	Enter PureCloud Session Agent hostname h pureCloud.com Port Number Port 0 Network IP Address 141.146.36.69 Network Gateway IP Address 141.146.36.65 ss DNS Domain	lere	BEGIN CERTIFICATE REQUEST	bbmVlcmluzzEQMA4GA: ADCCAQoCggEBA014P(yVATNBWLgQUMyo13) 2322r3sjDBUdVoP9ps: /Lo/lAd2aGfh+RiqIY' inSkfFkU7AmHRXVA1f; PmlprychG+lY4GGL1 MABWCuYDVR0PBAQDA FI2/KR+DoTpajvf69V 512/KR+DoTpajvf69V	RNwEQYDVQQH IIEAxMHU03D IIIdHBdyNzu ehR4xL7ZNgG ISUW0YEKIFO SWSJSLISTP 2xZC4MVZoJP IGKUBEWkIB4 gwgMA0GCSqG IZVZCL5pGWS dwWdW1Jg6g	Га Сору		
	Root Trusted Certificate Do you consent to installing i enabled Displaying 1-	the DigiCert High Assurance EV Root Cert 9 of 9	/ Edit	bQ4Yfv02h911umwx6503wZ5d0e5142rp2fL WrkrTi3F-cSinW3Y5d0sUC168WV36090 E2/26Dv5f2HY05f0C8Div46bg73V1V0/wKFX END CERTIFICATE REQUEST	e0G01ht17QpicMlei				

Click the copy button under the CSR and paste the output into a text file. Next, provide the txt file to your CA for signature. Once the certificate is signed by the CA, you will need to import that certificate into the SBC manually, either via ACLI or through the GUI.

Note: if you chose to import a certificate in PKCS12 format on page 3, the CSR tab will not be present under review.

Download and/or Apply

The template provides you with the ability to "Download" the config by clicking the "*Download*" tab on the top right. Next, click the "*Apply*" button on the top right, and you will see the following pop-up box appear.

Now you can click "*Confirm*" to confirm you want to apply the configuration to the SBC. The SBC will reboot. When it comes back up, the SBC will have a basic configuration in place for PureCloudPhone with Generic PSTN Sip Trunk.

Configuration Assistant Access

Upon initial login, if the Configuration Assistant Template does not immediately appear on the screen, you can access by clicking on the "SYSTEM" tab, top right of your screen. After that, click on the "Configuration Assistant" tab, top left. This allows end users to access the Configuration Assistance at any time through the SBC GUI.

9. Test Plan Executed

We have executed the following test plan to validate the interworking between Genesys PureCloud and Verizon Business SIP Trunk via Oracle SBC.

Test	Description	Pas	Fail
		S	
Outbound Local	Place an outbound call to a local number	YES	
Outbound Long- Distance	Place an outbound call to a long-distance number	YES	
Outbound International	Place an outbound call to an international number (if applicable)	YES	
Outbound Toll- Free	Place an outbound call to a toll-free number	YES	
Inbound	Place an inbound call to the range of numbers pointed to your system	YES	
Hold	Place an outbound call to any number, place call on hold for 1 minute, take call off hold	YES	
Transfer Call	Place a call, transfer the call, ensure both parties connect successfully	YES	
Call Forward	Enable call forward on phone, place call to phone, confirm call forwards successfully	YES	
Conference	Create a conference call with 3 or more people on the same call	YES	
DTMF	Call 1-800-COMCAST, confirm DTMF is received	YES	
Outbound Duration	Place outbound call, keep it connected for 10+ minutes	YES	
Inbound Duration	Place inbound call, keep it connected for 10+ minutes	YES	

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
 facebook.com/Oracle/
 twitter.com/Oracle

oracle.com

Oracle Corporation, World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065, USA

Integrated Cloud Applications & Platform Services

Copyright © 2021, 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.

Worldwide Inquiries

Fax: +1.650.506.7200

Phone: +1.650.506.7000

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