



ORACLE

Verizon Business IP Trunking with Oracle ESBC and Cisco CUCM

Technical Application Note

ORACLE

COMMUNICATIONS

Disclaimer

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

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Cisco CUCM and Verizon trunk	27 th November 2020
1.1	Refreshed the app note with testing of Verizon Trunk with CUCM 12.5 and Oracle SBC 9.0 version	22 nd May 2022

Table of Contents

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	5
2.1. VERIZON BUSINESS.....	5
2.2. CISCO CALL MANAGER (CISCO CUCM).....	5
3. INTRODUCTION	6
3.1. AUDIENCE	6
3.2. REQUIREMENTS	6
3.3. ARCHITECTURE.....	7
4. CONFIGURING THE CISCO CALL MANAGER (CISCO CUCM).....	8
4.1. CONFIGURING A NEW SIP TRUNK.....	8
4.2. CONFIGURE A NEW ROUTE PATTERN.....	10
4.3. END USER CONFIGURATION.....	12
4.4. ADDING SIP PHONE IN CUCM	13
4.5. ASSOCIATING END USER TO PHONE.....	15
5. CONFIGURING THE SBC	16
5.1. VALIDATED ORACLE SBC VERSION	16
6. NEW SBC CONFIGURATION.....	16
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	16
6.2. CONFIGURE SBC USING WEB GUI	20
6.3. CONFIGURE SYSTEM-CONFIG.....	22
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	23
6.5. CONFIGURE NETWORK INTERFACE VALUES	24
6.6. ENABLE MEDIA MANAGER.....	26
6.7. CONFIGURE REALMS.....	27
6.8. ENABLE SIP-CONFIG	29
6.9. CONFIGURE SIP INTERFACES	30
6.10. CONFIGURE SESSION-AGENT	31
6.11. CONFIGURE SESSION-AGENT GROUP	34
6.12. IKE/IPSEC CONFIG	34
6.13. CONFIGURE LOCAL-POLICY	36
6.14. CONFIGURE STEERING-POOL	39
6.15. CONFIGURE PING RESPONSE	40
6.16. SBC CONFIG FOR CISCO OFFER LESS INVITE	41
6.17. QOS MARKING	43
6.18. CONFIGURE TRANSLATION RULES	43
6.19. CONFIGURE SESSION TRANSLATION RULES.....	44
7. SBC CONFIGURATION FOR CISCO REMOTE WORKER	46
7.1. CONFIGURE REALMS.....	47
7.2. ENABLE SIP-CONFIG	49
7.3. ENABLE MEDIA MANAGER.....	50
7.4. CONFIGURE SIP INTERFACES	51
7.5. CONFIGURE STEERING-POOL	53
7.6. CONFIGURE LOCAL-POLICY (OPTIONAL)	54
8. NEW SBC CONFIG/DEPLOYMENT USING CONFIGURATION ASSISTANT	55
8.1. SECTION OVERVIEW AND REQUIREMENTS	55

8.2. INITIAL GUI ACCESS.....	55
8.3. CONFIGURATION ASSISTANT TEMPLATE NAVIGATION	58
8.3.1. PAGE 1-CISCO CALL MANAGER (CUCM) NETWORK.....	58
8.3.2. PAGE 2-OFFERLESS SDP INVITE.....	58
8.3.3. PAGE 3 - CISCO SIDE TRANSCODING	59
8.3.4. PAGE 4 - CISCO SIDE ADDITIONAL CONFIGURATION.....	60
8.3.5. PAGE 5 - VERIZON TRUNK NETWORK.....	60
8.3.6. PAGE 6 - VERIZON SESSION AGENT	61
8.3.7. PAGE 7 - VERIZON SIDE TRANSCODING	61
8.4. REVIEW	62
8.5. DOWNLOAD AND/OR APPLY	63
8.6. CONFIGURATION ASSISTANT ACCESS	64
9. EXISTING SBC CONFIGURATION	65
APPENDIX A	66

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 Cisco Call Manager (Cisco CUCM).

2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between on premises Cisco CUCM using Oracle SBC and Verizon trunk. The solution contained within this document has been tested using Oracle Communication **OS 840p3** and **OS900p3** version. Our scope of this document is testing the interoperability of Oracle SBC with CUCM and Verizon trunk.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the CUCM associated 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.

Please find the related documentation links below:

2.1. Verizon Business

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

2.2. Cisco Call Manager (Cisco CUCM)

Cisco Unified Call Manager provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management and is the core call control application of the collaboration portfolio.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Cisco CUCM 11.5 / CUCM 12.5 environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features.

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

For additional information on CUCM 11.5 and CUCM 12.5, please visit

<https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-11-5/index.html>

<https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-12-5/index.html>

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

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Cisco CUCM 11.5 / CUCM 12.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 11.5 / CUCM 12.5 server configuration, Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

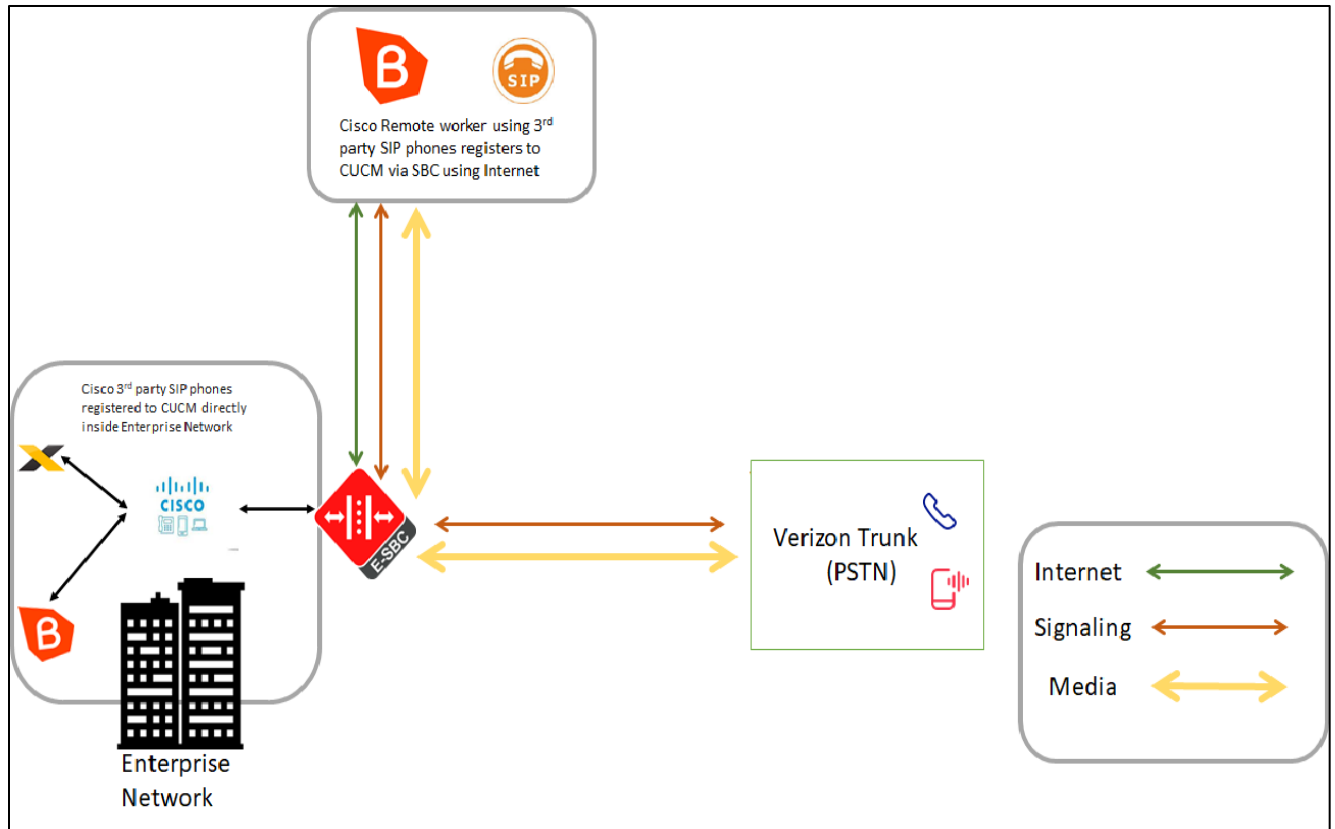
3.2. Requirements

- Fully functioning Cisco CUCM 11.5 / CUCM 12.5
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 / 9.0.0 version

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

Software Used	SBC Version	Cisco CUCM Version
Revision 1	8.4.0	11.5
Revision 2	9.0.0	12.5

3.3. Architecture

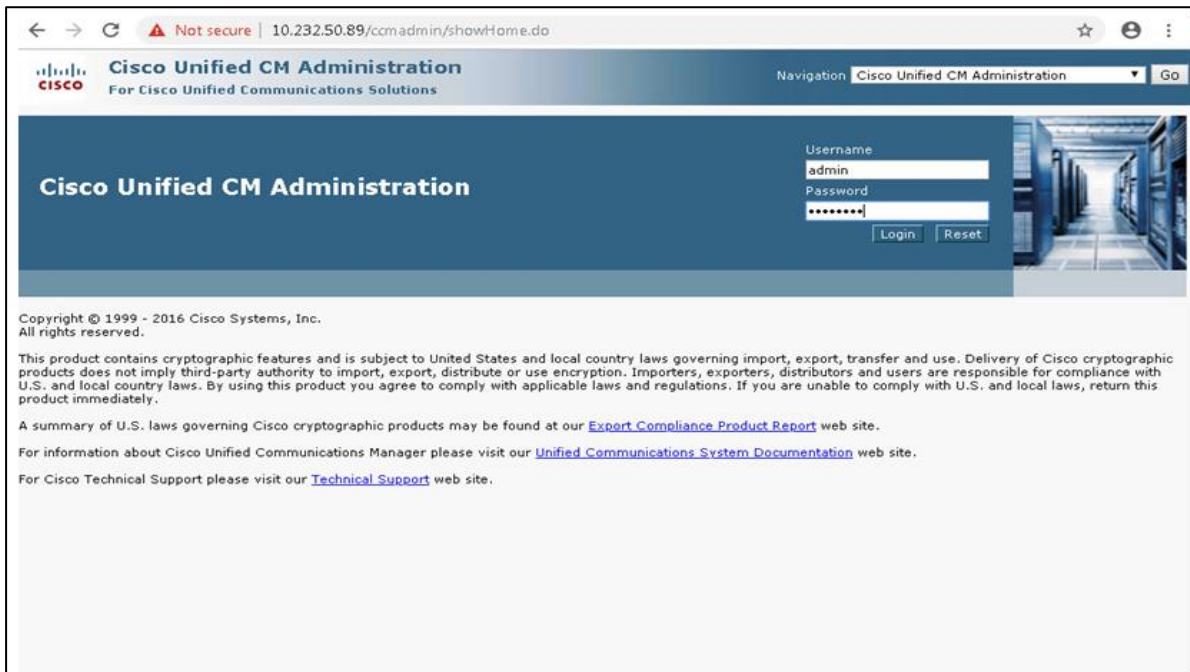


The configuration, validation and troubleshooting are the focuses of this document and will be described in three phases:

- Phase 1 – Configuring the Cisco Unified Call Manager v11.5 / V 12.5 for Oracle SBC.
- Phase 2 – Configuring the Oracle SBC.

4. Configuring the Cisco Call Manager (Cisco CUCM)

Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.



4.1. Configuring a new SIP Trunk

- 01) Go to Device ----- Trunk ----- Add New
- 02) Select Trunk Type – SIP Trunk and then Click Next
- 03) In the Device Name field, enter the SIP Trunk name and optionally provide a description.
- 04) In the Device Pool drop-down list, select a device pool id created already else select Default
- 05) Enter the Destination Address and Destination Port of the SBC under SIP Information.
- 06) Select appropriate SIP profile and SIP trunk security profile from the dropdown menu.
- 07) Click Save

← → ↻ Not secure | 10.232.50.89/camadmin/trunkEdit.do?prod=95

Cisco Unified CM Administration For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

admin | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration Related Links: Back To Find/List Go

➔ Next

Status

i Status: Ready

Trunk Information

Trunk Type* SIP Trunk ▾

Device Protocol* SIP ▾

Trunk Service Type* None(Default) ▾

Next

i *- indicates required item.

Cisco Unified CM Administration For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration

admin | Search Documentation | About

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration Related Links: Back To Find/List

Save Delete Reset Add New

Product: SIP Trunk

Device Protocol: SIP

Trunk Service Type: None(Default)

Device Name* CUCM-SBC

Description:

Device Pool* Default ▾

Common Device Configuration: < None > ▾

Call Classification*: Use System Default ▾

Media Resource Group List: < None > ▾

Location*: Hub_None ▾

AAR Group: < None > ▾

Tunneled Protocol*: None ▾

QSIG Variant*: No Changes ▾

ASN.1 ROSE OID Encoding*: No Changes ▾

Packet Capture Mode*: None ▾

Packet Capture Duration: 0

Media Termination Point Required

Retry Video Call as Audio

Path Displacement Support

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration
admin | Search Documentation | About |

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Trunk Configuration Related Links: [Back To Find/List](#)

Save Delete Reset Add New

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPV6	Destination Port	Status	Status Reason	Duration
1* 10.232.50.78		5060	up		Time Up: 0 day 0 hour 21 minutes

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard Sip Profile - Options Enabled ISR [View Details](#)

DTMF Signaling Method* RFC 2833

Normalization Script

Normalization Script < None >

Enable Trace

4.2. Configure a new Route Pattern

- 01) Go to Call Routing ----- Route/Hunt ----- Route Pattern and click Add New
- 02) Enter a Route Pattern according to the network requirements and calling plan.
- 03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.
- 04) Click Save. We can create other route patterns in the same way as shown below.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration
admin | Search Documentation | About |

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Route Pattern Configuration Related Links: [Back To Find/List](#)

Save Delete Copy Add New

Status

Status: Ready

Pattern Definition

Route Pattern* 1XXXXXXXX

Route Partition < None >

Description Route to SBC

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* CUCM-SBC [\(Edit\)](#)

Route Option

Route this pattern

Block this pattern No Error

The route patterns that has been created is shown below:

The screenshot displays the Cisco Unified CM Administration interface for 'Find and List Route Patterns'. The status indicates '2 records found'. The table below shows the details of the route patterns:

Route Patterns (1 - 2 of 2)	Rows per Page 50				
Find Route Patterns where Pattern begins with Find Clear Filter					
Pattern	Description	Partition	Route Filter	Associated Device	Copy
1XXXXXXXXXX	Route to SBC			CUCM-SBC	
91XXXXXXXXXX	Route to SBC			CUCM-SBC	

The created SIP trunk associated with the route pattern is shown below:

The screenshot displays the Cisco Unified CM Administration interface for 'Find and List Trunks'. The status indicates '4 records found'. The table below shows the details of the SIP trunks, with two rows highlighted in red:

Trunks (1 - 4 of 4)	Rows per Page 50										
Find Trunks where Device Name begins with Find Clear Filter	Select item or enter search text										
Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile
CUCM-ECB			Default					SIP Trunk	Full Service	Time In Full Service: 9 days 16 hours 37 minutes	Non Secure SIP Trunk Profile
CUCM-SBC			Default	1XXXXXXXXXX				SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 41 minutes	Non Secure SIP Trunk Profile
CUCM-SBC			Default	91XXXXXXXXXX				SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 41 minutes	Non Secure SIP Trunk Profile
sbccc			Default					SIP Trunk	No Service	Time not in Full Service: 7 days 19 hours 33 minutes	Non Secure SIP Trunk Profile

4.3. End User Configuration

- 01) Go to User Management ---- End User and click Add New
- 02) Enter in your User ID, password, pin, and Last Name
- 03) You must also enter in a password in the Digest Credentials and Confirm.
- 04) Click Save (remember the User ID and Password and DN of the device)

The screenshot shows the 'End User Configuration' page in Cisco Unified CM Administration. The 'User Information' section is active, displaying the following fields and values:

User Status	Enabled Local User
User ID*	isrvoip1
Password Edit Credential
Confirm Password
Self-Service User ID	18507904044
PIN Edit Credential
Confirm PIN
Last name*	isrvoip1
Middle name	
First name	
Display name	
Title	
Directory URI	
Telephone Number	18507904044

The screenshot shows the 'End User Configuration' page in Cisco Unified CM Administration. The 'Service Settings' section is active, displaying the following fields and values:

Home Number	
Mobile Number	
Pager Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC/Site Code	
Digest Credentials
Confirm Digest Credentials
User Profile	Standard (Factory Default) User Profile View Details
User Rank*	1-Default User Rank

Service Settings

- Home Cluster
 - Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
 - Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)
- UC Service Profile: Use System Default [View Details](#)

4.4. Adding SIP Phone in CUCM

- 01) Go to Device ---- Phone and click Add New
- 02) Select Third Party Sip Device (Basic) and click Next
- 03) Enter in a 12 digit MAC address (any dummy MAC address)
- 04) Enter the pertinent information for the SIP DEVICE settings – it should mostly be configured the same as a standard phone on your system except for the following settings
 - a) in the owner user ID field select the user you created above
 - b) in the Device Security Profile field select the security profile you created above
 - c) in the Digest User field select the user you created above
- 05) Click Save.
- 06) Configure the line settings for the SIP device – the line settings should match the line settings of your standard user's Cisco IP phones
There are no special attributes that we need to worry about on the line configuration.

The screenshot displays the Cisco Unified CM Administration web interface for configuring a SIP device. The page title is "Cisco Unified CM Administration" with the subtitle "For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The current page is "Phone Configuration", with a "Related Links" section containing "Back To Find/List".

The interface includes a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. The "Status" section shows "Status: Ready".

The "Association" section contains a table with two entries:

Association	
1	Line [1] - 18507904044 (no partition)
----- Unassigned Associated Items -----	
2	Line [2] - Add a new DN

The "Phone Type" section shows:

- Product Type: Third-party SIP Device (Basic)
- Device Protocol: SIP

The "Real-time Device Status" section shows:

- Registration: Registered with Cisco Unified Communications Manager CUCM-Cisco.pe.oracle.com
- IPv4 Address: 10.232.50.2
- Active Load ID: None
- Download Status: None

The "Device Information" section shows:

- Device is Active
- Device is not trusted
- MAC Address*: 00AABB11CCFF
- Description: ISRVolp1
- Device Pool*: Default [View Details](#)
- Common Device Configuration: < None > [View Details](#)
- Phone Button Template*: Third-party SIP Device (Basic)

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration
admin | Search Documentation | About

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Phone Configuration Related Links: Back To Find/List

Save Delete Copy Reset Apply Config Add New

Phone Button Template*	Third-party SIP Device (Basic)
Common Phone Profile*	Standard Common Phone Profile View Details
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Device Mobility Mode*	Default View Current Device Mobility Settings
Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)
Owner User ID*	isrvoip1
Mobility User ID	< None >
Use Trusted Relay Point*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Geolocation	< None >

Ignore Presentation Indicators (Internal calls only)
 Logged Into Hunt Group
 Remote Device

Apps AvayaSystemMan AvayaCM EOM ESBC NTT-SBC

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Phone Configuration Related Links: Back To Find/List Go

Save Delete Copy Reset Apply Config Add New

Remote Number

Calling Party Transformation CSS < None >
 Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)

Protocol Specific Information

BLF Presence Group* Standard Presence group
MTP Preferred Originating Codec* 711ulaw
Device Security Profile* Third-party SIP Device Basic - Standard SIP Non-Se
Rerouting Calling Search Space < None >
SUBSCRIBE Calling Search Space < None >
SIP Profile* Standard Sip Profile - Options Enabled ISR [View Details](#)
Digest User isrvoip1

Media Termination Point Required
 Unattended Port
 Require DTMF Reception

MLPP and Confidential Access Level Information

MLPP Domain < None >
Confidential Access Mode < None >

Name. Tarc

4.5. Associating End User to Phone

- 01) Go to User Management ----- End Users and search for the sip user you created above, once you find it, click on it
- 02) Scroll down to Device Association and click on the Device Association button
- 03) Locate and select the sip device you created above
- 04) Check the checkbox next to this device and click Save Selected/Changes
- 05) Click Go next to the Back to User related link near the upper right-hand corner
- 06) Click Save one more time on the End User Configuration screen.

The screenshot displays the Cisco Unified CM Administration web interface for the 'End User Configuration' page. The browser address bar shows the URL: 10.232.50.89/ccmadmin/userEdit.do?key=d464a40a-663c-b7a0-dad8-ca576d745f9d. The page title is 'End User Configuration' and the user is logged in as 'admin'. The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is divided into several sections:

- End User Configuration:** Includes buttons for Save, Delete, and Add New. Fields include Main ID, Manager User ID, Department, User Locale (set to '< None >'), Associated PC/Site Code, Digest Credentials, Confirm Digest Credentials, User Profile (Standard (Factory Default) User Profile), and User Rank* (1-Default User Rank).
- Service Settings:** Includes a checked 'Home Cluster' checkbox, an unchecked 'Enable User for Unified CM IM and Presence' checkbox, and an unchecked 'Include meeting information in presence' checkbox. The UC Service Profile is set to 'Use System Default'.
- Device Information:** Includes a 'Controlled Devices' field with the value 'SEP00DC296352B' and a 'Device Association' section with the text 'Line Appearance Association for Presence'.

With these steps, the CUCM configuration is complete.

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Call Manager (Cisco CUCM) and Verizon Trunk. If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Cisco Call Manager (Cisco CUCM) is by utilizing the [Configuration Assistant](#) feature.

5.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.4 / SBC 9.0 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME

6. New SBC configuration

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

6.1. Establishing a serial connection to the SBC

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

Please note that the above console connection procedure does not apply to VME or cloud deployments of SBC and can be applied only to hardware platforms.

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

```
Starting tLemd...
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 platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

Starting acliMgr...
password secure mode is enabled
Admin Security 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”.

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

```
Password:
%
% Only alphabetic (upper or lower case), numeric and punctuation
% characters are allowed in the password.
% Password must be 8 - 64 characters,
% and have 3 of the 4 following character classes :
%   - lower case alpha
%   - upper case alpha
%   - numerals
%   - punctuation
%
Enter New Password:
Confirm New Password:

Password is acceptable.
```

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

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

bootparam for 8.4 OS

```
NN3900-101# conf t
NN3900-101(configure)# bootparam

'.' = clear field; '-' = go to previous field; q = quit

Boot File           : /boot/nnSCZ840p4.bz
IP Address          : 10.138.194.136
VLAN                : 0
Netmask             : 255.255.255.192
Gateway             : 10.138.194.129
IPv6 Address        :
IPv6 Gateway        :
Host IP             :
FTP username        : vxftp
FTP password        : vxftp
Flags               : 0x00000010
Target Name         : NN3900-101
Console Device      : COM1
Console Baudrate    : 115200
Other               :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.

NN3900-101(configure)#
```

bootparam for 9.0 OS

```
NN4600-139(configure)# bootparam

'.' = clear field; '-' = go to previous field; q = quit

Boot File           : /boot/nnSCZ900p3.bz
IP Address          : 10.138.194.139
VLAN                : 0
Netmask             : 255.255.255.192
Gateway             : 10.138.194.129
IPv6 Address        :
IPv6 Gateway        :
Host IP             :
FTP username        : vxftp
FTP password        : *****
Flags               :
Target Name         : NN4600-139
Console Device      : COM1
Console Baudrate    : 115200
Other               :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.
```

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

```
NN3900-101# setup product
-----
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2020-07-21 04:51:24
-----
 1 : Product          : Enterprise Session Border Controller

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

Enable the features for the ESBC using the setup entitlements command as shown

Save the changes and reboot the SBC.

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

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1
  Session Capacity (0-128000)          : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3
*****
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
*****
  Admin Security (enabled/disabled)      :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5
  Transcode Codec AMR Capacity (0-102375) : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2
  Advanced (enabled/disabled)           : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10
  Transcode Codec OPUS Capacity (0-102375) : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11
  Transcode Codec SILK Capacity (0-102375) : 50
```

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

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

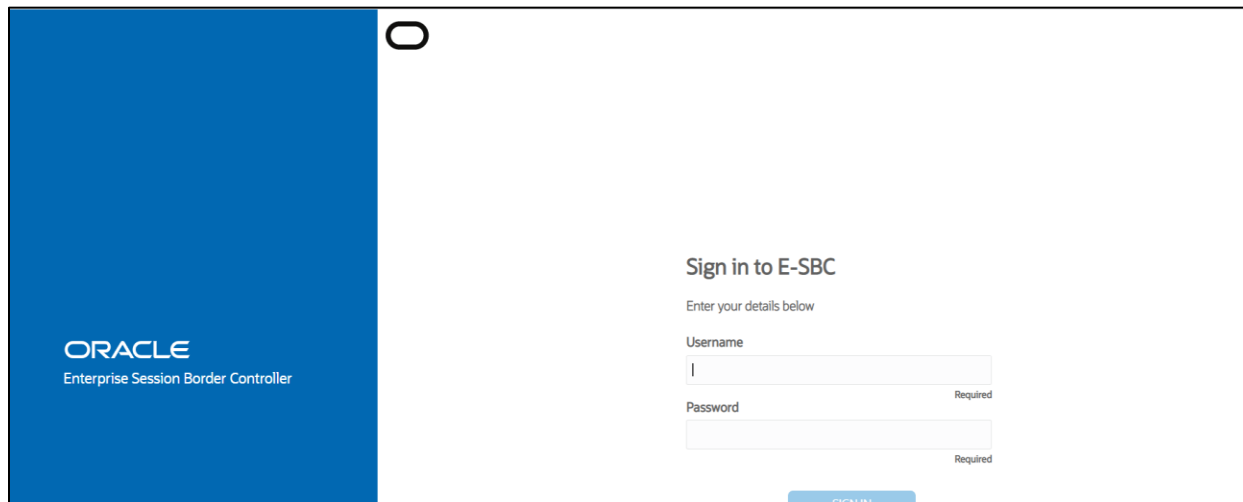
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
NN3900-101 (http-server) # show
http-server
  name                webServerInstance
  state               enabled
  realm
  ip-address
  http-state          enabled
  http-port           80
  https-state         disabled
  https-port          443
  http-interface-list GUI
  http-file-upload-size 0
  tls-profile
  auth-profile
  last-modified-by    @
  last-modified-date  2020-10-06 00:28:26
NN3900-101 (http-server) #
NN3900-101 (http-server) #
```

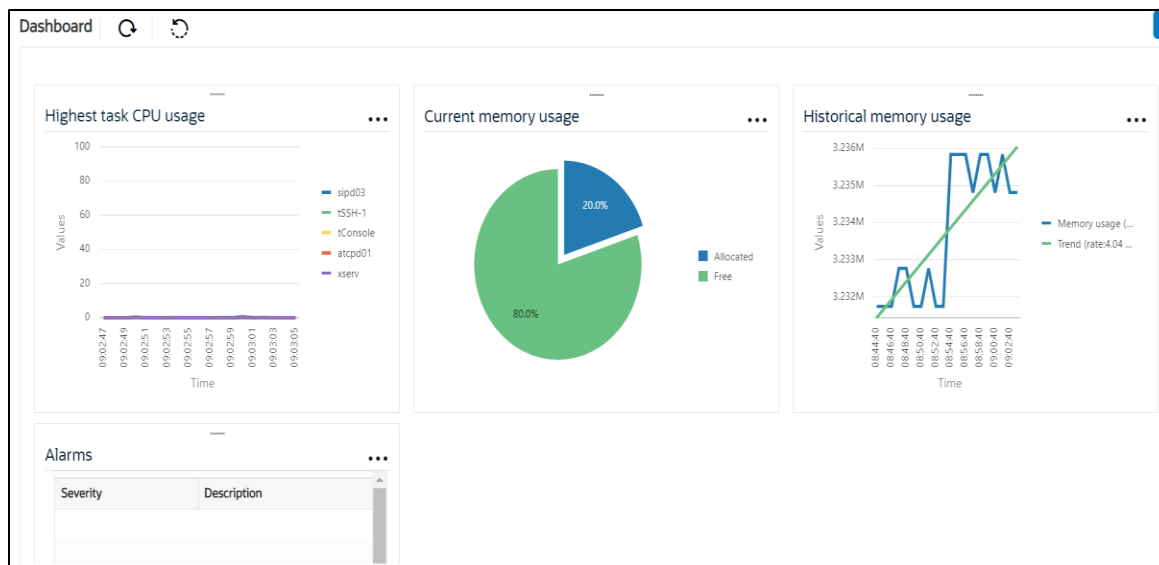
6.2. Configure SBC using Web GUI

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

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



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



Go to Configuration as shown below, to configure the SBC

The Configuration page is active, showing a list of Configuration Objects:

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

Displaying 1 - 11 of 42

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

<https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/webgui/web-gui-guide.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.

6.3. Configure system-config

Go to system->system-config

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active, and the 'system-config' option is selected in the left-hand menu. The main area displays the 'Modify System Config' form with the following fields:

- Hostname: OracleSBC
- Description: (empty text area)
- Location: (empty text field)
- Mib System Contact: (empty text field)
- Mib System Name: (empty text field)
- Mib System Location: (empty text field)
- Acp TLS Profile: (empty dropdown menu)

Buttons for 'OK' and 'Delete' are visible at the bottom of the form.

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

This screenshot shows the 'Modify System Config' page with additional configuration options. The 'Default Gateway' field is highlighted with a red rectangle and contains the value '10.138.194.129'. Other visible fields include:

- Options: (empty text field)
- Call Trace: enable
- Restart: enable
- Telnet Timeout: 0 (Range: 0..65535)
- Console Timeout: 0 (Range: 0..65535)
- HTTP Timeout: 5 (Range: 0..20)
- Alarm Threshold: (empty text field)

An 'Add' button is located below the Alarm Threshold field, and 'OK' and 'Delete' buttons are at the bottom.

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

<https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/releasenotes/esbc-release-notes.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.

6.4. Configure Physical Interface values

To configure physical Interface values, go to System->phy-interface.

Please configure M10 for Verizon side and M11 for Cisco side.

Parameter Name	Verizon Trunk (M00)	Cisco side (M11)
Slot	0	1
Port	0	1
Operation Mode	Media	Media

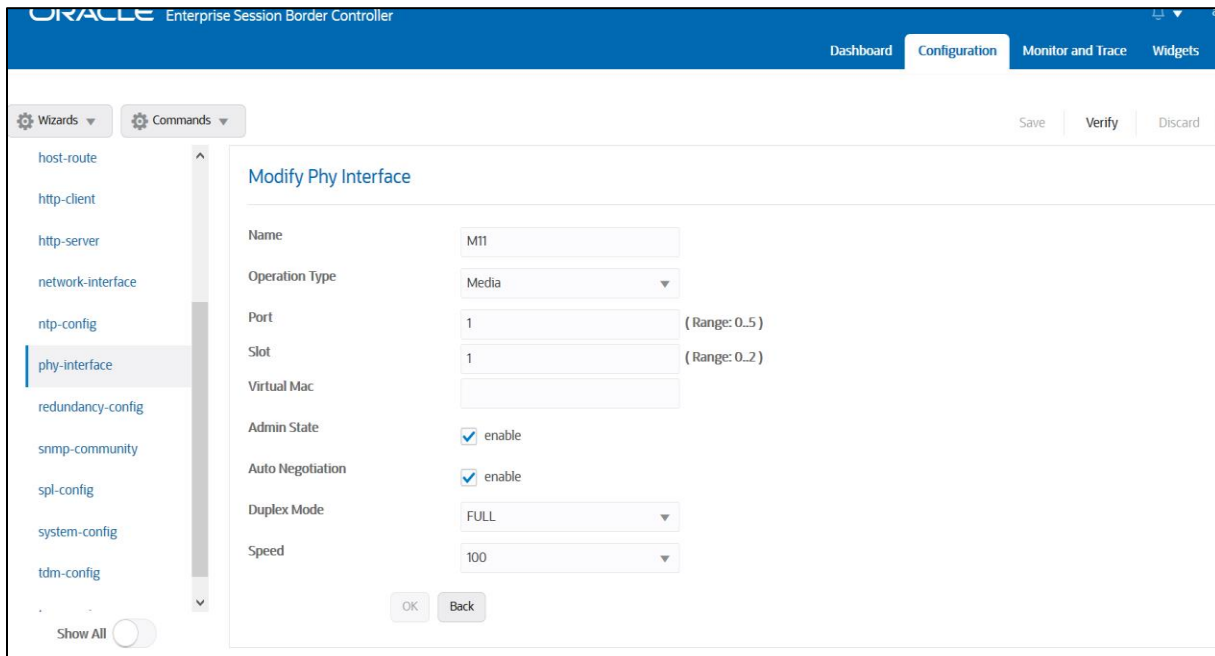
Please configure M10 interface as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', a user profile 'admin', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', and 'System'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'phy-interface' selected. The main area displays the 'Modify Phy Interface' form with the following fields:

- Name: M00
- Operation Type: Media
- Port: 0 (Range: 0..5)
- Slot: 0 (Range: 0..2)
- Virtual Mac: (empty)
- Admin State: enable
- Auto Negotiation: enable
- Duplex Mode: FULL

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is visible at the bottom left of the sidebar.

Please configure M11 interface as below



6.5. Configure Network Interface values

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

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

Parameter Name	Verizon Trunk Network Interface(M00)	Cisco side Network Interface(M01)
Name	M00	M11
Host Name		
IP Address	155.212.214.110	10.232.50.79
Net Mask	255.255.255.0	255.255.255.0
Gateway	155.212.214.65	10.232.50.1

Please configure network interface M00 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'System'. The left sidebar lists various configuration categories, with 'network-interface' selected. The main content area is titled 'Modify Network Interface' and contains the following fields:

Name	M00
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	155.212.214.110
Pri Utility Addr	

Buttons for 'OK' and 'Back' are located at the bottom of the form.

Similarly, configure network interface M11 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'network-interface' selected. The main content area is titled 'Modify Network Interface' and contains the following fields:

Name	M11
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	10.252.50.79
IP Address	10.252.50.79
Pri Utility Addr	
Sec Utility Addr	

Buttons for 'OK' and 'Back' are located at the bottom of the form.

6.6. 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 1. Go to Media-Manager->Media-Manager

The screenshot shows the 'Modify Media Manager' configuration page in the Oracle Enterprise Session Border Controller. The 'State' checkbox is checked and labeled 'enable'. The following parameters are configured:

Parameter	Value	Range
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hnt Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

Buttons: OK, Delete

The screenshot shows the 'Modify Media Manager' configuration page in the Oracle Enterprise Session Border Controller, focusing on the 'Media Policing' section. The 'Media Policing' checkbox is checked and labeled 'enable'. The following parameters are configured:

Parameter	Value	Range
Max Arp Rate	10	(Range: 0..100)
Max Signaling Packets	0	(Range: 0..4294967295)
Max Untrusted Signaling	1	(Range: 0..100)
Min Untrusted Signaling	1	(Range: 0..100)
Tolerance Window	30	(Range: 0..4294967295)
Untrusted Drop Threshold	0	(Range: 0..100)
Trusted Drop Threshold	0	(Range: 0..100)
Acl Monitor Window	30	(Range: 5..3600)
Trap On Demote To Deny	<input type="checkbox"/> enable	

Buttons: OK, Delete

Red arrows point to the 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields, both set to 1.

6.7. Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below
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 two realms used in this configuration:

Config Parameter	Verizon Trunk Side	Cisco Side
Identifier	Verizon	CUCMRealm
Network Interface	M00	M11
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FQDN		
Access Control Trust Level	High	High

In the below case, Realm name is given as Verizon for Verizon Trunk Side
Please set the Access Control Trust Level as high for this realm

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', a user profile 'admin', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', and 'System'. The left sidebar shows a tree view with 'media-manager' expanded, and 'realm-config' selected. The main content area is titled 'Modify Realm Config' and contains the following fields:

- Identifier: Verizon
- Description: (Empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (Empty list)
- Mm In Realm: (Empty list)

At the bottom of the form are 'OK' and 'Back' buttons. The interface also includes 'Wizards' and 'Commands' tabs, and 'Save', 'Verify', 'Discard', and 'Search' buttons.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

media-manager
codec-policy
media-manager
media-policy
realm-config
steering-pool
security
session-router
system
fraud-protection
hst-route
Show All

Add Realm Config

Out Translationid	<input type="text"/>	
In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
Average Rate Limit	<input type="text" value="0"/>	(Range: 0..4294967295)
Access Control Trust Level	<input type="text" value="high"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Untrusted Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Nat Trust Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Max Endpoints Per Nat	<input type="text"/>	

OK Back

Similarly, Realm name is given as CUCMRealm for Cisco side.
Please set the Access Control Trust Level as high for this realm too.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-manager
codec-policy
media-manager
media-policy
realm-config
steering-pool
security
session-router
system
Show All

Add Realm Config

Identifier	<input type="text" value="CUCMRealm"/>
Description	<input type="text"/>
Addr Prefix	<input type="text" value="0.0.0"/>
Network Interfaces	<input type="text" value="M1t0.4 X"/>
Media Realm List	<input type="text"/>
Mm In Realm	<input checked="" type="checkbox"/> enable

OK Back

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/9.0.0/security/security-guide.pdf>

6.8. Enable sip-config

SIP config enables SIP handling in the SBC.

Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below.

To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0 and forward-reg-callid-change.
- inmanip-before-validate

For more info, please refer to SBC security guide given in the above section.

The screenshot shows the 'Modify SIP Config' page in the Oracle Enterprise Session Border Controller. The left sidebar lists various configuration categories, with 'sip-config' selected. The main area contains the following settings:

- Enforcement Profile: [Dropdown]
- Red Max Trans: 10000 (Range: 0..50000)
- Options: inmanip-before-validate X, max-udp-length=0 X, forward-reg-callid-change X
- SIP Options: [Text Field]
- SIP Message Len: 0 (Range: 0..65535)
- Enum Sag Match: enable
- Extra Method Stats: enable

Buttons for 'OK' and 'Delete' are visible at the bottom.

6.9. Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please configure the below settings under the sip-interface.

- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.

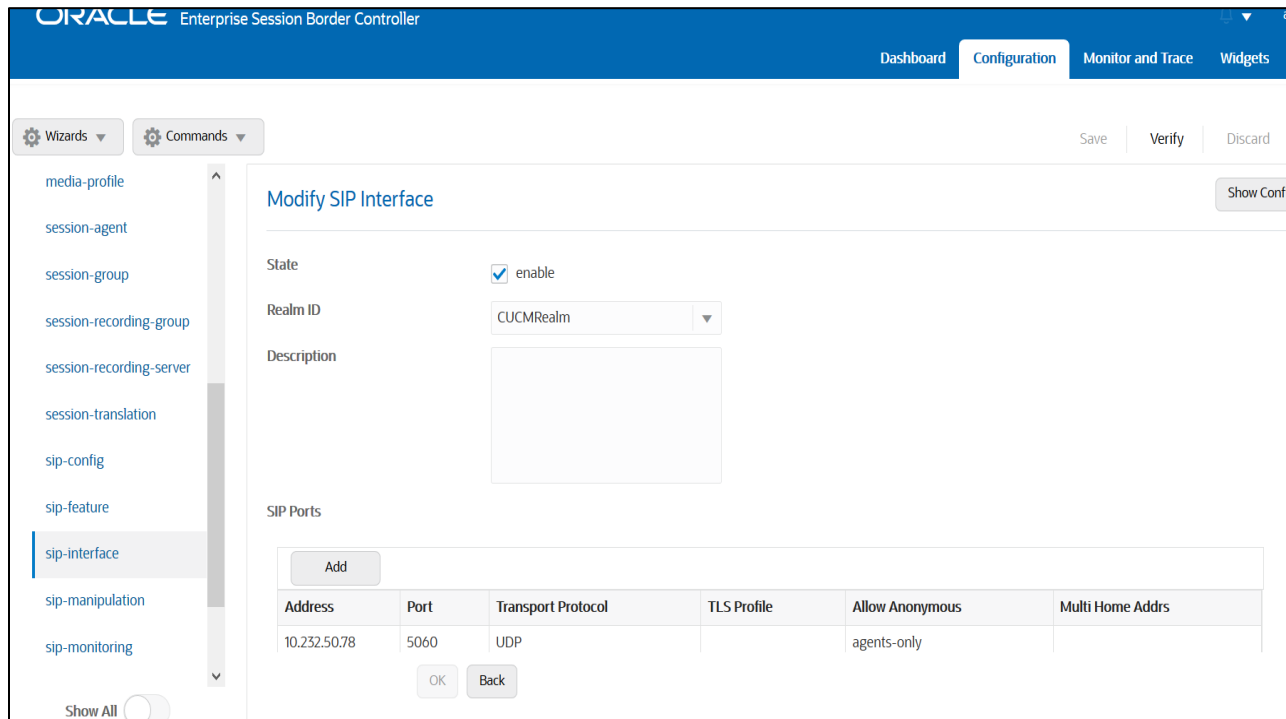
The screenshot shows the 'Modify SIP Interface' page in the Oracle Enterprise Session Border Controller. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main area contains the following settings:

- Realm ID: Verizon
- Description: [Text Area]
- SIP Ports Table:

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
155.212.214.110	5060	TCP		agents-only	
155.212.214.110	5060	UDP		agents-only	

Buttons for 'OK' and 'Back' are visible at the bottom.

Similarly, Please Configure sip-interface for the Cisco side as below:



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

6.10. 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.

Go to session-router->Session-Agent and Configure the session-agents for Verizon as below

- Host name to "sce10001.1259031211.globalipcom.com"and " sce10002.1259031211.globalipcom.com"
- IP Address to 152.188.29.19 and 152.188.28.147
- port as 66292 and 5201
- realm-id – needs to match the realm created for Verizon
- transport set to "UDP+TCP"

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets Sys

Wizards Commands Save Verify Discard

session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring sti-server translation-rules system Show All

Modify Session Agent

Show Configuration

Hostname: sce100011259031211.globalipcom.com

IP Address: 152.188.29.19

Port: 6292 (Range: 0,1025..65535)

State: enable

App Protocol: SIP

App Type:

Transport Method: UDP+TCP

Realm ID: Verizon

Egress Realm ID:

Description:

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets Sys

Wizards Commands Save Verify Discard S

session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring sti-server translation-rules system Show All

Modify Session Agent

Show Configuration

Hostname: sce100021259031211.globalipcom.com

IP Address: 152.188.28.147

Port: 5201 (Range: 0,1025..65535)

State: enable

App Protocol: SIP

App Type:

Transport Method: UDP+TCP

Realm ID: Verizon

Egress Realm ID:

Description:

OK Back

Similarly, configure the session-agents for the Cisco Side as below:

- Host name to FQDN of CUCM which is "CUCM-Cisco.pe.oracle.com" in our example. **We can also give Cisco CUCM IP address if there is no host name configured.**
- The same FQDN value should be configured in Cisco CUCM under System --- Enterprise Parameter ----Cluster FQDN.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main heading is "Add Session Agent". The configuration fields are as follows:

Hostname	CUCM-Cisco.pe.oracle.com
IP Address	10.232.50.89
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	UDP+TCP
Realm ID	CUCMRealm
Egress Realm ID	

Buttons: OK, Back

The screenshot shows the Cisco Unified CM Administration configuration page for Enterprise Parameters. The configuration is as follows:

Synching Mode for Enterprise Groups *	Differential Sync	Differential Sync
Service Manager TCP ports parameters		
Service Manager TCP Server communication port number	8883	8888
Service Manager TCP Client communication port number	8883	8889
CRS Application Parameters		
Auto Attendant Installed *	false	
PCC Express Installed *	false	
Clusterwide Domain Configuration		
Organization Top Level Domain	pe.oracle.com	
Cluster Fully Qualified Domain Name	CUCM-Cisco.pe.oracle.com	
Denial-of-Service Protection		
Denial-of-Service Protection *	True	True
TLS Handshake Timer		
TLS Handshake Timer *	60	60
TLS Resumption Timer		
TLS Resumption Timer *	3603	3600

6.11. Configure session-agent group

A session agent group allows the SBC to create a load balancing model.
Go to Session-Router->Session-Group

Please configure the following group for Verizon Session Agents

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The main window is titled "Add Session Group". The left sidebar lists various configuration categories, with "session-group" selected. The main content area contains the following fields:

- Group Name: VerizonGrp
- Description: (empty text area)
- State: enable
- App Protocol: SIP
- Strategy: RoundRobin
- Dest: sce10001.1259031211.globalipcom.com (with delete icon), sce10002.1259031211.globalipcom.com (with delete icon)

At the bottom right, there are "OK" and "Back" buttons.

6.12. IKE/IPSEC Config

The configuration elements required for IKE are not available via the Oracle ESBC GUI, and must be configured from CLI too.

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 purpose.

6.12.1. IKE Config

CLI Path: config t → security → ike → ike-config

Type Select, and use the below example to configure the global Ike configuration

ike-config

```
ike-version          1
log-level            NOTICE
phase1-dh-mode       dh-group2
phase2-exchangemode dh-group2
```

6.12.2. IKE Interface

ACL Path: config t → security→ike →ike-interface

ike-interface

```

ike-version          1
address             155.212.214.101
realm-id            Verizon
ike-mode            initiator
shared-password     *****
sd-authentication-method  shared-password
    
```

6.12.3. IKE Sainfo

ACL Path: config t → security→ike →ike-sainfo

ike-sainfo

```

name                VZ1
auth-algo           md5
encryption-algo     3des
tunnel-local-addr   155.212.214.101
tunnel-remote-addr  152.188.29.84
    
```

ike-sainfo

```

name                VZ2
auth-algo           md5
encryption-algo     3des
tunnel-local-addr   155.212.214.101
tunnel-remote-addr  152.188.28.212
    
```

6.12.4. Security Policy

Security Policies are part of the IPSEC configuration on the SBC,

This is also available through the GUI. GUI Path: security/ipsec/security policy

ACL 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
Network-Interface	S1p0:0	S1p0:0	S1p0:0	S1p0:0
Priority	0	1	2	3
Local IP addr match	155.212.214.101	155.212.214.101	155.212.214.101	155.212.214.101
Remote ip addr match	<Vz-IPSEC-IP>	<VZ-SIP-IP>	<VZ-IPSEC-IP>	<VZ-Sip-IP>
Local port match	500	0	500	0
Remote port match	500	0	500	0
Local 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
Ike-sainfo-name		VZ1		VZ2
Action	Allow	IPSEC	Allow	IPSEC
Outbound-sa-fine-grained-mask				

Local ip mask	255.255.255.255	255.255.255.0	255.255.255.255	255.255.255.0
Remote ip mask	255.255.255.255	255.255.255.224	255.255.255.255	255.255.255.224

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main content area is titled "Security Policy" and contains a table with the following data:

Name	Network Interface	Priority	Local IP Addr Match	Remote IP Addr Match	Local Port Match	Local Port Match Max
Verizon-Security-Policy-1	M00:0	0	[Redacted]	[Redacted]	500	65535
Verizon-Security-Policy-1A	M00:0	1	[Redacted]	[Redacted]	0	65535
Verizon-Security-Policy-2	M00:0	2	[Redacted]	[Redacted]	500	65535
Verizon-Security-Policy-2A	M00:0	3	[Redacted]	[Redacted]	0	65535

At the bottom of the table area, it says "Displaying 1 - 4 of 4".

6.13. Configure local-policy

Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

To route the calls from Cisco side to Verizon side, Use the below local -policy

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation

Show All

Add Local Policy

From Address

To Address

Source Realm

Description

State enable

Policy Priority

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace System

Wizards Commands Save Verify Discard Search

media-manager
security
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent

Show All

Modify Local Policy

State enable

Policy Priority

Policy Attributes

Add

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
sag:VerizonGrp	Verizon	replace-uri	disabled	0	enabled		single	

OK Back

To route the calls from the Verizon Trunk side to Cisco side, Use the below local –policy

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace System

Wizards Commands Save Verify Discard Search

media-manager security session-router access-control account-config filter-config ldap-config local-policy local-routing-config media-profile session-agent Show All

Modify Local Policy

From Address: * X

To Address: * X

Source Realm: Verizon X

Description:

State: enable

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

account-config filter-config ldap-config local-policy local-routing-config media-profile session-agent session-group session-recording-group session-recording-server session-translation Show All

Modify Local Policy

Description:

State: enable

Policy Priority: none

Policy Attributes

Add

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
CUCM-Cisco.pe.oracle.com	CUCMRealm	replace-uri	disabled	0	enabled		single	

OK Back

6.14. Configure steering-pool

Steering-pool config allows configuration to assign IP address(es), ports & a realm.

Cisco side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Steering Pool". The configuration fields are as follows:

Field	Value	Range
IP Address	10.232.50.79	
Start Port	10000	(Range: 1..65535)
End Port	15000	(Range: 1..65535)
Realm ID	CUCMRealm	
Network Interface		

Buttons: Save, Verify, Discard, Search, OK, Back. A "Show All" toggle is visible at the bottom left.

Verizon side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Steering Pool". The configuration fields are as follows:

Field	Value	Range
IP Address	155.212.214.110	
Start Port	10000	(Range: 1..65535)
End Port	10999	(Range: 1..65535)
Realm ID	Verizon	
Network Interface		

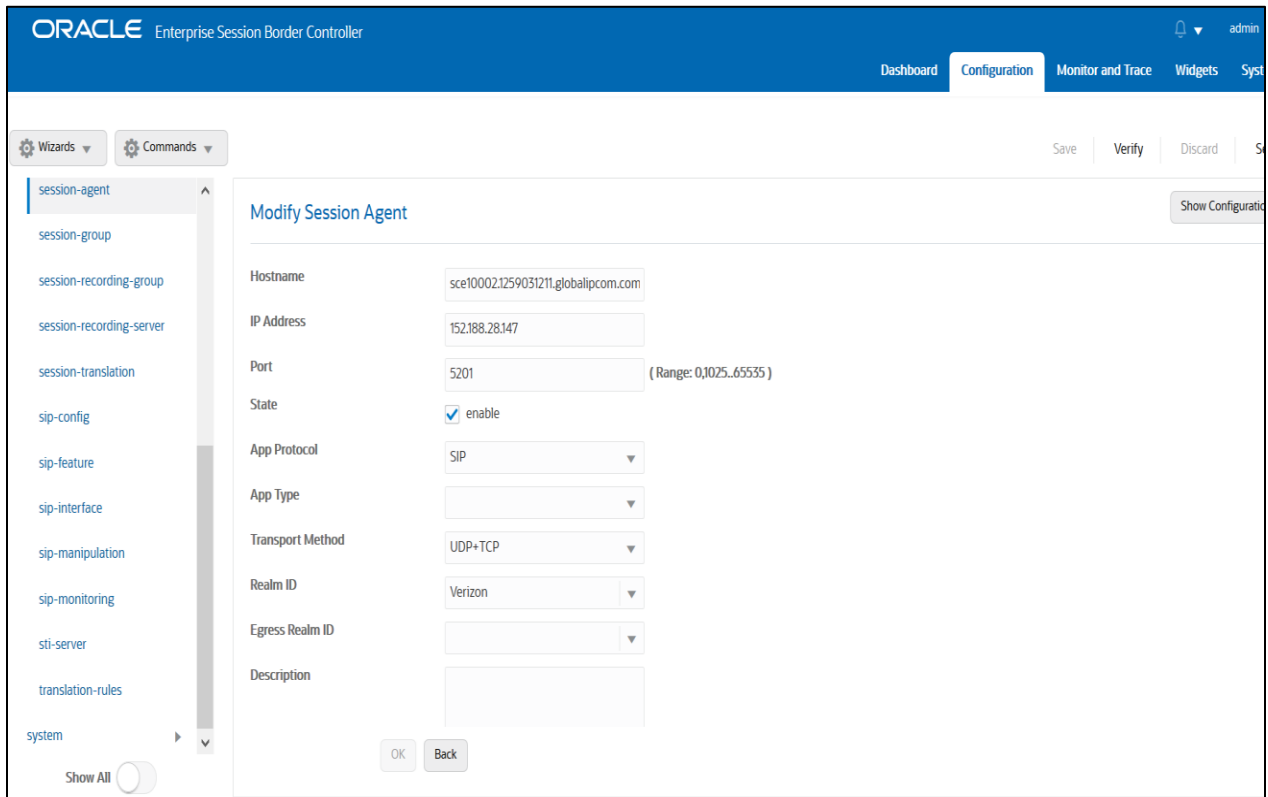
Buttons: Save, Verify, Discard, Search, OK, Back. A "Show All" toggle is visible at the bottom left.

6.15. Configure Ping Response

To simplify the ORACLE SBC configuration, from GA Release SCZ830m1p7, there is a new parameter introduced under the **Session agent** configuration element. The parameter name is **Ping response**.

Ping Response:

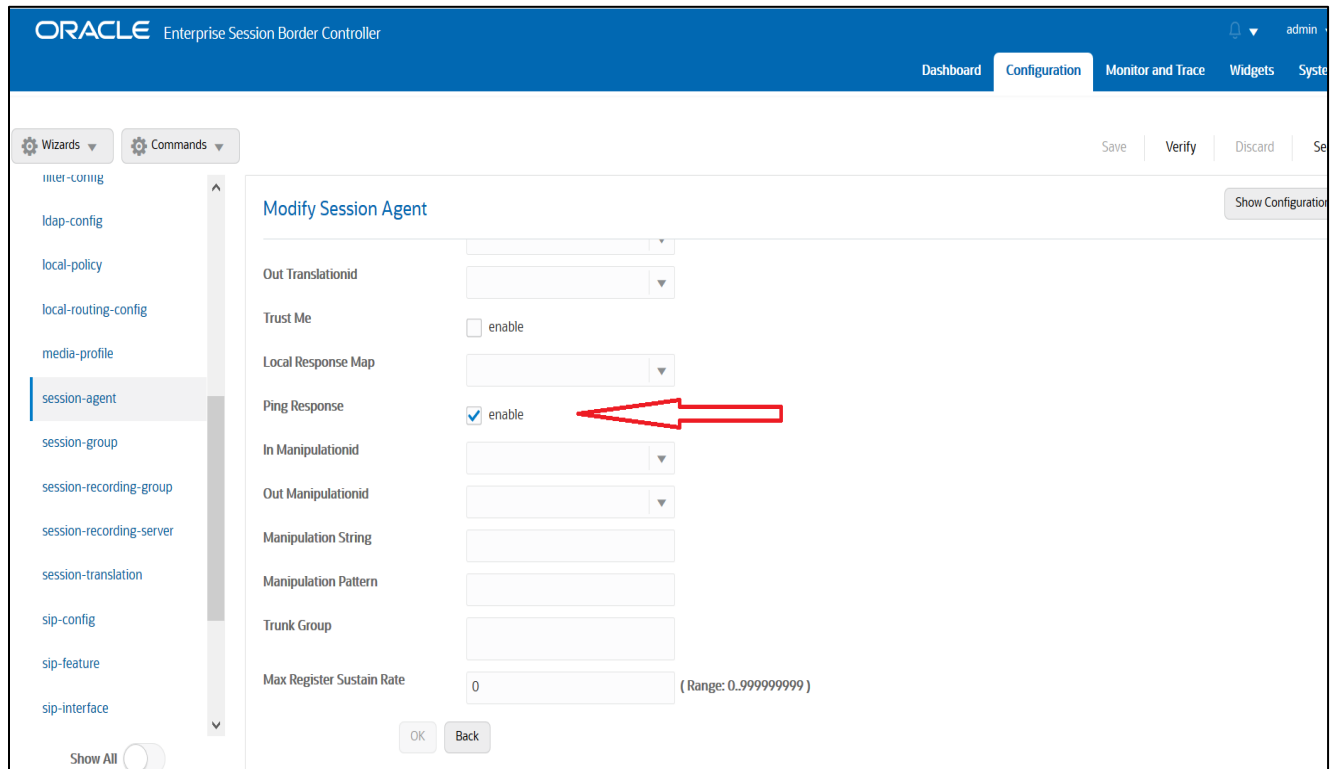
When this parameter is enabled, the SBC responds with a 200 OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RepondOptions.



The screenshot displays the ORACLE Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration elements, with 'session-agent' selected. The main area is titled 'Modify Session Agent' and contains the following fields:

Hostname	sce10002.1259031211.globalipcom.com
IP Address	152.188.28.147
Port	5201 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	UDP+TCP
Realm ID	Verizon
Egress Realm ID	
Description	

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is located at the bottom left of the sidebar.



6.16. SBC config for Cisco Offer less INVITE

When CUCM sends INVITE without SDP towards SBC and in that case, SBC needs to send out INVITE with SDP towards Verizon Trunk and vice versa. To do that, please set the parameter "**Add SDP Invite**" as both under Verizon sip interface as highlighted below. When this option is enabled, codecs have to be configured under the parameter "**Add SDP profiles**". The configured codecs is also shown below.

Note: this is an optional config – configure this only if CUCM sends offer less INVITE towards SBC.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring

Show All

Modify SIP Interface

State enable

Realm ID CUCMRealm

Description

SIP Ports

Add

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
10.232.50.78	5060	UDP		agents-only	

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
sti-server
translation-rules

Show All

Modify SIP Interface

TCP Keepalive none

Add SDP Invite both

Add SDP In Msg

P Early Media Header disabled

P Early Media Direction

Add SDP Profiles PCMU x PCMA x G729 x

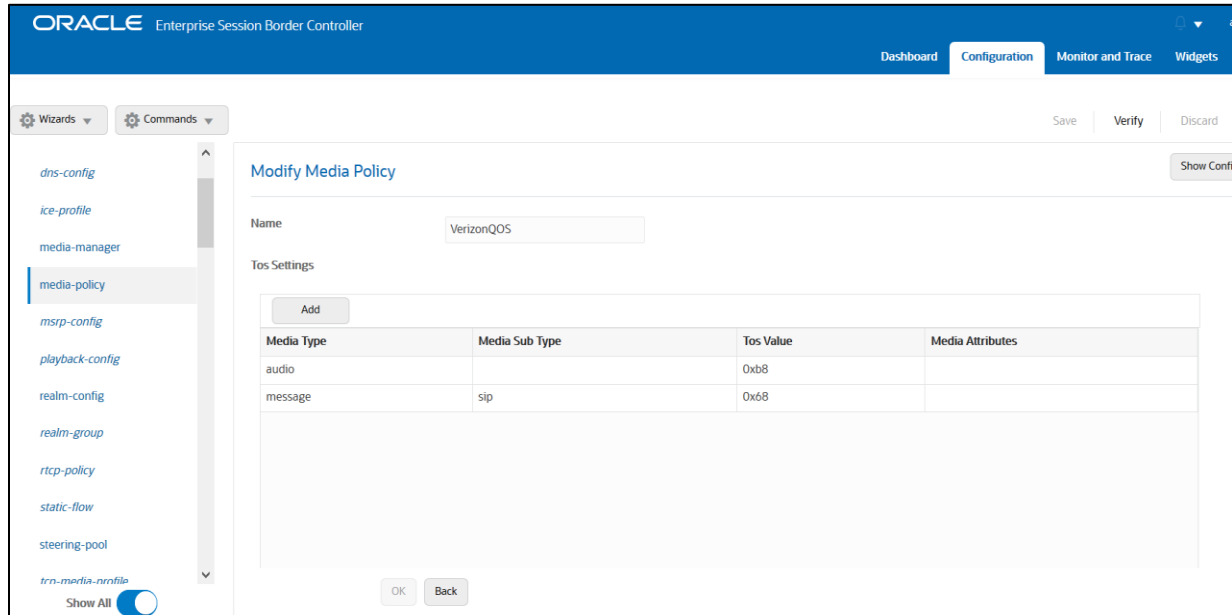
Add SDP Profiles In Msg

OK Back

6.17. QoS Marking

QoS marking allows you to apply a set of TOS/DiffServ mechanisms that enable you to provide better service for selected networks. Add this policy to Verizon Realm media policy.

Go to media manager/media policy



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

dns-config
ice-profile
media-manager
media-policy
msrp-config
playback-config
realm-config
realm-group
rtcp-policy
static-flow
steering-pool
trn-media-profile
Show All

Modify Media Policy

Name: VerizonQOS

Tos Settings

Add

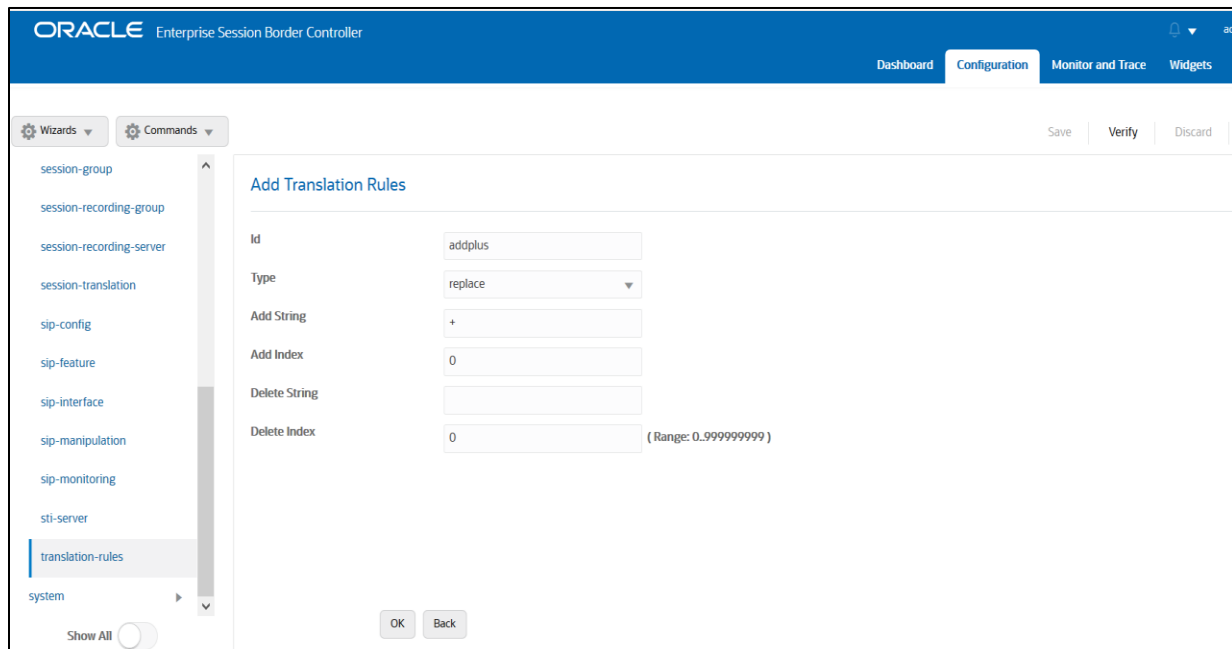
Media Type	Media Sub Type	Tos Value	Media Attributes
audio		0xb8	
message	sip	0x68	

OK Back

6.18. Configure Translation Rules

The translation rules sub-element is where the actual translation rules are created.

Go to Session router → translation-rules and create the below rule.



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
sti-server
translation-rules
system
Show All

Add Translation Rules

Id: addplus

Type: replace

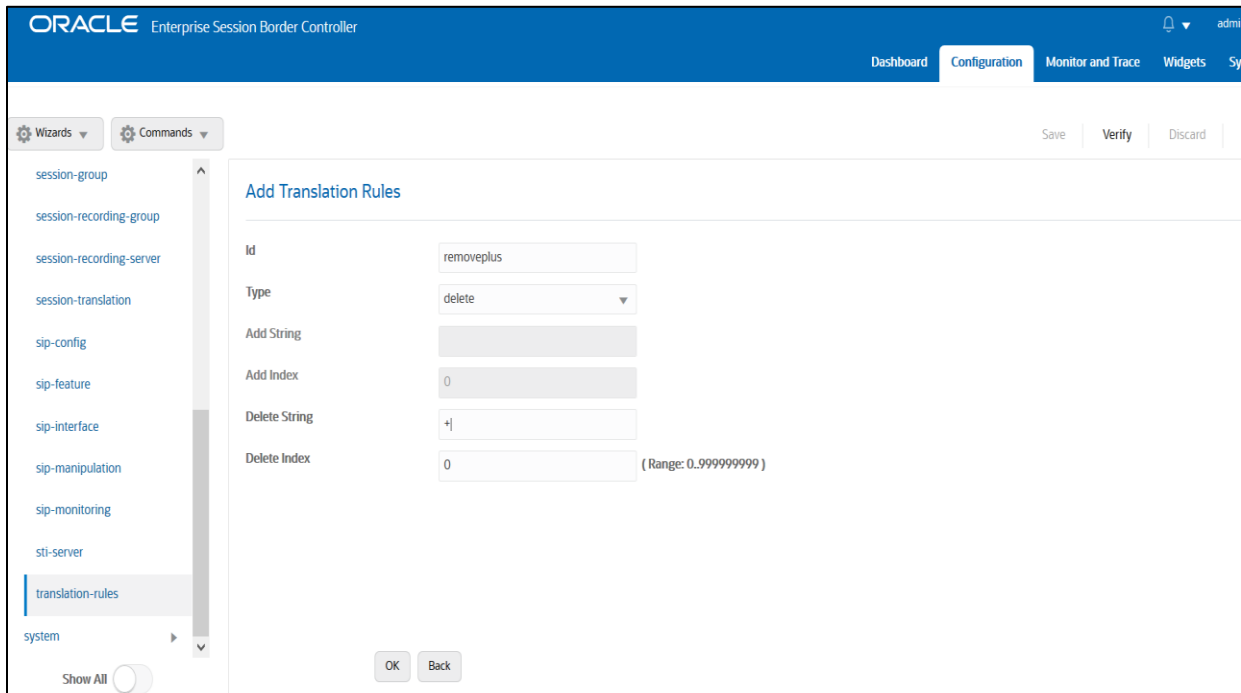
Add String: +

Add Index: 0

Delete String:

Delete Index: 0 (Range: 0..999999999)

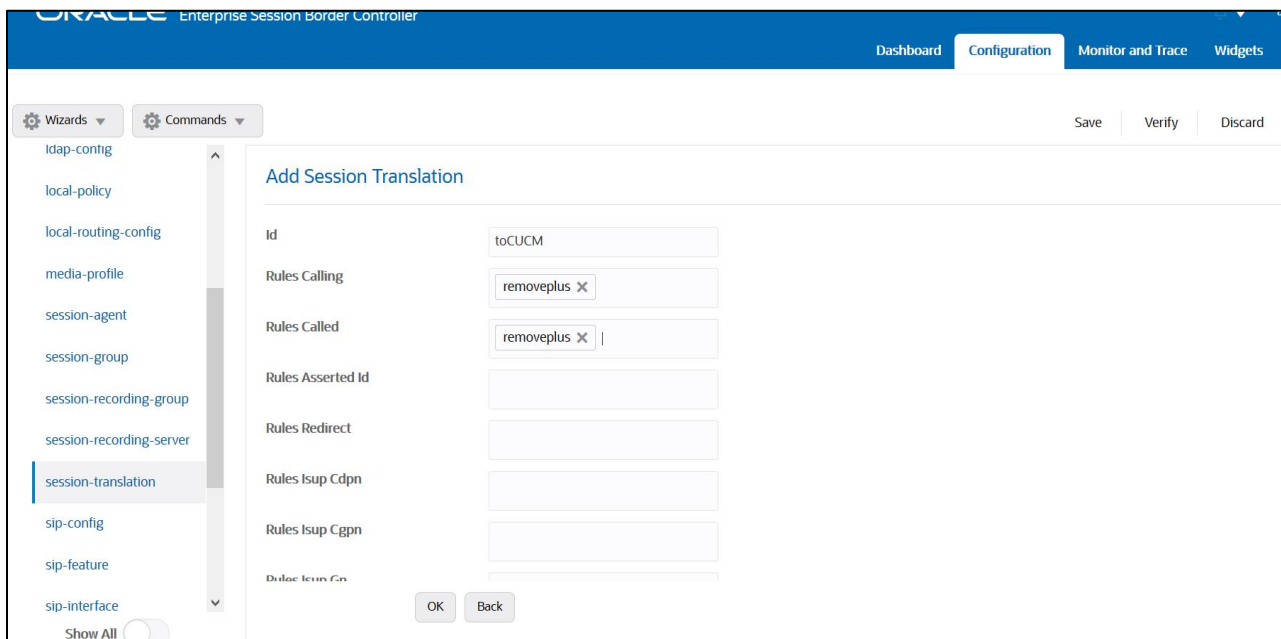
OK Back



6.19. Configure Session Translation Rules

A session translation defines how translation rules are applied to calling and called numbers. Go to Session Router → session-translation and configure the below translation rules.

Add the below translation rule to Cisco side.



Add the below translation rule to Verizon side as PSTN expects call with + sign.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'session-translation' selected. The main content area is titled 'Add Session Translation' and contains the following fields:

- Id:** toTwilio
- Rules Calling:** addPlus X
- Rules Called:** addPlus X
- Rules Asserted Id:** (empty)
- Rules Redirect:** (empty)
- Rules Isup Cdpn:** (empty)
- Rules Isup Cgpn:** (empty)

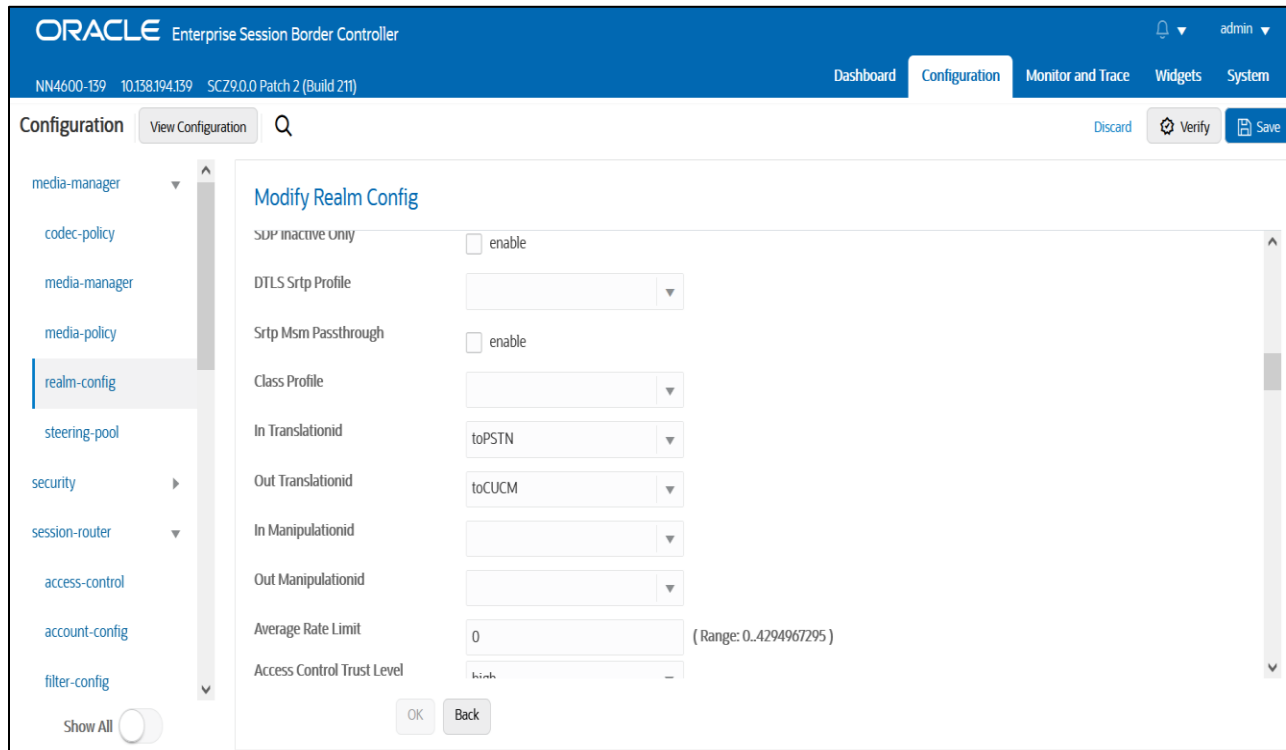
Buttons for 'OK' and 'Back' are located at the bottom of the form. 'Save', 'Verify', and 'Discard' buttons are visible in the top right corner of the configuration area.

Please add the above session translation rules to Cisco realm as shown below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Modify Realm Config'. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'realm-config' selected. The main content area is titled 'Modify Realm Config' and contains the following fields:

- Identifier:** CUCMRealm
- Description:** (empty text area)
- Addr Prefix:** 0.0.0.0
- Network Interfaces:** M1t:0.4 X
- Media Realm List:** (empty)
- Mm In Realm:** enable

Buttons for 'OK' and 'Back' are located at the bottom of the form. 'Save', 'Verify', and 'Discard' buttons are visible in the top right corner of the configuration area.



With this, SBC configuration is complete

7. SBC configuration for Cisco Remote Worker

This section of Cisco Remote Worker configuration is included for Cisco remote endpoints that register through the Oracle SBC to the Cisco Call Manager (Cisco CUCM). This would require additional configuration to be configured on the Oracle SBC along with the SIP trunking config as mentioned in the earlier description of the test bed. To complete the particular testing we have configured Cisco endpoints which will register to Cisco CUCM through the SBC. SBC will handle the calls based on the registration information present in the cache. **Please note that Cisco Remote worker Access side is secured (TLS/SRTP) and Cisco Core side is unsecured (UDP or TCP/RTP).**

Note: Remote worker configuration through TLS for Jabber clients is not supported by CUCM.

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

Access and Core Realm for Cisco Remote worker
 Steering Pool associated with the Realm for Cisco Remote worker
 Sip-interface associated with the Realm for Cisco Remote worker
 (Optional) A local-policy to route the registration requests from this Realm to the SIP Server.

Note -The local-policy element is optional as we can enable the Route to registrar parameter on the sip-interface config to route the requests to the Registrar.
 The registrar host and port is configured in the sip-config element on the SBC. The remote endpoint sends register requests from Cisco Access Realm onto the SBC and then SBC registers these endpoints onto

the Cisco Core Realm maintaining the registration cache in its database to route inbound calls to these endpoint.

Below are the snippets from the Oracle SBC Web GUI for the Remote worker configuration.

7.1. Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below. 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 two realms used in this configuration:

Config Parameter	Cisco Access Side	Cisco Core Side
Identifier	CUCMpublicRealm	CUCMCoreRealm
Network Interface	M10	M11
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High

In the below example, Realm name is given as CUCMpublicRealm for Cisco Access Side. Please set the Access Control Trust Level as medium for this realm

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-manager
codecs-policy
media-manager
media-policy
realm-config
steering-pool
security
session-router
system

Modify Realm Config

Out Manipulationid		
In Manipulationid		
Out Manipulationid		
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	medium	
Invalid Signal Threshold	10	(Range: 0..4294967295)
Maximum Signal Threshold	30	(Range: 0..4294967295)
Untrusted Signal Threshold	10	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)

OK Back

Show All

Similarly, Realm name is given as CUCMCoreRealm for Cisco Core side

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-manager
codecs-policy
media-manager
media-policy
realm-config
steering-pool
security
session-router
system

Modify Realm Config

Identifier	CUCMCoreRealm
Description	
Addr Prefix	0.0.0.0
Network Interfaces	Mt1:0.4 X
Media Realm List	
Mm In Realm	<input checked="" type="checkbox"/> enable

OK Back

Show All

7.2. Enable sip-config

SIP config enables SIP handling in the SBC.

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

To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length=0 and reg-cache-mode=from

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation

Modify SIP Config

State	<input checked="" type="checkbox"/>	enable
Dialog Transparency	<input checked="" type="checkbox"/>	enable
Home Realm ID		CUCMCoreRealm
Egress Realm ID		
Nat Mode		None
Registar Domain		*
Registar Host		*
Registar Port		5060 (Range: 0,1025..65535)
Init Timer		500 (Range: 0..4294967295)

OK Delete

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
sti-server

Modify SIP Config

Trans Expire		32 (Range: 0..4294967295)
Initial Inv Trans Expire		0 (Range: 0..999999999)
Invite Expire		180 (Range: 0..4294967295)
Session Max Life Limit		0
Enforcement Profile		
Red Max Trans		10000 (Range: 0..50000)
Options		max-udp-length=0 X reg-cache-mode=from X
SPL Options		
SIP Message Len		4096 (Range: 0..65535)

OK Delete

7.3. 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 9 which takes care of Access Realm. Go to Media-Manager->Media-Manager

The screenshot shows the 'Modify Media Manager' configuration page in the Oracle Enterprise Session Border Controller. The 'State' checkbox is checked and labeled 'enable'. Other parameters include Flow Time Limit (86400), Initial Guard Timer (300), Subsq Guard Timer (300), TCP Flow Time Limit (86400), TCP Initial Guard Timer (300), TCP Subsq Guard Timer (300), Hnt Rtcp (unchecked), Algd Log Level (NOTICE), and Mbcd Log Level (NOTICE). Range constraints are provided for several numeric fields.

Parameter	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hnt Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

The screenshot shows the 'Modify Media Manager' configuration page with additional parameters. The 'Media Policing' checkbox is checked and labeled 'enable'. The 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields are both set to 9, with red arrows pointing to their respective range constraints (0..100). Other parameters include Red Sync Comp Time (1000), Max Signaling Bandwidth (10000000), Tolerance Window (30), Untrusted Drop Threshold (0), Trusted Drop Threshold (0), and Acl Monitor Window (30). Range constraints are provided for several numeric fields.

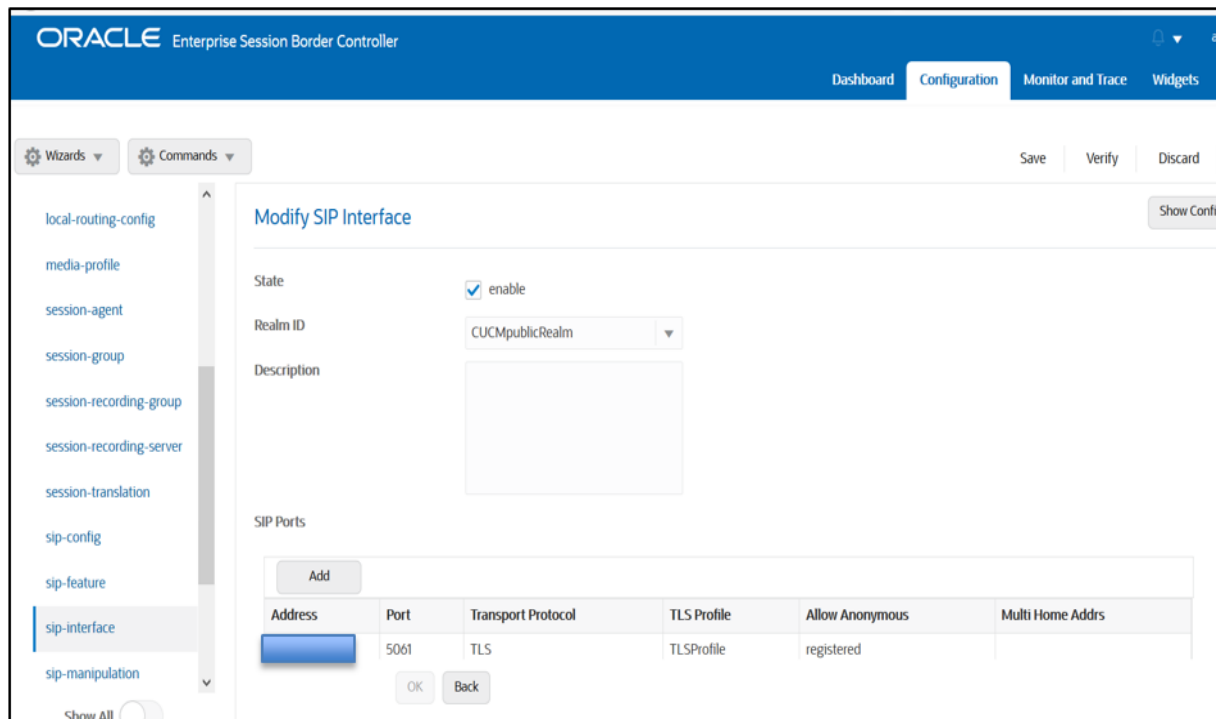
Parameter	Value	Range
Red Sync Comp Time	1000	(Range: 0..4294967295)
Media Policing	<input checked="" type="checkbox"/> enable	
Max Signaling Bandwidth	10000000	(Range: 71000..100000000)
Max Untrusted Signaling	9	(Range: 0..100)
Min Untrusted Signaling	9	(Range: 0..100)
Tolerance Window	30	(Range: 0..4294967295)
Untrusted Drop Threshold	0	(Range: 0..100)
Trusted Drop Threshold	0	(Range: 0..100)
Acl Monitor Window	30	(Range: 5..3600)
Trap On Demote To Deny	<input type="checkbox"/> enable	

7.4. Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please configure the below settings under the sip-interface.

Please Configure sip-interface for the for Cisco Access side as below:

- Set allow-anonymous to Registered to ensure traffic to this sip-interface only comes from the registered user.
- Set NAT traversal to always for the remote workers to register.
- Enable Registration Caching and Route to Register



The screenshot shows the Oracle Enterprise Session Border Controller configuration page for a SIP Interface. The page is titled "Modify SIP Interface" and is located under the "Configuration" tab. The left sidebar contains a navigation menu with items like "local-routing-config", "media-profile", "session-agent", "session-group", "session-recording-group", "session-recording-server", "session-translation", "sip-config", "sip-feature", "sip-interface" (highlighted), and "sip-manipulation".

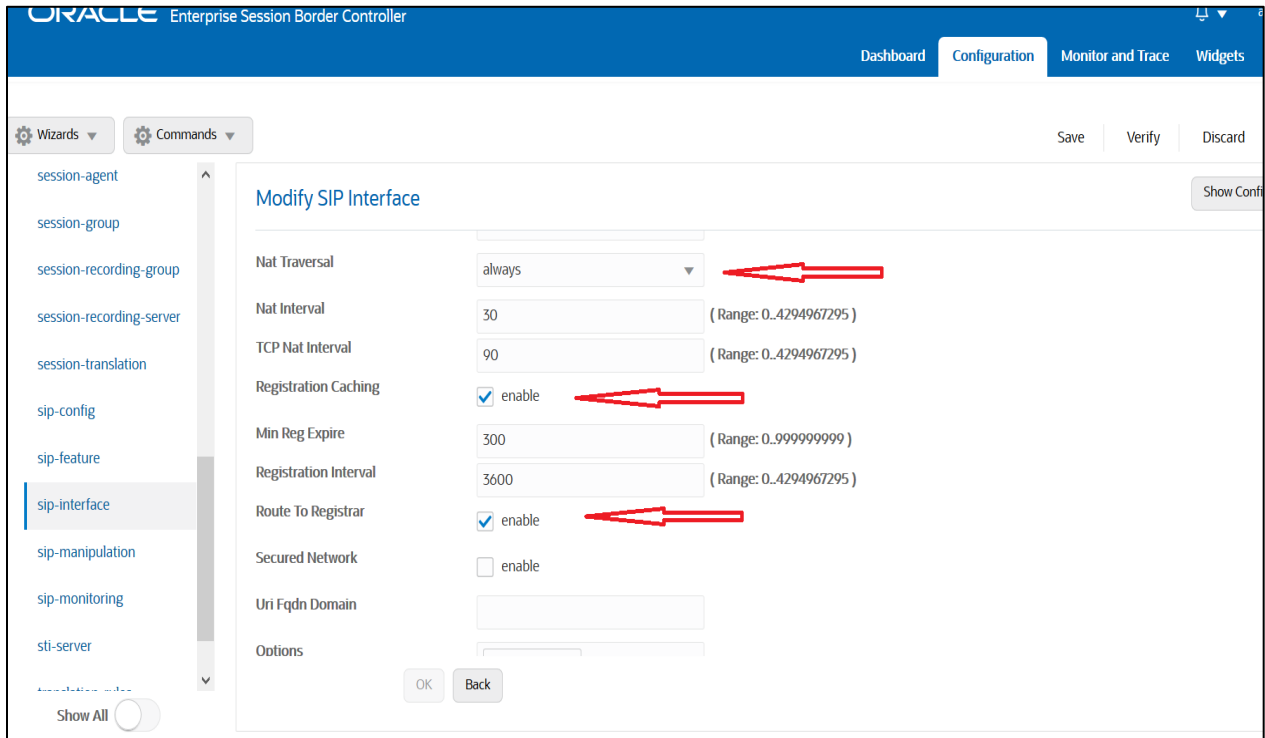
The main configuration area includes the following fields:

- State:** enable
- Realm ID:** CUCMpublicRealm
- Description:** (Empty text area)

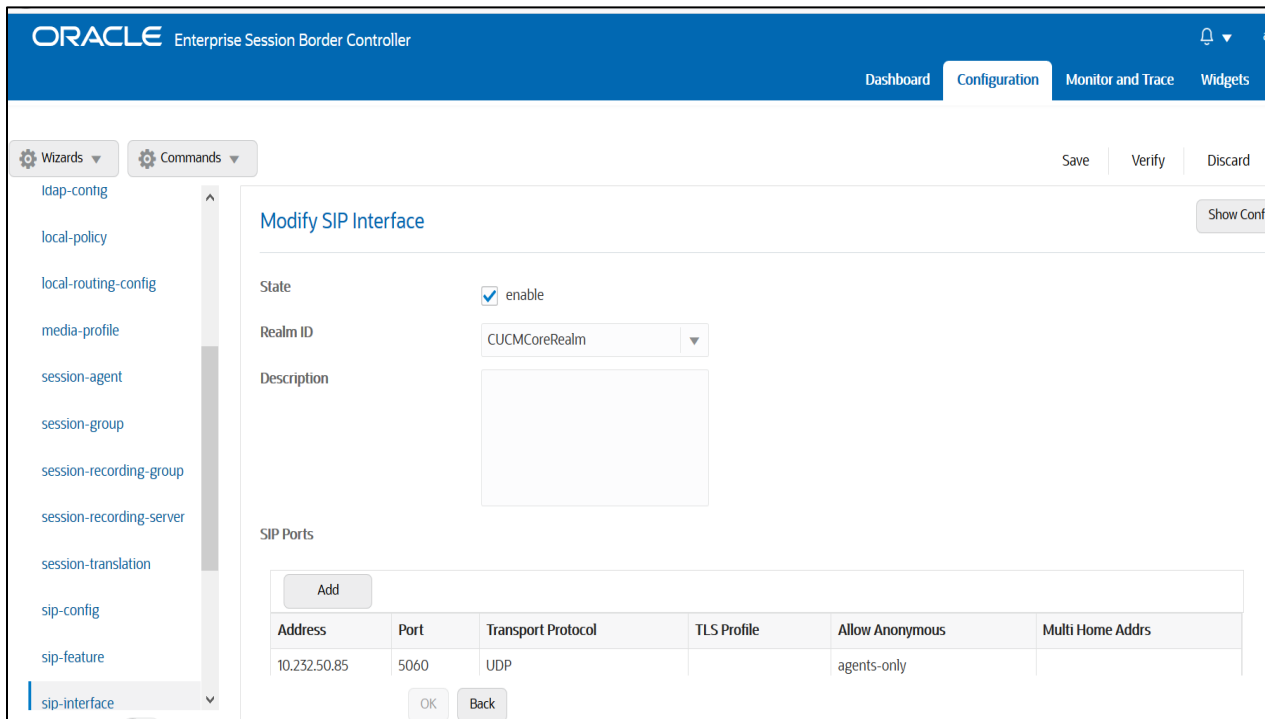
Below these fields is the "SIP Ports" section, which contains an "Add" button and a table with the following data:

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
	5061	TLS	TLSProfile	registered	

At the bottom of the SIP Ports section, there are "OK" and "Back" buttons.



Similarly, Please Configure sip-interface for the Cisco Core side as below:



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

7.5. Configure steering-pool

Steering-pool config allows configuration to assign IP address(es), ports & a realm.

Cisco Access side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Add Steering Pool". The left sidebar contains a navigation menu with the following items: media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool (highlighted), security, session-router, and system. The main configuration area contains the following fields:

IP Address	<input type="text"/>
Start Port	<input type="text" value="40000"/> (Range: 1.65535)
End Port	<input type="text" value="49999"/> (Range: 1.65535)
Realm ID	<input type="text" value="CUCMpublicRealm"/>
Network Interface	<input type="text"/>

At the bottom of the form, there are "OK" and "Back" buttons. The top navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", and "Widgets".

Cisco Core side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Add Steering Pool". The left sidebar contains a navigation menu with the following items: media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool (highlighted), security, session-router, and system. The main configuration area contains the following fields:

IP Address	<input type="text" value="10.232.50.85"/>
Start Port	<input type="text" value="30000"/> (Range: 1.65535)
End Port	<input type="text" value="35000"/> (Range: 1.65535)
Realm ID	<input type="text" value="CUCMCoreRealm"/>
Network Interface	<input type="text"/>

At the bottom of the form, there are "OK" and "Back" buttons. The top navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", and "Widgets".

7.6. Configure local-policy (Optional)

Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

To route the calls from Cisco Access side to Cisco Core side and vice versa, Use the below local –policy

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration sections, with 'local-policy' selected under the 'session-router' category. The main content area is titled 'Modify Local Policy' and contains the following fields:

- From Address: * x
- To Address: * x
- Source Realm: CUCMpublicRealm x
- Description: (empty text area)
- State: enable
- Policy Priority: none

Buttons for 'OK' and 'Back' are located at the bottom of the form.

This screenshot shows the same 'Modify Local Policy' configuration page, but with the 'Policy Attributes' section expanded. It includes an 'Add' button and a table with the following data:

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
CUCM-Cisco.pe.oracle.com	CUCMCoreRealm	replace-uri	disabled	0	enabled	SIP	single	

Buttons for 'OK' and 'Back' are located at the bottom of the form.

Cisco Offer less INVITE can happen in the Remote worker scenarios too. In that case, please set the parameter "Add SDP Invite" as both and "Add SDP profiles" under [Cisco Access side sip-interface](#). The configuration is similar to what we have done in [Sec 6.16](#).

8. New SBC config/Deployment Using Configuration Assistant

When you first log on to the E-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 E-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 [ACLI Configuration 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.**

8.1. 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 Cisco Call Manager and Verizon Trunk. The pre-requisite are given below.

- SBC running release SCZ840p7 or later which will have this template package by default added to the SBC code.

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

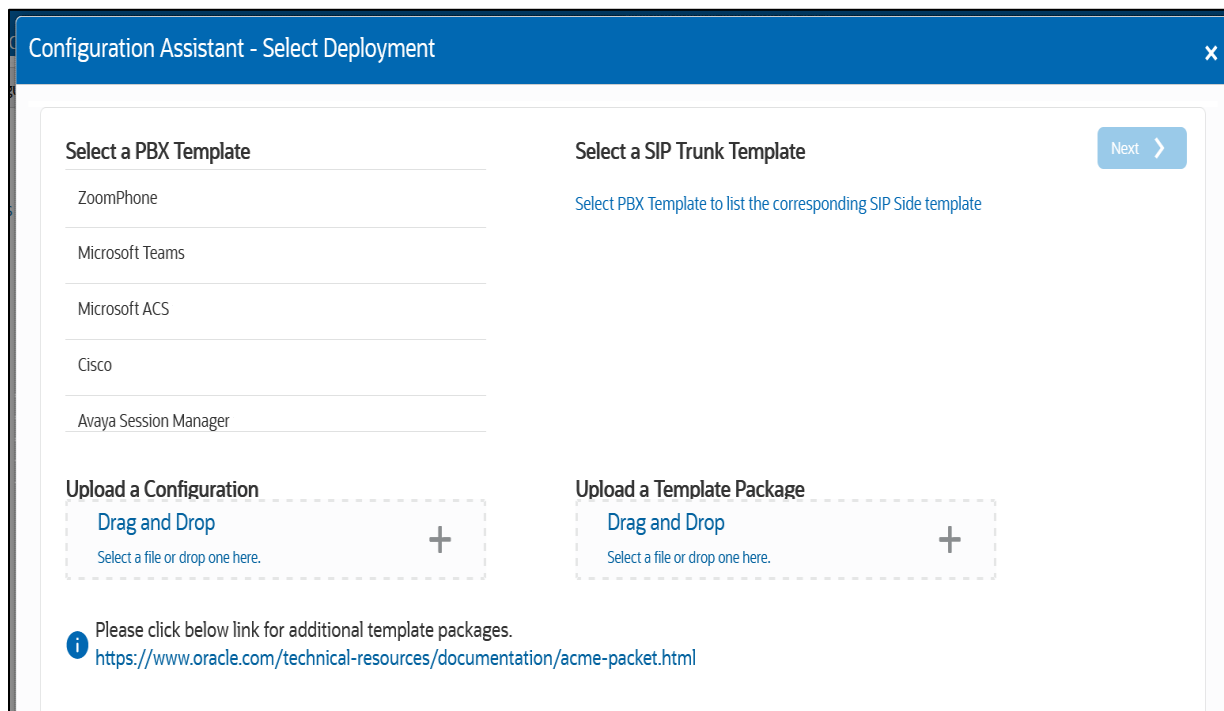
- Configured boot parameters for management access
- Setup Product
- Set Entitlements
- Configured HTTP-Server to establish access to SBC GUI

8.2. Initial GUI Access

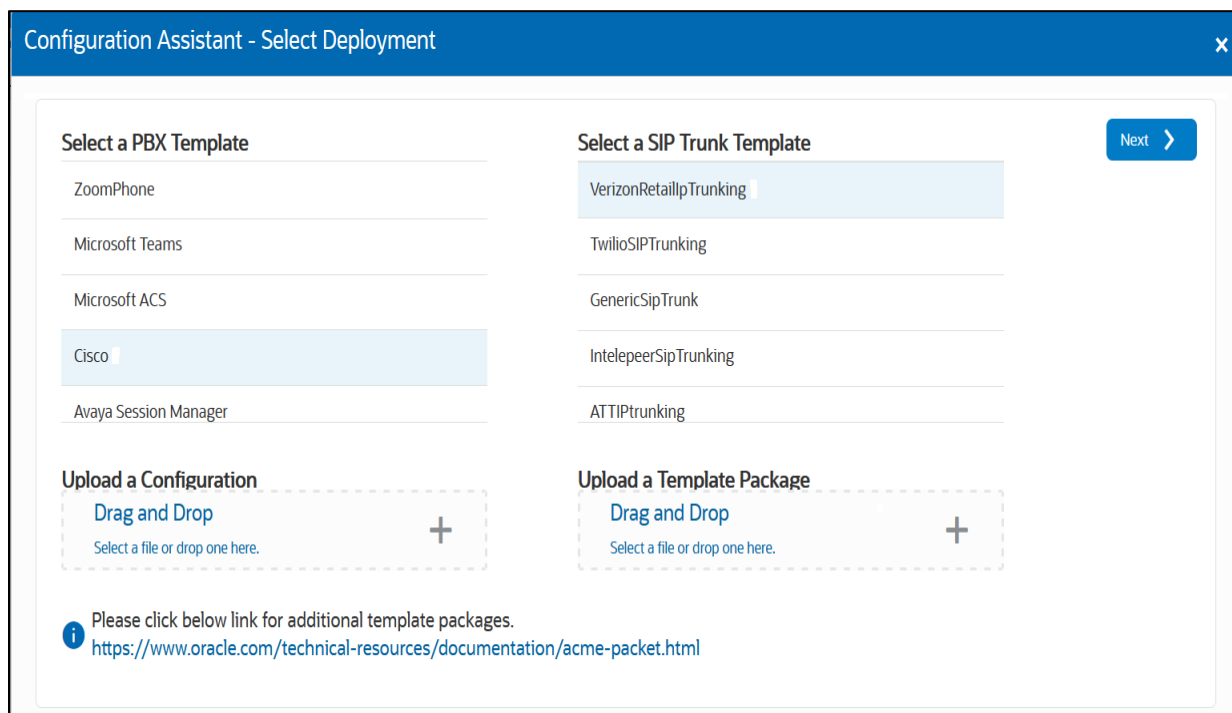
The Oracle SBC WebGui can be accessed by entering the following in your web browser: `http(s)://<SBC Management IP>`.

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



As we can see, there are some templates of PBX populated in the template and we can select the PBX template that we want to use with our Verizon trunk and for this document, we have selected Cisco template and once we select that, it asks us to select the SIP trunk template. After we select Verizon trunk template, the Next option would be enabled.



Click **Next**. The following “Notes” will be displayed related to pre-requisite

The screenshot shows a window titled "Configuration Assistant - Notes". It contains two columns of information. The left column is for the "PBX Template" and the right column is for the "SIP Trunk Template". Both columns include a "Warning" section stating that proceeding with the Configuration Assistant will erase existing configuration, and a "Pre-requisites" section with a list of requirements. The PBX prerequisites include connecting Port 0 of the SBC, installing transcoding resources, and setting session capacity and system time. The SIP Trunk prerequisites include connecting Port 1 of the SBC, installing transcoding resources, and setting session capacity and system time. Navigation buttons for "Back" and "Next" are visible at the top of the content area.

Configuration Assistant - Notes

PBX Template
Notes for Cisco

Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.

Pre-requisites:

- Connect Port 0 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only).
- This template supports ONLY UDP/TCP configuration.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

SIP Trunk Template
Notes for VerizonRetailIpTrunking

Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.

Pre-requisites:

- Connect Port 1 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only)(If Applicable).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only)(If Applicable).
- This template supports ONLY UDP/TCP configuration.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

Click **Next** and we get the below screen where we need to enter the details for SBC configuration.

The screenshot shows a window titled "Configuration Assistant - Configure CUCM Network here". At the top, there is a progress bar with seven steps: 1. Configure CUCM Network here (highlighted), 2. Offerless SDP configuration, 3. Cisco CUCM Transcoding, 4. Additional Configuration, 5. Verizon IP Trunk Network, 6. Verizon Session Agent, and 7. Verizon Transcoding. Below the progress bar, the text reads "Let's configure the interface that communicates with your CUCM". There are four input fields: "Realm Name", "Enter CUCM hostname here", "Enter the CUCM IP here", and "Enter the CUCM port here". Each field has a "Required" label and a help icon. Navigation buttons for "Back" and "Skip" are visible at the top of the content area.

Configuration Assistant - Configure CUCM Network here

1 — 2 — 3 — 4 — 5 — 6 — 7

Configure CUCM Network here Offerless SDP configuration Cisco CUCM Transcoding Additional Configuration Verizon IP Trunk Network Verizon Session Agent Verizon Transcoding

Let's configure the interface that communicates with your CUCM

Realm Name [?]

Required

Enter CUCM hostname here [?]

Required

Enter the CUCM IP here [?]

Enter the CUCM port here [?]

8.3. Configuration Assistant Template Navigation

8.3.1. Page 1-Cisco Call Manager (CUCM) Network

Page 1 of the template is where you will configure the network information to connect Cisco Call Manager. On this page, we will enter the CUCM hostname, IP and port which will be the next hop IP address/hostname for sip signaling to and from your CUCM

Configuration Assistant - Configure CUCM Network here

1 — 2 — 3 — 4 — 5 — 6 — 7

Configure CUCM Network here Offerless SDP configuration Cisco CUCM Transcoding Additional Configuration Verizon IP Trunk Network Verizon Session Agent Verizon Transcoding

Let's configure the interface that communicates with your CUCM

Realm Name ⓘ
Required

Enter CUCM hostname here ⓘ
Required

Enter the CUCM IP here ⓘ

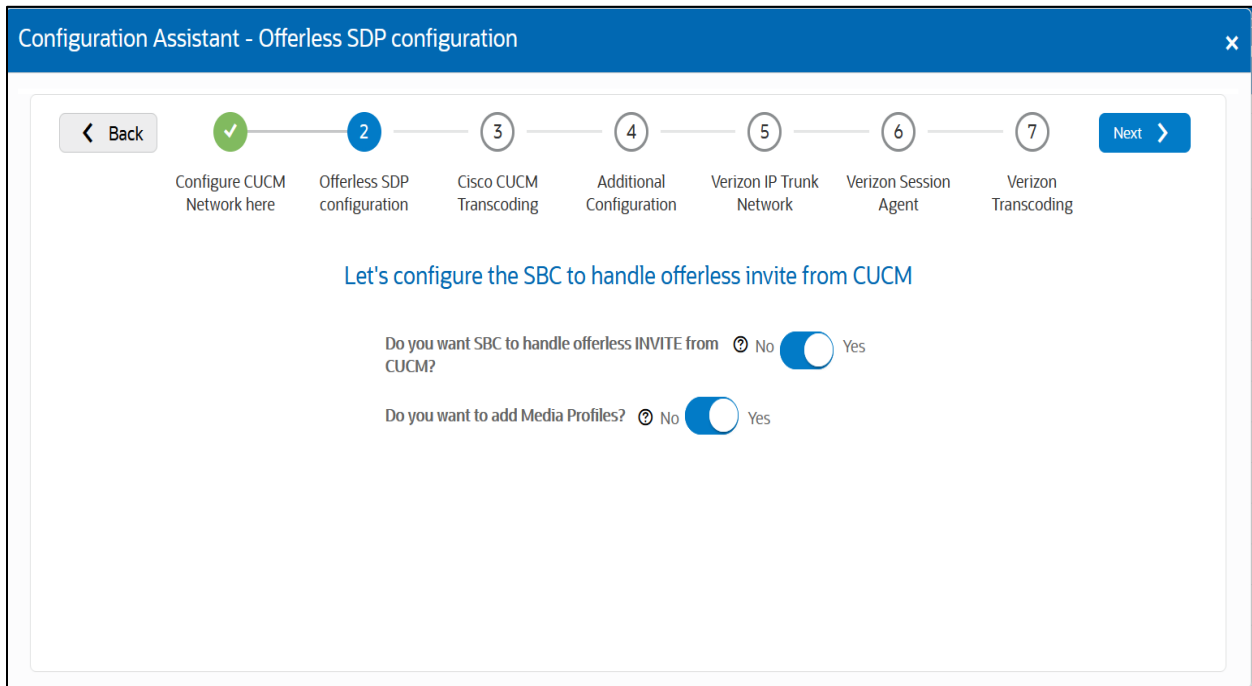
Enter the CUCM port here ⓘ

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 field. Also, pay close attention to which fields are listed as “required”.

8.3.2. Page 2-Offerless SDP Invite

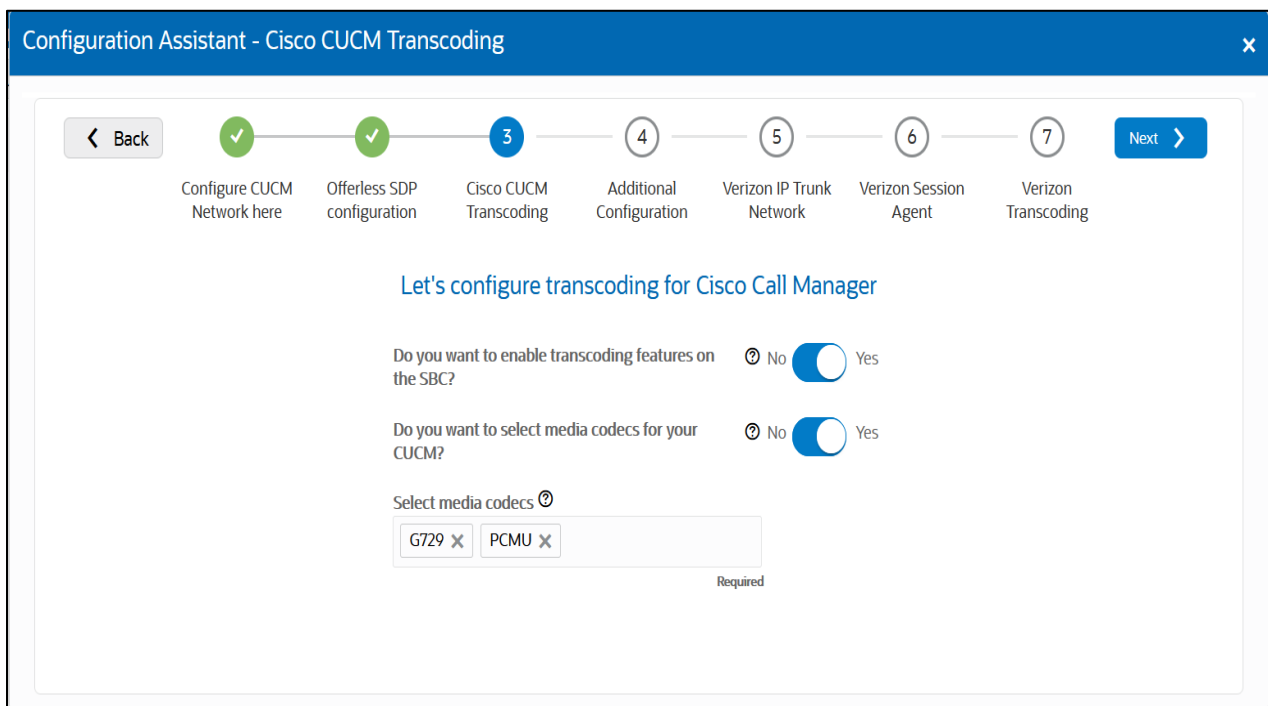
Page 2 of the template is where you will configure the information related to Cisco’s offer less SDP Invite configuration. You can enable or disable the configuration through the Yes/No Radio Button.

Note Click on the ? icon to know more about the configuration parameters and their usage.



8.3.3. Page 3 - Cisco side Transcoding

Page 3 is where you will be able to configure transcoding between the SBC and Cisco Call Manager. 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 Cisco Call Manger. 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.



8.3.4. Page 4 - Cisco side Additional Configuration

Page 4 is where you will be able to configure Session Agent Capabilities towards CUCM side. This includes enabling OPTIONS, enabling session translation etc towards CUCM side as shown below. . You can enable or disable the configuration through the Yes/No Radio Button

The screenshot shows a configuration assistant window titled "Configuration Assistant - Additional Configuration". At the top, a progress bar indicates seven steps: 1. Configure CUCM Network here (checked), 2. Offerless SDP configuration (checked), 3. Cisco CUCM Transcoding (checked), 4. Additional Configuration (active), 5. Verizon IP Trunk Network, 6. Verizon Session Agent, and 7. Verizon Transcoding. A "Back" button is on the left and a "Next" button is on the right. Below the progress bar, the heading "Let's configure Session Agent capabilities" is followed by three questions with radio buttons for "No" and "Yes":
1. "Do you want to enable OPTIONS ping towards CUCM?" with "Yes" selected.
2. "Do you want SBC to handle call transfer from your CUCM?" with "No" selected.
3. "Do you want to enable session translation towards CUCM?" with "Yes" selected.
Below these are two input fields: "Do you want to add or remove a string?" with a "Remove" button and an "Enter the string" field.

8.3.5. Page 5 - Verizon Trunk Network

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

The screenshot shows a configuration assistant window titled "Configuration Assistant - Verizon IP Trunk Network". The progress bar shows seven steps: 1. Configure CUCM Network here (checked), 2. Offerless SDP configuration (checked), 3. Cisco CUCM Transcoding (checked), 4. Additional Configuration (checked), 5. Verizon IP Trunk Network (active), 6. Verizon Session Agent, and 7. Verizon Transcoding. A "Back" button is on the left and a "Skip" button is on the right. Below the progress bar, the heading "Let's configure the interface that communicates with your Verizon Retail IP Trunk" is followed by three required fields:
1. "Realm Name" with a text input field and "Required" label.
2. "Port Number" with a dropdown menu showing "Port 0" and "Required" label.
3. "Slot Number" with a dropdown menu showing "Slot 0" and "Required" label.

8.3.6. Page 6 - Verizon Session Agent

Page 6 of the template is where you will configure the Verizon Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Verizon Trunk. Please fill the required fields and click Next.

Configuration Assistant - Verizon Session Agent

Back ✓ ✓ ✓ ✓ ✓ **6** 7 Next

Configure CUCM Network here Offerless SDP configuration Cisco CUCM Transcoding Additional Configuration Verizon IP Trunk Network **Verizon Session Agent** Verizon Transcoding

Let's configure the Session Agent for Verizon

Verizon Session Agent hostname [Ⓜ]
155.212.214.125
Required

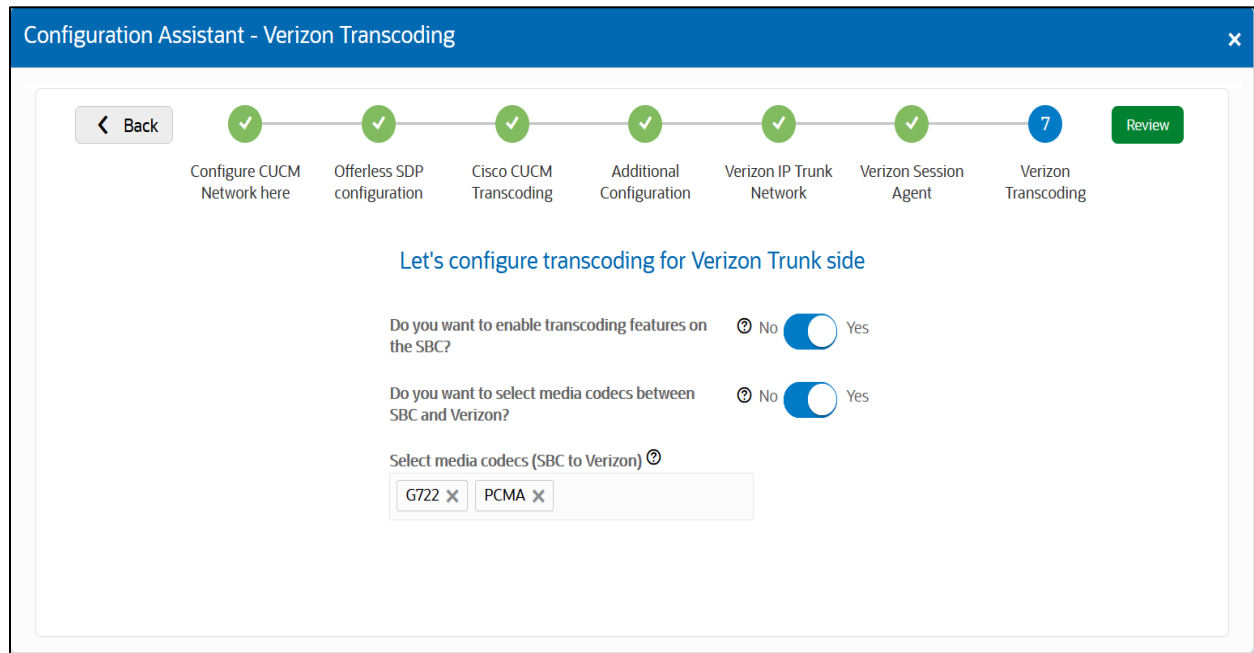
Verizon Session Agent IP Address [Ⓜ]
155.212.214.125

Verizon Session Agent Port [Ⓜ]
5060
Required

Did Verizon provide a second Hostname /IP No Yes

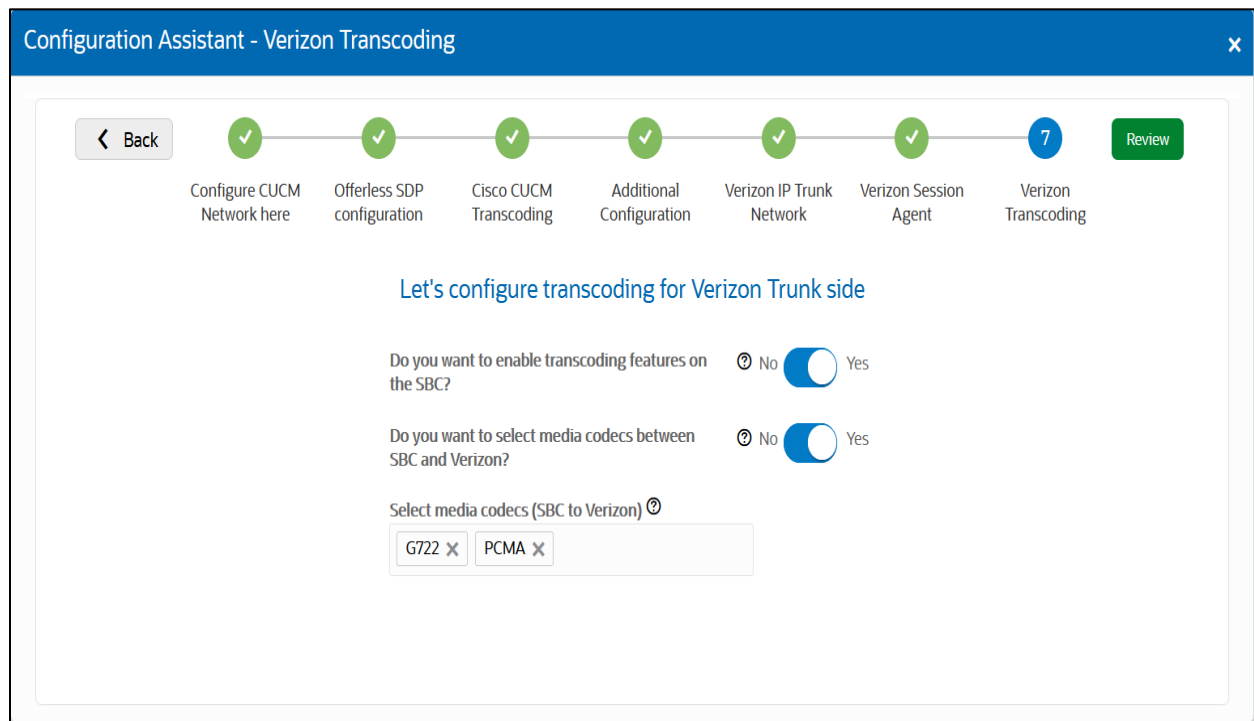
8.3.7. Page 7 - Verizon side Transcoding

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



8.4. Review

At the end of the template, you will notice in the top right, a **Review** tab. If all 7 pages presented across the top are showing green, indicating there are no errors with the information entered, click on the **Review** tab.



The screen looks like below after clicking the Review Tab.

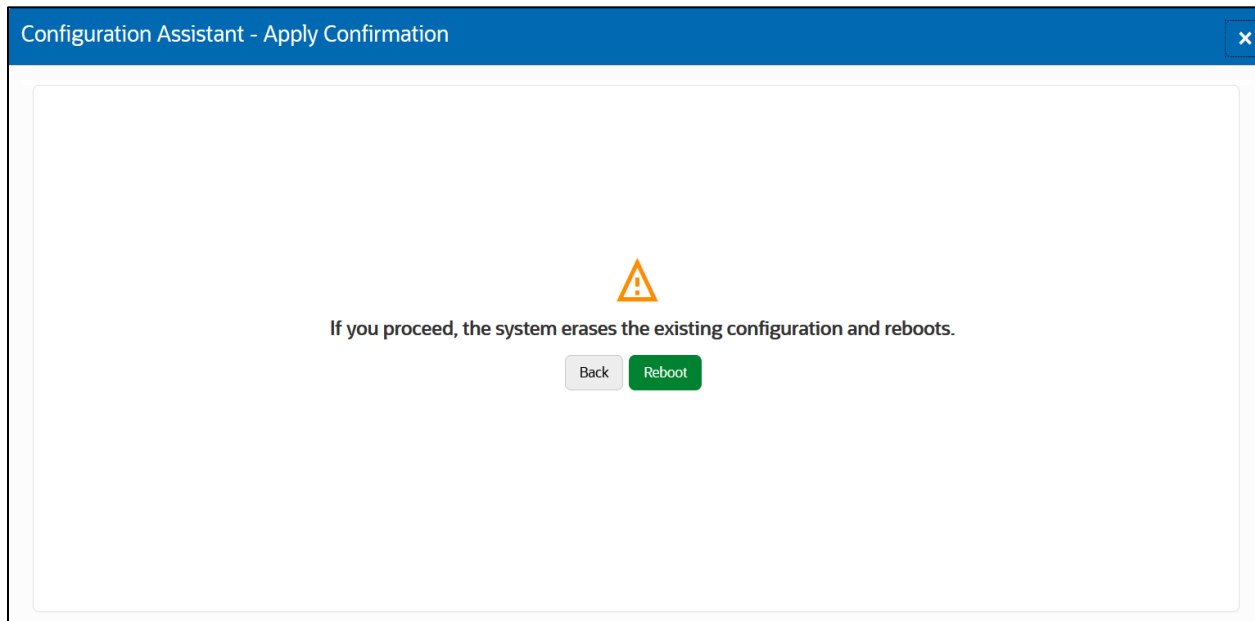


On the left side of the review contains the entries for each page. Each page has an “*Edit*” tab that can be used to make changes to the information entered on that specific page without having to go through the entire template again.

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.

8.5. Download and/or Apply

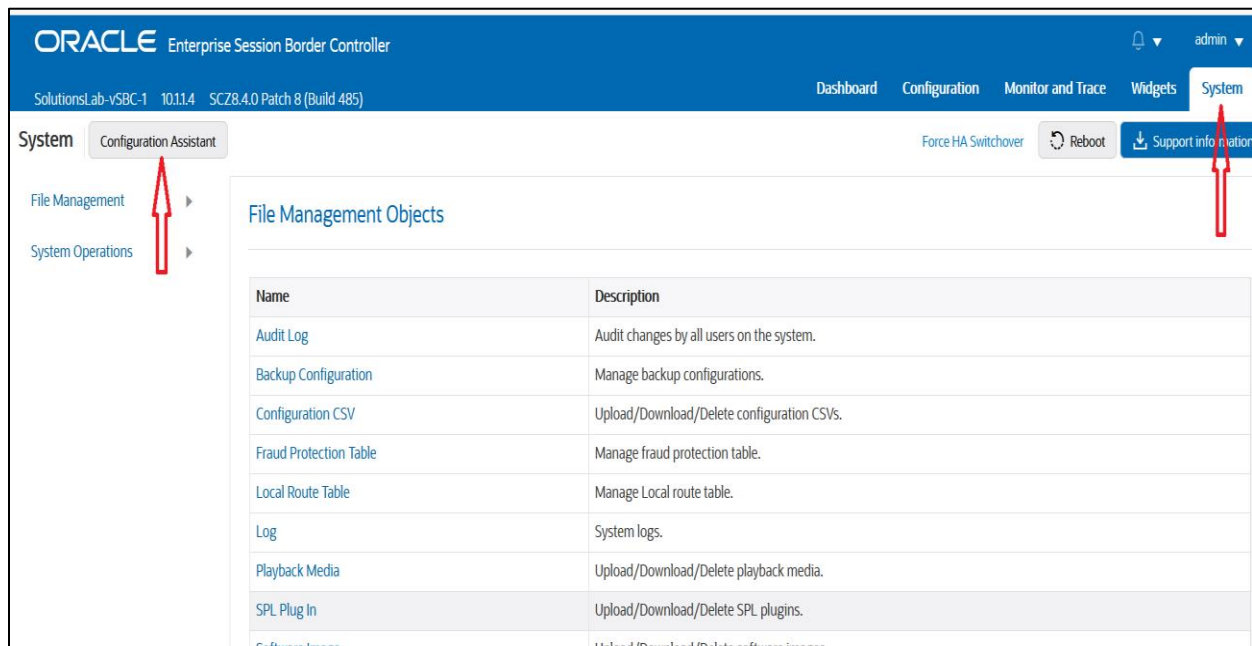
Now that the entries provided throughout the template have been reviewed, the template provides you with the ability to “Download” the config by clicking the “*Download*” tab on the top right. Next, click the “*Apply*” button on the top right, and you will see the following pop-up box appear.



Now you can click **“Reboot”** 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 Cisco Call Manager with Verizon Trunk.

8.6. 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. Existing SBC configuration

If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- [New realm-config](#)
- [New sip-interface](#)
- [New session-agent](#)
- [Session Agent Group](#)
- [New steering-pools](#)
- [New local-policy](#)
- [QOS Marking](#)
- [New Translation Rules](#)
- [Session Translation Rules](#)

Please follow the steps mentioned in the above chapters to configure these elements.

Appendix A

Following are the test cases that are executed between Cisco User with the Verizon Trunk (PSTN user). **Please note that Cisco User here refers both Cisco User inside Enterprise network as well as Cisco Remote worker.**

Serial Number	Test Cases Executed	Result
1	Cisco user disconnects an inbound connected call	Pass
2	Cisco user disconnects an outbound connected call	Pass
3	Verizon Trunk user disconnects an inbound connected call	Pass
4	Verizon Trunk User disconnects an outbound connected call	Pass
5	Cisco user places inbound call from Verizon Trunk user on hold and then resumes	Pass
6	Cisco user makes outbound call to Verizon Trunk user and put that call on hold and then resumes	Pass
7	Verizon Trunk user places inbound call from Cisco user on hold and then resumes	Pass
8	Verizon Trunk user makes outbound call to Cisco user and put that call on hold and then resumes	Pass
9	Cisco user places inbound call from Verizon Trunk user on hold for over 15/30 minutes and then resumes	Pass
10	Cisco user makes outbound call to Verizon Trunk user and places the call on hold for over 15/30 minutes and then resumes	Pass
11	Inbound Verizon Trunk call to Cisco blind transferred to second Cisco/ PSTN User	Pass
12	Outbound Verizon Trunk call from Cisco user blind transferred to second Cisco/ PSTN User	Pass
13	Inbound Verizon Trunk Call to Cisco consultatively transferred to Cisco/ PSTN User	Pass
14	Outbound Verizon Trunk call from Cisco user consultatively transferred to Cisco/ PSTN User	Pass
15	Cisco user makes outbound call to Verizon Trunk user and makes a conference call by adding another Cisco/ PSTN user.	Pass
16	Verizon Trunk user makes outbound call to Cisco user and Cisco user makes a conference call by adding another Cisco/ PSTN user.	Pass

17	Cisco user mutes inbound call from Verizon Trunk user and then unmutes	Pass
18	Cisco user mutes outbound call made to Verizon Trunk user and then unmutes	Pass
19	Verizon Trunk user mutes inbound call from Cisco user and then unmutes	Pass
20	Verizon Trunk user mutes outbound call made to Cisco user and then unmutes	Pass
21	Verizon Trunk User disconnects outbound call to Cisco user before it is answered	Pass
22	Cisco user disconnects outbound call to Verizon Trunk user before it is answered	Pass

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

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

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.

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